Cybersecurity Trends

Edizione italiana, N. 3 / 2017

- Disinformazione: impatto sul valore delle azioni
- Le sfide delle città connesse

INTERVISTA VIP:

- Il Garante Privacy Antonello Soro

GLOBAL CYBER SECURITY CENTER

ISSN 2559 - 1797 / ISSN-L 2559 - 1797

Speciale GDPR

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 a corsi di specializzazione e master

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

GLOBAL CYBER SECURITY CENTER

autore: Nicola Sotira

BIO

Nicola Sotira è Direttore Generale della Fondazione Global Cyber Security Center GCSEC e Responsabile di Tutela delle Informazioni in Poste Italiane divisione di Tutela Aziendale, con la responsabilità della Cyber Security e del CERT. 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.

Cari lettori,

I dati vengono ormai definiti il "nuovo petrolio", un business miliardario e che può offrire ancora molte opportunità a coloro che sapranno cogliere il cambiamento in corso. Un mercato che non è guidato solo dai soliti player; ad esempio la General Electric (GE)[1] ha inserito sensori su turbine a gas, motori a reazione e altri dispositivi; tutto connesso al CloudGE, allo scopo di analizzare il flusso dei dati raccolti e identificare i modi per migliorare la produttività e l'affidabilità delle macchine. Un investimento da 1 miliardo di dollari. Da questa esperienza di GE è nata Predix una piattaforma che utilizza Big Data e tecnologie di Machine Learning che promette l'aumento di efficienza nei processi produttivi attraverso la connessione dei diversi componenti industriali e la loro analisi. L'attenzione è anche verso gli oleodotti e le infrastrutture utilizzate per il trasporto del petrolio.

Un mercato, quello dei dati, che nel 2020 potrebbe raggiungere in Eurozona i 106 miliardi di euro, un'industria che avrà un impatto positivo nella nostra economia. Un mercato che ha la sua punta nel marketing basato su una profilazione più accurata dove anche le banche stanno giocando la loro partita. Determinare il comportamento dei correntisti, la loro spesa, le abitudini dei turisti, il comportamento e la propensione agli acquisti, tutti questi dati costituiranno un enorme patrimonio che fa molto più gola del vecchio oro nero. Ogni nostra attività digitale crea delle tracce e di conseguenza sempre più materiale digitale che aumenta in maniera esponenziale.

Una delle differenze con il petrolio è che i dati sono una risorsa infinita e non è in fase di esaurimento, anche se deve essere ancora capita pienamente.

È anche evidente che in questo nuovo scenario si deve assolutamente evitare la colonizzazione dei dati, la proprietà dei dati deve essere dell'utente la cui transazione li ha generati. Quindi le aziende che desiderano utilizzare questi dati lo devono fare sempre sulla base del consenso. La Privacy e la sicurezza dei dati diventano quindi determinanti e il nuovo Regolamento Europeo (GDPR) mette fortemente l'accento sulla protezione dei dati personali, un tema sul quale dovremo cambiare mentalità. I dati rappresenteranno per le aziende una grossa opportunità, ma solo se a questi dati sarà garantita la sicurezza necessaria e un trattamento conforme alla normativa. Il regolamento impone alle aziende un cambiamento che non è solo tecnologico, ma anche organizzativo. Un tema che tocca anche le infrastrutture IT, molte implementazioni tecniche derivanti dal nuovo regolamento richiedono il completamento del processo di trasformazione digitale che per molte aziende è ancora qualcosa di parziale. Con questo speciale dedicato al Regolamento Europeo sulla protezione dei dati (GDPR), vogliamo sì, porre l'attenzione sul tema dell'adeguamento che le aziende dovranno affrontare entro maggio 2018, ma anche alimentare la discussione sulla proprietà dei dati, la loro salvaguardia e tutela in questo nuovo mercato. ■

Buona lettura…

1 https://www.ge.com/digital/predix

Indice

Cybersecurity - Le Nazioni Unite (e non solo) agiscono all'unisono

autore: **Marco Obiso,**

Coordinatore per la cyber security, International Telecommunications Union, Ginevra

L'ITU, come richiesto dalla comunità internazionale durante il World Summit on the Information Society dell'ONU, ha assunto come principio fondamentale del suo mandato il bisogno di costruire fiducia e sicurezza nell'uso delle TIC. Sebbene le tecnologie dell'informazione e della comunicazione siano evolute parecchio sin dall'invenzione del telegrafo, la missione dell'ITU di "connettere il mondo" in un modo sicuro e protetto è rimasta identica.

145 anni or sono, l'ITU è stata fondata per occuparsi dei challenge e delle opportunità di quella che era allora l'alba dell'era dell'informazione. Oggigiorno, le TIC sono diventate una parte essenziale dello sviluppo umano. La gestione e l'approvvigionamento delle risorse idriche, le reti energetiche, le catene di distribuzione alimentare, il trasporto così come i sistemi di navigazione usano le TIC. I processi industriali e le catene di distribuzione sono rafforzate dalle TIC per poter proporre servizi più efficienti e anche per sostenere le formazioni umane necessarie per gestirne l'uso.

L'essenza del challenge della cyber security consiste nel fatto che né Internet né le TIC – in modo globale – sono stati concepiti con l'idea di base della sicurezza. L'ecosistema digitale di oggi è estremamente diverso a quello di sessant'anni fa, e mette costantemente alla prova molti degli approcci tradizionali di sicurezza, richiedendo innovazioni sempre più olistiche. Un aspetto, però rimane certo: la cyber security è un problema globale che può essere affrontato solo in modo globale.

Come agenzia leader dell'ONU per le TIC, l'ITU gioca un ruolo di pivot nel facilitare questa cooperazione globale. in collaborazione con i governi, il settore privato, la società civile e le organizzazioni internazionali, l'ITU può accelerare il processo che mira a raggiungere una cultura globale della cyber security, tramite:

- La facilitazione dell'armonizzazione dei framework nazionali, regionali e internazionali;
- La messa a disposizione di una piattaforma per discutere e accordarsi sui meccanismi tecnici da usare per mitigare i rischi legati all'uso improprio delle TIC;
- L'assistenza agli Stati membri nella definizione delle strutture organizzative necessarie per rispondere ai rischi cyber in modo proattivo, supportando la cooperazione con tutti gli altri stakeholder a livello nazionale ed internazionale;
- La promozione dell'importanza del Capacity Building e della cooperazione internazionale come elementi chiave di follow-up per acquisire competenze ed expertise nello scopo di creare una cultura di cyber security a livello nazionale, regionale e globale.

Nel maggio del 2011, il primo passo in questa direzione è stato compiuto dall'ITU e dall'United Nations Office on Drugs and Crime, con la firma di entrambe le istituzioni di un protocollo d'intesa per collaborare a livello globale nell'assistenza degli Stati membri a mitigare i rischi generati dal cybercrime, con l'obiettivo di assicurare un uso protetto delle TIC. È stata la prima volta che due organizzazioni all'interno del sistema dell'ONU si sono formalmente messe d'accordo per cooperare a livello globale nel campo della cyber security.

Nel giugno del 2017, l'ITU ha concluso una collaborazione simile con INTERPOL, con il fine comune di aumentare le risorse e aiutare le rispettive comunità.

L'ITU ha realizzato l'importanza della decentralizzazione e della distribuzione degli sforzi, proponendo alle organizzazioni ed entità che posseggono le dovute e specifiche conoscenze ed expertise di offrire assistenza non solo ai membri dell'ITU, ma anche alla comunità nel suo insieme.

Istituire una cyber security globale può sembrare un compito e una sfida complessa, ma se si agisce all'unisono i benefici ottenuti dalla nostra società dell'informazione possono offrire all'umanità le migliori opportunità che essa abbia mai avuto per il raggiungimento di una pace sostenibile con il suo corollario sicurezza e sviluppo. ■

Il cyber-potere, un pilastro essenziale dei poteri del futuro

Autore: Arthur Lazar,

Cyberint (centro speciale di cyber intelligence del Servizio Rumeno di Intelligence)

La rivoluzione tecnologica – il "mega trend" dell'inizio del 21° secolo

Uno dei trend più importanti del sistema attuale è quello dell'accelerazione dei cambiamenti in diversi campi scientifici e tecnologici. L'espansione delle tecnologie, e l'accesso relativamente facile e generalizzato a molte di esse rappresenta una grande opportunità ma anche un rischio. L'evoluzione delle tecnologie ha comportato una crescita esponenziale della velocità di circolazione delle informazioni, rendendoci capaci di processare e trasmettere a velocità impressionanti l'informazione. Ciò ha radicalmente cambiato non solo la nostra vita ma anche il nostro comportamento. Il primo website è stato creato nel 1991[1]. Nel 1993 si contavano solo 50 siti mentre nel 2000 erano già oltre i5 milioni[2]. La prima e-mail è stata trasmessa nel lontano 1971 mentre dal 2013 si scambiano più di 40 trilioni di mail all'anno[3].

Per di più, siamo circondati ovunque da un vero oceano di device e di computer. La centralità assunta dai computer nella nostra vita è ormai un fattore del quale non possiamo più fare a meno. Potremmo quasi dire che non si può più immaginare la vita senza l'accesso a tali strumenti, iniziando dalla lettura quotidiana delle notizie ogni mattina, per poi passare al controllo delle nostre mail e ad altre attività che fanno ormai parte della nostra routine giornaliera. Le tecnologie avanzate, in questo campo, ci rendono praticamente dipendenti.

Internet non rappresenta solo la trasmissione e il ricevimento di informazioni. Intere infrastrutture critiche, a cominciare dalle compagnie produttrici di energia, così come quelle dei trasporti o delle comunicazioni, sono gestite tramite computer.

È doveroso ricordare anche che tutti questi computer non esisterebbero da soli. Sono tutti legati tra di loro, definendo una rete immensa. In conseguenza, l'interconnessione globale è una delle caratteristiche fondamentali della cosiddetta "rivoluzione tecnologica".

Da qui si può già trarre una conclusione certa: grande parte della nostra vita quotidiana è direttamente dipendente dai device connessi tramite Internet, ciò vuol dire che una grande parte della nostra vita non trascorre più esclusivamente nel campo fisico, bensì in quello virtuale.

Una trasformazione simile avviene anche nella sfera dei poteri, nella prospettiva delle relazioni internazionali. La nuova realtà ha cambiato radicalmente la natura stessa dei poteri. La loro distribuzione si è accentuata, ma al tempo stesso, la loro diffusione ha raggiunto dei livelli altissimi (ad esempio, singoli attori pressoché anonimi possono arrivare a detenere delle risorse informative significanti, che convertite in potere effettivo possono creare problemi persino agli Stati sovrani).

Il cyber-potere – definizione e caratteristiche

La presenza di questo nuovo elemento di realtà virtuale come elemento intrinseco delle nostre vite ha avuto un'influenza maggiore nel cambiamento delle caratteristiche dei poteri dove, praticamente, ha generato una nuova categoria: il cyber-potere.

Esistono molti approcci per definire il cyber-potere. Solo la letteratura americana ne propone parecchie decine, ognuna delle quali rivela solo una delle molteplici facce di questo potere o al meglio una parte di tutto quello che contiene veramente il termine di cyber-potere.

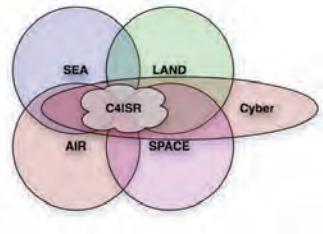
Una delle definizioni più complete del termine, ormai accettata nella letteratura specialistica, è quella proposta da Daniel Kuehl, che considera che *"il cyber-potere è l'abilità di utilizzare lo spazio cibernetico per crearsi dei vantaggi e influenzare elementi in tutti i campi operativi ed in tutti gli altri strumenti del potere"*[4].

A questo punto si impongono però un certo numero di precisazioni.

In primo luogo, il cyber-potere è un'espressione naturale dell'evoluzione della geografia, ovvero un nuovo campo dove si manifesta il potere. Due secoli or sono, il potere nella scena internazionale veniva esercitato principalmente in campo terrestre. Eserciti interi, fanteria, cavalleria pesante o leggera portavano il fardello della lotta sul terreno. Agli inizi del ventesimo secolo, lo sviluppo delle tecnologie navali e la comparsa delle flotte militari hanno permesso l'estensione allo spazio marittimo. Alfred Mahan, generale americano e professoreall'Accademia Navale di Guerra, ha fatto sfilare, agli inizi del 1900, un'immensa flotta da guerra americana, attirando sin da allora l'attenzione su di un nuovo potere che stava emergendo: gli USA[5]. In seguito, con lo sviluppo delle tecnologie dell'aviazione, anche lo spazio aereo ha iniziato a essere utilizzato come risorsa da sfruttare per il proprio potere. Si dice spesso che la vittoria della Seconda Guerra Mondiale è stata una conseguenza del contributo decisivo delle flotte aeree delle quali disponevano gli alleati. Infine, negli anni '60 e '70 e poi nel periodo dell'apogeo dell'amministrazione Reagan negli anni '80, con l'inizio del programma di "Guerra

Stellare" e una nuova corsa senza precedenti all'armamento, il campo di battaglia si è trasferito nello spazio. E, più recentemente, le risorse dello spazio cibernetico sono state sempre più spesso usate nello stesso scopo.

In secondo luogo, il cyber-potere non presenta un valore senza una capacità di proiezione. Nell'accezione comportamentale, ogni potere deve avere la capacità di imporsi sugli altri, producendo effetti, modellando e influenzando i comportamenti[6]. Per fare ciò, bisogna avere una grande capacità di proiettare i poteri. Esattamente come la comparsa delle flotte navali ha facilitato il trasporto delle truppe, allargando la mobilizzazione delle truppe e migliorando le capacità logistiche, la proiezione del cyber-potere dev'essere vista nella stessa logica, essendo anch'essa intrinsecamente una risorsa di potere. Nel caso dei cyber-poteri, la proiezione si realizza in modo quasi istantaneo. Come dichiarava un celebre stratega americano, utilizzando il cyber-potere, si possono produrre danni a infrastrutture situate a migliaia di chilometri in un solo secondo e con il solo aiuto del click di un mouse[7]. Il cyber-potere, che aveva già similitudini con gli altri tipi di potere (navale, aereo o spaziale) è però diverso da essi e, nello stesso tempo, superiore ad essi.



La conclusione logica di questa sintesi è che il cyber-potere possiede almeno quattro dimensioni, che si manifestano in ognuno degli spazi che abbiamo trattato (terreste- navale - aereo - spaziale).

Come terzo punto, sottolineo che il cyber-potere non è soltanto un'espressione del nuovo tipo di geografia o del nuovo tipo di spazio virtuale. Similarmente agli altri quattro tipi di potere (economico, militare, organizzativo o sociale) è una risorsa o, meglio, una un insieme di risorse che conta nell'indice generale del potere. Inoltre, siccome è una risorsa che può influenzare tutti gli altri tipi di potere, il cyber detiene ormai un peso significativo in tutte le formule destinate a fare classifiche e a calcolare l'indice generale di potere. Allora, nessuno di questi poteri poteva essere considerato singolarmente come un pilastro del potere in generale, ma solo, al massimo, un indicatore che aveva un risvolto in altri tipi di potere, generalmente quello economico o quello militare.

Il cyber-potere, espressione della realtà dei nostri giorni, accanto al potere economico, a quello militare, a quello organizzativo e a quello sociale, è diventato una colonna assestante dei poteri in generale, e quindi praticamente il quinto pilastro del potere generale.

Non si può però fare astrazione dei tipi di poteri tradizionali, perché continuano ad avere il loro peso. Molte dottrine militari sottolineano ancora che non si può parlare di dominazione in zone dove la fanteria non può giungere! Le recenti guerre in Iraq ed Afghanistan sembrerebbero dimostrare questo fatto. Ciò nonostante, è anche ovvio che questi tipi di guerre non vengono più fatte esclusivamente con i mezzi di combattimento tradizionali.

Questa è proprio l'accezione della nostra ricerca, ovvero che il potere nel sistema, già adesso ma ancor di più in futuro, dipende fondamentalmente dalle risorse cyber esistenti e di chi verrà a detenere il maggior numero di tali risorse.

Le risorse del cyber-potere

Il potere dipende da risorse ma il cyber-potere dipende in primis da risorse cyber e in special modo dalla capacità di trasformare queste risorse in dividendi reali di potere.

Paul Kennedy, nel suo studio legato all'ascensione e alla decadenza dei grandi poteri, dimostra che la dinamica dei cambi nel sistema è mossa principalmente dalle evoluzioni economiche e tecnologiche[8]. Queste evoluzioni sono sempre dipese da diverse categorie di risorse. Le strutture produttive si sono trasformate di epoca in epoca, fattore che ha avuto un impatto diretto sull'economia e sulla tecnologia. La capacità di innovazione tecnologica ha sempre fatto la differenza, in tutti i periodi storici. Di conseguenza, la capacità di conversione delle risorse è fondamentale e offre un vantaggio certo a una società rispetto ad altre.

La comparsa dei galeoni a lungo percorso e lo sviluppo del commercio nello spazio atlantico nel Cinquecento ha portato grandi benefici ai paesi europei che hanno saputo farli fruttare, esattamente come avvenuto più tardi l'apparizione del motore a vapore, basato sullo sfruttamento delle risorse di carbone e metallo, ha incrementato massicciamente il potere di alcuni Stati-nazione a discapito di altri[9].

Così detto, la ricchezza (o potere economico) sono necessari a sostenere il potere militare esattamente come il potere militare è necessario per ottenere e produrre ricchezza. I tipi di risorse e di potere vengono a influenzarsi reciprocamente e creano vantaggi al livello degli Stati che si trovano al vertice della gerarchia.

Però, nessuna di queste risorse di potere non ha mai avuto un'influenza multilaterale sugli altri strumenti dei poteri, contrariamente a quello che succede con le risorse del cyber-potere. La comparsa del nuovo spazio virtuale è la causa di questo stato di fatto, poiché mai nella storia una dimensione ha acquisito un'influenza così stravolgente su tutte le altre. Nello stesso modo, questa stessa categoria di risorse ha un'influenza determinante sul modo nel quale si conducono alcune guerre al giorno d'oggi. Il Ventunesimo secolo è per eccellenza il secolo delle risorse di tipo cyber. La globalizzazione e la rivoluzione dell'informazione genera nuove risorse per i poteri. Il controllo delle reti e delle connessioni diventano una fonte importante di potere.

Il cyber-potere utilizza le capacità dello spazio digitale per manifestarsi. Le sue risorse sono quelle che nascono dal mondo digitale ma la sua efficacia dipende anch'essa dai tipi tradizionali di potere, cosicché si possono combinare tutti i tipi di risorse. Per fare ciò bisogna avere una conoscenza quanto più approfondita possibile dello spazio digitale. Come i poteri, anche lo spazio digitale è osservato secondo una moltitudine di accezioni ed è poi analizzato da una quantità infinita di variabili[10].

Nell'accezione generale, si può dire che *"lo spazio digitale è una realtà virtuale, omnicomprensiva, all'interno della quale gli utilizzatori delle reti informatiche del pianeta possono comunicare e reagire reciprocamente"*[11]. Questo spazio è di accesso relativamente semplice per una gamma assai ampia di attori, e allo stesso tempo sono relativamente

buon mercatoi mezzi che offrono agli stessi attori non solo varie opportunità ma anche e soprattutto rischi.

Trattando in queste pagine il cyber-potere e lo spazio digitale nella prospettiva delle relazioni internazionali, è doveroso sottolineare il fatto che lo spazio digitale e le nuove tecnologie che vi sono associate hanno iniziato, sin dagli anni novanta, a cambiare le dottrine militari di guerra. La guerra centrata sulla rete *(network centric)* ha cominciato a sostituire quella centrata su piattaforme (capacità militari), un aspetto già sottolineato vent'anni or sono da Jay Johnson (capo delle operazioni navali della US Navydal 1996 al 2000)[12]. Praticamente, il meccanismo di guida di un missile, durante la sua traiettoria, dipende dal modo di posizionamento di un satellite che a sua volta dipende da un'infrastruttura e da comandi che utilizzano lo spazio digitale. Andando più in là, il parere unanime degli specialisti è che la trasformazione delle dottrine e dei meccanismi operativi degli eserciti moderni dipende in parte sempre maggiore da uno sfruttamento sempre più qualitativo ed efficiente delle capacità dello spazio digitale.

Tornando alle più importanti categorie di risorse utilizzate e applicate nello spazio digitale, possiamo sintetizzare che queste possono essere classificate in tre grandi categorie[13]:

1. **Risorse fisiche:** si tratta di *device* fatti dall'uomo, ai quali si aggiunge l'infrastruttura che permette di far circolare l'informazione (computer, smartphone, fibre ottiche, sistemi di comunicazioni speciali, infrastrutture critiche, sistemi industriali).

Il controllo delle risorse fisiche che compongono lo spazio digitale è estremamente importante nell'indice del cyber-potere. In questo senso, l'intera comunità euro-atlantica è quanto meno preoccupata dell'invasione nei suoi mercati di equipaggiamenti cinesi. Il prezzo bassissimo proposto dalle compagnie produttrici di questi equipaggiamenti è pressoché impossibile da combattere in un contesto di economia globale, mentre allo stesso tempo la natura stessa degli equipaggiamenti può esporre a gravi vulnerabilità.

Il "Gruppo Equation", associato alla maggior parte degli esperti in reverse engeneering con un gruppo di spionaggio elettronico della NSA – il TAO *(Tailored Acces Operations)*, ha basato la sua strategia di attacco sull'infezione del *firmware* degli *hard disk* fabbricati dalle più importanti compagnie del mercato libero[14]. Per fare ciò, è stato sicuramente necessario l'accesso alla documentazione di base degli hard disk, un elemento che in realtà presuppone di accedere a categorie di risorse che solo pochissimi possono permettersi.

2. **Il know-how** per far circolare l'informazione; Il know-how è anch'esso molto importante. Né Stuxnet né Duqu non avrebbero potuto produrre danni cosi devastanti nei sistemi industriali iraniani se non fossero stati il risultato di un'ingegneria tecnologica molto avanzata e sofisticata. Negli anni, gli esperti dell'AIEA (Agenzia Internazionale dell'Energia Atomica) e un apparato intero di specialisti

dello Stato iraniano non sono riusciti a trovare una spiegazione plausibile sulla causa che condusse alla defezione sistemica delle centrifughe delle centrali di arricchimento di uranio di Natanz, una città del centro del paese dove vi si trovavano circa 9000 di questi apparecchi. La proporzione di defezione di queste centrifughe, in condizioni normali di uso, era di circa 10% all'anno. E in qualche mese fu necessario sostituirne più di 2000[15]. Solo qualche anno dopo, una piccola ditta ucraina di *reverse engeneering* ne scoprì la causa: Stuxnet era una delle più sofisticate armi cibernetiche mai create, nascosta in più di 500 KB di memoria istallata in seno ad un pacchetto "legittimo" di dati immesso nei server che controllavano le centrifughe menzionate. L'immenso scandalo internazionale che apparve nella prima metà del 2010 ha dimostrato con evidenza come il cyber-potere può essere uno strumento estremamente efficace esattamente laddove un embargo o altri metodi tradizionali non funzionano.

3. **Il fattore umano**. Anche il fattore umano è una delle più grandi risorse del potere. Il cyber-potere essendo un pilastro dei poteri ha anche esso bisogno di un fattore umano efficace. Più il fattore umano è altamente qualificato, e più cresce l'efficacia dei cyber-poteri. È ben noto il fatto che i gruppi attivisti cinesi, che detengono una porzione significativa nell'economia dei gruppi attivisti a livello mondiale, riescono a provocare problemi maggiori sulla scena internazionale sia nell'attacco di infrastrutture critiche, sia nelle attività intrusive associate allo spionaggio. Bisogna sottolineare che questi gruppi organizzati di hacking sono costituiti da un grandissimo numero di individui, con alta preparazione tecnologica. Il fattore umano, a sua volta, può anche diventare una grande vulnerabilità. Edward Snowden ha provocato danni enormi alla NSA con la sua decisione di rendere pubbliche le operazioni segrete dell'agenzia. In più, il suo avvicinamento al potere russo e al Cremlino pare avere offerto a questo stato opportunità che non avrebbe potuto ottenere in un altro modo.

A queste risorse, in funzione del contesto, possiamo aggiungere l'informazione intesa come risorsa supplementare di potere, lo spazio virtuale essendo *in sine* uno spazio informazionale dove le informazioni vengono create, depositate e poi comunicate. L'ulteriore conoscenza che deriva da questo processo e da queste rapidissime interazioni è considerata una risorsa di potere e aiuta, ad esempio, nei processi di decision-making[16].

Joseph Nyedimostra che il cyber-potere, come tipo importante di potere, ha una doppia natura: hard e soft. Nello stesso tempo, questo potere si può manifestare sia all'interno che all'esterno dello spazio virtuale[17]. I cyber-attacchi che mirano a un bersaglio rappresentano un tipo di risorsa "hard" mentre una campagna di diplomazia pubblica svolta sulla rete e destinata ad influenzare l'opinione pubblica può essere considerata una risorsa "soft" del cyber-potere. In questo processo, è significativa la credibilità dell'attore che divulga il messaggio,

e quindi anche la credibilità può essere vista come una risorsa di potere[18]. Più grande è la credibilità di un attore, e più grandi saranno le chances di efficacia del messaggio di quest'ultimo. La credibilità, però, è difficile da costruire e può essere persa in un attimo. La strategia con la quale si mantiene e si conserva la credibilità è un'arte che, in realtà, posseggono pochissimi attori mondiali. Di conseguenza, come scrive lo stesso politologo americano, oggigiorno le guerre possono essere vinte da "coloro che hanno la miglior narrazione"[19] e, potremmo aggiungere, da coloro che hanno la miglior narrazione credibile.

La sfida maggiore alla quale ci confrontiamo oggi quando cerchiamo di analizzare il potere e le sue risorse è quella di riuscire a valutare il peso di ognuna di queste risorse nell'indice generale del potere. E, in caso del cyber-potere, ogni risorsa ha sicuramente un'influenza diversa sull'equazione finale.

Inoltre, queste ultime dipendono anche dal contesto dove si manifestano, esattamente come il potere in generale. Rimane quindi responsabilità del mondo accademico continuare fare proposte sempre più affinate sul calcolo del peso associato ad ogni risorsa nell'equazione finale del potere.

"Hacking"e"reverse engeneering" – le due facce del cyber-potere

Come nel caso delle altre forme di potere, il cyber-potere non si esprime solo tramite le risorse delle quali dispone o della sua capacità di proiettarsi. Non meno importante è la sua capacità di difesa, che è un attributo essenzialmente degli Stati, soprattutto quando si tratta di proteggere grandi infrastrutture critiche. La capacità di proiezione della forza o del potere deve allora essere allineata con le capacità di protezione, perché nulla potrebbe essere più devastante dell'esplosione di una sicurezza difensiva debole o di vulnerabilità che appaiono nel sistema quando le protezioni sono inefficienti.

Nel tempo, nelle forme tradizionali di potere, la capacità di difendersi era direttamente influenzata da risorse difensive specifiche dello spazio fisico del quale disponevano gli attori del sistema. Esistevano quindi cittadelle e fortificazioni poste nei siti strategici, così come reggimenti ed eserciti estremamente mobili, pronti a proteggere un territorio. Poi si aggiunsero flotte navali e aeree con attributo di difesa degli attori del sistema.

Al contrario, le due facce del cyber-potere non azionano in modo separato. Molte dottrine militari sostengono che la miglior forma di difesa è l'attacco. Così, oggigiorno, un sistema di protezione avanzata può essere considerato come una minaccia. Ad esempio, è il caso del sistema di difesa antimissili degli USA, dislocato in diversi Stati europei e visto dalla Russia come una minaccia diretta alla sua sicurezza, anche se il sistema ha come obiettivo fondamentale di proteggere il territorio americano e non ha capacità di attacco. Lo sviluppo di un sistema internazionale, specialmente dopo la Seconda Guerra Mondiale, ha dimostrato che, in pratica, gli attori principali del sistema hanno preferito mantenere un'eventuale conflitto militare lontano dalle loro frontiere nazionali. Ed è così che i meccanismi di difesa delle forze hanno spinto le guerre verso spazi periferici, in paesi del terzo mondo – la Corea, il Vietnam o l'Afghanistan ne sono solo alcuni esempi.

Nel caso del cyber-potere, la situazione ha subito un cambio maggiore, e la realtà degli ultimi anni dimostra che anche i più potenti possono essere colpiti all'interno, e non per forza all'esterno delle loro frontiere, in funzione delle capacità cibernetiche dell'attaccante.

Esistono quindi due facce del cyber-potere, chiaramente correlate tra di loro:

- Una componente difensiva – chiamata cybersecurity nei testi specializzati.
- Una componente offensiva che sta soprattutto nella capacità di proiezione del potere.

Affinché un attore del sistema possa detenere un cyber-potere significante, non solo ha bisogno di possedere capacità in tutti e due i sensi, ma deve identificare anche un meccanismo di bilanciamento di questi tipi di risorse. Il problema maggiore nel caso del cyber-potere è che, contrariamente alle forme tradizionali di potere, le due facce (offensiva e difensiva) presuppongono l'uso di tipi diversi di risorse. È così che le vulnerabilità derivanti da un sistema di protezione inefficace non possono essere sostituite dalle capacità di attacco.

Per quanto riguarda il concetto di cybersecurity, l'accezione pressoché unanime è che la protezione è efficace se adempie tre obiettivi principali[20]: la confidenzialità, l'integrità ela disponibilità.

La confidenzialità si riferisce alla protezione fisica dei dati, e si realizza attraverso tecniche di cifratura e di controllo degli accessi.

L'integrità presuppone meccanismi tali che il sistema non possa essere toccato senza una specifica autorizzazione. Ad esempio, nel caso di Stuxnet, il pericolo e i danni ulteriori sono apparsi in seguito all'accesso al sistema e alle sue risorse da un'intrusione che pareva legittima, in modo che il sistema anti-infrazione (firewall ed antivirus istallati) non solo non ha rivelato l'intrusione, ma l'ha considerata come un'azione normale.

La disponibilità del sistema presuppone la capacità di mantenere le risorse e il funzionamento complessivo per un certo periodo di tempo. Il principio dal quale si parte è che il sistema sia creato in modo tale da impedire l'uso, da parte di un'attaccante, delle vulnerabilità che portano a disfunzioni. La disconnessione di una intera rete di infrastrutture da attacchi di tipo DDoS può esemplificare al meglio questa caratteristica.

Nella visione Singer – Fridman, a queste tre caratteristiche bisognerebbe aggiungerne una quarta: la resilienza[21].

Quest'ultima parte dalla premessa che l'inevitabile avverrà comunque, e quindi che il sistema deve essere mantenuto funzionante anche quando è attaccato. Per fare ciò, però, c'è bisogno di grandi risorse che solo pochi attori possono permettersi.

Le due facce del potere agiscono pure in modi diversi; le risorse usate da ciascuna sono diverse, cosi come le strategie. Paradossalmente, fare *reverse engeneering* è almeno tanto complicato quanto fare *hacking*. Per analogia, è come lo spionaggio e il contro-spionaggio. Il primo metodo mira a captare informazioni, spesso con uno scopo a sé stante, mentre il secondo mira a trovare soluzioni di protezione del sistema contro attaccanti, a loro volta spie. I problemi appaiono quindi quando gli avversari non sono visibili, e vengono praticamente ad azzerare l'efficienza delle misure.

Le soluzioni per un sistema di cybersecurity avanzato non sono molte. Potremmo ad esempio sviluppare certe entità di protezione antivirus (ditte o software) per

proteggere i sistemi. Queste sono però molto costose e, spesso, si avverano inefficaci. In altri casi, i partenariati pubblico-privato sono visti come una variante aggiuntiva, con la menzione che non tutti gli Stati sono disposti a fare proteggere i propri segreti esternalizzando i servizi di sicurezza a degli enti privati. *Last butnotleast*, si ricorre a dei programmi di security *awareness* o di *ealry warning*, svolti all'interno delle agenzie governative per i propri impiegati, perché le armi cibernetiche sono altamente tecnologiche e usano un know-how sofisticato che, spesso, rendono inefficaci i sensori di protezione.

Gli attori del cyber-potere

Quando trattiamo di attori del cyber-potere, ci confrontiamo con una barriera importante: l'impercettibilità di questi attori. Questa caratteristica deriva della natura stessa dello spazio digitale che, come abbiamo accennato, è sempre più permissivo e offre non solo a Stati ma anche ad altri attori (non statali) la possibilità di manifestarsi.

Da ben più di cent'anni, il sistema internazionale è stato costruito attorno alla nozione fondamentale di Stato. Indifferentemente dalla loro forma (unipolare, bipolare, multipolare) sin dalla conclusione del trattato di pace di Vestfalia, gli Stati-Nazione sono diventati la pietra angolare del sistema mondiale. Il potere era quindi naturalmente distribuito soltanto tra questi, e le differenze si manifestavano in tutti i sensi solo ed esclusivamente rapportandosi a tali entità. Il potere degli Stati e le risorse delle quali disponevano erano visibili e misurabili, si misuravano ad esempio tramite potenti eserciti, considerevoli risorse naturali, tecnologie avanzate o economie efficienti. Comunque, il potere era percettibile.

Oggigiorno, non solo gli attori statali possono accumulare potere, ma anche i singoli individui possono porre problemi, nello spazio digitale, persino ad attori molto più grandi come gli Stati e i loro *assets*. Si può quindi dedurre che oggi i *"players"* del sistema sono distribuiti secondo una formula che mette a un estremo l'individuo, poi le aggregazioni o i gruppi di individuicon una relativa organizzazione (gruppi non statale, ONG, attivisti) e, all'estremo opposto, lo Stato.

Questo tipo di classifica, senza altre spiegazioni, è però semplicistica quando dobbiamo parlare di distribuzione dei poteri nel sistema internazionale. Il problema maggiore che si pone è quello legato ai tipi di trasformazione che possono veramente produrre effetti all'interno del sistema.

Dato che trattiamo qui il sistema internazionale e l'indice generale di potere, una delle domande che dobbiamo porci nella nostra analisi è quella legata agli attori, risorse ed eventi che possono realmente influenzare la classifica del sistema. Per questo motivo, il problema posto dagli attori come elemento di definizione del cyber-potere nel quadro internazionale deve essere trattato in correlazione con i tipi di minacce sviluppate nonché del loro impatto e delle loro conseguenze. *Last but not least*, le intenzioni degli attori e il tipo di risorse utilizzate rappresentano un indicatore della natura delle entità che detengono cyber-potere all'interno del vasto sistema globale. In altre parole, le domande da porsi sono: qual è l'intenzione dell'avversario? Quali sono i suoi bersagli? A che tipo di risorse può accedere? Quale sarebbe l'impatto della minaccia, se attuata?

Queste nozioni sono importanti e le ritroviamo naturalmente anche nel sistema delle equazioni tradizionali che permettono di definire il potere. La differenza però è che se nel sistema tradizionale gli indicatori rispettivi aiutano piuttosto a sfumare i meccanismi dei poteri, nel caso del cyber-potere sono essenziali per aiutare il processo di attribuzione. Se non fosse così, non si potrebbero creare classifiche "cyber" se non basandosi su paragoni tra gli attori in campo. Per fare ciò bisogna quindi sapere chi sono gli attori e quale è il loro potenziale di potere.

Un aspetto strettamente legato a questi assiomi è quello del contenuto dalle risorse già in uso. Con altre parole, l'accesso – o la permissività – di tutti gli attori del sistema si manifesta, o no, in modo uniforme per tutte le categorie di risorse? Proprio tutti gli attori, individui, gruppi (più o meno organizzati), hanno, o no, accesso alle reti di fibra ottica che attraversano gli oceani? Sono tutti, o no, capaci di utilizzare delle risorse costosissime del tipo "Zero Day"? Evidentemente, no!

Se tracciamo un'analogia con le forme tradizionali dei poteri, le entità che potevano veramente mobilizzare somme considerevoli di risorse erano gli Stati. La creazione o l'uso di un certo tipo di risorsa – come ad esempio una squadriglia di bombardieri strategici – non solo era costosissima ma era anche l'attributo esclusivo di pochi Stati. La squadriglia di aerei non era in mano né a gruppi consolidati ad hoc, e nemmeno di individui cosparsi nei luoghi più remoti del pianeta. Ancor di più, l'uso di questo tipo di risorsa produceva effetti sull'esercizio stesso dei poteri nel sistema.

Nel caso del cyber-potere, la situazione è diversa. La permissività dell'accesso alle risorse e la rapidità delle trasformazioni può fare sì che, prima o poi, una categoria assai vasta di entità le possano utilizzare a loro buon piacimento.

Infine, le intenzioni e le conseguenze che dipendono da una minaccia possono veramente cambiare il potere dell'altro? Nelle forme tradizionali di potere, l'intenzione era rappresentata in modo preponderante dalla volontà degli attori del sistema di ottenere posizioni dominanti nel loro rapporto cogli altri, in generale cogli avversari. È ancora valida quest'equazione nel caso del cyber-potere?

L'aggiunta di elementi di interpretazione legati alle intenzioni, ai valori, alle forme organizzative ci portano nella zona delle teorie costruttiviste e, a prima vista, possono complicare il meccanismo di valutazione del cyber-potere dal punto di vista delle sue potenzialità. La realtà dimostra però che l'intenzione può essere una connessione estremamente importante quando si tentano esercizi di attribuzione di attacchi ad un cyber-potere specifico. Le intenzioni vengono ad offrirci degli indici supplementari legati alla qualità dell'attore. Per esempio, un

hacker che si trova a Singapore potrebbe volere ottenere le credenziali di carte di credito/debito di clienti di una banca specifica, per poter rubare soldi. In un'altra situazione, un gruppo organizzato di hacker potrebbe iniziare ad attaccare una ditta per venderne i segreti alla concorrenza. È poco probabile che questo tipo di attività – e le conseguenze che portano con loro – producano effetti maggiori nel sistema internazionale. Al contrario, se un gruppo attivista riesce a paralizzare il sistema bancario di uno Stato, in un periodo di crisi, allora abbiamo a che fare con tutt'altro. Se la crisi è associata ad un contesto militare teso, abbiamo allora indici supplementari legati all'identità potenziale degli attori implicati. Se, ad esempio, l'attacco implica l'accesso a risorse considerevoli, allora è ragionevole ipotizzare che alle spalle degli attaccanti possa esserci un attore statale.

La conclusione che emerge da qui è che anche se il potere è sempre più distribuito in seno al sistema, i più importanti detentori di risorse rimangono ancora gli Stati. Questi non sono solo i più importanti, ma anche "i più pericolosi"[22]. L'esperienza dimostra che il cyber-spionaggio ed il cyber-sabotaggio entrano per eccellenza negli attributi degli Stati, più precisamente di quei pochi Stati che hanno, almeno ad oggi, le risorse ma anche le intenzioni e le motivazioni per svolgere tali attività.

Ma come affermare che un'arma "cyber" è utilizzata da uno Stato o da un gruppo attivista indipendente? Quali sono i criteri che ci permettiamo o meno di fare tale affermazione? Se un esercito è visibile e misurabile, allora può essere associato facilmente a un potere preciso. Ma nel caso delle armi "cyber" risulta difficile percepire questa correlazione. Gli specialisti di cyberintelligence dovranno affinare i criteri di attribuzione. Fino ad allora, possiamo ragionevolmente solo cercare di trovare criteri plausibili di attribuzione[23].

In questo, abbiamo numerosi meccanismi che ci aiutano ad arrivare ad attribuzioni plausibili. Possiamo, tra di essi,menzionare la vittimologia, le intenzioni dell'attaccante e le risorse adoperate. Sicuramente, possiamo aggiungere l'ingegneria dei meccanismi di ricerca specifici al *reverse engeneering*. Troviamo oggigiorno molte ditte specializzate in queste attività, che forniscono rapporti di nicchia su questo tema. Non tutte, però sono credibili, e spesso le "prove" che pubblicano si dimostrano chiaramente insufficienti. Questo segmento di ricerca rimane quindi ancora una ricerca aperta – e forse una delle più importanti in assoluto – per consolidare uno spazio digitale sicuro al livello delle entità nazionali.

Così, se combiniamo il quantum delle risorse, della vittimologia (distribuzione geografica e qualità dei bersagli) con le intenzioni dell'attaccante, possiamo ottenere indici ragionevoli legati al potenziale di cyber-potere degli attori del sistema e possiamo arrivare a identificarli.

Sintetizzando, esistono 3 strati o, meglio, 3 livelli di concentrazione del potere[24]: quello delle agenzie governative (Stati), quello delle organizzazioni altamente strutturate (corporazioni, ONG, gruppi attivisti) e quello delle organizzazioni poco strutturate (individui).

Bisogna però sottolineare che questi livelli non sono stabili. Gli individui ed il loro know-how possono diventare attori di livello 2, ovvero quello delle organizzazioni ben strutturate. Queste, a loro volta, interagiscono coi loro governi, sia nel quadro di partenariati pubblico-privato, sia, come è il caso in Russia o in Cina, come una conseguenza della cultura dello spazio, in base ad un controllo dello Stato messo bene a punto. Il know-how circola quindi in ambe le direzioni e in funzione di questo flusso, assistiamo all'incremento di risorse di potere di certi attori mentre altri perdono quota.

Bisogna anche aggiungere che al livello superiore del sistema internazionale, anche se attori non statali possono accumulare un livello di potere significante, è solo una questione di tempo fino a quando questi verranno connessi agli interessi di uno stato. Prima o poi, un attore statale cercherà di accaparrarli e di usarli nel suo proprio interesse. Anche se ci troviamo qui su di una zona di "speculazioni", la realtà degli ultimi anni dimostra che gli attacchi "cyber" più significanti sono tutti stati legati, con diverse variabili, a uno Stato-Nazione.

Stuxnet, Duqu, Animal Farm, APT 28, RedOctober, sono solo alcuni esempi di armi „cyber" usate, pare, sia dal blocco NATO, sia da paesi esterni a questa unione militare. Il paradosso che ne risulta è che in un futuro prossimo, è veramente poco probabile che assisteremo alla nascita di un nuovo potere egemonico nel sistema. Tutti sono in concorrenza con tutti, con armi sempre più sofisticate. Questo stato di fatto ci porta ad un'altra conclusione: le risorse offensive "cyber" hanno creato un nuovo tipo di bilanciamento globale. La differenza sta ormai nella capacità di convertire gli "outcomes" in dividendi reali di potere, portando a raggiungere nuovi „inputs" e producendo nuovi orizzonti di conoscenza; quindi, è proprio il modo col quale gli attori della scena internazionale riescono a combinare le risorse a diventare, a sua volta, fondamentale.

Cyberberkut, il gruppoattivista che lotta nella cyber-guerra ucraina

All'inizio del 2014, dopo lunghe proteste anti-governative organizzate dai movimenti pro-europei favorevoli al processo di avvicinamento tra Ucraina ed UE, il presidente ucraino pro-russo Viktor Yanukovich è stato obbligato a lasciare il paese e a esiliare in Russia. Poco tempo dopo, quando la Rada (parlamento) ucraino votò una legge che ridusse la lingua russa allo statuto di lingua regionale, l'esercito russo mobilizzò forze considerevoli alla frontiera. Poche settimane più tardi, il presidente della Federazione Russa, Vladimir Putin, ricevette il voto pressoché unanime della Duma (parlamento) della Federazione per intervenire militarmente in Ucraina. Il risultato del referendum rapidamente organizzato dalle forze pro-russe in Crimea, analizzato secondo i provvedimenti della Costituzione della Federazione Russa – che stipulano la protezione dei propri cittadini all'estero – permise a Vladimir Putin di intervenire con truppe nella penisola, un territorio che era de *iure* sotto giurisdizione ucraina. Malgrado le pressioni dell'Occidente e degli USA, le forze militari russe furono mantenute, arrivando cosi a un conflitto in piena regola.

Il ruolo geopolitico dell'Ucraina e la sua importanza per la Russia non possono essere messi in dubbio, così come il fatto che l'Ucraina sia fondamentale per la Russia. La battaglia

che nacque allora acquisì una delle sue componenti più significative nello spazio digitale, dove i gruppi attivisti si sono dimostrati estremamente attivi.

Tra di essi, l'uno dei più visibili è il gruppo Cyberberkut.

Si tratta di un gruppo pro-russo apparso subito dopo l'annessione della Crimea da parte di Vladimir Putin. Il nome stesso del gruppo deriva da quello delle ex-forze speciali della polizia ucraina – Berkut– create nel 1992 e sciolte come conseguenza della repressione dell'Euromaidan. Cyberberkut personifica quindi l'ex unità armata, mettendo un accento nel ruolo maggiore che vuole svolgere „a supporto delle libertà e dei diritti degli Ucraini, rubate da hooligans pro-occidentali che lottano contro la Russia".

La storia, in breve, delle attività di Cyberberkut riflette attacchi di tipo DDoS condotti contro numerose infrastrutture critiche e altrettante agenzie governative dell'Ucraina, ma anche su bersagli di massima importanza al livello della NATO e dell'Unione Europea.

Secondo il sito del gruppo, esso avrebbe cominciato la sua attività in marzo 2014, quando attaccò diversi siti pro-occidentali ucraini, che sostenevano la rivoluzione[25]. In seguito agì contro militanti di destra, riuscendo a bloccare le comunicazioni di più di 800 smartphone utilizzati da questi militanti[26]. Gli eventi che sottolineeremo poi sono solo esempi scelti della vera e propria cyber guerra che attua il gruppo:

- 15.03.2015: attacco DDoSsu diversi siti NATO, incluso il Centrodi Eccellenza per la Difesa Cibernetica di Tallinn (Estonia)[27]. L'attacco è stato confermato dalla NATO;

- 22.05.2014: pochi giorni prima delle elezioni presidenziali in Ucraina, Cyberberkut annuncia che ha attaccato e distrutto la rete della Commissione Elettorale Centrale dell'Ucraina[28];

- 26.07.2014: attacco all'indirizzo email personale di un alto ufficiale del Ministero della Difesa ucraino[29];

- 14.08.2014: il gruppo annuncia il blocco del sito del presidente della Polonia e della Borsa di Varsavia;

- 22.11.2014: il gruppo pubblica numerosi documenti sulla cooperazione militare e tecnica tra USA e Ucraina, all'occasione della visita a Kiev del Vicepresidente americano Joseph Biden[30];

- 07.01.2015: annullamento dei conti Twittere Facebook del Parlamento tedesco e del Cancelliere Angela Merkel, con la motivazione che gli USA ela Germania appoggiano le forze fasciste pro-europee dell'Ucraina nella lotta contro i loro propri concittadini[31];

- 11.07.2015: il gruppo pretende l'accesso al computer personale del Senatore John McCain e pubblica un file video fabbricato in uno studio professionale, mettendo in scena un attacco terrorista. Il film è stato specialmente ideato per giustificare le ulteriori misure di ritorsione contro Stati del Medio Oriente[32].

Probabilmente, uno degli interventi più spettacolari del gruppo avvenne il 05 marzo 2014, quando fu postata sulla rete una conversazione telefonica, nella quale discutevano della situazione in Ucraina il Ministro estone degli Affari Esteri, Umas Paete l'ex-Alto Rappresentante per gli Affari Esteri dell'Unione Europea, Catherine Ashton. Il Ministero estone degli Affari Esteri ha confermato l'autenticità della conversazione, precisando che datava del 26 febbraio 2014, e che al momento dei fatti il Ministro estone si trovava in patria mentre Catherine Ashton era a Bruxelles[33].

Possiamo fare, su tutti questi fatti, qualche affermazione.

In primis, la vittimologia riflette una vasta gamma di bersagli: Ucraina, UE, Germania, Polonia, USA, NATO ed altri esempi. Il gruppo pare lottare contro tutti i paesi ostili all'intervento russo in Crimea.

In un secondo tempo, bisogna sottolineare la diversità degli attacchi e dei bersagli:

- Blocco o distruzione di siti, pagine web, sistemi di comunicazioni e talvolta persino infrastrutture critiche;

- Esfiltrazione di dati di e-mail di alti ufficiali riflettendo accordi segreti tra Ucraina e paesi della NATO e dell'U.E., così come pratiche di ufficiali ucraini legate agli interventi militari dell'Est del paese;

- Cyber-spionaggio dimostrato dall'attacco e dall'esfiltrazione di documenti che riflettono i piani militari così come l'assistenza militare accordata dall'Occidente alle truppe ucraine;

- Propaganda intensa del gruppo in favore dell'intervento pro-russo e profondamente contro le forze pro-europee. Questo sembrerebbe essere uno degli obiettivi principali del gruppo, perché la produzione del *soft power* è efficace.

Come terza osservazione, le attività del gruppo testimoniano le grandi qualità di versatilità e rapidità.

Poi, bisogna sottolineare che le capacità tecniche del gruppo sembrano molto avanzate, permettendo loro di poter intercettare e registrare conversazioni telefoniche di reti mobili europee ed ucraine.

Non da meno, le risorse umane delle quali dispongono sembrano significative, come dimostrano le capacità di reazione immediata dimostrata durante quasi tutti gli eventi maggiori del paese.

La sesta ed ultima osservazione è che l'analisi delle attività del gruppo riflette un'evoluzione delle tipologie degli attacchi, da quelli di tipo DDoS al furto di diritti di proprietà. È evidente che il gruppo riesce ad adattarsi molto velocemente ad un gran numero di attività che si svolgono nello spazio fisico, per produrre danni laddove le misure tradizionali sono inefficaci.

Da tutte queste osservazioni, se analizziamo la vittimologia, le risorse, le intenzioni e il comportamento dell'organizzazione creata, otteniamo un'attribuzione plausibile e ragionevole ad un attore statale che ha interessi maggiori in Ucraina e che è ostile alla NATO. Però, malgrado tutto ciò, non abbiamo nessuna certezza tecnica. L'attore è diffuso e i bersagli sono colpiti dalla sua forza in modo inaspettato. Ci troviamo di fronte a un potere geograficamente diluito e quindi a un'attribuzione plausibile. Una sola cosa è certa: il legame tra il gruppo e un potenziale attore statale riflette una parte delle capacitàcyber che questo Stato possiede.

Conclusioni

Il cyber-potere è un'espressione di un nuovo tipo di spazio, apparso coll'esplosione dell'Internet e dei mezzi moderni di comunicazione. È fondamentalmente diverso da tutte le altre forme di potere, non solo per gli

ingredienti che lo compongono, ma soprattutto per l'influenza che esercita su tutti gli altri poteri. La sua diffusione, forza di propagazione e impercettibilità lo rendono, spesso, impossibile da fronteggiare. Dello stesso cyber-potere possono essere vittime senza difficoltà grandi attori del sistema, senza che questi possano percepire a tempo questo fatto. Però, fino a quando le risorse dello spazio fisico rimarranno importanti, il cyber-potere e le sue risorse non potranno sostituirsi alle risorse tradizionali del potere. Possono, con certezza, amplificarne l'importanza e, spesso, fare la differenza. Per questo motivo, il cyber-potere è un pilastro del potere generale e la sua posizione nell'indice generale del potere è significativa.

Come i poteri tradizionali, il cyber-potere è contestuale, cumulativo e rinnovabile. Gli attori che riusciranno a massimizzare queste caratteristiche del cyber-potere avranno le più grandi chances di occupare le più alte posizioni della classifica.

Infine, se le sue risorse sono più accessibili a una vasta gamma di attori, la realtà degli ultimi anni dimostra che solo gli Stati possono veramente accedere a quegli asset che possono realmente fare la differenza. Si può quindi dedurre che il cyber-poterecome pilastro dei poteri nel sistema internazionale è un attributo *"smart"* di alcuni stati *"smart"*. È proprio nel modo col quale gli attori del sistema combineranno tutti i tipi di risorse per trasformarle in potere effettivo che dipenderanno non solo il modo di esercitare il potere ma anche il modo col quale questo sarà distribuito nel quadro del sistema internazionale. ■

1 Singer Paul, Friedman Allan, Cybersecurity and cyberwar, Oxford, University Press, 2014, p. 2
2 Nye Joseph, Cyber power, Harvard Kennedy School, BelferCenter for science, May 2010, p 2
3 Singer Paul, Friedman Allan, op.cit., p. 2
4 Kuehl Daniel, From Cyberspace to cyberpower, defining the problem, in Kramer Franklin, Stuart Starr, Wentz Larry, Cyberpower and national security, US National Defence University Press, Washington DC, 2009, p. 24
5 Paul Popescu Alina Bârgăoanu, Geopolitica, NUSPA, Bucharest, 2004, p. 46
6 Baldwin David, Power and international relations, Carlsnaes Walter, Risse Thomas, Beth Simmons, Handbook of international relations, Sage publications ltd, 2013, p. 275
7 Singer Paul, Friedman Allan, op.cit., p.4
8 Paul Kenedy, Ascensiuneaşidecădereamarilorputeri, Polirom, Bucureşti, 2011, pag. 391
9 Ibidem pag 15
10 Kuehl Daniel, op.cit. p.3
11 Apud Samuel McQuade, Encyclopedy of cybercrime, GreenwoodPublishing Group p 52, în Şapte teme fundamentale pentru România, 2014, p.190
12 George Cristian Maior, State, Networks, Companies and Individuals: cyberspace paradoxes, in p. 190, in Seven fundamental issues for Romania, RAO Class, 2014, p.190
13 Singer Paul, Friedman Allan, op.cit., p.13
14 https://www.f-secure.com/weblog/archives/00002791.html
15 Zetter Kim, Countdown to zero day, Crown Publishers, New York, 2014, p. 3
16 Daniel Kuehl, op.cit, p.6
17 Nye Joseph, op.cit., p. 5
18 Maior George Cristian, op.cit. p. 191
19 Nye Joseph, The future of power, Polirom, Bucharest, 2012, p 12
20 Alexander Klimburg, Cyberpower and international security in international relations, seminar, spot in https://mediacapture.brown.edu:8443/ess/echo/presentation/8792278f-7098-40ec-87a7-a51ac98c49fa
21 Singer Paul, Fridman Allan, op.cit. p. 36
22 Cosmoiu Florin, The impact of Global Cyber threat. Evolutions and perspectives in Romania, in Seven fundamental issues for Romania, RAO Class, 2014, p.283
23 Klimburg Alexander, https://mediacapture.brown.edu:8443/ess/echo/presentation/8792278f-7098-40ec-87a7-a51ac98c49fa
24 Nye Joseph, Cyber power, Harvard Kennedy School, BelferCenter for science, May 2010, p.10
25 http://cyber-berkut.org/en/olden/index5.php
26 ibidem
27 http://www.rt.com/news/nato-websites-ddos-ukraine-146/
28 http://www.globalresearch.ca/unconfirmed-reports-electronic-files-of-ukraine-central-election-commission-cec-disabled-dnipropetrovsk-administration-computer-network-destroyed-unconfirmed-report-by-cyberberkut-hackers/5383742
29 http://cyber-berkut.org/en/olden/index1.php
30 ibidem
31 http://www.ibtimes.co.uk/german-government-websites-including-angela-merkels-hit-by-severe-cyberattack-1482345
32 http://leaksource.info/2015/07/12/leaked-video-shows-making-of-islamic-state-execution-in-studio-via-cyberberkut-hack-of-sen-mccain-staffer/
33 http://leaksource.info/2014/03/05/ukraine-leaked-call-estonia-foreign-minister-and-catherine-ashton-snipers-allegedly-hired-by-maidan-leaders/

Bibliografia

1. Singer Paul, Friedman Allan, *Cybersecurity and cyberwar*, Oxford, University Press, 2014
2. Nye Joseph, *Cyber power*, Harvard Kennedy School, Belfer Center for Science, May 2010
3. Nye Joseph, *The future of power*, Polirom, Bucharest, 2012
4. Kuehl Daniel, *From Cyberspace to cyberpower, defining the problem*, in Kramer Franklin, Stuart Starr, Wentz Larry, Cyberpower and national security, US National Defence University Press, Washington DC, 2009
5. Popescu Paul, Bârgăoanu Alina, *Geopolitica*, NUSPA, Bucharest, 2004
6. Baldwin David, *Power and international relations*, Carlsnaes Walter, Risse Thomas, BethSimmons, Hanbook of international relations, Sagepublicationsltd, 2013
7. Kenedy Paul, *The rise and fall of greatpowers*, Polirom, Bucharest, 2011
8. Maior George Cristian, *State, Networks, Companies and Individuals: cyberspace paradoxes*, in p. 190, in Seven fundamentalissues for Romania, RAO Class, 2014
9. ZetterKim, *Countdown to zero day* Crown Publishers, New York, 2014
10. Klimburg Alexander, *Cyberpower and international security in international relations*, seminar, spot in https://mediacapture.brown.edu:8443/ess/echo/presentation/8792278f-7098-40ec-87a7-a51ac98c49fa
11. CosmoiuFlorin, *The impact of Global Cyber Threat. Evolutions and perspectives in Romania*, in Seven fundamentalissues for Romania, RAO Class, 2014
12. http://cyber-berkut.org/en/olden/index5.php
13. https://www.f-secure.com/weblog/archives/00002791.html
14. http://www.globalresearch.ca/unconfirmed-reports-electronic-files-of-ukraine-central-election-commission-cec-disabled-dnipropetrovsk-administration-computer-network-destroyed-unconfirmed-report-by-cyberberkut-hackers/5383742
15. http://www.rt.com/news/nato-websites-ddos-ukraine-146/
16. http://www.ibtimes.co.uk/german-government-websites-including-angela-merkels-hit-by-severe-cyberattack-1482345
17. http://leaksource.info/2015/07/12/leaked-video-shows-making-of-islamic-state-execution-in-studio-via-cyberberkut-hack-of-sen-mccain-staffer/
18. http://leaksource.info/2014/03/05/ukraine-leaked-call-estonia-foreign-minister-and-catherine-ashton-snipers-allegedly-hired-by-maidan-leaders/
19. http://natocouncil.ca/cybersecurity-and-the-ukraine-crisis-the-new-face-of-conflict-in-the-information-age/
20. http://thediplomat.com/2015/03/russia-tops-china-as-principal-cyber-threat-to-us/

Cosa si può mettere online e cosa si deve tenere per sé

Arnaud Velten

Autore: Laurent Chrzanovski

Laurent Chrzanovski: Sig. Velten, al "Grappa Hat" di Aosta nel 2015 e poi in altri convegni, ha impressionato il pubblico con una conferenza intitolata "Are you what you sign? I say no", un vero e proprio manifesto sulle precauzioni da prendere prima di accettare o di firmare qualsiasi cosa online. Tra le sue numerose specialità nel campo della cyber security, perché ha scelto di privilegiare questo tema?

Arnaud Velten: Questo tema mi sta a cuore perché è il riflesso di un'esperienza personale.

Appena diventato adulto, ero piuttosto timido e introverso. Dal momento che lavoravo tra l'altro a progetti grafici, una delle prime comunità ad avermi accettato fu quella degli artisti delle serate che frequentavo: musici, DJs, clubbers. La mia sete di riconoscenza, che si vide "consacrata" da un invito a partecipare a discoteche private sul Lago di Annecy, era allora accompagnata da un nomignolo del quale, nell'immediato, non misurai la portata. Visto che all'epoca ero molto magro, questa comunità mi 'battezzò' "Auschwitz".

Per conservare questa prima cerchia di amici, non dissi nulla e non mi sono posto domande sino al giorno in cui, molti anni più tardi, ho saputo che mio nonno, resistente dalla prima ora, era stato arrestato dalla Gestapo e buttato in un vagone merci a destinazione di Dachau, dopo aver partecipato ad una delle più gloriose operazioni della resistenza, quella del "Maquis des Glières". È riuscito a salvare la pelle evadendo dal treno a Digione per raggiungere i gruppi antinazisti del Giura. In quel momento realizzai che non avrei mai più accettato scherzi o nomignoli stupidi solo per fare parte di una comunità.

Laurent Chrzanovski: la Sua riflessione, che avrebbe potuto fermarsi agli "amici", va molto più lontano.

Arnaud Velten: Sì. Perché il fatto tutto sommato banale, per un adolescente, di accettare anche "il peggio" per integrarsi è l'inizio della discesa che lo porterà a diventare il cittadino rassegnato di domani. Se non rimette in causa l'accettazione di ogni "amico" sulle reti sociali, se "firma", anche con un semplice click, la sua adesione a qualsivoglia sito scegliendo di ignorarne le clausole contrattuali, finirà per non leggere nemmeno le condizioni, i doveri e gli obblighi riguardanti un contratto di lavoro nel mondo reale. Grosso modo, la sua vita sarà in ogni momento dettata da terzi, senza che la persona stessa se ne renda conto, almeno all'inizio…

Laurent Chrzanovski: come possiamo muoverci in modo sicuro in questo complesso mondo digitale di cui la maggioranza degli adulti ne ignora i rischi?

Arnaud Velten: Per quello che mi riguarda, avevo due opzioni se teniamo conto del mio percorso professionale: diventare un *"black hat"* e *"attaccare i sistemi"*, oppure mettere le mie forze al servizio di progetti di trasparenza e di prevenzione. Ho scelto la seconda via, diventando un *"White Jedi"*. Il problema più difficile da risolvere oggi è quello dell'iper-connettività completamente incompresa dagli utenti (persino da molti specialisti del campo delle TIC) mentre Internet è il più grande archivio che sia mai esistito.

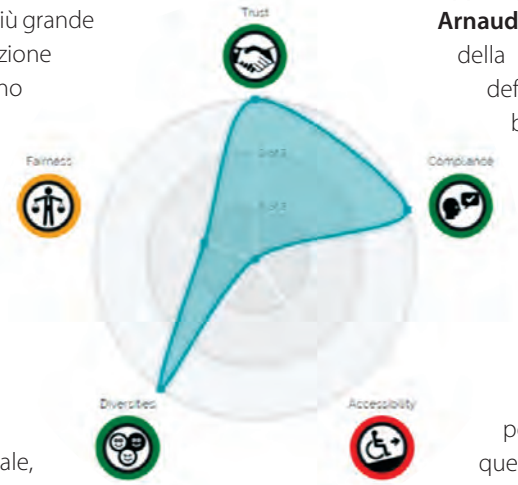
BIO

Esperto in strategia e tattica digitali, Arnaud Velten (@bizcom) ha fatto i suoi primi passi nell' underground informatico quando era adolescente, prima di studiare comunicazione, arti audiovisuali e infine marketing prima di specializzarsi in *intelligence* strategica.
Nel corso del suo percorso professionale (giornalismo, blogging, arte, gestione eventi) ha messo a frutto acquisito sulla scena underground, applicandolo alla comunicazione digitale. E così che nel 2007 ha eseguito il primo curriculum vitae isometrico (l'isomap) e, nel 2009, ha ideato un metodo di Brainstorming battezzato *"Emerge map"* …
Osservatore discreto, ottimo networker, contribuisce dal 2010 a numerosi eventi come moderatore e come *influencer*. Nel 2014 è diventato membro dello staff della Cybersecurity Alliance e del Summit *Intelligenza Economica, Security e Safety* (IE2S Chamonix).

Durante le mie presentazioni sulla prevenzione, uso spesso parallelismi tratti dall'attualità dei media, come ad esempio un uomo d'affari che si affidava ciecamente a Bernard Madoff, oppure l'ecologista americano che credeva di guidare "pulito" perché aveva una macchina tedesca, fino al giorno in cui… tutto ciò crollò davanti ad una realtà ben più scura. Con queste immagini di "successi" diventati degli "scandali", voglio far capire a che punto l'uomo è intrinsecamente naïf quando offre la sua fiducia ad un individuo o ad una marca che hanno un'immagine che pare perfetta.

Laurent Chrzanovski: qual è il Suo scopo con questi esempi?

Arnaud Velten: Bisogna portare il subcosciente collettivo a fare un'introspezione sul modo col quale ognuno di noi si connette. Sì, utilizziamo le reti sociali, ma sappiamo che queste stesse reti, nelle quali abbiamo fiducia, stanno mettendo a punto la più grande intrusione possibile sviluppando motori di ricognizione facciale ad altissima velocità? Quando questi saranno messi in servizio, non vi sarà più nessuna immagine di noi stessi, dei nostri cari, che verrà ignorata, ivi comprese tutte quelle che oggi si trovano "smarrite" nel deep web. Ed è così che tutto il nostro passato, e non per forza il più "glorioso" per chi è un addetto della messa online sistematica di immagini, salterà agli occhi di tutti.



Laurent Chrzanovski: come potremmo tecnicamente evitare 'sciagure', almeno con quello che non abbiamo ancora messo online?

Arnaud Velten: Lavoro in un gruppo internazionale, Thinkservices, costituito da volontari allo scopo di creare un'estensione, facile da utilizzare, di *crowd sourcing*. La sua missione, quando l'internauta l'avrà inserita nel suo motore di ricerca, sarà di indicargli immediatamente la fiducia che può più o meno accordare ad un sito o ad una rete sociale, secondo cinque parametri semplici: l'accessibilità e la diversità (fattori d'attrazione) messi a confronto con la *compliance*, la fiducia e l'onestà del sito. In questo momento, ci focalizziamo, come inizio, sui servizi Cloud, sotto la direzione di Pascal Kotté del Professore Jean Henry Morin dell'Università di Ginevra, che desidero ringraziare per la fiducia accordatami.

Le valutazioni di ognuno di questi parametri, che verranno inserite dagli internauti stessi, diventeranno a loro volta una garanzia di oggettività (dovuta al numero di partecipanti e al concetto di volontariato) e una dimostrazione chiara della complessità del sistema: ogni utilizzatore della rete potrà allora scegliere con consapevolezza quello che decide di accettare (nella sua vita privata, nei suoi risparmi se sceglie un sito a pagamento) per preservare la sicurezza della sua "reputazione digitale". La cartografia, una delle mie vecchie passioni, permette di rendere un'immagine, in termini di impatto, tanto quanto decine di lunghi discorsi.

Laurent Chrzanovski: com'è passato dal mondo della grafica e dei white jedi alla gestione della comunicazione di un evento delicatissimo come l'IE2S?

Arnaud Velten: È un risultato della stessa riflessione, raddoppiata dai miei studi nel campo del Marketing, dell'Intelligence Strategica e dei Media. Il problema, per eventi strategici e confidenziali come l'IE2S, è di assicurare la sicurezza della parte "closed doors", che solo i partecipanti conoscono (luogo dell'incontro, agenda di indirizzi, contenuto delle discussioni tematiche) sempre rimanendo visibile. Una persona o un evento senza presenza digitale (immagini, testi, video, hashtags) è semplicemente inesistente al giorno d'oggi. Gli eventi strategici, contrariamente a dei grandi convegni aperti a tutti, devono essere documentati con molta finezza e con un po' di distacco necessario, proprio quello che permette ogni volta di porsi la domanda: "se metto questo online, quale immagine verrà percepita dall'internauta?"

Laurent Chrzanovski: quali sono le parole chiave di una tale comunicazione, e cioè quello che non deve essere (troppo) spiegato?

Arnaud Velten: In primis, gli obiettivi della comunicazione devono essere definiti dagli organizzatori dell'evento ben prima dell'incontro, ed il "comunicatore" deve capire l'evento per adattarsi e non derogare a questi obiettivi.

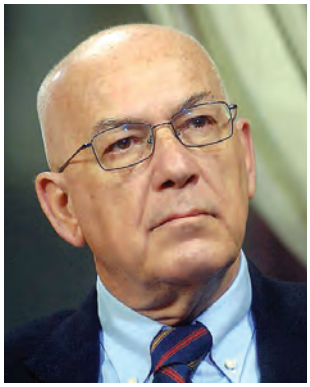
Ci sono alcune regole d'oro, di qualsiasi evento strategico si tratti. La più importante è di documentare senza mai mentire. La soggettività non ha posto per ciò che verrà reso pubblico in questo tipo di incontri. Per fare ciò, in termini di fotografia, ad esempio, bisogna sempre rispettare l'immagine degli oratori e delle persone presenti. Giocando con l'obbiettivo, si cercherà sempre di fotografare solo il volto dello speaker. Se uno scatto è pessimo o indelicato, bisogna immediatamente distruggerlo. Poi ci sono anche cose che sembrano banali: portare un apparecchio fotografico di grandi dimensioni, ben visibile, indica a tutti che si è lì proprio per prendere immagini: la circospezione e la paura della "foto rubata" sparisce e guadagnate la fiducia delle persone presenti, che sanno che possono rifiutare di essere ritratte ma anche validare la messa online o chiedervi di eliminare tale scatto.

Poi, bisogna assolutamente marchiare in modo indelebile le fotografie autorizzate prima di postarle sulle reti, permettendo agli organizzatori di distinguerle da quelle prese da terzi senza autorizzazione e quindi, se queste ultime appariranno online, di agire in conseguenza. Infine, bisogna adattare il corpus delle immagini e delle sequenze con la linea voluta dagli organizzatori.

La chiave del successo, al di là di imparare sempre dai propri errori, è di lavorare in profondità con gli organizzatori per decidere cosa deve essere messo online "nell'immediato" e quello che può aspettare la fine della mezza giornata, della giornata o dell'intero evento per poter fare una scelta a freddo con cognizione di causa. ■

I vent'anni della Privacy in Italia e le nuove sfide del digitale

Intervista VIP con Antonello Soro, Presidente Autorità Garante per la Protezione dei dati personali



Antonello Soro

Autore: Massimiliano Cannata

Massimiliano Cannata: L'8 maggio del 1997 è entrata in vigore in Italia la legge sulla protezione dei dati personali. Sono passati vent'anni di grandi trasformazioni sociali, economiche e culturali. Presidente Soro come va declinato oggi il concetto di Privacy?

Antonello Soro: L'introduzione nel nostro ordinamento del diritto alla protezione dei dati ha segnato un radicale cambiamento culturale e sociale che ha fatto fare al Paese grandi passi avanti nella tutela della riservatezza, della libertà e della dignità delle persone. A distanza di vent'anni lo stesso termine "privacy" risulta riduttivo e oggi la tutela dei dati personali viene finalmente considerata per quello che veramente è: un diritto fondamentale della persona, da rispettare in ospedale, sul posto di lavoro, sul web.

Massimiliano Cannata: Ammetterà che è difficile difendere questo valore in una società assetata di informazioni.

Antonello Soro: Proprio perché la sfida è ardua diventa più affascinante affrontarla. E' ormai chiaro che il diritto alla privacy non è più o non è soltanto una prerogativa del singolo, ma un valore collettivo che tutti dobbiamo concorrere a costruire. In questi anni la raccolta e l'analisi dei dati personali hanno sempre più rappresentato un asset strategico per gli Stati come per le grandi imprese dell'economia digitale. Va anche precisato che la centralità del diritto alla protezione dei dati personali assume oggi una posizione cruciale per la difesa dell'individuo da forme intrusive di controllo e manipolazione e da un'inconsapevole delega delle proprie scelte alla tecnologia.

I nuovi confini della libertà *nell'information society*

Massimiliano Cannata: Nel corso dell'ultima relazione annuale Lei ha denunciato la preoccupante emersione di nuove "schiavitù volontarie",

BIO

Presidente dell'Autorità Garante dal 19 giugno 2012, Antonello Soro è stato Vice Presidente dei Garanti privacy europei (WP art. 29) dal 26 novembre 2014 al 12 dicembre 2016. Primario Ospedaliero, è stato sindaco di Nuoro e consigliere regionale della Sardegna e nel 1994 viene eletto deputato. Dal 1998 al 2001 è stato presidente del Gruppo parlamentare "Popolari e democratici - L'Ulivo", dal 2007 al 2009 presidente del Gruppo del partito democratico della Camera. É stato membro di diversi organi parlamentari dal 1994 al 2012 quando si è dimesso per incompatibilità da deputato a seguito della nomina all'Autorità. Ha presentato numerose proposte di legge come primo firmatario tra cui le norme deontologiche relative al trattamento dei dati personali, anche acquisiti mediante intercettazioni, nell'ambito dell'attività giornalistica e le norme in materia di disciplina del procedimento legislativo.

connesse a uno sviluppo tecnologico che, se non adeguatamente regolamentato, rischia di diventare "distotipo" e "dispotico". Possiamo spiegare cosa significa questa coppia di termini?

Antonello Soro: Quello a cui stiamo assistendo è la progressiva cessione della nostra libertà in cambio di utilità e servizi digitali. Sempre di più deleghiamo alla tecnologia le scelte e la risoluzione dei problemi, affidando la nostra vita quotidiana a device, così finiamo col rafforzare la nostra dipendenza dai software che usiamo. Si tratta di un fenomeno inquietante che va ridimensionato con grande razionalità ed equilibrio.

Massimiliano Cannata: "Internet è il più grande spazio di libertà che l'uomo abbia conosciuto", la nostra è ormai una digital life viviamo dentro il web, in una dimensione quasi omeopatica. Stefano Rodotà aveva lavorato al progetto di una "Costituzione per Internet". Le pare che sia un'idea ancora valida?

Antonello Soro: L'idea di una Carta che fissi una cornice di principi comuni e condivisi ha un enorme valore simbolico, e una forza attrattiva anche per gli Stati al di fuori dell'Europa. Al potere globale dei colossi della rete occorre rispondere con misure globali. Le nuove tecnologie hanno dimostrato infatti capacità enormi di scardinarne i presupposti essenziali dello Stato: in primo luogo la territorialità, quale criterio di competenza ed applicazione della legge. Gli Over the Top sempre più spesso intervengono, in un regime prossimo all' autodichia, per comporre istanze di rilevanza primaria, quali informazione e diritto all'oblio, libertà di espressione, dignità e tutela dalle discriminazioni, veridicità delle notizie diffuse.

Massimiliano Cannata: Quello che si impone è una riflessione sui nuovi confini della libertà disegnati dal prepotente sviluppo della società digitale. Qual è il suo giudizio in merito?

Antonello Soro: L'esempio degli *Over the Top* che ho richiamato prima è emblematico perché fa comprendere come la concentrazione in capo a pochi soggetti privati di un rilevantissimo potere, non solo economico, ha determinato e sta determinando un mutamento sostanziale nei rapporti tra individuo e Stato, tra pubblico e privato. Un numero esiguo di aziende possiede un patrimonio di conoscenza gigantesco e dispone di tutti mezzi per indirizzare la propria influenza verso ciascuno di noi. La misura delle nostre libertà è, dunque, fortemente condizionata dall'operato delle grandi imprese dell'economia digitale.

Verso una privacy *continentale*

Massimiliano Cannata: Rimaniamo allo scenario globale. Il Nuovo quadro giuridico europeo potrà segnare un passaggio decisivo e instaurare una collaborazione efficace tra gli Organismi di vigilanza che operano nei diversi Stati?

Antonello Soro: Una delle novità più importanti introdotte dal Regolamento sta nell'aver previsto l'applicazione dell'ordinamento europeo anche agli OTT. A partire dal 25 maggio del prossimo anno chiunque e in qualunque parte del mondo tratti dati di cittadini europei dovrà rispettare le regole europee e assicurare le garanzie previste nell'Ue. Questo consentirà peraltro anche di superare la disparità di trattamento inaccettabile anche sotto il profilo concorrenziale, rispetto a operatori continentali che offrono i medesimi servizi. Va peraltro sottolineato che le sanzioni previste dal Regolamento per le aziende che violino la normativa sulla protezione dati possono arrivate fino al 4 per cento del loro fatturato annuo. Non è una cifra da poco.

Massimiliano Cannata: Riusciremo a definire in tempi brevi una "privacy continentale" condivisa, fondata su norme semplici, omogenee universalmente applicabili?

Antonello Soro: Per quanto riguarda questo aspetto possiamo dire che l'obiettivo del Regolamento è proprio quello di creare un'area omogenea di principi e regole uniformi da applicare in ogni Stato membro, superando le asimmetrie che si sono riscontrate nel recepimento della Direttiva del 1996. Ciò consentirà sicuramente una maggiore e più efficace collaborazione tra le Autorità di protezione dati e un'armonizzazione anche delle procedure.

Massimiliano Cannata: Il 25 maggio 2018 scatterà una scadenza molto importante con l'entrata in vigore del Regolamento europeo in materia di Protezione dei dati Personali. Che cosa cambierà da quel momento?

Antonello Soro: Oltre all'estensione del quadro giuridico ai soggetti stabiliti al di fuori dell'Ue, vanno sicuramente evidenziati almeno due nuovi diritti che, superando gli anacronismi della vecchia disciplina, pongono il nuovo quadro regolatorio al passo con lo sviluppo tecnologico del mondo digitale. Penso al diritto all'oblio, che trova la sua codificazione dopo le sentenze della Corte di giustizia dell'Ue, e quello alla portabilità dei dati, che riguarderà qualunque soggetto tratti dati, non solo i provider telefonici e di comunicazioni elettroniche, e che consentirà di trasferire i propri dati da un gestore di servizi ad un altro in un formato interoperabile. Dunque, maggiore libertà per gli utenti in un mercato digitale più aperto alla concorrenza.

Massimiliano Cannata: Imprese private e PA sono al centro di questo importante flusso di trasformazioni. Quali impatti bisognerà prevedere?

Antonello Soro: Sicuramente in prima battuta verrà richiesta una maggiore responsabilizzazione sia alla pubblica amministrazione che ai soggetti privati tramite l'adozione di misure che tengano conto costantemente del rischio che un determinato trattamento di dati personali può comportare per i diritti e le libertà degli interessati. Concretamente mi riferisco all'obbligo di prevedere una valutazione di impatto privacy prima di procedere a trattare i dati e adottare prassi di "privacy by design" (garanzie fin dalla progettazione) e "privacy by default" (impostazioni predefinite). Va inoltre evidenziato il ruolo che è chiamata a svolgere la nuova figura del Responsabile della protezione dati (RPD) che dovrà assicurare una gestione corretta dei dati personali, che sarà obbligatoria nelle amministrazioni pubbliche e nelle aziende che effettuano particolari trattamenti delle informazioni.

Il ruolo chiave dell'RPD

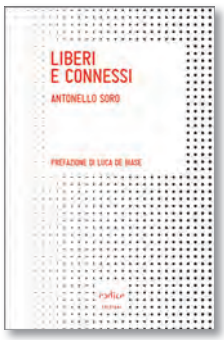
Massimiliano Cannata: Figure fino a oggi inedite saranno create, come il RPD, ci sarà bisogno di lavorare sulle competenze e sulla formazione per rafforzare una cultura adeguata a tutti i livelli delle organizzazioni. Le aziende grandi e piccole stanno lavorando per adeguare i propri modelli organizzativi alla normativa. Che consiglio si sente di poter dare?

Antonello Soro: Il consiglio che mi sento di dare è di non sottovalutare la figura e il ruolo del RPD. Bisogna, insomma, non cadere nell'errore di designare uno qualunque dei propri dipendenti o il primo consulente che si propone. Il RPD ha un ruolo chiave e occorre che sia un esperto, che abbia le *skills* adatte ai delicati compiti che è chiamato a svolgere come indicato nelle Linee guide messe a punto dai Garanti della privacy Ue: deve possedere qualità professionali e conoscenze specialistiche, competenze giuridiche e informatiche, legate alla necessità di garantire la sicurezza dei dati.

Massimiliano Cannata: Un'ultima domanda, dal momento che ci rivolgiamo a un pubblico che si occupa di queste tematiche. La cyber security è una componente strategica della sicurezza nazionale e pubblica. Nel 2016 gli attacchi informatici avrebbero causato alle imprese italiane danni per nove miliardi di euro, mentre risulta che meno del 20 per cento delle aziende investe per proteggere il patrimonio informatico. Come si può colmare questo gap?

Antonello Soro: I recenti gravissimi attacchi hacker e i dati che emergono dalle ricerche dimostrano che la *cybersecurity* non è ancora diventata una componente strategica per imprese e pubbliche amministrazioni. Secondo stime recenti, nello scorso anno le infrastrutture critiche sarebbero state oggetto del 15 per cento di attacchi in più rispetto all'anno precedente e sarebbero cresciuti del 117 per cento quelli riconducibili ad attività di *cyberwarfare*, volte a utilizzare canali telematici per esercitare pressione su scelte geo-politicamente rilevanti. Proteggere i dati è un compito primario che tutti gli Stati sono chiamati ad assolvere senza indecisioni o problemi di bilancio. Quando ad essere attaccate sono strutture sanitarie, università e quindi mondo della ricerca, infrastrutture strategiche, sistemi di comunicazione, ogni ritardo diventa esiziale. Software non aggiornati e misure di sicurezza obsolete non possono essere tollerati. La resilienza informatica nel contrasto delle minacce cibernetiche deve, dunque, rappresentare ciò che la resilienza della democrazia rappresenta nel contrasto del terrorismo. E per garantire davvero la cyber sicurezza e la sicurezza nazionale è necessario evitare il rischio della parcellizzazione dei centri di responsabilità, con una centralizzazione di competenze e un'organica razionalizzazione del patrimonio informativo, anzitutto pubblico. ■

Liberi e connessi (Antonello Soro, Codice edizioni).



E' l'uso della congiunzione liberi (e) connessi che marca una profonda differenza semantica: sarebbe stato forse più facile e persino anche più banale contrapporre le due categorie, considerando libero chi riesce a stare al di fuori del recinto digitale costituito dalle reti e dalle infostrutture entro cui tutti ormai viviamo immersi come in una dimensione omeopatica. Antonello Soro, Presidente dell'Autorità Garante per la Protezione dei dati personali, non corre il rischio di schierarsi dalla parte di chi vuole "fermare il vento con le mani", illudendosi di negare il progresso, negando ogni valore all'innovazione. In questo bellissimo saggio viene offerta infatti al lettore una stimolante panoramica delle profonde trasformazioni che stanno cambiando radicalmente la vita di ognuno, il nostro modo di relazionarci agli altri, la concezione del lavoro e della produzione. Sperimentare il flusso del cambiamento significa conquistare la consapevolezza che la libertà va conquistata nel digitale rispettando la cultura del diritto e delle regole, che si evolvono rispondendo alle sollecitazioni della scienza e della tecnologia, questo il messaggio di fondo del saggio. Occorre, in altri termini, interpretare con lucidità la nuova categoria dell'essere, quel *"virtuale"*, per usare una celebre definizione del filosofo Pier Levy, dentro il cui orizzonte ontologico ed esistenziale va ricercato il senso della contemporaneità.

Tutte le sezioni del volume risultano interessanti, tanto che la trattazione risulta una vera e propria "bussola" di orientamento, rivolta non solo agli addetti ai lavori. L'osservatorio del Garante è, infatti, un punto privilegiato di analisi di grandi questioni del nostro tempo a partire dalla classica dicotomia che riguarda il rapporto tra libertà e sicurezza, tra diritto dell'informazione e privacy in un mondo globale che non ha più limiti e che dovrà al più presto preoccuparsi di ridefinire il concetto di territorialità per ridare il giusto peso all'esercizio della sovranità statale nella difesa dei diritti fondamentali.

Ma di fronte alla rivoluzione digitale vi sono limiti da imporre alla scienza? E' questo l'interrogativo su cui bisognerà insistere per comprendere a fondo dove ci porterà quell'universo delle app ben descritto in uno dei capitoli del libro. Tutti dovranno poter accedere ai benefici offerti senza alcuna discriminazione, nessuno può usare l'innovazione scientifica e tecnologica per disporre del corpo altrui senza il consenso dell'interessato, per trasformarlo in una macchina da controllare. Dai trapianti agli impianti tecnologici nel corpo, tutto questo nuovo universo ci parla della possibilità di scelte consapevoli anche là dove prima comandavano soltanto le leggi di natura. Questa rappresentazione che già molti studiosi definiscono del post-umano troverà i suoi criteri regolatori che accompagnano l'umano, cioè nel ricorso ai principi di libertà, eguaglianza, dignità? Una cosa è certa intorno a questi valori si dovrà costruire il nuovo orizzonte di "costituzionalismo globale", tracciando il percorso di una nuova stagione dei diritti, ancora in larga parte tutta da scrivere. ■

Massimiliano Cannata

GDPR: un framework per l'implementazione e la conformità

Autori: Giancarlo Butti e Maria Roberta Perugini

Il GDPR ha cambiato l'approccio alla compliance privacy da parte delle imprese?
Quali sono le azioni da attuare per essere pronti ad affrontare l'efficacia del GDPR alla data del 25 maggio 2018?
È possibile definire un framework per attuare e comprovare la conformità? E come si sviluppa un piano operativo per la sua implementazione?
Il seguente articolo si pone come obbiettivo di rispondere in modo pratico ai precedenti quesiti.

BIO

Giancarlo Butti - Ha acquisito un master di II livello 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…
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 8 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.

Il GDPR introduce un cambiamento di grandissima portata, che trasforma radicalmente l'approccio alla privacy che le imprese devono avere. Non si tratta soltanto di un tema tecnologico, ma è una sfida che coinvolge tutta l'organizzazione dell'impresa.

L'adeguamento non richiede solo nuove soluzioni tecniche, ma è una sfida che coinvolge aspetti organizzativi, di *governance* e legali e, in generale, comporta un nuovo modo di operare e di affrontare le responsabilità connesse alla protezione dei dati e dei diritti e delle libertà fondamentali delle persone fisiche, anche sviluppando in ogni area aziendale nuove competenze e professionalità.

Bisogna insomma sapere collegare aspetti legali e possibili soluzioni tecniche ed organizzative, per essere in grado di:

- identificare gli interventi necessari, assegnando le relative responsabilità;
- pianificare ed ottimizzare gli interventi con una prospettiva che ne copra l'intero ciclo di vita;
- misurare e dimostrare se e quanto le iniziative hanno portato i risultati attesi;
- recuperare gli investimenti pregressi (effettuati per l'adeguamento a normative specifiche o per certificazioni e accreditamenti).

Questo richiede un approccio multidisciplinare (legale, governance, tecnico, organizzativo), con l'obiettivo di definire un unico schema integrato *("framework")* di implementazione del GDPR che l'impresa possa attuare nel continuo in un contesto di autonomia.

Per facilitare un approccio sistematico e potere pianificare e documentare quanto fatto in modo ottimale, abbiamo costruito un modello[1] che elenca e classifica le varie attività secondo due dimensioni:

1 **La tipologia dell'intervento:** si tratta di raccogliere informazioni, di definire policy o processi, di assegnare ruoli…

2 **La fase nella quale, in un ideale ciclo di vita della conformità al GDPR, l'intervento stesso può essere collocato:** acquisizione iniziale di informazioni sul contesto in cui si opera, costruzione di tutele, pianificazione di monitoraggi o risposte ad eventi, recupero o ripristino da incidenti…

Abbiamo quindi collocato nelle "caselle" di incrocio le attività dedotte da una analisi del GDPR.

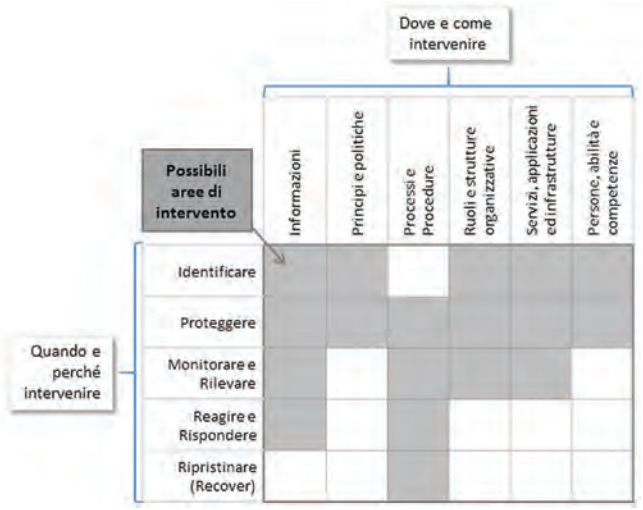


***Fig. 1** – Il modello del framework*

Vantaggi e benefici

Questo tipo di approccio comporta una serie di vantaggi e benefici, fra i quali:

- ridurre la complessità ed operare **efficacemente**, in modo sequenziale e sistematico, seguendo, se possibile ed utile, **standard e buone pratiche**
- garantire risultati in linea con quanto richiesto dalle norme, avendo sempre presente un **"obiettivo guida"**
- operare in **modo integrato** con altre iniziative dell'organizzazione / azienda in cui si opera, in particolare per quanto riguarda la sicurezza
- adottare un effettivo approccio **risk-based**: considerando, ad esempio, le possibili conseguenze sugli interessati di una non conformità
- operare in modo proattivo con azioni preventive, in grado di rilevare e correggere situazioni anomale e coerenti con quanto richiesto dalla norma in termini di **protezione dei dati fin dalla progettazione e protezione per impostazione predefinita**.

Dopo una prima analisi è anche possibile valutare quanto l'organizzazione ha già realizzato:

- per il rispetto di normative precedenti nell'ambito della protezione dei dati personali (ad esempio il D.Lgs 196/03)
- per il rispetto di altre norme in vigore in altri ambiti (ad esempio normativa sulla safety)
- per il rispetto di standard già adottati dall'organizzazione (ad esempio ISO 9001)
- applicando buone pratiche finalizzate alla tutela di altri asset, quali ad esempio il knowhow aziendale o più in generale alla tutela degli asset aziendali tangibili e intangibili.

Fra gli altri, un approccio di questo tipo si presta particolarmente bene per produrre linee guida per settori specifici.

Dove e come intervenire

Le possibili aree di intervento e le loro principali caratteristiche sono:

1 - Informazioni

La conformità al GDPR e la possibilità di dimostrarla si basa sulla disponibilità di informazioni aggiornate, complete, facilmente interpretabili e raggiungibili.

2 - Principi e politiche

Costituiscono il principale veicolo per affermare e comunicare gli indirizzi, le scelte e le istruzioni aziendali a chiunque operi nel contesto dell'organizzazione.

3 - Processi e procedure

Un PROCESSO è costituito da un insieme di PROCEDURE che, partendo da opportuni input, genera risultati concreti (documenti, reports o servizi, risposte a richieste degli interessati…).

L'individuazione dei processi implica una chiara, preventiva (e dimostrabile) assegnazione dei RUOLI e delle RESPONSABILITÀ (RACI).

BIO

Maria Roberta Perugini - Avvocato, partner di Jacobacci& Associati, Studio legale con base internazionale attivo nell'IP, di cui dirige la divisione data protection. Ha maturato una particolare ed approfondita esperienza in materia di tutela della privacy, settore nel quale opera sin dal 1995 fornendo ad imprese e gruppi anche multinazionali, attivi nei più svariati settori di mercato, consulenza sia per la compliance sia per lo sviluppo di progetti speciali in questa materia, correntemente integrata dall'assistenza sui connessi profili contrattuali e più prettamente civilistici.
Partecipa come relatrice a convegni in materia di protezione dei dati personali ed organizza eventi e seminari volti a consolidare ed ampliare la conoscenza e consapevolezza da parte del mercato delle problematiche di data protection, nonché workshop di formazione ed aggiornamento presso imprese e associazioni di categoria. Redige e divulga note di aggiornamento e riflessione su problematiche attuali di data protection e contribuisce a europrivacy.info

1 Tratto da: GDPR: Nuova privacy La conformità su misuraG.Butti. A. Piamonte ITER (www.iter.it/gdpr)

Fig. 2 *– Uno stralcio del modello*

Ne possono venire misurate (e dimostrate) le prestazioni (capability-maturity), ad esempio attraverso l'uso di KEY INDICATOR di processo (in genere leadindicators) o di risultato (lagindicators)

4 - Ruoli e strutture organizzative

Soggetti ed unità organizzative interne od esterne all'azienda operano con preciso mandato che identifica compiti, responsabilità e potere decisionale.

5 - Servizi/applicazioni e infrastrutture

Strumenti, spesso informatizzati, che nell'ambito di specifici processi sono in grado di fornire opportune funzionalità (pseudonimizzazione, accesso diretto ai dati, gestione registro dati, elaborazioni e reportistica...).

6 - Persone, abilità e competenza

Disponibili all'interno o all'esterno dell'azienda e in possesso dei requisiti per ricoprire i ruoli previsti.

Raggruppare gli interventi secondo una sequenza naturale

La moderna *governance* suggerisce di strutturare gli interventi secondo il loro naturale "ciclo di vita": considerando la correlazione che esiste tra di loro ed evidenziando quali obiettivi vanno raggiunti prima di passare alla fase successiva.

Le funzioni del Piano di implementazione

Gli interventi individuati possono venire organizzati secondo una sequenza logica: ogni attività è chiaramente correlata ad un obiettivo (il "perché") da raggiungere, ed in questi termini va interpretata.

1 - Identificare: Funzione legata alla comprensione del contesto nel quale si opera: i dati personali, le risorse utilizzate ed i trattamenti critici per il business ed i rischi derivanti per i diritti e le libertà delle persone fisiche. Non vanno trascurati coloro che, al di fuori della nostra organizzazione, vengono in qualche modo in contatto con i dati personali che noi trattiamo e di cui siamo responsabili.

Tale comprensione permette di definire risorse ed investimenti in linea con la strategia di gestione dei rischi di non conformità e con gli obiettivi aziendali.

2 - Proteggere: Questa funzione è associata all'implementazione delle misure fondamentali per la protezione dei dati personali. Tali misure vanno dalla dichiarazione dei principi che vogliamo seguire, all'assegnazione delle responsabilità, all'integrazione con altre funzioni aziendali che già esistono (sicurezza informatica, sviluppo applicativo sicuro, formazione…), ampliandole, se necessario, per tenere conto dei requisiti del GDPR. Va infine considerata l'adozione delle tecnologie specifiche per la protezione dei dati personali. Valutiamo anche i rischi e i potenziali impatti di incidenti ai quali i dati personali sono esposti.

3 - Rilevare e Monitorare: Sviluppare e attuare la capacità di identificare:

- il verificarsi di un evento che impatti sulla sicurezza informatica. Probabilmente anche in questo caso non dovremo partire da zero, ma piuttosto integrare i protocolli di gestione incidenti e i corsi di formazione con gli opportuni riferimenti alla protezione dei dati personali
- le modifiche che coinvolgano:
  - trattamenti (interessati, dati trattati…)
  - risorse informatiche
  - processi aziendali
  - ....

4 - Rispondere: Dobbiamo anche essere preparati e pronti ad intervenire. Quando? Innanzi tutto se un interessato vuole far valere un proprio diritto, quale ad esempio la portabilità dei dati che lo riguardano. Considerando le potenziali conseguenze, la tempestività non è opzionale! Naturalmente tutto questo andrà fatto seguendo precisi protocolli che evitino, ad esempio, di ledere i diritti di altri. Se poi capita un incidente, una perdita di dati, dovremo essere preparati e rispondere in modo tempestivo e corretto, seguendo protocolli definiti e condivisi. Si deve inoltre essere in grado di rispondere ad una richiesta di un'Autorità di controllo, RENDICONTANDO quanto messo in atto per il rispetto della normativa.

5 - Ripristinare (Recover): La Funzione è associata alla definizione e attuazione dei piani per il ripristino dei processi che trattano dati personali. Tale funzione va quindi integrata con quelle di Business Continuity e Disaster Recovery che garantiscono la resilienza dei sistemi e delle infrastrutture e, in caso di incidente, consentono il recupero tempestivo delle business operations.

L'attività di ripristino deve tuttavia essere considerata una eccezione, in quanto le organizzazioni devono aumentare la loro resilienza adottando soluzioni che garantiscano l'alta affidabilità dei propri sistemi informativi.

Conclusioni

Il framework illustrato si è rivelato efficace nella definizione di un piano operativo di intervento completo, che permette di coinvolgere e responsabilizzare da subito l'azienda – sia nella fase di implementazione delle misure di adeguamento al GDPR sia nella successiva fase di mantenimento nel continuo della piena conformità ai requisiti normativi, che acquisisce al riguardo una elevata autonomia operativa.

Le fasi operative dell'implementazione e del mantenimento

A. FORMAZIONE

Oggetto della formazione

1. Sintesi del GDPR. In particolare:
   a. confronto con D. Lgs. 196/03: da misure minime a *"risk based approach"*
   b. nuovi ruoli e responsabilità: *accountability e privacy by design e by default*
2. Individuazione e riutilizzo degli investimenti pregressi (certificazioni e accreditamenti acquisiti)
3. Proposta del modello informatizzato per la mappatura dei trattamenti di dati personali in essere

Obiettivi della formazione

Condurre l'impresa a:

1. effettuare correttamente la raccolta e la mappatura delle informazioni necessarie alla Gap Analysis
2. essere parte attiva nello sviluppo del piano di primo adeguamento al GDPR
3. gestire in autonomia l'implementazione nel continuo del GDPR.

Modalità della formazione

Attività di *workshop – in house –*: la formazione come guida per un corretto percorso di conformità.

B. GAP ANALYSIS

1. Mappare le singole *"accountabilities"* per poterne verificare sistematicamente l'applicazione nel contesto analizzato, definendo per ognuna:
   a. applicabilità ed importanza *(profiling)*
   b. grado di implementazione *(capability maturity)* attuale e desiderato (*Gap* individuale)
   c. dimostrabilità (riferimento a pratiche / politiche, standard adottati, certificazioni, sigilli, codici di condotta, ecc.)
   d. *ownership*
2. Strutturarle secondo una logica di tempi (sequenze: cosa fare prima, cosa dopo) e di aree di intervento (informazioni da raccogliere, procedure da definire, ruoli da assegnare ecc.)
3. Raggruppare gli scostamenti individuati (*Gap* individuali) con l'obiettivo di definire un piano di adeguamento complessivo (attività, tempi e responsabilità)

C. PIANO DI ADEGUAMENTO

Verificare, implementare e documentare le azioni pianificate al punto precedente

D. PIANO DI MANTENIMENTO

1. Definire un piano di mantenimento dei livelli di "capability / maturity" individuati (es. prevedendo audit, test, verifiche di variazioni legislative)
2. Definire un piano per la reportistica utile a dimostrare la conformità
3. Definire un piano di verifica periodica

Fig. 3 *- Obiettivi e Principi del GDPR*

Il principio base è quello della responsabilizzazione, in primo luogo, del titolare del trattamento (cioè l'impresa e chi la rappresenta), cui la legge chiede di garantire, ed essere in grado di dimostrare (accountability) che il trattamento è effettuato conformemente al GDPR, in un'ottica di privacy by design: quest'ultimo principio, alla base del GDPR, costituisce la premessa "culturale" per affrontare il relativo percorso di conformità. Per fare un esempio si è accountable, non di rispettare un limite di velocità, ma di ridurre gli incidenti stradali: why e non how.

Fig. 4 *- Gli strumenti per garantire la conformità*

Gli strumenti per garantire e dimostrare questa conformità possono essere i più diversi e non bastano adempimenti formali, ma il titolare oggi si deve assumere la responsabilità di scegliere autonomamente strumenti realmente efficaci per rispettare le norme, tarando queste scelte sulla propria concreta realtà aziendale.

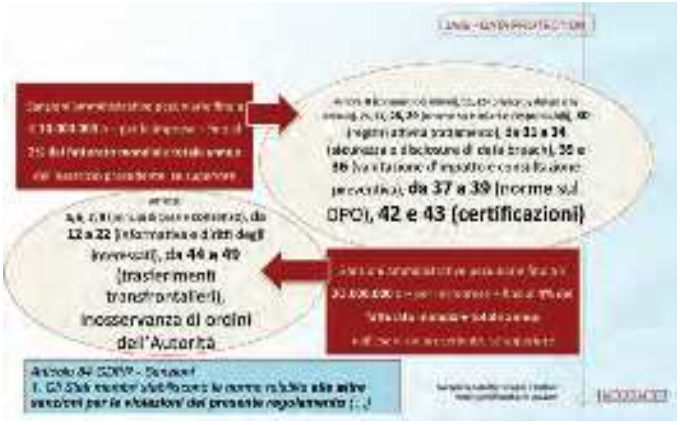


Fig. 5 *- Le sanzioni*

L'eventuale violazione del Regolamento causa l'attivazione di un impianto sanzionatorio estremamente rafforzato rispetto alla disciplina previgente, nell'ottica di applicare sanzioni che siano *"effettive, proporzionate e dissuasive"*: sono previste sanzioni amministrative pecuniarie articolate ed economicamente assai gravose (fino a 20 milioni di euro e al 4% del fatturato annuo di gruppo).

Fig. 6 *- Il risarcimento dei danni*

Un approccio diverso e maggiormente responsabilizzante riguarda anche la responsabilità risarcitoria nei confronti dell'interessato: il danno è risarcibile quando è provocato da un trattamento non conforme al Regolamento, ossia da eventi dannosi che sono dipesi da scelte di attuazione del Regolamento errate o negligenti per quanto riguarda il titolare e, quanto al responsabile, da violazione delle norme ad esso specificamente rivolte o da mancato adempimento delle istruzioni legittime del titolare.

A ciò si aggiunge la solidarietà della responsabilità risarcitoria tra tutti i soggetti cui sono imputabili il trattamento e la responsabilità del danno da esso causato, a garanzia dell'effettivo risarcimento dell'interessato. ■

GDPR: il *privacy impact assessment* come strumento fondamentale di data governance

Autore: **Giangiacomo Olivi**

La società dell'informazione mostra una sempre maggiore attitudine alla *digital disruption* (digitalizzazione dirompente) a fronte della quale la privacy degli individui viene spesso messa a rischio. Con l'introduzione del nuovo Regolamento europeo in materia di protezione dei dati personali ("GDPR") il legislatore europeo ha introdotto un quadro normativo incentrato su una serie di principi che segnano il passaggio da una concezione formale di mero adempimento ad un approccio sostanziale basato sulla tutela effettiva dei dati e degli interessati. Il GDPR mira ad anticipare la protezione e a responsabilizzare il titolare del trattamento per prevenire eventuali vulnerabilità. In questa ottica si inquadra il principio di *accountability*, in italiano "responsabilizzazione", già sviluppato nel corso della trentaduesima conferenza mondiale in tema di privacy svoltasi a Gerusalemme nel 2010. L'*accountability* implica, da un lato, l'adozione di misure tecniche e modelli organizzativi atti a garantire la corretta gestione e conservazione dei dati in maniera conforme ai principi di protezione dei dati personali elencati all'articolo 5 del GDPR e, dall'altro, la capacità di dimostrare la conformità a tali principi delle operazioni di trattamento effettivamente svolte. Una delle principali misure di attuazione del principio di *accountability* è la valutazione d'impatto del trattamento (*privacy impact assessment*, "PIA"), che consiste in una procedura interna volta a stimare la necessità, la proporzionalità e l'incidenza che una determinata operazione di trattamento può avere sulla privacy, al fine di adottare preventivamente le soluzioni opportune per mitigare o, ove possibile, eliminare tale impatto sui dati degli interessati. La valutazione di impatto privacy, unitamente ad altri adempimenti formali come la tenuta dei registri dei trattamenti sostituisce l'obbligo generale di notificare all'Autorità di controllo il trattamento dei dati personali.

I riferimenti espliciti al PIA a livello europeo che precedono l'emanazione del GDPR sono molteplici, tuttavia la centralità del tema e la complessità organizzativa e d'investimento che la valutazione d'impatto esige hanno reso necessario un intervento chiarificatore delle autorità competenti.

Il 4 aprile 2017 il WP29 ha adottato le Linee guida in materia di valutazione d'impatto sulla protezione dei dati personali *(Guidelines on Data Protection Impact Assessment)* per meglio esplicitare due questioni fondamentali: quando è necessario effettuare il PIA e come deve essere svolto. In linea con l'approccio basato sul rischio su cui si fonda il GDPR non tutte le operazioni di trattamento devono essere sottoposte a PIA, l'articolo 35 del GDPR prevede, infatti, che il titolare del trattamento debba effettuare una valutazione d'impatto prima di procedere al trattamento stesso ogniqualvolta il trattamento possa presentare un "rischio elevato per i diritti e le libertà delle persone fisiche". Il legislatore europeo ha scelto un approccio di ampio respiro che estende l'ambito di applicazione del PIA non solo alla protezione dei dati personali, ma anche ai più ampi "diritti fondamentali" degli interessati. Un trattamento di dati può quindi considerarsi "elevatamente rischioso" laddove sia suscettibile di cagionare un danno materiale, consistente nella violazione delle misure di sicurezza, ma anche in perdite finanziarie o altro danno economico, oppure immateriale, come il furto o usurpazione d'identità, un danno reputazionale, la perdita di riservatezza dei dati personali protetti da segreto professionale.

Per poter adeguatamente soppesare l'opportunità di condurre un PIA, deve tenersi conto della natura, dell'oggetto, del contesto e delle finalità del trattamento, considerando in particolar modo se per effettuare il trattamento vengono adottate nuove tecnologie la cui diffusione potrebbe

avere un impatto imprevedibile sia a livello personale che sociale e potrebbe incidere sulle modalità stesse di raccolta, trattamento e analisi dei dati.

Si pensi, ad esempio, al settore dell'Internet of Things, carro trainante dell'Industry 4.0, che si estende dalle tecnologie prettamente B2C come i gadget wearable che monitorano le nostre condizioni di salute alle applicazioni B2B, come i sensori che controllano le condizioni microclimatiche per massimizzare la capacità produttiva delle coltivazioni. Questo nuovo paradigma tecnologico così pervasivo ed onnipresente, progettato per rilevare e condividere dati senza soluzione di continuità, permette agli oggetti stessi di essere partecipi attivi dell'ecosistema economico-produttivo, interagendo sia con gli esseri umani, sia tra di loro in totale autonomia. In questo contesto i modelli basati su informativa e consenso sembrano cedere il passo a modelli che si fondano sempre più sulla progettazione e valutazione preventiva del trattamento, come il PIA.

© ENISA

Il GDPR individua alcune operazioni di trattamento che richiedono necessariamente lo svolgimento di un PIA (ma la lista non è esaustiva, lasciando spazio all'integrazione da parte dei Garanti europei). La valutazione è richiesta nello specifico per i trattamenti che comportano: l'elaborazione su larga scala di categorie particolari di dati (dati sensibili/genetici/biometrici) o di dati personali relativi a condanne penali e reati; il monitoraggio sistematico di una zona accessibile al pubblico su larga scala; la valutazione sistematica e globale degli aspetti personali relativi a persone fisiche che si basa su un trattamento automatizzato, tra cui profilazione, e su cui si basano le decisioni che producono effetti giuridici riguardanti la persona fisica o che influenzano significativamente la persona fisica.

Quanto alle modalità di svolgimento la valutazione va condotta prima del trattamento per soppesare la particolare probabilità e gravità del rischio, ma trova applicazione durante tutto il ciclo vitale del prodotto/servizio, dovendo essere aggiornata in seguito ad eventuali modifiche o integrazioni, onde mantenere costante il livello di protezione dei dati. Il titolare del trattamento nello svolgimento del PIA deve consultarsi con il Data Protection Officer eventualmente designato, il quale deve inoltre costantemente monitorare il rendimento del PIA come previsto dalle Linee Guida sul DPO emanate dal WP29.

Il GDPR, ispirato al criterio di neutralità procedurale e tecnologica, individua solo alcuni requisiti fondamentali (articolo 35 (7), e considerando 84 e 90) prevedendo che siano obbligatoriamente inclusi: una descrizione delle operazioni di trattamento previste e degli scopi del trattamento; una valutazione della necessità e della proporzionalità del trattamento; una valutazione dei rischi per i diritti e le libertà delle persone; le misure previste per affrontare i rischi e dimostrare la conformità al GDPR. Nelle Linee Guida sul PIA il gruppo dei Garanti europei ha ulteriormente specificato delle buone prassi da adottare relative ad esempio alla raccolta delle opinioni degli interessati o dei loro rappresentanti sul trattamento previsto o all'adozione di policy interne e codici di condotta.

BIO

L'avv. Giangiacomo Olivi è il Partner co-responsabile del dipartimento Intellectual Property & Technology che comprende i gruppi di IP, TMT, Data Protection e Commercial. Ricopre inoltre il ruolo di Global Co-Chair del gruppo internazionale Retail. Lavora presso l'ufficio di Milano.
Ha maturato una vasta esperienza nei settori delle tecnologie, media e telecomunicazioni, e in relazione alla protezione dei dati personali, assistendo in ambito strategico e commerciale numerosi clienti nazionali e internazionali.
Dal 2006 viene riconosciuto quale miglior avvocato italiano nel settore TMT dalle più prestigiose guide internazionali, incluse Chambers Europe e The Legal 500 EMEA. È tra gli avvocati italiani più premiati, essendogli stato spesso attribuito il premio avvocato dell'anno TMT, Media e IT da varie riviste o organizzazioni.
L'avv. Olivi è docente di cyber security e data protection, oltre che di tecnologie e servizi di media presso l'Università di Milano e partecipa in qualità di relatore a numerosi seminari organizzati da università e gruppi editoriali. Con il suo gruppo, gestisce un blog su tematiche legali legate al settore IPT. http://blogs.dlapiper.com/iptitaly/ e in collaborazione con Il Corriere della Sera, L'Ora Legale - oralegale.corriere.it/ (blog in italiano).

Il GDPR, lascia quindi ai titolari del trattamento un margine di flessibilità nel determinare la struttura del PIA, cosicché questo possa adattarsi ai processi aziendali e alle pratiche di lavoro esistenti. Per essere realmente efficace, il PIA deve infatti essere calato nella realtà dei processi aziendali, ad esempio, con l'individuazione di punti di contatto con procedure esistenti, dalle procedure di management, gestione del rischio e certificazione, sino ai processi *"agile"* di sviluppo software che potrebbero già coordinarsi con alcune fasi del PIA. Tutto questo dovrà avvenire nel modo più semplice ed immediato possibile, ad esempio impostando nel PIA domande che siano di immediata comprensione per tutti i livelli aziendali e prevedendo solo ove necessario più ampi livelli di approfondimento e coinvolgimento. Solo così il PIA potrà costituire non solo un sistema efficace per ridurre significativamente i rischi, e con essi anche eventuali riflessi economici negativi, ma anche, se adeguatamente comunicato, uno strumento di differenziazione da concorrenti meno attenti, stimolando la fiducia di clienti e interessati. ■

Data Breach Notification: dal codice privacy al nuovo regolamento europeo

Autore: Michele Gallante

BIO

Michele è un Security Consultant di Alfa Group, società di Sicurezza Informatica e Consulenza Integrata. Laureato in Giurisprudenza presso l'Università degli Studi Roma Tre, ha svolto la ricerca tesi con titolo "Dilemmi giuridici sull'utilizzo dei Droni nei Conflitti Armati" alla University of Washington, School of Law, Seattle, US. Dopo gli studi ha svolto la pratica forense ed ottenuto un Master in "Homeland Security" presso l'Università Campus Bio-Medico di Roma, dove ha approfondito argomenti riguardanti la Security, Data Protection e Risk Management. Ha svolto attività di ricerca presso la fondazione Global Cyber Security Center di Poste Italiane in merito a problematiche giuridiche riguardanti la sicurezza informatica. Attualmente è membro e collabora con alcune importanti associazioni tra cui l'Oracle Community for Security, Federprivacy e Croce Rossa Italiana per la divulgazione di argomenti di sicurezza, protezione dei dati e diritto internazionale umanitario.

Il progressivo sviluppo tecnologico ha costretto il legislatore ad adeguarsi alle richieste degli utenti, desiderosi e bisognosi di tenere al sicuro i propri dati personali, disciplinando nel modo più opportuno la complessa materia riguardante la privacy e la protezione dei dati personali.

Non che ci fosse un vero e proprio vuoto normativo in materia. Infatti, sin dall'epoca romana era riconosciuto il diritto di escludere gli altri dal godimento di un bene di proprietà; si trattava dello *"ius excludendi alios"*, la cui *ratio* era proprio quella di difendere la proprietà privata. Con il passare del tempo, il termine anglosassone "privacy", che si può banalmente tradurre in "isolamento", ha cambiato la sua accezione originaria, ampliando sempre più gli ambiti di applicazione. In epoca moderna, i primi a scrivere e parlare di questo diritto sono stati il giudice americano Louis Brandeis e l'avvocato Samuel Warren, che definirono la privacy come "diritto di essere lasciati in pace". Questo diritto, che ha assunto sempre più importanza, è stato riconosciuto come **diritto fondamentale** dalla Carta dei Diritti Fondamentali dell'Unione Europea.

L'innovazione culturale e tecnologica, se da un lato ha portato a un'eccezionale interconnessione mondiale, dall'altro ha generato un'incontrollata diffusione dei dati e delle informazioni nella falsa speranza di una fantomatica sicurezza assicurata dagli strumenti tecnologici. Come ricordato da Bruce Schneier, crittografo e saggista statunitense: *"If you think technology can solve your security problems, then you don't understand the problems and you don't understand the technology"*. Infatti, ogni strumento elettronico presenta delle vulnerabilità sistemiche capaci di permettere una violazione della macchina, capace di compromettere dati e informazioni.

Il legislatore italiano si è adattato pian piano alle prescrizioni europee sulla protezione dei dati personali in generale e agli obblighi previsti per quanto riguarda la specifica previsione della notifica di un data breach. Originariamente il Codice privacy del 2003 non conteneva una definizione di violazione dei dati personali, introdotta solo successivamente al recepimento delle direttive europee 2002/58/CE (c.d. Direttiva e-Privacy) e 2009/136/CE, tramite il Decreto legislativo 28 maggio 2012 n. 69, con il quale il Governo ha dato attuazione alla delega prevista nell'art 9 della legge comunitaria del 2010 (legge 15 dicembre 2011, n. 217, pubblicata in G.U. 2 gennaio 2012, n. 1).

Con il suddetto decreto è stata così introdotta la definizione di **violazione dei dati personali**, che viene intesa come la "violazione della sicurezza che comporta anche accidentalmente la distruzione, la perdita, la modifica, la rivelazione non autorizzata o l'accesso ai dati personali trasmessi,

memorizzati o comunque elaborati nel contesto della fornitura di un servizio di comunicazione accessibile al pubblico" (art. 4, comma 3, lett. g-bis, del Codice).

Un'altra importante modifica al Codice è stata fatta con l'introduzione dell'articolo 32-bis recante "Adempimenti conseguenti ad una violazione di dati personali". L'obbligo di comunicare senza indebito ritardo la violazione al Garante è stato però inizialmente circoscritto al caso del fornitore di servizi di comunicazione elettronica, e non a tutti i titolari che trattino dati personali. Per quanto riguarda le sanzioni perviste per l'omessa o ritardata comunicazione della violazione di dati personali al Garante, è punita con una sanzione amministrativa da 25.000 a 150.000 euro; e, l'omessa o ritardata comunicazione della violazione al contraente o ad altra persona, è punita con la sanzione amministrativa da 150 a 1.000 euro per ciascun contraente o altra persona interessata.

L'importanza della materia consiste nel fatto che un evento che coinvolga dati personali, se non trattato in modo adeguato e tempestivo, può provocare un grave danno economico e sociale al contraente, tra cui l'usurpazione di identità.

L'evoluzione tecnologica intercorsa dopo tutti questi vari accorgimenti normativi, pensati per rendere alcuni ambiti più sicuri e proteggere i diritti degli interessati, ha reso necessario un ampliamento delle previsioni legislative, vuoi perché inizialmente circoscritta ad alcuni settori, vuoi perché le organizzazioni rimanevano spesso noncuranti dell'obbligo di comunicazione imposto.

Il Garante, per disciplinare la materia in modo più appropriato, ha adottato nel 2013 un provvedimento che fissa gli adempimenti per i casi in cui dovessero verificarsi i c.d. data breach, specificatamente nel campo delle comunicazioni elettroniche. Successivamente, nel 2014, ha emanato un altro provvedimento prescrittivo in tema di biometria, e, nel 2015, altri due riguardanti il Dossier Sanitario elettronico e le misure di sicurezza e modalità di scambio dei dati personali tra Amministrazioni Pubbliche.

Il 25 maggio 2018 diventerà definitivamente vincolante il **Regolamento Europeo UE 2016/679** (GDPR, General Data Protection Regulation) relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati, che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati). Il Regolamento, al pari di altre previsioni normative di futura emanazione o già vincolanti (PSD2, eIDAS, NIS, Circolare 285 di Banca d'Italia…), pongono degli obblighi da seguire in tema di notifica di violazione dei dati. È quindi nel pieno interesse delle aziende prevenire violazioni o incidenti di sicurezza, onde evitare di doversi esporre ad una notifica pubblica che avrebbe importanti ripercussioni anche in termini di reputazione e immagine.

Lo scopo del regolamento è quello di evitare l'insorgenza o l'aggravamento alla perdita di controllo dei dati personali, o semplicemente di una loro limitazione capace di comportare l'usurpazione di identità, perdite finanziarie o pregiudizio alla reputazione e perdita di riservatezza, estendendo la l'obbligo di notifica a tutti i titolari di trattamento dati personali. La determinazione di specifiche tempistiche per la comunicazione dell'evento pregiudizievole, permetterà di ridurre gli effetti negativi derivanti dal fatto, aumentando la resilienza in seguito ad eventi imprevisti.

Come prescritto dagli articoli 33 e 34 del regolamento, non appena il titolare viene a conoscenza dell'avvenuta violazione dei dati personali trattati, deve **notificare** l'accaduto all'Autorità di controllo competente, **senza ingiustificato ritardo**, e se possibile, **entro 72 ore**. In caso di rischio elevato per i diritti e le libertà della persona, sarà comunicato anche all'interessato, al fine di permettergli di prendere le adeguate precauzioni. L'obbligo non scatta nel caso in cui il Titolare del trattamento sia in grado di dimostrare di aver messo in atto le misure tecniche e organizzative adeguate alla protezione dei dati, ad esempio in modo da rendere i dati personali incomprensibili a chiunque non sia autorizzato (es. cifratura, pseudonimizzazione dei dati).

La notifica dovrà necessariamente contenere:

- Una descrizione della natura della violazione dei dati personali compresi, ove possibile, le categorie e il numero approssimativo di interessati in questione nonché le categorie e il numero approssimativo di registrazioni dei dati personali in questione;
- Il nome e i dati di contatto del responsabile della protezione dei dati o di altro punto di contatto presso cui ottenere più informazioni;
- Una descrizione delle probabili conseguenze della violazione dei dati personali;
- Una descrizione delle misure adottate o di cui si propone l'adozione da parte del titolare del trattamento per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuare possibili effetti negativi.

Le **sanzioni** in violazione degli obblighi derivanti dalle presenti previsioni comporta sanzioni amministrative pecuniarie fino a 10.000.000,00 EUR o per le imprese fino al 2% del fatturato mondiale totale annuo dell'esercizio precedente, se superiore.

Per questo servono tecnologie che ci aiutino a prevenire a monte l'evento pregiudizievole che potrebbe causare nocumento all'interessato e all'organizzazione. Ogni struttura dovrà valutare, attraverso un'attenta analisi del rischio che permetta di allocare le risorse nel modo più adeguato possibile, l'adozione di strumenti capaci di identificare, analizzare, proteggere e rispondere alle minacce (Access Control, Data Loss Prevention, Cyber Threat Intelligence, Vulnerability & Risk Management, Continuous Security Monitoring, Data Governance, etc…).

L'affidabilità delle società alle quali affidiamo i nostri dati, e la cura con cui si adopereranno per trattarli in maniera *compliance,* sarà determinante nella scelta a cui affidarsi. Un corretto sistema di gestione della privacy, unitamente a un'adeguata sicurezza infrastrutturale, garantirà la difesa di questo diritto fondamentale, senza cascare in artifici o raggiri di coloro che millantano protezione e sicurezza senza però adottare le opportune previsioni normative.

"Chi è pronto a dar via le proprie libertà fondamentali per comprarsi briciole di temporanea sicurezza, non merita né la libertà né la sicurezza" Benjamin Franklin. ■

Sicurezza e Privacy dell'Internet of Things

Autore : Gianluca Bocci

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.

Dal rapporto McKinsey Global Institute del 2013, si evinceche diverse tecnologie, alcune già note ed affermate sul mercato, altre meno, saranno *"disruptive"* nei prossimi anni e modificheranno profondamente il nostro stile di vita, i mercati e l'economia globale. Tra queste tecnologie troviamo quelle mobili, l'Intelligenza artificiale, i big data, la roboticaavanzata, l'internetof things (IoT) e molte altre. Tecnologie che, utilizzate singolarmente o combinate tra loro, consentiranno di concepirenuovi modelli di business e servizi innovativi in moltissimi settori merceologici.In tutto questo c'è però il c.d. rovescio della medaglia, ossia nuove tipologie di rischi che, già da subito, ci obbliganoa riflettere sugli aspetti di sicurezza eprivacy. In questo articolo, secondo le direttrici di analisi appena accennate, sarà fatto un approfondimento dell'IoTcome fenomeno di convergenza tra il mondo virtuale basato sulla rete Internet e quello deglioggetti fisici "intelligenti" che, interagendo con il mondo esterno,generano, trasmettono e ricevono datiche, analizzati,consentiranno di crearevalore aggiuntoa supporto dei processi decisionali.Secondo la visione di Goldman Sach i dispositivi IoT sono caratterizzati da una serie di attributi che trovano la loro sintesi nell'acronimo *S-E-N-S-E*[1] *- Sensing, Efficient, Networked, Specialized e Everywhere,* ossia:

- *"Sensing"* che fa riferimento all'applicazione di sensori (ad es. di pressione, di temperatura, etc.) su ogni *"cosa"*, con la conseguente capacità di generare grandi quantità di dati;
- *"Efficient"* che fa riferimento all'attitudine di dotaredi "intelligenza" ed "efficienza" i processi, sfruttando proprio le informazioni raccolte e analizzate;
- *"Networked"* che fa riferimento agli oggetti che sono comunque e sempre connessi alla rete Internet;

- *"Specialized"* che fa riferimento alla specificità degli oggetti IoT e, ancor di più, alle soluzioni realizzate in maniera del tutto "verticale" a differenza di quanto avviene nell'IT tradizionale. Infatti difficilmente possono essere applicate logiche di "reusability" da un progetto o una soluzione IoT concepita per un ambiente Healtcare ad un ambiente industriale;
- *"Everywhere"* che fa riferimento alla pervasività che tali oggetti hanno ed avranno sempre di più nella vita di tutti noi e nei processi aziendali.

Secondo l'Osservatorio Internet of Things del Politecnico di Milano[3] il numero di dispositivi intelligenti connessi alla rete nel 2020, sarà dell'ordine dei 25 miliardi; una convergenza, che trasforma radicalmente il modello di comunicazione globale, dove i dati e le informazioni non sono più un prodotto delle sole persone ma anche delle "cose". Nel settore bancario, per i pagamenti saranno sempre più utilizzati dispositivi *"wearable"* come ad esempio gli orologi; anche il settore assicurativo farà largo uso di queste tecnologie che consentiranno di verificare lo stile di guida dei propri Clienti per proporre polizze assicurative personalizzate; sempre il ramo assicurativo potrà ottenere altri benefici dall'IoT, associando alla polizza assicurativa della

casa o del palazzo, dispositivi capaci di proteggere l'ambiente e le persone (Smart Home& Smart Building). A livello metropolitano l'IoT potrebbe consentire una gestione ottimale del traffico, ad esempio regolando la segnaletica semaforica in base ai dati forniti dalletelecamere, anticipando ai conducenti le alternative possibili alle vie più congestionate verso le quali stanno andando incontro (Smart City). Proprio il settore automobilistico è uno di quelli più in fermento, con applicazioni dedicate al comfort, alla sicurezzaeall'infotainment (Smart Car). Di esempi di questo tipo se ne potrebbero fare tanti altri e per diversi settori merceologici nei quali l'IoT staormai diventando sempre di più una realtà (eHealth, Smart Factory, Smart Agricolture, Smart Asset Management, Smart Logistic, Smart Metering & Smart Grid, etc.). Fatte questeconsiderazioni,è evidente come la sostenibilità dei nuovi modelli di business e dei servizi innovativi che sfruttano l'IoT è legata all'esito di alcune importanti sfide che dovranno essere affrontate, come quella della sicurezza e della privacy.

Sicurezza IoT

La dimensione del fenomeno IoT offre una superficie di attacco immensa per chi vuole servirsene per condurre attività illecite nel dominio cibernetico, indipendentemente dalle finalità. La previsione di TrendMicro[3],

già per il 2017, non è certo confortante; si aspettano infatti malware analoghi a quello Mirai che, utilizzati per compremettere dispositivi IoT, consentiranno attacchi DDoS di centinaia e centinaia di Gbps, simili a quelli avvenuti nell'ultimo trimestre del 2016. Dello stesso avviso è CheckPoint[4], sostenendo che molti attacchi sfrutteranno dispostivi IoT ed interesseranno sempre di più gli ambienti industriali. Interessante è quanto emerge dal report sulle minacce di McAfee Labs[5] in cui si afferma che nuove tecniche di compromissione dei dispositivi IoT sfrutteranno l'inserimento di codice malevolo direttamente nel firmware, così da renderne molto più difficile l'individuazione. Sempre McAfee fa notare come queste tecniche permetteranno ai malware di godere di eccezionali privilegi, agendo senza limiti anche in virtù del fatto che nel kernel i controlli di sicurezza sono minimali.Spesso i dispositivi IoT vengono compromessi sfruttando la console di amministrazione web del dispositivo, ad esempio protetta da password di default, oppure attraverso una connessione SSH non protetta, per essere utilizzati come proxy e consentire in una fase successiva di sferrare il vero e proprio attacco verso il sistema target d'interesse. Questi problemi di sicurezza in generale dipendono però dall'insieme articolato dei diversi operatori che concorrono alla filiera del servizio IoT e da molteplici fattori riconducibili all'organizzazione, ai processi, alle tecnologie e agli aspetti culturali delle risorse coinvolte. Tra gli operatori, *"in primis"* troviamo i produttori dei dispositivi intelligenti, a seguire i fornitori dei servizi che quasi sempre coinvolgono installatori e società di integrazione di sistemi hardware e softwarenecessari per realizzare il servizio stesso ed infine tutte le diverse tipologie di utenti che li utilizzano. I produttori di dispositivi tipicamente si preoccupano di realizzare questi oggetti con nuove funzionalità e a basso costo; spesso utilizzano sistemi operativi "embedded", con una capacità computazionale limitata che ne pregiudica l'aggiornamento e\o il patching, adottano sistemi di autenticazione e autorizzazione insufficienti e forniscono limitate capacità di configurazione. C'è poi il problema dell'interoperabilità di questi dispositivi

che, estremamente eterogenei tra loro, utilizzano spesso protocolli di comunicazione diversi. Molti dei problemi citati dovrebbero essere indirizzati oltre che dai produttori, anche da parte delle grandi organizzazioni che, proponendosi come fornitori di servizi, dovrebbero creare una sana pressione nei confronti di chi realizza dispositivi IoT affinchè gli aspetti di sicurezza e di privacy, vengano tenuti in debita considerazione; ad esempio attraverso la scelta di produttori, installatori e integratori di sistema che, altamente qualificati, rispondono a determinati requisiti per garantire la sicurezza e la privacy, la pubblicazione di bandi di gara e la predisposizione di contrattualistica che tende ad escludere coloro che non sono in linea con queste caratteristiche.I fornitori di servizi dovrebbero inoltre affrontare i progetti IoT secondo un approccio di tipo risk-based per essere sin dall'inizio consapevole di quali accorgimenti (a livello organizzativo, di processo e tecnologico)devonoporre in essere per erogare un servizio sicuro. Per tale ragione anche nei confronti dell'infrastruttura IT (componente di back-end) va postala massima attenzione, sia per

garantirne la sicurezza, ma anche la sostenibilità del servizio stesso. Per queste ragioni, il fornitore di servizi IoT dovrebbe attuare sistematicamente, sin dall'inizio, per il rilascio del sistema in produzione, ma anche nelle fasi successive e periodicamente, un vero e proprio programma di sicurezza che include il monitoraggio dei sistemi, l'attuazione di vulnerability assessment e penetration test, inclusa l'interfaccia utilizzata per interagire con gli oggetti intelligenti che spesso sfrutta tecnologie mobili ed in particolare smartphone e\o tablet, etc... Se pur accennato, si desidera enfatizzare come il successo dell'IoT e dei relativi servizi, dipenderà anche da altri fattori; in particolare dall'adeguamento del modello operativo attraverso una trasformazione dell'IT che potrebbe richiedere l'uso di hardware dedicati, software evoluti per l'analisi e la correlazione di grandi quantità di dati, tecnologie di storage e di rete, il tutto senza vincoli e limiti di scalabilità.La sicurezza IoT passa anche per gli utentifinali che, resi più consapevoli, potranno giocare un ruolo attivo nello sviluppo di questa tecnologia, ad esempio attraverso campagne di sensibilizzazione oppure somministrando agli addetti ai lavori specifici programmi di formazione. Infatti, spesso chi utilizza dispositivi IoT non esegue, anche se possibile, quelle configurazioni minimali come il cambio della password di defaulto l'installazione di protezioni per i dispositivi mobili utilizzati per interagire e scambiare dati con gli oggetti intelligenti, come

ad esempio gli antivirus e i firewall locali; addirittura ci sono utenti che, per diverse ragioni, attuano tecniche di rooting o jailbreaking sui propri smartphone e tablet, ignorando completamente che, tali azioni,alterano e compromettono gli schemi di sicurezza predisposti dalla fabbrica, espongono a gravi rischi i datitrattati e possono rendere vulnerabile, a loro insaputa, l'oggetto intelligente che può essere controllato da remoto. Al riguardo si evidenzia come i dispostivi mobili e più in generale il paradigma del Mobile Internet, costituisce un driver tecnologico dell'IoT dal momento che permette a a chiunque, uomini e oggetti, di essere sempre connessi e scambiare informazioni con le applicazioni sviluppate.

Privacy IoT

L'IoT pone grandi problemi per gli aspetti di privacy, molto di più di quelli causati dall'IT tradizionale. Se pur non in maniera esaustiva ne citiamo qualcuno:

- non sempre gli utenti si rendono conto che hanno a che fare con dispositivi capaci d'interagire con la rete e con questa scambiare dati che possono rientrare nella sfera personale
- non sempre, anzi quasi mai, hanno il controllo del flusso dei dati; in altre parole non si rendono neanche conto se vengono attivate delle connessioni, verso chi e quali sono i dati trasmessi;
- spesso c'è una totale mancanza di trasparenza tra i dati grezzi raccolti dal dispositivo, successivamente inviati a soggetti terzi, e quelli eventualmente mostrati all'utente;

▸ questi dispositivi, con l'obiettivo di garantire una maggiore autonomia per le batterie, evitano di utilizzare qualunque sistema di cifratura per la trasmissione dei dati

▸ le informazioni raccolte da un dispositivo, anche se sono anonimizzate, potrebbero combinarsi con informazioni prodotte da altri dispositivi, consentendol'identificazione del soggetto.

Tutto questo si traduce nel rischio di divulgare dati personali, se non addirittura sensibili ed in maniera del tutto inconsapevole per l'utente. Un problema di ampia portata che, se è iniziato con l'uso dei dispositivi wearable, tenderà a crescere via via che nel tempo l'IoT sarà utilizzato nei tanti settori già citati all'inizio dell'articolo; per fare un esempio basti pensare alle Smart City e alla grande mole d'informazioni che, raccolte dalle videocamere, potranno essere analizzate con tecniche che consentono di determinare le abitudini e gli stili di vita delle persone. Le risultanze dell'analisi potrebbero mettere in evidenza che la probabilità d'incidente

per chi passa in una determianta zona è molto piu' alta e, avendo acquisito le targhe e i relativi percorsi fatti nel tempo, si potrebbero creare dei profili da riutilizzare a beneficio delle compagnie assicurative all'atto della stipula della polizza auto. Volendo fare altri esempi, potremmo riferirci a tutti quei dispositivi che consentono di raccogliere informazioni sul nostro stato di salute e\o sulle nostre prestazioni sportive, informazioni che in un modo o nell'altro potrebbero far gola sia alle compagnie assicurative, sia alle case farmaceutiche. Senza dilungarci con altri esempi, possiamo affermare ancora una volta che la privacy si pone come una grande sfida per l'IoT.Al riguardo se già precedentemente abbiamo avuto modo di fare alcune considerazioni su come le aziende fornitrici di servizi basati sull'IoT dovrebbero agire per ridurre questo specifico rischio, ricordiamo che in aiuto ci viene anche il nuovo Regolamento UE 2016/679 sulla protezione dei dati personali. Un regolamento con il quale la Commissione Europea intende rafforzare e unificare la protezione dei dati personali entro i confini dell'Unione Europea attraverso una semplificazione e armonizzazione delle diverse leggi Europee adottate dagli Stati Membri e prodotte ai sensi della precedente Direttiva (95/46/CE) che sarà abrogata a partire dal 25 Maggio 2018. Grazie a questo nuovo regolamento, anche i produttori di dispositivi IoT dovranno adeguarsi alle nuove indicazioni previste per la tutela dei dati personali, così da non incorrere nelle sanzioni previste a livello amministrativo. Tra le indicazioni più importanti troviamo:

▸ l'obbligo di analizzare il trattamento durante l'intero ciclo di vita dei dati personali, dalla raccolta alla cancellazione, partendo dalla fase della progettazione e adottando misure di carattere tecnico ed organizzativo come la minimizzazione e la pseudonimizzazione, il tutto secondo il c.d. Principio della Privacy by Design;

▸ l'obbligo di adottare impostazioni predefinite e configurazioni di default dei sistemi informatici per garantire la tutela dei dati personali con la possibilità di effettuare eventuali modificheda parte dell'utente solo manualmente ed in una fase successiva rispetto al momento in cui il prodotto viene rilasciato, il tutto secondo il c.d. Principio della Privacy by Default;

▸ la valutazione dell'impatto sulla privacy perdeterminare la necessità e la proporzionalità del trattamento dei dati personali oltre ai rischi per i diritti e le libertà delle persone fisiche che consentiranno d'individuare, già a partire dalla fase di progettazione, le più adeguate misure di sicurezza da adottare per ridurli a valori accettabili.

Possiamo concludere ritenendo che l'azione congiunta del nuovo Regolamento europeo e le pressioni che possono arrivare in diverse forme da parte delle grandi organizzazioni che intendono sviluppare il proprio business con le tecnologie IoT, favoriranno la regolamentazione di questo specifico settore ritenuto strategico per l'economia dell'intero pianeta. ■

1 http://www.goldmansachs.com/our-thinking/outlook/internet-of-things/iot-report.pdf
2 https://www.osservatori.net/it_it/osservatori/osservatori/internet-of-things
3 http://www.trendmicro.it/informazioni-sulla-sicurezza/ricerca/previsioni-sulla-sicurezza-2017/index.html
4 http://www.adnkronos.com/magazine/cybernews/2016/11/17/cloud-mobile-infrastrutture-iot-ecco-gli-obiettivi-degli-hacker-nel_EBLpk0qO1reGNq3Z3X1TXO.html?refresh_ce
5 https://www.mcafee.com/it/resources/reports/rp-quarterly-threats-jun-2017.pdf

Sfide etiche e giuridiche delle città connesse

Autore: Pascal Verniory

Pascal Verniory si esprime in questa sede a titolo personale. Le sue opinioni non pretendono riflettere quelle del suo datore di lavoro.

Introduzione

Le città connesse che alcuni definiscono "intelligenti" *(Smart Cities)* fanno parlare molto. La governance delle megalopoli diventa un tema a forte impatto sociale in un'epoca in cui ci si predice una demografia planetaria esplosiva, essenzialmente cittadina, e quindi una fonte di caos se non correttamente gestita. Ma, come tutto ciò che riguarda l' "intelligenza" artificiale, le città connesse nutrono i fantasmi più ingenui e aguzzano gli appetiti più vivaci, in un clima fortemente ostile a ogni riesame della questione. Il fatto è che queste città "intelligenti" fanno nascere delle speranze smisurate di ordine e di confort ai quali è difficile rinunciare quando se ne ignora il prezzo reale. È allora tanto più urgente interrogarsi sui loro apporti reali al fine di trarre il migliore beneficio senza dimenticare per altro la vigilanza che si rende necessaria per fronteggiare i pericoli connessi, salvo rinunciare ad alcune delle loro promesse, troppo costose in termini di vita privata e di libertà.

Le linee che seguiranno mi permettono di ritornare sulla presentazione fatta il 3 novembre 2016 a Yverdon, nel quadro della *CyberSec Conference* e di affrontare alcuni aspetti rimasti indiscussi.

BIO

Pascal Verniory è avvocato iscritto all'albo, dottore in filosofia, titolare di un brevetto di avvocato e, da numerosi anni, giurista dello Stato Maggiore della Direzione generale dei sistemi di informazione dello Stato di Ginevra. Ha sviluppato nel quadro della sua tesi transdisciplinare una visione critica del diritto d'autore attuale racchiude l'orientamento di parecchie discipline (antropologia, sociologia, etica, economia, storia, estetica e diritto comparato); in continuità della sua riflessione sui rapporti che il nucleo della personalità intrattiene con l'attività creatrice, adotta un approccio originale e, anche qui, critico della robotica e dell' "intelligenza artificiale".

La città connessa

Precisiamo subito ciò che è una città connessa. Si tratta di un ecosistema fondato sulla cattura, l'aggregazione e la condivisione di dati[1] relativi all'utilizzazione della città dai suoi abitanti. In questo contesto, che il dato è la "materia prima" delle città connesse.

Le fonti di questi dati sono multipli: generate automaticamente da sensori o da oggetti connessi, ma anche provenienti da base di dati raccolti dalle amministrazioni pubbliche o le imprese private, o anche prodotte dagli stessi utilizzatori-contributori.

Gli scopi perseguiti da questa raccolta sono molteplici. In modo generale, si invoca il miglioramento della qualità di vita dei cittadini, la buona gestione delle risorse collettive, l'agevolazione della mobilità o ancora l'attenzione alla sicurezza. Si tratta di creare un legame per informare a distanza e in tempo reale i cittadini sulla disponibilità degli equipaggiamenti collettivi (ingombro delle strade, tasso di occupazione dei parcheggi, localizzazione

di trasporti in comune, prenotazione di impianti sportivi…), ma anche di informare sulla vicinanza, l'ubicazione e gli orari di apertura di negozi o di curiosità turistiche, di informare sui servizi esistenti o di gestire le infrastrutture collettive. Questi pochi esempi illustrano bene i propositi virtuosi dell'impresa, ma non evidenziano i suoi rischi ed i suoi pericoli.

In questa raccolta, in effetti, la protezione della sfera privata presenta una posta cruciale e mette in luce gli aspetti più oscuri del sistema che si sta installando. Quattro sono i principali aspetti da tenere in conto nel contesto delle città connesse: la raccolta automatica dei dati sul dominio pubblico (a), i dati considerati come "pubblici" che gli individui si scambiano tramite i telefoni "intelligenti" (b), la loro integrazione nell'informatica del cloud (c) e soprattutto, l'interpretazione di questa massa di dati in vista di una *"governance algoritmica"* (d). Le inclinazioni di questa politica numerica ci permettono infine, in di conclusione, di stabilire un parallelo fra il rispetto della sfera privata ed il riconoscimento sociale della libertà individuale.

Dati captati automaticamente sul dominio pubblico

Numerosi dati delle città connesse sono generati automaticamente da sensori situati sulla via pubblica o posti all'interno di infrastrutture private aperte al pubblico.

Ma la scelta di un sensore non ha niente di innocuo. Così la sorveglianza del traffico può essere fatta in molti modi: attraverso il conteggio del numero di veicoli che passano su un anello magnetico, attraverso la registrazione video del traffico o attraverso la registrazione dei segnali GPS che permettono di identificare i veicoli in circolazione. Se il conteggio dei veicoli attraverso un anello magnetico non genera dati personali ma un semplice incremento statistico, non è lo stesso però nel caso delle videocamere e ancor meno della presa dei segnali GPS.

Dal momento che la raccolta dei dati sulla via pubblica *può* generare dati personali, conviene rispettare a titolo preventivo i principi posti dalle leggi applicabili in materia di protezione della persona.

In primo luogo, il principio di liceità (in Svizzera, art.4, al. 1 LPD; art.35 LIPAD) vuole che il trattamento sia giustificato dall'adempimento di un compito previsto da una base legale o da un consenso chiaro dell'interessato. Questo riduce di colpo gli scopi che possono giustificare la presa dei dati. In quanto al principio di proporzionalità (in Svizzera, art.4, al.2 LPD ; art.35 al.1 e 2 ; art 36 al.1 LIPAD), esso esige dal responsabile del trattamento che si assicuri che la lesione occasionata dimori ragionevole in rapporto allo scopo perseguito.

Questi principi incitano a sviluppare una riflessione ben prima della raccolta, al fine di assicurare la confidenzialità dal concepimento del progetto *("Privacy by Design")*. Verranno privilegiati così, ogni volta che lo scopo perseguito lo permette, i sensori che non generano dati personali: il responsabile del trattamento sarà, così, libero di calcolare i dati per assicurare la loro confidenzialità dai sensori alla sala macchine, anche durante tutto il ciclo della loro vita.

La protezione dei dati si dimostra ancora più cruciale nel campo privato aperto al pubblico: i dati sono allora trattati da attori privati, senza che sia possibile resistere alla loro cattura: ai giorni nostri, rifiutare di entrare in un'area video-protetta, si riduce a rinunciare a frequentare la maggior parte dei negozi, a cominciare dai grandi magazzini.

La necessità di applicare questo insieme di principi dimostra già bene il pericolo di una raccolta selvaggia di dati sul dominio pubblico per la protezione della sfera privata. Essa evita in aggiunta una tentazione propria a ogni tecnica: quella di focalizzarsi sui mezzi, tanto da dimenticarne gli scopi perseguiti. La storia delle tecniche mostra che l'umanità ha la tendenza a utilizzare una tecnica al di là dei suoi bisogni immediati e ragionati, per il solo fatto che è disponibile, fino a creare nuovi bisogni: è allora allettante far uso delle tecniche digitali le più sofisticate per affermare la propria modernità.

Dati generati dagli utenti

I dati raccolti nel quadro delle città connesse non si limitano a quelli catturati automaticamente sul dominio pubblico o aperto al pubblico. Gli utenti creano essi stessi, attraverso il loro telefono "intelligente" *(smartphone)*, numerosi dati personali geo-localizzati, sia attraverso la comunicazione di informazioni sulle reti sociali o per il solo fatto che essi interrogano per strada i servizi di informazione della città. Questi apparecchi portabili possono allora essere considerati come dei veri sensori.

Altri oggetti connessi rilasciano la loro mole di dati. Alcuni di questi vengono ad aggiungersi a quelli della città connessa. Si pensa, per esempio, ai dati relativi al consumo aggregato delle famiglie. Essi permettono di comparare le loro abitudini di consumo privato con quelle dei loro vicini per migliorarli. La connessione di tali sensori a Internet permette di essere avvertiti a distanza, sul telefono "intelligente", di ogni consumo programmato o intempestivo. Una applicazione largamente diffusa, *Sense*, permette in effetti di disgregare in tempo reale la curva di carica elettrica globale della famiglia, poi di identificare quali apparecchi sono utilizzati in casa e quando[2]. Il sistema dietro all'applicazione, paragonando le curve di consumo a quelle degli altri utilizzatori, che gli sono ritrasmesse, arriva a saperne di più sull'andamento di una casa che i proprietari stessi, e potrebbe redigere un quadro delle abitudini di vita dei suoi abitanti, e perfino delineare le basi di un profilo della loro personalità.

A questo quadro si aggiunge il fatto che gli oggetti connessi, spesso, sono elaborati da fabbricanti di oggetti poco informati sulle questioni della sicurezza informatica: numerose falle riguardanti la sicurezza permettono allora a terzi di visionare le immagini considerate confidenziali. È così che delle videocamere connesse per permettere ai loro proprietari di sorvegliare a distanza i dintorni delle loro case possono dare a dei ladri preziose informazioni sulle loro assenze. Il sito www.shodan.io, ad esempio, registra nel suo repertorio le immagini provenienti da videocamere non protette.

Il fenomeno degli oggetti connessi ha preso una tale importanza che Ubisoft, l'editore di "Watch Dogs" proclama *"Noi siamo i dati"* sul suo sito in occasione

dell'uscita della seconda versione del "gioco". Non affrettiamoci troppo a vedere qui un disprezzo degli utenti per la loro sfera privata. Questo è un discorso dei promotori delle reti sociali e le imprese che vivono della condivisione dell'informazione su Internet ai soli fini di estendere il loro potere, ma vale la pena di esaminare da vicino queste incoerenze.

Per prendere un esempio, nel 2009, il PDG di Google ed ex-PDG di Novell, Eric Schmidt, lanciò una frase che diede i brividi ad alcuni e sembrò ad altri intrisa di buon senso: "Se voi fate qualcosa che nessuno deve sapere, sarebbe forse preferibile che non cominciate a farla." Eric Schmidt non faceva altro che riprendere un proverbio tradizionale di origine cinese, da qui la furtiva impressione di saggezza che ne emana.

Osservatori attenti hanno compreso che Eric Schmidt la applicava alle ricerche effettuate su Internet, e che questo cambiava tutto. Questa frase fece temere il peggio in materia di violazioni della vita privata. Ma questo stesso profeta della "morte della vita privata", ha difeso la sua propria vita al di là del ragionevole: nel 2005, non ha forse intentato causa alla giornalista Elinor Mills per il suo articolo *Google balances privacy, reach*[3], nel quale l'autrice riferiva certi dettagli della sua vita privata (fortuna, azioni recentemente vendute in Borsa…) ottenute su Internet proprio grazie al motore di Google dedicato ai giornalisti, CENT (News.com)?

Hubert Guillaud, basandosi su uno studio di Joseph Turow, Michael Hennessy e Nora Draper datato 2015, ci ricorda tra l'altro che "più della metà dei consumatori americani non desiderano perdere il controllo sulle loro informazioni, ma pensano anche che questa perdita di controllo sia già avvenuta". Lungi dal considerare la cessione di questi dati personali in cambio di offerte personalizzate come il compromesso dove ciascuno ci guadagna, il pubblico apparirebbe piuttosto *rassegnato e sprovveduto*. Siamo lontani dal discorso trionfalista dei mercanti.

E Hubert Guillaud conclude con pertinenza: "L'impotenza non è il consenso"[4].

Città connesse e informatica nel Cloud

Creare legami: chi penserebbe di criticare questo scopo apparentemente virtuoso portatore d'armonia universale? Gli scopi perseguiti dalla città connessa presuppongono una comunicazione dei dati e dei sistemi fra di essi, o perlomeno l'impiego di una semantica comune facente appello a degli standard. In altri termini, la città connessa passa in pratica dall'informatica al cloud *("Big Data")*. Città connesse e informatica nel cloud si completano: i dati delle città connesse alimentano l'informaticanel cloud e quest'ultimo, in cambio, offre chiavi di interpretazione per fare confronti con altre fonti.

Dal momento che devono essere considerate come dati personali tutte le "informazioni che si riferiscono a una persona identificata o identificabile"[5], i dati personali non esistono indipendentemente dal loro contesto. In altri termini, rari sono i dati che sono in sé personali: è il legame a una persona (determinata, o *determinabile*) che li costituisce come tali. La città connessa, come l'informatica nel cloud, creando legami, partecipa potenzialmente alla creazione di dati personali… e quindi all'erosione della sfera privata.

Il legame a una persona fisica può essere fatto attraverso gli oggetti che essa stessa utilizza, *anche se non sono espressamente ricollegabili ad essa*. Basta che questi dati siano associati a un *ancoraggio stabile*. E` per questo che gli indirizzi IP dei computer privati sono considerati come dati personali. La corrispondenza con altri dati fa il resto. Basta che una sola volta sia stabilito un legame voluto tra la macchina e il suo utente, per esempio attraverso un formulario di acquisto, che l'insieme dei dati raccolti attorno all'indirizzo IP possono essere ricollegati a una determinata persona fisica.

Ora, il responsabile del trattamento ha il dovere di assicurare la confidenzialità dei dati personali che si trovano nella sua sfera di influenza. Non si possono quindi mettere a disposizione dati in apparenza anodini tenendo conto dell'informatica nel cloud e delle possibilità di corrispondenza stupefacenti che essa offrirà ai beneficiari. Le regole di sicurezza devono per questo essere regolarmente riconsiderate e rinforzate, in particolare quelle che garantiscono l'anonimato. Colui che apre dei dati deve anche assicurarsi di poter mettere fine in ogni momento alla loro distribuzione così come alla

riutilizzazione da parte di terzi quando infrangono le regole ed i trattamenti che garantiscono l'anonimato. Solo la distribuzione sotto licenza permette un tale dominio, nel diritto se non nei fatti. Le licenze libere possono a questo titolo servire d'esempio, a condizione di riorientarle in favore di un mantenimento dell'anonimato piuttosto che dell'apertura, i due scopi non essendo del resto necessariamente incompatibili.

L'interpretazione dei dati e la *governance* algoritmica.

È l'interpretazione dei dati della città connessa che può nascondere i pericoli più gravi. Una volta integrati all'informatica nel cloud, questi dati possono, per correlazione, completare il profiling degli individui e la loro chiusura in modelli da cui è difficile sfuggire.

Lo scopo dell'informatica nel cloud rimane il profiling generico degli utenti e la loro classificazione in categorie, in modo da predire il loro comportamento nel consumo per meglio manipolarli. L'informatica nel cloud è un potente strumento di controllo, che va molto più lontano della confusione fra il nascosto e l'illegale sulla quale i *vendor* hanno costruito la fragilità della sfera privata. Oltre al carattere estremamente riduttivo del fatto e l'inaccettabile riduzione dell'altro a "oggetto" che esso comporta, questo profiling riduce gli individui alla mercé dei loro fornitori e questo per parecchie ragioni.

La prima ragione è che la fragilità della sfera privata nasconde prima di tutto un rapporto di potere. È merito di Daniel J. Solove, professore di diritto americano, di averlo dimostrato. Hubert Guillaud cita il parere di un esperto in sicurezza, Bruce Schneier, intervistato nel 2006: "La nozione di vita privata ci protegge da coloro che hanno il potere, anche se non facciamo niente di male quando siamo sorvegliati. (…) Se siamo sotto osservazione in ogni occasione, (…) perdiamo la nostra individualità". Hubert Guillaud ne conclude: "La sfida della vita privata, è la tensione democratica fra il forte e il debole"[6].

Ma il profiling messo in opera dall'informatica nel cloud va più lontano. Daniel J. Solove, ancora lui, trovando che l'analogia fra Internet e il *Big Brother* di Orwell proposta da alcuni non era pertinente, si doveva preferire un parallelo con *Il processo*, celebre romanzo di Franz Kafka. Il professore di diritto si è domandato a cosa rimandasse il sentimento di oppressione in questo romanzo considerando che il suo eroe, Joseph K., si trova giudicato sulla base di fatti che non gli sono comunicati, da gente che non conosce, in applicazione di regole e valori che gli rimangono misteriosi e nell'ignoranza delle conseguenze possibili della procedura in corso[7]. Questo produce molte incognite e toglie soprattutto ogni possibilità di difesa. Quale potere può essere più arbitrario? E Daniel J. Solove si interroga: "non siamo tutti un po' come Josef K. di fronte al GAFAM[8] e alle autorità estranee che li governano?"

Antoinette Rouvroy, giurista e ricercatore del FNRS all'Università di Namur, non si scosta da questa linea di pensiero: "Vi si classificherà in categorie in funzione di dati grezzi che per voi non hanno nessun significato, in funzione di algoritmi di cui non sapete come funzionano, e questo avrà un impatto sulla vostra vita, (…) alla maniera di un riflesso"[9].

Questo è il principale pericolo che nasconde il concetto delle città connesse, che Antoinette Rouvroy ha battezzato "la *governance* algoritmica". Qui, il pericolo non risiede tanto nel dato quanto nella sua interpretazione e la sua strumentalizzazione. Pretendendo che questi dati captati massicciamente e in modo automatico possano per questo solo fatto pretendere alla "obbiettività", gli ingegneri informatici e i loro finanziatori non si accontentano di presentare ai dirigenti politici la raccolta dei dati come un mezzo per verificare l'efficacia delle politiche pubbliche e del loro grado di adozione da parte della popolazione; essi propongono loro di attingere nei dati la "ragione" delle politiche pubbliche future. Il loro obiettivo è la correlazione massiccia come pensiero maestro e le macchine come guard-rail dell'umano. Si tratta, insomma, della versione più moderna della confusione ricorrente dei mezzi e dei fini, doppiata da una severa ignoranza delle specificità della natura umana.

Qui bisognerebbe fare tutto in una volta il processo dell' "intelligenza" artificiale, della teoria dell'informazione e della visione "meccanista" della vita – e dell'umano.

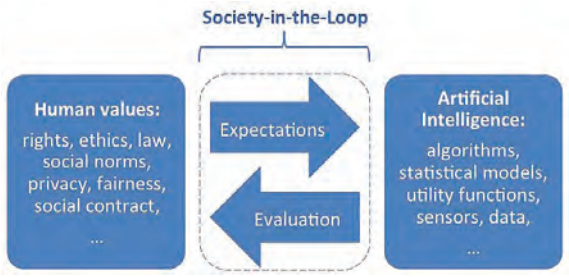
Mi accontenterò di sottolineare un punto essenziale: categorizzando il comportamento delle persone secondo le correlazioni tratte dall'analisi della somma gigantesca di dati, gli ingegneri informatici ci privano di ogni avvenire, scalzando la riconoscenza sociale della libertà individuale, già ben intaccata dai gestori. Ci reprimono così in modelli radicalmente inadatti e terribilmente disingannati.

Un esempio fra gli altri ci permette di cogliere meglio la natura delle derive da temere per ciò che riguarda le città connesse. Alcune persone, visibilmente mal ristabilite dalle "imperfezioni" umane, hanno creduto bene di sostituire i giudici con… dei robot. L'applicazione delle leggi e delle giurisprudenze si ritroverebbe più rigorosa – intendete con questo: più sensibile – all'intelligenza della situazione. Si verrebbe così a giudicare l'autore di un reato in funzione di statistiche, detto in altro modo di una conoscenza parziale del passato applicata all'avvenire.

Esiste modo migliore per negare ogni possibilità di evoluzione della persona che di negare alla stessa ogni diritto di essere ascoltata? La fase seguente consisterà senza dubbio nell'instaurare una giustizia predittiva, in altri termini a fermare coloro il cui profilo li designerà come criminali in potenza… L'idea è del resto già stata evocata. Potremo così vantarci di aver raggiunto un livello ineguagliato di barbarie nella storia.

Giudicare qualcuno sul passato degli altri, non è fargli subire una violenza inammissibile? Una volta installato questo sistema, quale giudice, quale dirigente avrà il coraggio di pronunciare una decisione contraria alle predizioni statistiche elaborate dalla macchina?

Sarebbe ancor più ingenuo pensare che i dati sono *oggettivi* per il solo fatto che sono stati presi automaticamente: un dato non ha niente di un "dono", esso è stato costruito. Le teorie dell'informazione l'hanno troppo spesso dimenticato. Il ricercatore non trova in



generale ciò che cerca; può così ignorare l'essenziale senza neanche rendersene conto. È il merito della fenomenologia, attraverso la nozione di intenzionalità, di avercelo ricordato[10].

Allo stesso modo, i sensori possono catturare di continuo i dati, essi non registrano che una parte della realtà, non per forza la più pertinente.

Il sensore non fa nient'altro che filtrare il reale in funzione delle *intenzioni* – o dei *pregiudizi* – di colui che li installa tace le *possibili* alternative allo stato di intenzione. Ora, questi ultimi sono essenziali per capire l'avvenire. Non è forse a tastoni che si inventa il futuro? Solo una critica coerente può permettere la messa in prospettiva delle nostre informazioni e dei mezzi utilizzati per raccoglierle.

In quanto al profiling, considerato come il dato reso infra-individuale per diventare *calcolabile,* poi artificialmente ricomposto in profili supra-individuali attraverso correlazioni, non evacua forsei *Soggetti* che noi siamo[11]? E se i dati non sono il *reale* e essi non hanno *senso* per coloro dei quali pretendono, però, di il comportamento, una *governance* della città *attraverso* i dati può ancora pretendere di essere pertinente?

Inoltre, niente prova che le correlazioni fra i dati segnalino un rapporto di causa ed effetto. La saggezza popolare afferma: "il confronto non è una ragione". Ora il cuore stesso dell' "intelligenza" artificiale riposa sulla confusione fra correlazione e rapporto di causalità. Questo può comportare le conseguenze più assurde. Vogliamo veramente sottometterci a questo? Allora se l' "intelligenza" artificiale, basandosi sulle correlazioni, rinuncia al senso e si accontenta di predire senza comprendere, è ancora possibile considerare di allineare le nostre politiche sulle nostre suggestioni? Mentre le scienze dell'universo si sono ricredute sul modello scientifico per il quale la realtà sarebbe interamente contenuta nel "nucleo primordiale"[12], l' "intelligenza" artificiale limita il futuro a una semplice proiezione del passato; è ragionevole lasciarle chiudere il nostro avvenire?

I punti che abbiamo appena menzionato sottolineano la necessità di combattere i progetti che mirano all' "organizzazione automatizzata del mondo"[13], come quello condotto da *SidewalkLabs*, una filiale di Alphabet, l'impresa che è a capo di Google. Si tratta né più né meno di concepire una città interamente "costruita a partire da Internet", attraverso anelli di retro-azione, per poi applicare questo modello all'intero pianeta[14]. Dare il potere a qualcuno di decidere per tutta l'umanità del più piccolo dei gesti dei suoi rappresentanti, non solo la *Google City*, eradica di fatto ogni programma politico, ma corrisponde all'aspetto più terrificante del totalitarismo. Hannah Arendt non diceva forse che quest'ultimo non mirava soltanto a restringere la libertà, ma a eradicare ogni traccia di spontaneità?[15] Non è esattamente ciò che avverrebbe se noi accettassimo il progetto di Alphabet? Quando si pensa che la spontaneità per HannahArendt non ha niente di fantasia, ma corrisponde piuttosto all'espressione dell'interiorità, alla manifestazione sorprendente e per definizione imprevedibile dell'*originalità del nostro proprio essere al mondo,* si capisce che la Google City nutre in definitiva l'ambizione trans-umanista di eradicare l'umano nell'uomo.

Essere soggetto al giorno d'oggi

La grande questione non è in fin dei conti di sapere chi siamo e che cosa desideriamo diventare? Vogliamo accettare di essere ridotti a dei dati o di paragonarci a degli automi? Non siamo *molto di più*? Abbiamo forse dimenticato il nostro valore specifico? Mentre il robot, riproducibile all'infinito, ha il pensiero dell'errore e del risultato, l'essere umano, unico a condizione di diventare *Chi* egli è, non ha piuttosto il pensiero della finalità?

Nei campi del senso e della libertà che ci caratterizzano, *i possibili*, dal momento che dicono qualcosa della nostra natura profonda, non sono forse più essenziali che i *risultati*? Aristotele non lo ha forse sottolineato in modo stupefacente affermando che nell'attualizzazione di una potenzialità dimora tuttavia una potenzialità, insistendo sul carattere dinamico e creatore dell'agire umano? Gli avvenimenti essenziali della nostra esistenza, quelli che fanno sì che la vita merita ai nostri occhi di essere vissuta, sono solamente calcolabili o traducibili in termini di risultati? Si spera che questo non sia il caso, poiché il risultato è cieco al senso come il mezzo può esserlo allo scopo. Ora, contrariamente ai dati, non siamo noi *fonte di senso*?

In definitiva, lo scopo di ogni esistenza umana non è forse il lavoro interiore che ci permette di divenire *Chi* siamo veramente appropriandoci della nostra storia? Su questo cammino, i fallimenti non insegnano almeno tanto quanto le vittorie? E che non ci si venga a dire che il senso della nostra vita non deve essere considerato all'interno delle politiche economiche o sociali, poiché se così fosse, a cosa servirebbero in fine queste ultime?

Un immenso lavoro ci aspetta per passare dalle "scienze umane" alle "discipline del soggetto", e cioè per concepire l'essere umano nelle sue specificità stesse, non come l'*oggetto* di una scienza ma in quanto *soggetto.*

Questo necessita lo sviluppo di uno metodo diverso da quello utilizzato dalle scienze tradizionali. Le esigenze di riproducibilità, di quantificazione e di confutabilità devono far posto ad altri approcci, propri dello studio del *Soggetto*[16]. Questo potrebbe particolarmente evitare alle "scienze" umane di auto-convalidare le loro ipotesi su "oggetti" attraverso metodi inadatti.

La grande erosione

L'informatica nel cloud erode la sfera privata nello stesso modo in cui la *governance* algoritmica scalza le fondamenta del riconoscimento sociale della nostra libertà individuale. L'importanza dei dati comparativi attuali in mano ai fornitori di servizi fa si che il nostro comportamento diventi spesso *più prevedibile* per i nostri fornitori di servizi che per noi stessi. Questo fa dire ad Alexandre Lacroix che l'essere libero di domani sarà colui il cui comportamento si rivelerà meno prevedibile per i venditori che per lui stesso[17]… E in questo che sfera privata e libertà individuale sono legate, la protezione della sfera privata garantendo la nostra libertà.

Se, per parafrasare il titolo della celebre opera di Karl Polanyi, *La Grande Transormation*, dovessimo caratterizzare il principale effetto dell'informatica nel cloud, questo sarebbe "la grande erosione".

Si aprono davanti a noi parecchie strade per evitare questo Prima di tutto, ciascuno di noi deve rimanere *padrone* dei suoi dati personali. Si può parlare di *proprietà*, ma ancora bisogna farlo nel senso che le Lumières gli accordavano, che differisce dal senso capitalista ed escludente che gli attribuiamo attualmente. In effetti, mentre per le Lumières la proprietà è la garanzia materiale data a ciascuno - come rinforzo di quella degli altri- contro il potere di *uno solo* (il tiranno), per il capitalismo, la proprietà è il diritto *esclusivo* di ciascuno contro tutti (Thomas Hobbes).

Questo scopo può essere raggiunto se le autorità politiche impongono alla distribuzione dei dati della città connessa l'obbligo di assicurare loro l'anonimato nel tempo e che permetta di tener conto delle evoluzioni

dell'informatica nel cloud. La non re-identificazione dei dati della città connessa deve quindi essere un imperativo e suppone una vigilanza di ogni istante. Arvind Narayanan e Vitaly Shmatikov ci ricordano a questo proposito che *"La polivalenza e la potenza degli algoritmi di re-identificazione implicano che termini quali "personalmente identificabili" e "quasi identificanti" non hanno semplicemente alcun significato tecnico. Mentre certi attributi possono identificare in modo unico, ogni attributo può essere identificato in combinazione con gli altri."*[18]

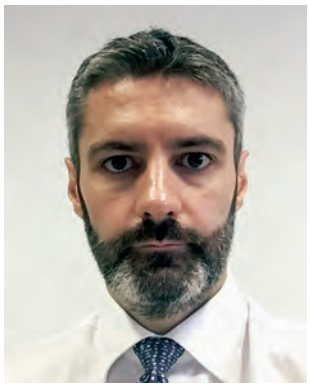
Inoltre, è necessario accertarsi il carattere aperto dei dati raccolti e ciascuno dovrebbe sapere quali algoritmi, quali regole di interpretazione si applicano ai dati che li concernono.

Infine, in modo più fondamentale, risulta urgente ripensare le relazioni fra *individuie collettività* e confrontare la teoria dell'*informazione* alle teorie della *conoscenza*.

"Vasto programma" direbbe Charles De Gaulle., che si scopre ancor più appassionante. ■

1 Le nozioni di dati e di informazione sono compresi in maniera diametralmente opposta dagli informatici e dai giuristi: per i giuristi, il dato rappresenta la forma bruta(senza la messa in contesto né interpretazione) dell'informazione, mentre per la teoria dell'informazione –e quindi gli informatici- è l'informazione che diventa "dato"attraverso la sua messa nel contesto. Nel quadro di questo articolo, la nozione di "dato" deve essere compresa nel senso inteso dalla legge.
2 BOGOST Ian, Home Monitoring Will Soon Monitor You, The Atlantic (Washington), 11.11.2016.
3 MILLS Elinor, Google balances privacy, reach, 14.07.2005, CNET News, https://www.cnet.com/news/google-balances-privacy-reach-1/, consultato il 25.03.2017.
4 GUILLAUD Hubert, Donnéespersonnelles : l'impuissance n'est pas le consentement, 11.06.2015,http://www.internetactu.net/2015/06/11/donnees-personnelles-limpuissance-nest-pas-le-consentement/, consultato il 25.03.2017.
5 In Svizzeta Art. 3 lett. a della legge federale sulla protezione dei dati personali(LPD - RS 235.1); art. 2 lett. a della legge del Canton Ginevreasull'informazione del pubblico, l'accesso ai documenti e la protezione dei dati personali (LIPAD – RSGe A 2 08)
6 GUILLAUD Hubert, La valeur sociale de la vieprivée, in InternetActu.net, n°241 (23.10.2009), http://www.internetactu.net/2009/10/21/la-valeur-sociale-de-la-vie-privee
7 SOLOVE Daniel J., The Digital Person : Techology and Privacy in the Information Age,New York UniversityPress, New York 2006 ; « I'veGot Nothing to Hide » and OtherMisunderstandings of Privacy, in San Diego Law Review, vol. 44 (2007),pp. 745-772 ;http://papers.ssrn.com/sol3/papers.cfm ?abstract_id=998565
8 GAFAM:Google, Amazon, Facebook, Apple, Microsoft
9 ROUVROY Antoinette, STIEGLER Bernard, Le régime de vérité numerique - De la gouvernementalité algorithmique à un nouvel Etat de droit, 07.10.2014, in Socio, La nouvelle revue des sciences sociales, 4/ 2015, Dossier : Le tournant numérique… Et après?, pp. 113-140 ; http://socio.revue.org/1251
10 A questoproposito, vederesegnatamente ; BORTOFF Henri, Prenons l'apparence au sérieux, Trades, 2012
11 ROUVROIY Antoinette, STIEGLER Bernard, Le régime de vérité numérique, op. cit.
12 STAUNE Jean, Notre existence a-t-elle un sens ? Une enquête scientifique et philosophique, Librairie Arthème Fayard/Pluriel, Paris 2017 (2007), Avant-Propos, p. XII; Jean Staunesviluppa a questopropositouna « teoriadellosfalsamento ».
13 SADIN Eric, La Silicolonisation du monde – L'irrésistible expansion du libéralisme numérique, L'Echappée, Paris 2016, pp. 108- 109
14 PIRENA Alexis, Et si Google créait sa propre ville avec ses propres règles ?, 06.04.2016, www.numerama.com/tech/161094-et-si-google-creait-sa-propre-ville-avec-ses-propres-regles.html, consultato il 28.03.2017
15 ARENDT Hannah, Le Système totalitaire – Les Origines du totalitarisme, Le Seuil, coll. Points, Paris 2002, p. 190
16 VERNIORY Pascal, ""Human Sciences" or "Disciplines of the Subject" ?", in Human and Social Studies- Research and Practices, Iasi (Romania), vol, 2, n°3 (settembre 2013),pp.33-58
17 LACROIX Alexandre, En finir avec le hasard ?, in Philosophie Magasine, n° 102 (settembre 2016)
18 NARAYANAN Arvind, SHMATIKOV Vitaly, Myths and fallacies of Personality identifiable information », Communications of the ACM 53, n°6 (2010)

L'impatto della disinformazione sul valore azionario



autore : Massimo Cappelli

Questo articolo vuole essere una riflessione e più che fornire risposte, suscita un insieme di interrogativi che, chi si occupa di Information Security, deve porsi nel breve e lungo periodo.

L'Information Security viene definita come quell'insieme di processi e metodologie che sono disegnati e implementati per proteggere **informazioni** private, confidenziali, sensibili, siano esse elettroniche, stampate o di qualsiasi altra natura, dall'accesso non autorizzato, dall'uso, dal cattivo uso, dalla divulgazione, distruzione, modifica, o danneggiamento.

Spesso l'Information Security viene identificata con la sicurezza informatica, che è solo una parte delle attività che devono essere poste in essere, in quanto l'informazione viaggia attraverso diversi strumenti, non solo attraverso le reti informatiche.

La valutazione del rischio sull'informazione non deve basarsi solo sulle considerazioni di tipo meramente "elettronico" ma deve essere un processo che valuta tutti gli aspetti anche relativi a luoghi e persone. Lo illustra chiaramente Kevin D. Mitnick nel *"L'arte dell'Inganno"* del 2001, dove presenta una serie di casi in cui si riesce a recuperare informazioni utili ai propri scopi, semplicemente parlando con le persone e raccogliendo porzioni di informazioni che assieme creano una base solida di credenziali con cui avere accesso a ulteriori informazioni ancora. Per questo, in alcune realtà, si parla di Tutela delle Informazioni, appunto per indicare quei processi e metodologie previste nell'Information Security con un perimetro più ampio rispetto la sicurezza informatica.

Nella maggior parte dei casi, le informazioni tutelate sono quelle aziendali. Lo sguardo è rivolto all'interno: informazioni su clienti, su contratti, su strategie, su brevetti e così via. Il primo interrogativo che sorge riguarda il perimetro di competenza. È sufficiente monitorare l'uso e la custodia delle informazioni interne? Probabilmente no, per tutelare la propria azienda è necessario guardare anche all'esterno, a quelle minacce che comunque ledono la reputazione del nostro brand o del nostro business. Alcuni esempi sono i siti di phishing o i profili di consulenti fasulli che si spacciano per dipendenti dell'azienda per carpire informazioni o credenziali dal cliente. Tutti gli istituti finanziari monitorano il web per segnalare e bloccare siti di phishing, cioè guardano fuori dal perimetro per bloccare informazioni nocive per l'azienda.

Ma è sufficiente monitorare e verificare solo l'utilizzo improprio o fraudolento del marchio? Oppure ci sono altri aspetti da considerare?

Negli ultimi anni, la cronaca è stata inondata da articoli, discussioni e dichiarazioni sul fenomeno delle *"fake news"*, utilizzate per la **disinformazione**, soprattutto politica o per meri ricavi economici.

L'endorsement di Papa Francesco per Donald Trump è stato condiviso e commentato circa 960.000 volte su Facebook. Chissà se ha influito o no sulla sua elezione…

A tutti noi è capitato di incappare in un amico o collega che ci ha riportato una notizia falsa. Presumibilmente, pure noi siamo stati vittime e veicoli inconsapevoli di almeno una notizia fasulla, letta sui social network, velocemente fra un morso al cornetto e un sorso di caffè.

La disinformazione si può manifestare attraverso un'incompleta rappresentazione dei fatti, una rappresentazione dei fatti fasulla o una rappresentazione dei fatti manipolata. L'obiettivo dell'agente disinformatore è di spingere la notizia quanto più possibile su più canali di comunicazione portando il lettore ad una convinzione precisa.

La disinformazione ha un obiettivo semplice quello di indirizzare il lettore su una **determinata posizione** sia essa a favore sia essa a sfavore di un argomento.

BIO

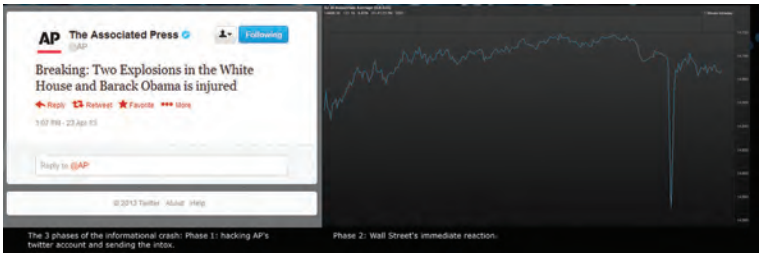
Massimo Cappelli è operations planning manager presso la Fondazione GCSEC. Da gennaio ricopre anche il ruolo di responsabile del CERT e della cyber security di Poste Italiane all'interno della funzione Tutela delle Informazioni. Nella sua passata esperienza ha lavorato come consulente in Booz Allen Hamilton e Booz & Company nella practice Risk, Resilience and Assurance.

È creata per suscitare un **sentimento** di empatia o avversione. Il sentimento a sua volta può portare a delle azioni come proteste, boicottaggi, dimostrazioni.

Rimanendo alle recenti elezioni americane, il caso di una nota bevanda analcolica americana può essere un esempio. 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 (condizionale d'obbligo) *"CEO Tells Trump Supporters to Take Their Business Elsewhere"*. La notizia era stata totalmente distorta dalla fonte e da chi ha reinoltrato la notizia, ma l'impatto sembra si sia ripercosso sull'azienda in termini di gradimento nei confronti dell'azienda stessa e in termini di valore azionario. Ora potrebbe essere stato un caso, ma il giorno stesso della notizia riportata, il punteggio del gradimento *(sentiment)* 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 comunicazione.

Esulando dal contesto elettivo, un altro caso che ha fatto storia è un caso di un'azienda farmaceutica, che chiameremo XY. Nel gennaio del 2012, un articolo apparso su Seeking Alpha, un sito specializzato in finanza, dichiarava che l'azienda XY, quotata a Wall Street, stava lavorando allo sviluppo di un trattamento sperimentale per il cancro, più economico e competitivo dei concorrenti. Le azioni della società nel giro di 5 mesi avevano totalizzato un aumento del valore azionario pari al 263%, forse merito anche della notizia pubblicata. Solo dopo circa due anni, a fronte del report sul nuovo trattamento, si scoprì che in realtà era una delusione. La stessa SEC (Security & Exchange Commission) scoprì che l'articolo era stato commissionato dalla stessa società farmaceutica XY attraverso una commissione indiretta. Il risultato è stato un tonfo del valore azionario della società.

La tecnica, in passato, era conosciuta come "Pump & Dump" cioè pompare e scaricare. Il titolo azionario viene pompato attraverso notizie fasulle che lasciano intravedere ampi aumenti di valore, per poi essere scaricato (venduto) una volta raggiunto il valore voluto. È un esempio di frode finanziaria in cui i soggetti mal informati ne subiscono le conseguenze.



Altro caso nel 2013 ha avuto un impatto sistemico. Il tweet uscito da due account dell'Associated Press (AP) relativo ad un attentato in cui era rimasto ferito il Presidente Obama, fece "bruciare" più di 130 miliardi di dollari in Borsa. Gli account AP erano stati hackerati.

Supponiamo, ipoteticamente, di essere un'azienda Beta appetibile sul mercato perché presente in diverse aree geografiche, con infrastrutture consolidate, con accordi commerciali solidi e posizione sul mercato monopolistica. Il valore del titolo è elevato e potenziali scalate risulterebbero onerose al valore azionario attuale. Se l'azienda Alpha fosse interessata a Beta, fosse sleale e volesse acquisire quota parte delle mie azioni per influire sulle strategie o per consolidare la sua presenza all'interno di Beta, potrebbe utilizzare la disinformazione per far abbassare il valore azionario e acquisirne quota parte?

Le attività disinformative possono essere di breve o lungo periodo. Probabilmente se parlassimo con un dirigente di azienda anglosassone o con uno asiatico, anche sul breve e lungo periodo ci potrebbero essere degli interrogativi.

- **Opzione 1:** Se fossi l'azienda Alpha potrei far pubblicare da più fonti una falsa dichiarazione del CEO dell'azienda Beta, come il caso della bevanda analcolica di cui sopra. Questa iniziativa potrebbe portare ad un abbassamento del valore azionario della società Beta. La società Alpha potrebbe approfittare per acquistare quota parte delle azioni ad un prezzo inferiore di circa il 5%, attraverso acquisti indiretti e frammentati nel tempo.
- **Opzione 2:** Se fossi sempre la società Alpha, potrei anche far pubblicare informazioni sull'azienda Beta, similari a quelle dell'azienda farmaceutica di cui sopra. In questo caso, l'obiettivo finale sarebbe sempre quello di acquisizione ma attraverso un processo di screditamento della azienda target. Si potrebbe far perdere fiducia agli investitori attraverso il rilascio di notizie false sulle future strategie vincenti dell'azienda per poi smentirle e quindi fare esplodere la bolla speculativa. Ci sono i controlli delle varie commissioni di vigilanza, ma scommetto che con i dovuti accorgimenti e, se ben pianificato, i modi per acquisire anche indirettamente le quote senza farsi scoprire ci sono, soprattutto se alle spalle ci sono governi a supporto.
- **Opzione 3:** Questa attività di disinformazione potrebbe essere effettuata anche nel lungo periodo affidandosi a

profili fasulli. Supponiamo di poter avere un numero ingente di profili fasulli di qualche social media e supponiamo che questi profili inizino a condividere informazioni non proprio gradevoli sulla società Beta: disservizi, scarsa qualità dei prodotti, inaffidabilità dei dipendenti, scandali sul management. Le informazioni false, come tante piccole gocce cinesi, verrebbero riversate massivamente in un mare di informazioni, inquinandolo. Queste informazioni sono difficilmente scremabili. Si pensi alla *sentiment analysis* che potrebbe essere impattata da notizie fasulle che fanno crollare la fiducia e le vendite dei prodotti. I prodotti venduti sui siti di eCommerce sostengono tutti la prova delle "recensioni" del cliente. Sfido chiunque a non porsi il dubbio sull'acquisto nel momento in cui vede apparire due recensioni positive e una negativa o viceversa. La recensione negativa influenzerà molto di più la psiche rispetto quelle positive.

E se al posto di un'azienda ci fosse un Paese? Un Paese che dal punto di vista logistico potrebbe essere un trampolino di lancio per iniziative economiche o per il passaggio di importanti infrastrutture internazionali. Screditare l'affidabilità del Paese e dei suoi governanti potrebbe avvenire anche attraverso campagne di disinformazione sulle politiche fiscali, sul turismo di bassa qualità, su tutti quegli indicatori che potrebbero portare a destabilizzare il Paese stesso o a impoverirlo, permettendo un "saccheggio" delle risorse o delle infrastrutture. Il PIL cala a causa dei mancati introiti dal turismo o dal capitale investito internamente in attività produttive. Il calo del PIL porta ad un calo delle tasse versate, che porta ad una mancanza di copertura per la manutenzione di infrastrutture. Per sopperire alla mancanza della copertura ma mantenere l'infrastruttura il Paese è costretto a venderne quota parte o la sua totalità o indebitarsi ulteriormente. Tutto è ipotetico ovviamente.

Il mercato finanziario è soggetto alle informazioni che riceve e cerca di trasformarle in valore.

Si pensi, anche, ai sistemi di High Frequency Trading (sistemi di transazioni ad alta frequenza sui mercati che utilizzano algoritmi matematici). Alcuni di essi sono stati dotati anche di capacità di analisi quantitative di Big Data e di *news parsing system* per monitorare in tempo reale news e aggiustare i valori transati anche in base ad altre informazioni, oltre a quelle di pura analisi finanziaria.

La presenza di innumerevoli informazioni la cui attendibilità non è verificata e la cui fonte non è classificata per la sua affidabilità può portare in futuro a distorsioni sempre maggiori dei mercati, a politiche di espansione anche geoeconomica attraverso l'uso dell'informazione. I sistemi High Frequency Trading saranno potenziati e affideranno le proprie analisi e giudizi sempre più sui Big Data.

Se aggiungiamo in futuro anche di ampliare la possibilità dei singoli investitori ad investire con frequenze più alte, l'uso corretto dell'informazione diventa vitale per i mercati.

Come proteggersi? Questo è l'ultimo interrogativo che mi pongo nell'articolo. Certamente tutti dovrebbero ricoprire un ruolo a tutela del sistema finanziario. Colpevolizzare e perseguire chi pubblica "fake news" è una attività che seppur lodevole, richiederebbe tempistiche che poco si sposano con la volatilità dei mercati. Di certo si potrebbero imporre delle regole per la selezione delle fonti all'interno dei sistemi di transazione rapida, attraverso una certificazione di affidabilità in base all'attendibilità delle informazioni pubblicate nel tempo. In questo modo si eviterebbe il rischio di fonti inquinanti ma non si risolverebbe potenziali problemi di account compromessi come il caso Associated Press.

Lato azienda, una regola fondamentale da ricordare è "Comunicare per primi". È la regola base per gestire le crisi ma in una società fortemente pervasa dall'informazione deve diventare una attività quotidiana. Nel saggio *"Deception – Disinformazione e propaganda nelle moderne società di massa", si esprime il concetto che "la velocità è un elemento essenziale, in quanto quello che conta è la prima affermazione: le smentite non hanno alcuna efficacia."*

Pertanto è il caso che le aziende inizino a dotarsi di strutture in grado di monitorare i social media, di analizzare le informazioni che pubblicano e di verificarne il potenziale impatto sulla propria azienda per muoversi con anticipo attraverso comunicati stampa in grado di definire chiaramente la posizione dell'azienda. Monitorare i social media, non significa ovviamente solo i classici social media. L'analisi va condotta anche a livello multi-dimensionale, verificando che non vi siano fili diversi che riconducono allo stesso bandolo, fonte ultima di un attacco disinformativo.

Non si deve inseguire la notizia per arginarla, per smentirla o correggerla. Una informazione mal gestita può trasformarsi in una Idra di Lerna. Una chiara posizione ufficiale dell'azienda, ben strutturata e largamente diffusa può dipanare dubbi e ridurre le incertezze degli stakeholder. Per questo è necessario mettere in piedi un impianto capillare di comunicazione che sia in grado di raggiungere più strati di stakeholder. La comunicazione deve essere semplice, lineare e di facile comprensione con livelli stratificati di dettaglio in base agli stakeholder che si vuole raggiungere: analisti finanziari, azionisti, associazioni di consumatori e consumatori, istituti di vigilanza e così via. Nell'era dell'informazione, è l'informazione stessa la miglior arma che si possa usare.

Ecco che il perimetro della tutela delle informazioni per le aziende potrebbe ampliarsi notevolmente. Potrebbe richiedere sforzi aggiuntivi e competenze sempre più trasversali con team rapidi di risposta non solo tecnica ma anche comunicativa, in grado di supportare gli uffici stampa e di comunicazione in operazioni di informazione a contrasto della disinformazione. ■

“I molteplici volti della cittadinanza globale: un problema identitario”

Autore : Frédéric Esposito

Con la nascita delle reti sociali, abbiamo osservato un cambiamento tanto grande quanto incontestabile sia riguardo la *governance* degli Stati (democratica o meno), sia sullo stesso concetto dello spazio pubblico. Ciò nonostante, da ben trenta anni assistiamo alla nascita di nuovi spazi pubblici, come conseguenza della mutazione funzionale delle città e del passaggio a una “società di massa” sempre più importante.

Questi nuovi spazi pubblici, però, sono sempre stati di ordine infrastrutturale: centri commerciali, stazioni ferroviarie, aeroporti, piattaforme multimodali, zone turistiche accoglienti, nuove zone urbane, grandi stadi e strutture sportive, grandi musei, complessi di divertimento e di cinema. Tutti questi spazi pubblici possiedono le stesse caratteristiche: gigantismo, mescolanza delle funzioni e degli usi (le stazioni vengono ad accogliere eventi culturali, ad esempio), modalità di accesso differenziate, flussi complessi di persone, concentrazione della ricchezza e dell’informazione, mobilità sempre maggiore delle persone e dei beni, afflusso e concentrazione di gruppi a rischio.

Con lo sviluppo delle reti sociali, viene ad aggiungersi un nuovo livello di complessità, che esacerba ancora di più le caratteristiche dello spazio pubblico, specialmente:

1. L’incontro fortuito

Lo spazio pubblico diviene uno spazio per la rappresentazione di se stesso, di messa in scena di se stesso nello spazio. A questo titolo, vi sollecita lo sguardo dell’altro e permette l’avvicinamento o il dialogo.

2. Un luogo di confronto

L’aspetto dell’altro può certo sedurre ma altrettanto provocare. La differenza dell’essere, si suscita uno sguardo curioso e anche la propria accettazione in nome della propria differenza.

3. Un luogo produttore di interazioni

La natura di queste interazioni è molto eterogenea. Mi riconosco nell’altro, non mi riconosco nell’altro e quindi continuo il mio cammino… sono incoraggiato al dialogo… Lo spazio d’interazione è quindi uno spazio di movimenti che si oppone ai concetti di indifferenza, di ripiego su sé stesso e di rifiuto dell’altro.

Lo sviluppo di una dimensione cyber ha ridefinito il quadro delle pratiche individuali e collettive ponendo nuovi riferimenti, soprattutto in termini di *governance* elettronica, e questo sin dalla fine della

BIO

Politologo, il Dr. Frédéric Esposito è Direttore dell’Osservatorio universitario sulla sicurezza e Professore Associato al Global Studies Institute dell’Università di Ginevra. Il suo cursus comprende una laurea e un dottorato ottenuti presso l’Università di Ginevra; in seguito, ha effettuato studi avanzati in relazioni internazionali presso l’Institut universitaire des hautes études internationales et du développement (HEID) e in studi europei presso l’Istituto Universitario Europeo di Firenze, dove è stato ricercatore; è inoltre Professore Associato alla Facoltà di Giurisprudenza dell’Università di Ginevra, e svolge la funzione di direttore esecutivo del programma universitario « Democrazia e terrorismo » promosso dalla Società Accademica di Ginevra. È membro del Consiglio Consultativo di Sicurezza del Cantone di Ginevra. Può essere contattato scrivendo a: Frederic.Esposito@unige.ch

> *L' identità è volontariamente plurale, perché deve portare tanti messaggi quanti sono gli strati che la compongono.*

seconda guerra mondiale[1]. Infatti, l'idea di democrazia elettronica è ben anteriore alla nascita di Internet ed ha conosciuto tre principali tappe di evoluzione. La prima nacque con la fine della seconda guerra mondiale, sotto forma di un modello cibernetico capace di proporre una gestione razionale delle società. Questa "macchina di governo" era basata su di un'utopia, e cioè che i computer potessero gestire migliaia di dati per una miglior *governance* in termini di razionalità e di efficacia. La seconda evoluzione si è prodotta negli anni settanta con l'emergenza della televisione e del video. A tale stadio, ci si immagina lo sviluppo di questi nuovi strumenti tecnici per favorire uno spostamento dei centri di dibattito verso la periferia, migliorando il legame tra eletti e cittadini. Questa teledemocrazia è percepita come uno strumento al servizio delle comunità locali ma anche come un laboratorio di democrazia forte. Bisognerà però aspettare l'inizio degli anni 2000 e l'emergenza delle reti sociali combinate alla globalizzazione per assistere all'avvenimento del livello locale come promotore della democrazia *bottom-up*. Infine, la terza tappa apparve con l'emergenza della democrazia elettronica e lo sviluppo della cyber-democrazia, durante gli anni novanta, con l'idea che il cyber spazio simbolizza l'ultimo stadio dell'auto-organizzazione politica, consacrando il "villaggio globale".

Questo villaggio globale crea un nuovo spazio aperto, de-territorializzato e non gerarchizzato. In altre parole, il cyber-spazio vuole essere un catalizzatore che permetta di sorpassare i sistemi politici e di favorire l'emergenza di un contropotere, o persino di una contro-società.

Nel campo politico, l'avvenimento di una rete globale di protesta illustra questa evoluzione connettendo tra di loro attori e rivendicazioni, come avvenuto nella primavera araba (rivoluzione tunisina, rivolte in Egitto, in Libia, nel Bahrein, in Yemen), ma anche in Europa (Spagna e Grecia). Questi eventi confermano il ruolo cruciale delle reti sociali e, più globalmente, quello della democrazia elettronica in quanto strumento per captare e diffondere le rivendicazioni dei popoli. La e-democracy è diventata un elemento inaggirabile per favorire il dibattito democratico ma non ne è un sostituto, come lo ricordò Hillary Clinton in un suo discorso del 2011[2]: *"The internet has become the public space of the 21st century.What happened in Egypt and what happened in Iran, which this week is once again using violence against protestors seeking basic freedoms, was about a great deal more than the internet. In each case, people protested because of deep frustrations with the political and economic conditions of their lives. They stood and marched and chanted and the authorities tracked and blocked and arrested them. The internet did not do any of those things; people did. In both of these countries, the ways that citizens and the authorities used the internet reflected the power of connection technologies on the one hand as an accelerant of political, social, and economic change, and on the other hand as a means to stifle or extinguish that change".*

Questo potere delle reti può essere illustrato, come ad esempio ha fatto Wael Ghonim, blogger egiziano, all'origine della creazione, su Facebook, del gruppo *"We are all Khaled Said"* in omaggio al giovane connazionale torturato e picchiato a morte da poliziotti ad Alessandria, il 6 giugno 2010. Questo gruppo ha favorito una presa di coscienza della gioventù egiziana per sfidare l'autoritarismo del regime.

In un altro contesto, l'esempio del Presidente filippino Joseph Estrada è anch'esso rivelatore del potere delle reti sociali. Il 17 gennaio 2001, Estrada è oggetto di una procedura di destituzione per corruzione. Ciò nonostante, ottiene l'appoggio del Congresso, che rifiuta di rendere pubbliche prove considerate pesantissime. In meno di due ore, migliaia di Filippini convergono verso Manila all'appello di *"whistleblowers"* che stava denunciando la situazione via SMS, diventando milioni a manifestare nei giorni successivi. La capacità del pubblico di coordinarsi in massa e così rapidamente – si parla di 7 milioni di SMS scambiati in quei pochi giorni – ha fatto piegare la volontà del Congresso, che ha votato di nuovo, questa volta a favore della messa a disposizione delle prove tangibili per i fatti di corruzione. Il 20 gennaio 2001, il Presidente si dimette, considerandosi vittima della "generazione sms".

Questo contropotere conta certo su alcune personalità di spicco, ma viene definitivamente a cancellare ogni pista utilizzando l'anonimato come cavallo di Troia per imporre nuovi comportamenti e nuove regole. Ad esempio, dopo gli attentati del 13 novembre 2015 a Parigi, il gruppo Anonymous ha minacciato lo Stato Islamico con questi termini: "Sappiate che vi troveremo, e che non molleremo nulla. Stiamo per lanciare la più importante operazione mai condotta contro di voi; aspettatevi numerosissimi cyber-attacchi. La guerra è iniziata, preparatevi".

Anonymous aveva già *"dichiarato la guerra"* allo Stato Islamico in seguito agli attentati contro Charlie-Hebdo e l'hyper-casher (7-9 gennaio 2015). Da allora, il gruppo di hackers ha pubblicato nel marzo del 2016 una lista di 9200 account Twitter associati, secondo loro, allo Stato Islamico, con lo scopo di spingere la rete sociale a eliminarli per avere, come solo obiettivo *"un serio impatto sulla capacità dello Stato Islamico di diffondere la sua propaganda e reclutare nuovi membri"*.

L'attività degli Anonymous pone interrogativi, perché agendo in nome dell'interesse generale, diventano una sorta di "sceriffi del web". Possiedono il proprio sistema di valutazione e di valori, che non risulta

chiaro se disturba oppure aiuta il contro-terrorismo. L'immagine del gruppo, quella della maschera ispirata sia dal rivoluzionario inglese Guy Fawkes, che progettò un attentato contro il parlamento di Londra 407 anni or sono, sia da un comic ("V come Vendetta"), è ormai diventata un simbolo della contestazione e dell'anti-sistema.

Il cyber-spazio può quindi comporre un'immagine senza definirla. Il gruppo terrorista Daesh si è dotato di un'identità visuale basata su una serie di video testimonianze della sua capacità militare (immagine 1), della sua capacità d'infiltrazione (immagine 2), della distruzione di beni culturali e della barbarie.

Immagine 1: convoglio di combattenti di Daesh

Immagine 2: foto che illustra la creazione di una cellula dormiente in Marocco, destinata a preparare attentati

L'identità è volontariamente plurale, perché deve portare tanti messaggi quanti sono gli strati che la compongono. Infatti, il messaggio va adattato in funzione del pubblico mirato per diventare a sua volta religioso, politico, sociale o culturale. Nel primo caso (Anonymous) come nel secondo (Daesh), l'immagine che viene cosi creata è difficile da inquadrare perché diventa uno stendardo per cause e progetti portati da individui dalle motivazioni molto diverse. Si costruisce e si decostruisce nello stesso tempo.

Le imprudenze della nostra vita digitale, nel contesto della società globalizzata e dei suoi soprassalti, ridefiniscono senza il minimo dubbio la nostra identità. Infatti, le reti di contestazione sono globalizzate e diviene difficile conoscerne tutti gli attori. Da Anonymous a Daesh, attraversando tutti i gruppi più 'tradizionali' della società civile, l'identità numerica sconvolge le regole del gioco democratico e modifica il concetto stesso di sicurezza.

Con lo sviluppo dell'IoT che non pochi qualificano come 4a rivoluzione industriale, col formidabile potenziale di interconnessione tra individui, oggetti, infrastrutture (trasporti, energia…) si sta disegnando di fatto uno "spazio identitario" incontrollato. Appare quindi fondamentale fissarne le regole in modo di non farci imporre le componenti della nostra propria identità. ■

1 *Thierry Vedel, « L'idée de démocratie électronique: origines, visions, questions », in Pascal Perrineau, Le désenchantement démocratique, La Tour d'Aigues, L'Aube, 2003, pp. 243-266.*

2 *Hillary Clinton, « Internet Rights And Wrongs: Choices & Challenges In A Networked World", conferenza tenuta alla George Washington University, li 15 Febbraio 2011 (http://www.state.gov/video).*

"La cyber security deve seguire la stessa crescita in termini di educazione della compliance"

Intervista VIP con Mohit Davar, Presidente dell'International Association of Money Transfer Networks

Mohit Davar

Autore: **Norman Frankel**

È passato ormai un anno dal famoso cyber hackeraggio della Bangladesh Bank. Ricordiamo che nel febbraio 2016, la Banca Centrale del Bangladesh ricevette via rete SWIFT l'ordine di trasferire 951 milioni di dollari in diversi conti bancari dello Sri Lanka e delle Filippine. I media riportarono che gli attacchi sulla stessa proseguirono durante tutto il 2016.

Considerando le similitudini tra il SWIFT e le compagnie di *money transfer*, siamo stati ricevuti da Mohit Davar, Presidente dell'International Association of Money Transfer Networks (IAMTN), e abbiamo discusso con lui delle lezioni apprese dai membri dell'IAMTN dai cyber-attacchi su SWIFT per prevenire reati similari sui loro sistemi. Ne abbiamo approfittato per chiedere a Mohit Davar qual è la sua visione sullo stato attuale della sicurezza SWIFT.

Mohit Davar: Sono sicuro che ogni volta che succede un caso come quello che ha menzionato, la SWIFT programmi controlli sempre più fitti sia nelle procedure che nei sistemi, per contrastare quanto accaduto. Naturalmente, questo non garantisce che non succeda qualcosa di nuovo, ma penso che il challenge per SWIFT come servizio di messaggeria è, in fin dei conti, che la qualità dei suoi sistemi sia buona quanto quella delle banche che lo usano. Ad esempio, se degli attacchi succedono perché la banca X nel paese Z non ha eseguito i controlli adeguati, allora il sistema SWIFT rimane vulnerabile a larga scala, perché la porta d'entrata è aperta. Questo è un challenge che richiederà tempo per essere risolto, fino a quando tutte le banche non faranno i dovuti upgrade ai loro sistemi e li renderanno sicuri.

È un challenge simile a quelli affrontati dalle compagnie di *money transfer,* in particolare quelle che lavorano con agenti: possono avere il miglior livello di sicurezza del loro sistema, ma se i sistemi degli agenti non sono sicuri, esiste sempre la possibilità che qualcuno entri illegalmente usando la porta lasciata aperta dall'agente. Questo è il vero rischio.

Norman Frankel: Esistono tipi precisi di attacchi dei quali gli operatori di money transfer dovrebbero essere a conoscenza, e a quali dovrebbero dare la priorità quando fanno la valutazione dei loro bisogni in cyber security?

Mohit Davar: Quando ero in Medio Oriente c'erano tanti attacchi agli agenti che avevano accesso loro stessi ai sistemi di *money transfer*. I sistemi di transfer potevano essere piratati perché gli agenti vi accedevano attraverso siti web che non avevano veri e propri controlli firewall. Gli hacker penetravano allora nei sistemi delle compagnie di *money transfer* e vi eseguivano delle transazioni fittizie. E potevano veramente creare una transazione, diciamo da Dubai verso il Kenya, rendendo disponibile il denaro in Kenya. Nonostante queste transazioni fossero fittizie, l'agente e la compagnia di *remittance* perdevano soldi. Insisto su questo aspetto perché era qualcosa che avveniva spesso mentre parliamo di un'epoca che non usava veramente il digitale ma ancora il modello tradizionale dell'agenzia.

L'industria del *money transfer* si è recentemente spostata massicciamente dal tradizionale al digitale. E quando ci si muove nel mondo digitale, ci si espone sempre e sempre di più ai cyber attacchi, essendo la nostra vulnerabilità più alta di prima.

Norman Frankel: Esistono compagnie di money transfer preparate ad affrontare questa vulnerabilità che va sempre crescendo?

Mohit Davar: Secondo me, nel mondo del *money transfer* in generale, la cyber security non viene presa così sul serio come dovrebbe. Spesso, o non è considerata

una problematica , oppure lo è solo per la zona sotto il controllo del dipartimento IT, quindi non è realmente tenuta in considerazione come dovrebbe, ovvero una problematica chiave per il CEO ed il consiglio d'amministrazione.

Norman Frankel: Quali sono i Suoi consigli in questo campo?

Mohit Davar: Penso che le compagnie dovrebbero prendere sul serio la *cyber security* e credo che deve essere affrontata esattamente come la *compliance*.

Se si risale a prima del 9/11, anche la *compliance* non era considerata una problematica. Questa industria non era veramente regolamentata, e questo aspetto non veniva considerato nei piani di nessuno. E poi venne una nuova fase, quando la *compliance* divenne un obbligo e abbiamo tutti dovuto accettarlo, non c'era scelta. Ora siamo in una fase dove è appena stata integrata completamente e fa parte del nostro business giornaliero. Oggi, più lei è *compliant*, e più ha in mano un vantaggio competitivo, non solo verso i clienti, ma anche verso le sue banche e altri stakeholder.

Penso che la *cyber security* deve attraversare lo stesso diagramma di educazione. Forse proprio adesso i responsabili si trovano tra la fase del *"ci pensiamo grosso modo"* e quella del *"è una faticaccia, ma dobbiamo affrontarla"*. Ma non è sufficiente.

Dovrebbero tutti realizzare che questa è una parte del puzzle del nostro business, e, esattamente come un negozio pieno di cash sarebbe sottoposto a strettissima osservazione nel mondo della sicurezza fisica, un operatore che esegue transazioni online non dovrebbe anche essere attentissimo alla *cyber security*, giusto? Questo sarà uno dei rischi maggiori che bisognerà identificare e affrontare, ma non credo che sia già nella cultura delle aziende. L'unico momento in cui pare diventare una priorità è quando si è colpiti e c'è un problema, e allora è troppo tardi.

Norman Frankel: Che tappe pratiche raccomanderebbe ai membri dell'Associazione che presiede - e alle compagnie di money transfer in generale - per affrontare questa problematica?

Mohit Davar: Credo che sia una minaccia reale per il loro business, e quindi non dovrebbero scartarla, ma al contrario inserire la cyber security nell'agenda dirigenziale e farne una priorità.

Dovrebbero sia costruire le proprie capacità di sicurezza all'interno dell'azienda– il metodo che seguono le grandi compagnie – oppure affidarla in outsourcing ad aziende specializzate come l'iCyber-Security Group ed altre. Dovrebbero almeno fare dei *penetration test* e avere controlli annuali sulla robustezza dei propri sistemi di sicurezza, visto che ormai le minacce che sono sul mercato hanno un'evoluzione rapidissima.

Dovrebbero anche ingaggiare dei consulenti che possano dare loro il conforto di sapere che i loro sistemi sono sicuri – o che, se non sono sicuri, che possano portarli rapidamente al livello necessario per effettuare tutti i controlli necessari per prevenire il successo di cyber-attacchi. In più, come detentori di dati dei clienti, devono essere a norma con la legislazione, e questo diventa un grande problema se il sistema viene violato.

Norman Frankel: In Europa le regole sulla protezioni dei dati cambiano a maggio del 2018, quando l'EU General Data Protection Regulation (GDPR) sarà applicabile, e multe cospicue sono previste per le aziende che non saranno compliant con queste nuove regole, in particolar modo per non aver rivelato l'esistenza di data breach. Secondo Lei, le compagnie cambieranno atteggiamento per quello che riguarda le "disclosures"?

Mohit Davar: Penso che lo faranno, non è un problema. Il challenge è che non appariranno mai in pubblico, perché nessuno vuole che i clienti sappiano cos'è successo, come nessuno vuole che i clienti perdano la fiducia nei propri servizi. Quindi, faranno una dichiarazione al regolatore, ma questa non verrà resa pubblica. Se iniziamo invece a dire che la disclosure dovrebbe essere pubblica – in tal caso avrebbe un impatto diretto sulla loro reputazione, e quindi sul volume degli affari – allora forse le compagnie prenderebbero tutto ciò in modo molto più serio.

Credo che ogni operatore di Money Transfer d'Europa dovrebbe fermarsi attentamente su queste norme e assicurarsi della sua compliance. Soprattutto perché oggigiorno queste norme hanno un senso anche per gli operatori di Money Transfer fuori Europa, se sono usate come punto di partenza o di riferimento o come buone pratiche. Gli USA hanno anche loro adottato nuove ammende per i data breach che riguardano cittadini americani, e che possono arrivare a 2 milioni di dollari. Siccome tantissime operazioni provengono dagli USA, questo fatto anche preso da solo dovrebbe essere una motivazione supplementare per l'industria nell'adozione di buone pratiche nel lavoro quotidiano. ■

BIO

Mohit Davar è un esperto in pagamenti e lavora nel settore da più di 25 anni.
Ha iniziato la sua carriera presso Sedgwick Noble Lowndes (dipartimento *internal audit*) per poi trasferirsi al Thomas Cook Group, (dipartimento *corporate finance*). Nel 1997, il suo apporto è stato significativo nella realizzazione della *joint venture* tra MoneyGram Inc. (compagnia listata alla NYSE) e Thomas Cook. Ha poi diretto questa *joint venture* fino al 2003, quando i 49% di azioni in possesso della Thomas Cook sono stati rivenduti alla MoneyGram, realizzando una cospicua plusvalenza. Ha, inoltre, creato la Travelex Money Transfer, una filiale di Travelex Group. Quest'ultima è stata comperata dalla Coinstar Inc. (compagnia listata alla NASDAQ) nel 2006. Ha continuato a trasformare Coinstar Money Transfer in una compagnia di *remittance* di successo globale, per poi venderla alla Sigue Financial Corporation nel 2011. In quel momento, Mohit Davar ha aperto la sua propria agenzia di consulenza e strategia a Dubai. Ha partecipato al consiglio d'amministrazione di Eastnets, ufficio di servizi swift a Dubai, ed è stato attivo in numerosi progetti di *payment / mobile wallet* nella regione. É adesso nel consiglio d'amministrazione e consulente per numerose compagnie di payment. Mohit è Presidente dell'International Association of Money Transfer *(remittance trade body)* e membro dell'Institute of Chartered Accountants per l'Inghilterra ed il Galles.

Vecchi comportamenti ma risorse umane sfasate dalla loro variante 4.0

Autore: Laurent Chrzanovski

In questi mesi, i lavori di gran parte degli specialisti europei della cyber security e i loro risvolti mediatici destinati al grande pubblico si sono focalizzati su tre punti chiave: la guerra globale di info-intox 4.0 e le sue conseguenze sui nostri ecosistemi, le lezioni da trarre da WannaCry e da GoldenEye e, infine, le ultime normative europee (GDPR, PSD2, NIS) e il da farsi per essere *compliant* rimanendo resilienti.

A giocare, purtroppo, il ruolo di cenerentola in questo quadro multinazionale sono, più che mai, le relazioni interumane nella vita professionale e privata nella loro "variante digitale". Le risorse umane delle aziende e delle amministrazioni statali, alle quali spetta il compito di selezionare impiegati idonei e di risolvere i conflitti interpersonali tra i dipendenti, hanno difficoltà ad applicare certe dinamiche del mondo fisico a quello digitale. Come molte altre categorie professionali preesistenti al web, le "HR" sono state colpite dal falso quanto pesante preconcetto che sin dal "2.0" aveva cambiato tutto ovvero che l'anonimato di certi comportamenti indecenti, se non criminali, faceva si che questi, anche se palesemente effettuati *intra muros*, non erano più di loro competenza perché mancano le prove oggettive per determinarne gli autori.

Lo stesso vale anche, in grande parte, per le autorità di sicurezza dello Stato che hanno il compito di risolvere i reati perpetrati a danno dei singoli cittadini. In questo campo, gli agenti addestrati a capire il *modus vivendi* legato alla trasformazione digitale sono ancora, in tutta Europa, ultra-minoritari in paragone con gli agenti formati "all'antica", cioè usi a risolvere casistiche legate a reati svolti nel mondo fisico. Tra le forze statali osserviamo però due campi che si sono quasi completamente "digitalizzati", grazie a enormi dotazioni tecniche e umane, ovvero i servizi volti a combattere la pedofilia online e a contrastare le frodi finanziarie in rete.

In questo contesto, la lettura del primo studio esaustivo sulla violenza sessuale digitale contro le donne adulte, ci lascia con un amarissimo gusto di ribellione e di costernazione. Illustrata con centinaia di dati concreti, casistiche reali e il loro triste decalogo di vittime umane, la ricerca di Anastasia Powell e Nicola Henry[1] ci offre un capolavoro pionieristico ed esaustivo. Lo studio molto preciso è tratto dall'analisi parallela delle realtà di due Stati: il Regno Unito e l'Australia, scelti sia per la mole dei documenti disponibili (sinora quasi interamente trascurati) sia per le loro diversità socio-culturali.

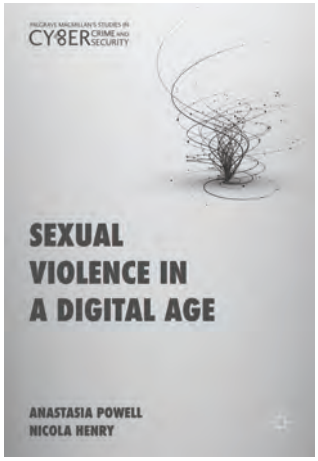
É da lodare già l'idea stessa di scegliere un paese importante della "Vecchia Europa", con una cultura e una mentalità ancorata ad un ricchissimo passato statale, morale, filosofico e giuridico, e un "Paese nuovo" con una propria cultura dove spicca un'importante componente adattativa, destinata a corrispondere al meglio ad una realtà sociale costituita da un *"melting pot"* multiculturale di successo in permanente mutazione.

Come viene sottolineato dallo studio, il vettore digitale non ha né fatto nascere né visceralmente cambiato la natura delle offese e dei crimini a carattere sessuale: li facilita e ne amplifica la profusione, accentuando il

BIO

Professore Universitario di archeologia, storia e sociologia, Laurent Chrzanovski dirige ricerche nel quadro della Scuola dottorale e post-dottorale dell'Università di Sibiu. Regolarmente invitato a tenere corsi nelle maggiori università europee, è autore/editore di 18 libri e più di un centinaio di articoli scientifici, ai quali vanno aggiunti innumerevoli articoli destinati al grande pubblico. Nel campo della cyber-security, si è specializzato nello studio antropologico dei comportamenti individuali nell'uso delle nuove tecnologie; è membro e consulente contrattuale del "Roster of Experts" dell ITU e di numerosi gruppi di lavoro in Romania ed in Svizzera. Ha fondato e dirige il congresso annuale "Cybersecurity in Romania. A macro-regional public-private dialogue platform", dal quale è nata l'idea della rivista Cybersecurity Trends, nel quadro della quale svolge il ruolo di redattore capo.

vittimismo delle vittime che, colpite nel mondo digitale e non quello fisico, sono ancor meno propense a denunciare il fatto.



Molto importanti risultano essere i dati dalle analisi: ormai, la violenza sessuale si esprime in Australia, UK e USA nel mondo del lavoro con una percentuale uguale a quella del mondo casalingo o di quello della famiglia in senso più esteso (tra 6 e 8% dei casi) (p. 249), anche se la percentuale rimane ridotta rispetto a quella delle stesse violenze a opera di sconosciuti (tra i 38 e 27 % dei casi) o di amici /conoscenti (tra 26 e 18% dei casi).

Vediamo qui una ripartizione che fa drammaticamente salire gli abusi sul luogo del lavoro e nella propria cerchia di conoscenze, rispetto a un mondo predigitale dove le violenze coniugali erano predominanti, assieme alle violenze subite da parte di sconosciuti. L'anonimato e la relativa difficoltà di prevenire il passaggio all'atto spingono naturalmente gli istinti più bassi di persone conosciute e la barriera fisica viene a sparire.

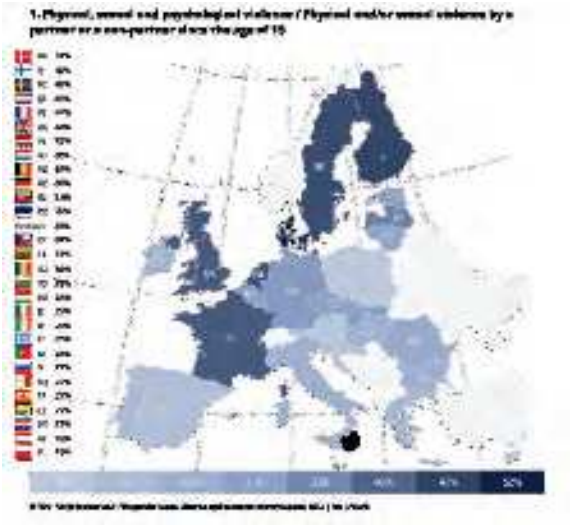
Lo studio ribadisce anche l'ineguaglianza socio-professionale tra uomini e donne, che sentiamo troppo spesso negare o minimizzare. Ora, se teniamo conto che lo studio è stato eseguito in paesi anglosassoni, non osiamo nemmeno immaginare i risultati di uno studio similare in paesi più «maschilisti». Purtroppo gli Stati, ben lungi dal trovare nel digitale una delle soluzioni per ridurre questa ineguaglianza, ne hanno potenziato loro malgrado le motivazioni accettando la profusione di manifesti di *"gender hate"*.

Peggio ancora, un paese come l'Australia, che è pioniere nella prevenzione del bullismo e del *sexting / grooming* per il mondo dei minori (bambini e adolescenti) con risultati tangibili e miglioramenti reali anno dopo anno, può servirci da esempio per quanto nociva sia stata, quasi ovunque, la scelta di creare con minori e adulti due nicchie distinte mentre i problemi sono quasi tutti uguali. Per chiara volontà politica e mancanza di lungimiranza, i mezzi tecnici e umani sono così stati massicciamente impiegati esclusivamente per la protezione dei bambini e degli adolescenti, lasciando a poche ONG il compito di svolgere una missione quasi identica nel mondo, molto più poliforme e meno strutturato, degli adulti.

Come riassumono bene gli autori alla fine del volume, *"Communications technologies gives us a frightening glimpse into the deeply embedded racial, gendered, class and sexual prejudices that continue to permeate the collective consciousness; paradoxically they alsooffer a provocative assortment of tools and platforms for facilitating vigilantism, activism and informal justice."* (p. 290).

Se veniamo ora all'Italia, osserviamo che non è troppo tardi per agire, contrariamente ad altri Stati, perché è uno dei paesi europei che vanta tra i più bassi tassi reali di violenza contro le donne (i.e. analisi fatte sulla base dei ricoverati o morti/popolazione e non a denunce penali / popolazione) e possiede pure una posizione in classifica ben sotto la media europea in quello che riguarda i tassi analitici eseguiti dalla FRA su di un campionario di 43'000 donne[2] (Agenzia dell'Unione Europea per i Diritti Fondamentali).

Ci vuole però, come sottolinea lo studio citato, una volontà comune dello Stato e del settore privato. L'analisi di Anastasia Powell e Nicola Henry dimostra bene che per agire contro il fenomeno aggravato dall'uso dei media



digitali, si possono usare proprio gli stessi media, facendo quello che gli anglosassoni chiamano *"digital justice"* o *"justice through recognition"*. In tale modo, sia l'elaborazione con le vittime di testi di prevenzione che, soprattutto, la diffusione di esempi di vittime possono sensibilizzare rapidamente ed efficacemente un pubblico molto ampio: è il fenomeno del *"survivor selfie"* che, aiutato da ONG e gruppi di volontari, prende una dimensione virale.

Il sistema accademico dovrà riformarsi rapidamente in modo da proporre al mercato specialisti in Risorse Umane al passo con le tecnologie e coi danni che queste possono portare all'interno di un ecosistema professionale[3].

Tale ruolo potrebbe essere svolto in partenariato con CISO e CSO che, a loro volta, lottano contro le varie forme di spionaggio industriale e di hacking che usano come vettore principale proprio le vulnerabilità umane degli impiegati tramite tecniche di ingegneria sociale.

Sebbene, come sottolineato dagli autori, dal preambolo alle conclusioni, il volume costituisce un *"technofeminist and criminological framework"*, i suoi metodi, la sua pertinenza, e, last but not least, il modo esaustivo di affrontare il fenomeno della violenza sessuale contro le donne, sono un elemento fondamentale per chi deve assicurare il benessere e la buona interazione socioprofessionale del personale. La concretizzazione della violenza, come il suicidio, hanno un lungo percorso digitale, che influisce in modo deleterio sin dal primo giorno nell'ambiente dove lavora la vittima e, forse, pure l'aggressore. ■

1 Anastasia Powell, Nicola Henry, Sexual Violence in a Digital Age (PalgraveStudies in Cybercrime and Cybersecurity), Melbourne 2017 (323 pp.)
2 http://fra.europa.eu/en/publications-and-resources/data-and-maps/survey-data-explorer-violence-against-women-survey
3 In questosenso, tragliesempiimplementati, si veda il programma pionieristico e trans-disciplinaredellaRutgersUniversity (NJ, USA) : http://endsexualviolence.rutgers.edu/

web for your business
swiss webacademy

together with:

Ville de Porrentruy
Histoire Vie Nature Formation

Presents:

CYBERSECURITY SWITZERLAND CONGRESS
1st Edition

ITU

Western European Public-Private Dialogue Platform

December 7-8, 2017, Porrentruy, Switzerland

https://cybersecurity-switzerland.ch

Your direct contacts:

Dr. Jean-Jacques Wagner, IUT de Belfort-Montbéliard
jean-jacques.wagner@univ-fcomte.fr
+33 (0)6 75 86 31 64

Prof. Dr. Laurent Chrzanovski, Conference Manager
l.chrzanovski@icloud.com
+40 730 362 544

Luca Tenzi, Corporate Security Senior Advisor
tenzi.luca@gmail.com; luca.tenzi@itu.int
+41 (0)79 249 48 49

Arnaud Velten, Expert en stratégie et tactiques digitales
arnaud.velten@gmail.com
+33 (0)6 49 57 71 20

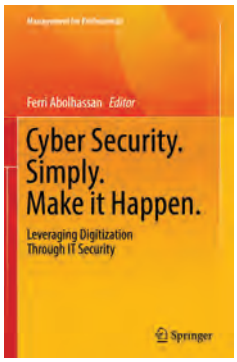
Proteggere i bambini on-line è una sfida globale che richiede un approccio globale. Mentre molti sforzi per migliorare la protezione online dei bambini sono già in corso, la loro portata finora è stata più di carattere nazionale che globale. L'ITU (Unione Internazionale delle Telecomunicazioni) ha avviato l'iniziativa Child Online Protection (COP) per creare una rete di collaborazione internazionale e promuovere la sicurezza online dei bambini in tutto il mondo. COP è stato presentato al Consiglio ITU nel 2008 e approvato dal Segretario generale dell'ONU e da capi di Stato, Ministri e capi di organizzazioni internazionali provenienti da tutto il mondo.
Poste Italiane, insieme alla propria Fondazione GCSEC e alla Polizia Postale e delle Comunicazioni ha prodotto la Versione italiana delle linee guida ITU, guida per la protezione dei bambini nell'uso di Internet e guida per genitori, Tutori ed insegnanti per la protezione dei bambini nell'uso di Internet.

Scaricatele su: www.distrettocybersecurity.it/linee-guida-itu

www.itu.int/cop

Bibliografia - Cybersecurity Trends

Ferri Abolhassan (ed.), **Cyber Security. Simply. Make it Happen. Leveraging Digitization Through IT Security**, Cham 2017 (Springer), 136 pp.



Questo volume, pubblicato e promosso da Telekom Germania, è probabilmente uno dei migliori *vademecum* per dirigenti che abbiamo letto fino ad oggi. In meno di 140 pagine, i suoi autori riescono a guidare il lettore attraverso tutti i temi di base della Cyber security odierni. Offrono così, ad ogni dirigente non-tecnico, uno strumento fondamentale, non solo per capire la situazione attuale, ma anche per riflettere sulle sue responsabilità e quelle della struttura a lui subordinata, e quindi come migliorare la propria resilienza personale nonché fare le scelte giuste per aumentare il livello di sicurezza dell'intera struttura. Il testo, redatto in uno stile chiaro e gradevole, segue un filo d'Arianna impeccabile, dove ogni argomento non solo è correlato con quanto scritto nelle pagine precedenti, ma soprattutto è spiegato con esempi reali e comprensibili per tutti.

Ripetuto numerose volte in ogni capitolo, troviamo un argomento di peso che viene a facilitare la benevolenza dei dirigenti durante la lettura: una buona sicurezza non è per forza né costosa né tantomeno un freno alla qualità ed alla velocità del buon rendimento della struttura. Se analizziamo il solo indice del volume, appare subito lodevole il fatto che è stato pensato per chi ha poco tempo: quasi tutti gli argomenti che "parlano" al manager sono riassunti nelle prime 26 pagine, in modo speciale gli aspetti di sicurezza legati alla transizione al Cloud, alla protezione dei dati e alle regolamentazioni in vigore. Questi punti, ed altri ancora, vengono poi dettagliati, insistendo permanentemente su due aspetti: la fiducia da raggiungere nei prodotti e nei prestatori terzi all'azienda (e le chiavi per valutare se accordare o meno questa fiducia) e l'ormai sempiterno bisogno di rinforzare quanto più rapidamente la resilienza del fattore umano, da risolvere con l'offerta a tutti gli impiegati di cursus modulabili di sicurezza, dalla prevenzione alla formazione. Molto pertinente è la sezione che spiega come motivare gli impiegati a seguire tali trainings e come renderli molto gradevoli (dal *gaming* al *team-building* a *role-play* in esercizi di crisi). Non è omessa, ovviamente, la minima expertise che dovrebbe ormai possedere ogni dirigente.

In seguito viene spiegato con cura cosa sono le grandi sfide di oggi: cos'è il *trattato Safe Harbour,* quali sono le leggi e le normative dell'UE e le loro conseguenze.

L'ultimo quarto del libro insiste in modo molto *"business oriented"* sui criteri per capire, nel vasto campo della cyber security, cosa si può affidare a terzi (outsourcing), quando è conveniente e con quali criteri di fiducia, ed invece cosa non dovrebbe mai essere esternalizzato. Si spiegano infine ai dirigenti quali sono debolezze potenziali di ogni ecosistema professionale, ovvero le porte semi-aperte grazie alle quali i criminali riescono ad infiltrarsi in un'azienda. Questo passaggio è essenziale nel quadro tracciato prima: outsourcing, *plug and play security*, ma a condizione sine qua non (e non a discapito!) di avere un CSO ed una équipe di sicurezza ben allenata all'interno dell'azienda.

Le ultime pagine spiegano le evoluzioni osservate nel campo dei pericoli online e sulle capacità degli hackers che vanno sempre crescendo, tutto ciò per ricordare che non è assolutamente difficile capire le basi della cyber security e implementarla in modo efficace senza intaccare né il budget né il buon funzionamento dell'azienda se l'implementazione è costante, progressiva, tecnica e umana. Il volume si chiude con esempi magistrali di quanto sono invece costati, in termine di immagine e di denaro, incidenti recenti che hanno colpito aziende impreparate, danni ai quali ormai si aggiungeranno multe e processi in tutta Europa in caso di data leak e di non compliance…

Thomas J. Holt, Olga Smirnova, Yi-Ting Chua, **Data Thieves in Action. Examining the International Market for Stolen Personal Information**, New York 2016 (Palgrave Macmillan), 164 pp.

Questa ricerca meramente scientifica, con abbondanti risorse bibliografiche, ha il vantaggio di offrire uno dei primi studi approfonditi ed esaurientemente documentati a tutti i lettori desiderosi di sapere dove finiscono i dati rubati e perché – soprattutto quelli a carattere economico o medico – sono diventati così attraenti, proponendo pure una gamma precisa dei loro valori sul mercato, appoggiati da cifre reali tratte dal *deep/dark* web sul valore preciso di molti tipi di dati in funzione delle persone e dei paesi.

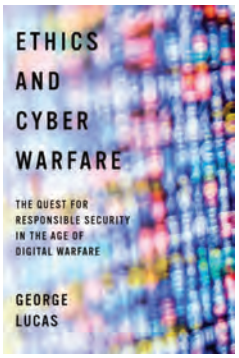
Dall'analisi sul "prezzario" di tutti i tipi possibili di dati (dalla semplice carta di credito, in funzione del paese e della banca dov'è stata rilasciata, al *fullx* che include pure il codice PIN, sino ad exploits complessi nei sistemi di *money-transfer*) realizziamo subito quanto sono cospicui i ricavi dei criminali che operano nel settore.

In seguito, si analizzano i costi economici ed i rischi affrontati da ogni attore. Multe ed onta per la ditta vittima di una perdita di dati, mercato quasi senza rischio di migliaia di dollari ad operazione per i rivenditori di dati, ed invece numerosi problemi per gli acquirenti di dati rubati: possono ricavarne milioni o essere a loro volta vittime di un raggiro.

Il vantaggio dell'opera risiede nel farci capire che, per quanto illegale e complessa è questa attività, dipende anch'essa da un sistema di business arci-classico dove contano la fiducia tra il venditore e l'acquirente, le variazioni frequenti dei prezzi e quindi dei benefici possibili in funzione delle lingue, dei paesi, della macro-economia e di molti altri parametri. Affinando la ricerca, gli autori spiegano l'organizzazione sociale, molto complicata, dell'ecosistema del mercato illegale dei dati. In riassunto, questo volume farà senz'altro storia: pur senza riuscire l'impossibile – ovvero dare un'estimazione credibile delle perdite annue per l'economia reale direttamente

generate dal furto di dati – permette una prima documentatissima immersione in questo mondo criminale, facendoci capire i suoi modi di funzionare, i suoi modelli di interazioni, e la natura dei rapporti tra i suoi vari attori.

George Lucas, **Ethics and Cyber Warfare: The Quest for Responsible Security in the Age of Digital Warfare**, Oxford 2016



Un anno dopo la pubblicazione, come editore, del fondamentale *Routledge Handbook of Military Ethics* (2015), George Lucas ci offre una rivista completa del rapporto tra etica e realtà del mondo cyber. Il testo è così appassionante che ad ogni pagina invoglia il lettore a saperne di più continuando a leggere. L'autore sa combinare con brio uno stile a dir poco straordinario con asserzioni choc e non raramente commentari cinici, illustrati da centinaia di esempi reali. Il concetto di base di Lucas è che, esattamente come gli eserciti devono ormai combattere quasi esclusivamente contro nemici non-convenzionali e quindi adattare le proprie regole etiche di guerra – o talvolta persino rinunciarvi – il campo del "cyber" è un altro mondo dove gli Stati, gli eserciti, le agenzie di intelligence, ma anche ogni individuo deve imperativamente riconsiderare le sue convinzioni morali. Dopo aver tracciato il grande quadro delle principali minacce di chi sa usare il cyber warfare, il testo ci incita ad imparare a distinguere le attività criminali da quelle legate al warfare, e si domanda non senza ironia se esiste ancora un ruolo per l'etica e la legge in un cyber conflitto. Impariamo a seguito quali sono per il mondo anglosassone i diversi tipi di "etica" che si affrontano: la "Folk Morality", i quadri legali e normativi, e la teoria del "Just war". Questa descrizione è utile per situare il dibatto e tornare alla base fondatrice di qualsivoglia etica: una morale comunemente accettata. Con un cinismo dichiarato, ci richiama alla filosofia greca nel capitolo *"If Aristotle Waged Cyberwar: How Norms Emerge from Practice"*, per ribadire che solo da una morale comune già adottata nei comportamenti quaotidiani può emergere un consenso sull'etica. A seguire, insiste sulla forma mentis sbagliata che molti hanno oggi, ovvero di considerare leggi e norme sullo stesso piano. Indica in particolare il mondo degli affari, dove regna una tremenda confusione in funzione dei settori di attività, e dove spesso i regolamenti sono considerati a torto come leggi. Lucas insiste sul fatto che in tutta la storia umana, ci sono stati motivi ben precisi, in *governance* pubblica, nella scelta di inserire un obbligo o un altro nel testo di una legge, di un regolamento o di una direttiva.

L'ultimo terzo del volume ci immerge nel dilemma morale causato dal desiderio di anonimità che va al contrasto di quello di privacy. Le problematiche legate ad ognuno di questi concetti fanno che, nel campo della cybersecurity, anonimato e privacy sono diventati veri e propri antagonisti, contrariamente alla credenza diffusa nell'opinione pubblica.

La fine del libro, volontariamente polemica per incitarci alla riflessione sull'etica che ognuno di noi dovrà trovare, analizza la morale e l'etica sia dei *"whistleblowers"* che della NSA e di altre agenzie di intelligence. Lucas spiega che se volessimo essere coerenti, dovremmo considerare tutte e due le categorie come immorali, ognuna nella sua propria ricerca di "essere morale", come ben sottolinea con una affermazione senza appello: *"And so - like all those who wage war, use deadly force against other human beings, lie, cheat, and steal - Mr. Snowden must be called to account for his actions".*

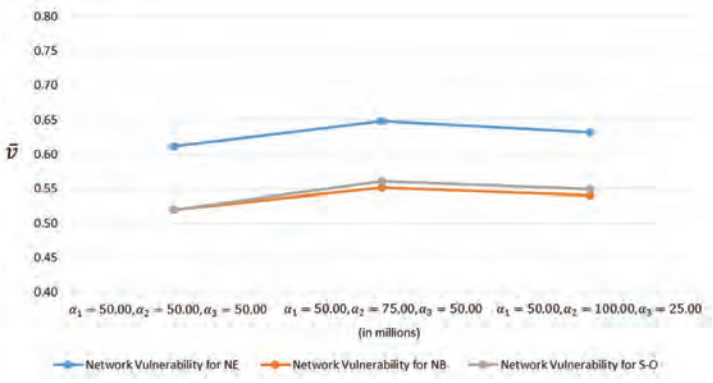
Questo libro è semplicemente un "must" per tutti quelli interessati a capire i bisogni vitali di mettere a punto almeno una dose ad *minimam* di morale e di etica nel campo digitali. Come afferma, giustamente, questa riflessione è vitale per noi europei. Vogliamo continuare ad essere i custodes della democrazia? Allora dobbiamo capire che un sistema che implica oneri e doveri sia per lo Stato che per i cittadini, è nato e può funzionare solo su di una base morale ed etica stabilita e nota a tutti. Lucas ci offre poi un decalogo vastissimo di chiavi per riuscire a rispondere positivamente a questa domanda, sottolineando che né i "policy makers", né tantomeno nessuno di noi cittadini avremmo nulla da "perdere" avendo un quadro etico, che al contrario potrebbe diventare una vera e propria arma supplementare per difenderci nel quadro globale della cyberwar e del cybercrime.

A. Nagurney, S. Shukla, **Multifirm models of cybersecurity investment competition vs. cooperation and network vulnerability**, in European Journal of Operational Research 260 (2017) 588–600

L'analisi matematica e dettagliatissima proposta dagli autori viene de facto ad offrirci la prima dimostrazione reale che lo scambio di informazioni sulle vulnerabilità, anche tra competitori, è l'arma più efficiente nella crescita della resilienza ed anche nell'economia di somme importanti, che vengono spesso spese in modo sbagliato (da capirsi come la creazione di un *"security competitive advantage"*), che potrebbero allora essere usate per scopi molto più utili. Facendo astrazione degli algoritmi ed altri diagrammi ad uso degli addetti ai lavori, l'articolo brilla per i suoi riassunti grafici che parlano da sé. Essi dimostrano senza equivoco possibile, con simulazioni di situazioni reali con ditte reali, che le vulnerabilità della rete sono nettamente più ridotte se le ditte decidono di adottare un sistema di *"Nash Bargaining"* (NB) – cioè scambiarsi regolarmente informazioni utili in un modo che non danneggi né la loro propria sicurezza né il vantaggio che hanno se usano il sistema *"Nash Equilibrium"* (NE) – ovvero scambi di informazioni scarsi o nulli. Una "terza via" è pure esaminata, quella del *"system-optimization"* (S-O), dove tutte le capacità cyber "ideali" di una ditta vengono portate al massimo, con uso massiccio di risorse. Ma, anche in questo scenario, i risultati si rivelano peggiori in paragone a quelli ottenuti se si adotta uno scambio di informazioni equo per tutti gli attori (idealmente un PPP).

Alla fine del testo, troviamo le economie realizzate dall'adozione di un framework cooperativo. Non sembrano a prima vista molto grandi, ma se vengono associate con una resilienza nettamente aumentata, costituiscono un punto supplementare a favore dell'assioma che

Bibliografia - Cybersecurity Trends



non solo lo scenario collaborativo funziona, ma che produce pure benefici:

„An increase as high as 1.24 million in expected utility was observed for Target and 1.25 million for Home Depot if NB was employed instead of NE (…) Increases as high as 2.61 million for JPMC, 2.24 million for Citibank, and 4.25 million for HSBC in expected utility were observed if NB was adopted in place of NE".

Non vi sono dubbi che questo studio diventerà uno degli argomenti più solidi nonché incontestabili venendo ad aiutare tutti i promotori della *"vulnerability disclosure"* in Europa, come il GCSEC.

Syed Taha Ali, Patrick McCorry, Peter Hyun-Jeen Lee, Feng Hao, **ZombieCoin 2.0: managing next-generation botnets using Bitcoin**, in International Journal of Information Security (2017), pp. 1-12

Addetto delle monete virtuali?Attenzione! È appena apparsa una minaccia di ultimo grido… ancora rara ma che potrebbe rivelarsi una vera *pandemia* in futuro. Nel 2016, un team di ricercatori aveva già rivelato che persino gli antivirus, durante la loro messa a giorno, potevano essere vettori di… virus. Ora, uno studio viene a dimostrare che esiste un fenomeno nascente anche se era già stato anticipato dagli osservatori più acuti: l'uso di *"zombiecoins"*. Il testo viene a dimostrare come funziona un botnet con meccanismo di *command-and-control* se viene impiantato sulla rete *Bitcoin*. I ricercatori sono infatti riusciti ad implementare *"ZombieCoin bots"* e a diffonderli sulla rete *Bitcoin*. La problematica maggiore che l'articolo vuole sottolineare è la fiducia totale che hanno gli utilizzatori del sistema *Bitcoin*, un elemento-chiave che rende l'intero sistema estremamente attraente per i criminali sebbene rimane molto difficile da attaccare. Il merito dell'articolo è certamente di suonare a tempo l'allarme su di una minaccia che è ancora sottostimata benché si percepisce che diventerà una delle maggiori sfide del futuro prossimo. Questa infiltrazione si rivela estremamente polivalente, come illustra questo lavoro, perché gli esempi di vulnerabilità scoperte nel modus operandi dei Bitcoin potrebbero essere utilizzati anche contro altri sistemi. È tra l'altro il motivo principale che ha già spinto le massime autorità ad osservare il fenomeno da vicino: *"Interpol researchers at the Black- Hat Asia conference recently demonstrated a malware which downloads specific coded strings from the Bitcoin blockchain (where they are stored as transaction outputs) and stitches them together into one command and executes it".*

Hans de Bruijn, Marijn Janssen, **Building cybersecurity awareness: The need for evidence-based framing strategies**, in Government Information Quarterly 34 (2017), pp. 1–7

Ben lungi da essere utile solo ai policy-makers, questo articolo è una dimostrazione delle ragioni dell'impatto ridottissimo di molte campagne di prevenzione nel campo della cyber security. Affrontando prima i problemi legati al modo digitale e poi quelli, più recenti, degli ecosistemi IoT, gli autori sottolineano che ci troviamo davanti ad un "Pandora's box" di paradossi (fig. 1), che costituisce ormai la principale sfida nel costruire una campagna di prevenzione efficace. Vengono poi a proporre una soluzione ideale per non perdersi nella trappola di questo labirinto multiforme, semplicemente… evitandolo!

(Fig.1)

Adattando il messaggio al modo dei film e delle immagini nel quale viviamo tutti, suggeriscono di adottare il modello-base delle trame hollywoodiane: lo schema *Victim-Villain-Hero* (VVH). Per fare ciò, identificano cinque criteri che augurano il successo: *"Frames are catchy; We intuitively agree with frames; Frames contain a villain; Frames challenge your opponent's core values; Frames tap into social undercurrents ".* Questo punto di vista, apparentemente riduttore, aiuta invece e facilita grandemente la definizione dei bisogni e dei pubblici per potere poi concepire le strategie adeguate profilando persone, istituzioni e fatti reali nello schema VVH (fig. 2). Questo testo apre così tante porte a ricerche specifiche per campagne di prevenzione mirate a pubblici diversi, offrendo un quadro semplice che permette ai dirigenti di basarsi sugli effetti vitali dell'impatto primordiale (choc visivo) destinato a suscitare la curiosità e l'interessa del pubblico. I decision-makers ne sono ben consapevoli, essendo usi ad indirizzare messaggi (scritti o orali) al pubblico, un mondo dove l'entrata in materia è cruciale e dove, se questa è sbagliata, ogni sforzo successivo è inutile. Non possiamo che raccomandare la lettura di questo testo appassionante anche ai dirigenti privati ed ai CISO/CSO, perché darà loro molteplici idee di come dare una nuova forma ai messaggi che destinano ad un'utenza larga (dai propri impiegati al pubblico esterno).

(Fig.2)

Internet Infrastructure Security Guidelines for Africa. A joint initiative of the Internet Society and the Commission of the African Union, 30 May 2017, 30 pp.

https://www.internetsociety.org/sites/default/files/AfricanInternetInfrastructureSecurityGuidelines_May2017.pdf

Queste linee guida, e specialmente il modo nel quale sono state pensate, sono un capolavoro di ciò che dovrebbe essere implementato – anche in Europa – per costruire fondamenta di una serie di buone pratiche mirate a rinforzare la sicurezza dell'ecosistema digitale di una nazione. Contrariamente a numerose linee-guida, strategie o direttive recentemente fatte pubbliche, l'Unione Africana (AU) addita le buone pratiche più rilevanti (NIST, ENISA, OECD), ma inizia con una presa di posizione ben diversa, perfettamente in sinergia con la realtà del web di oggi: *"it is difficult to clearly differentiate between Internet infrastructure security, and network security and traditional information assurance practices".*

Su questo punto, il capitolo 2 (ivi specialmente il punto 3), dedicato ai *policy-makers* del continente africano responsabili dall'elaborazione di strategie nazionali di cyber security, è estremamente chiaro. All'opposto dei testi occidentali che danno ancora un'enfasi al lato tecnologico del problema e agli investimenti in questo campo, l'ordine delle priorità definiti dall'AU nel presente volume conferisce all'umano il ruolo centrale. Così, i quattro principi secondo i quali si devono costruire le strategie sono: prevenzione, responsabilità, cooperazione, diritti e proprietà fondamentali nel mondo digitale.

La prevenzione (che qui racchiude anche l'educazione, le formazioni continue, le valutazioni) come punto di partenza è, a nostro avviso, un passo enorme verso il futuro se paragonato con tutti i documenti ufficiali che considerano questo mezzo tra le ultime – e quasi collaterali – misure da prendere nell'ordine delle priorità urgenti di difesa.

La responsabilità è considerata come l'obbligazione da parte dei CISO/CSO statali e privati di *"take into account the potential impacts of one's actions or inactions on other stakeholders before taking action"*, mentre la cooperazione punta una delle grandi fragilità degli Stati moderni, anche i più avanzati: la poca propensione a lavorare in gruppo e ad assumere una *"collective responsibility among all stakeholders, not just the government and a selected number of stakeholders".*

La spiegazione del principio di diritti e proprietà fondamentali nel mondo digitale è anch'essa molto esplicita: *" voluntary collaboration, open standards, reusable technological building blocks, integrity, permission-free innovation, and global reach".*

Come osserviamo, con la scelta di dibattere dell'infrastruttura in un campo separato, la Commissione dell'AU offre ai suoi membri la possibilità, indipendentemente del loro livello di ricchezza, di migliorare rapidamente la loro resilienza investendo nel fattore umano e nella collaborazione. Sperando che questo testo promuova la nascita di strategie nazionali che porteranno il suo spirito, ci auguriamo che venga letto ampiamente anche in Europa, da dirigenti pubblici come privati, perché in sole 30 pagine riesce ad inquadrare perfettamente l'insieme dei rischi e a portare soluzioni reali e rapidamente implementabili proprio sul punto che tutti gli specialisti chiamano ormai "l'anello debole", ovvero… l'umano.

Il 29 giugno scorso, la Commissione Europea ha annunciato, tramite un comunicato stampa[1], l'accelerazione delle misure di prevenzione contro la radicalizzazione e contro le minacce cibernetiche, all'occasione della pubblicazione dell'Ottavo Rapporto sui progressi dell'UE nel campo della sicurezza[2]. Nel documento, veniamo anche informati che a settembre verrà approvata una nuova Strategia di Sicurezza Cibernetica dell'Unione Europea. Proponiamo a seguito l'estratto del comunicato riguardante la cyber security:

Rafforzare la resilienza e la sicurezza informatica

Come annunciato nella revisione intermedia della strategia per il mercato unico digitale, la Commissione sta accelerando le proprie iniziative allo scopo di colmare le lacune esistenti nell'attuale quadro normativo sulla sicurezza informatica. Per rafforzare la nostra risposta all'aggravarsi della minaccia informatica occorre attuare un certo numero di interventi operativi a breve termine nell'ambito di un più ampio riesame della strategia 2013 per la sicurezza informatica, previsto per il mese di settembre.

- *Potenziamento dei sistemi e delle reti:* nell'ambito del meccanismo per collegare l'Europa, la Commissione assegnerà a 14 Stati membri un ulteriore finanziamento pari a 10,8 milioni di EUR, al fine di rafforzare la rete dei gruppi nazionali di intervento per la sicurezza informatica in caso di incidente (rete CSIRT). Europol dovrebbe dotare di ulteriori competenze informatiche il Centro europeo per la lotta alla criminalità informatica (EC3), in prima linea nella risposta dei servizi di contrasto all'attacco WannaCry.
- *Giustizia penale:* la Commissione sta valutando la possibilità di adottare misure legislative miranti al miglioramento dell'accesso transfrontaliero alle prove elettroniche. Sta inoltre esaminando le sfide poste dall'utilizzo della crittografia da parte di criminali e presenterà le sue conclusioni entro il mese di ottobre 2017. ■

1 http://europa.eu/rapid/press-release_IP-17-1789_it.htm
2 https://ec.europa.eu/home-affairs/sites/homeaffairs/files/what-we-do/policies/europe-an-agenda-security/20170629_eighth_progress_report_towards_an_effective_and_genuine_security_union_en.pdf

Le recensioni sono state eseguite da Laurent Chrzanovski e non esprimono necessariamente il punto di vista della rivista e dei suoi editori

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

AGORA get to know! e

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:
Bd. Dimitrie Cantemir nr. 12-14,
sc. D, et. 2, ap. 10, settore 4,
040234 Bucarest, Romania
Tel: 021-3309282
Fax 021-3309285

Viale Europa 175 00144 Roma, Italia
Tel: 06 59582272
info@gcsec.org

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

GLOBAL CYBER SECURITY SUMMIT

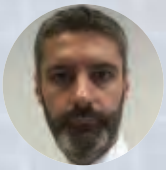
DEVELOPING A ROBUST CYBER DEFENSE STRATEGY
October 12 – 13, 2017 - LONDON, UNITED KINGDOM

The Global Cyber Security Summit is a day and a-half meeting bringing together senior level executives heading up information security, legal, finance, operations, risk, governance, audit and compliance from multinational corporations.

Unlike many other cyber events, this program is designed to inspire a highly interactive exchange on creating a holistic corporate cyber defense strategy. This is not a technology-focused program. It is entirely dedicated to helping senior executives across the organization to connect and build an overall resilience strategy that monitors and combat rapidly emerging threats.

Learn more at https://skytopstrategies.com/global-cyber- security-summit- 2017-uk/

FEATURED SESSION LEADERS



MASSIMO CAPPELLI
Operations Planning Manager
Global Cyber Security Center
Rome, Italy

CAROLYN DITTMEIER
Assicurazioni Generali
Autogrill
Alpha Bank
Ferrero
Milan, Italy

GENE FREDRIKSEN
Chief Information Security Officer
PSCU
Tampa, FL

DR. YOAV INTRATOR
Chief Technology Officer
Hapoalim Bank
Tel Aviv, Israel

MICHAEL MADON
Chief Executive Officer
Ataata
New York, NY

ERIC GARDNER YVELIN DE BEVILLE
Client Relations Officer, Avocat, Co-Managing Director HRCG
Consejero Asesor Ayming & Atrevia
Madrid, Spain

CARSTEN MAPLE
Professor of Cyber Systems Engineering, Cyber Security Centre
Warwick Manufacturing Group
Coventry, UK

ZVI MAROM
Founder and Chief Executive Officer
BATM
Tel Aviv, Israel

JUSTIN MCCARTHY
Chairman of the Global Board
PRMIA
Dublin, IR

LINDA MILLS
Member Board of Directors
AIG
Member Board of Directors
Navient
McLean, VA

KATE O'LEARY
Global Executive Litigation Counsel
General Electric Company
Boston, MA

LARRY SHOUP
Chief Executive Officer
ClearArmor
Riegelsville, PA

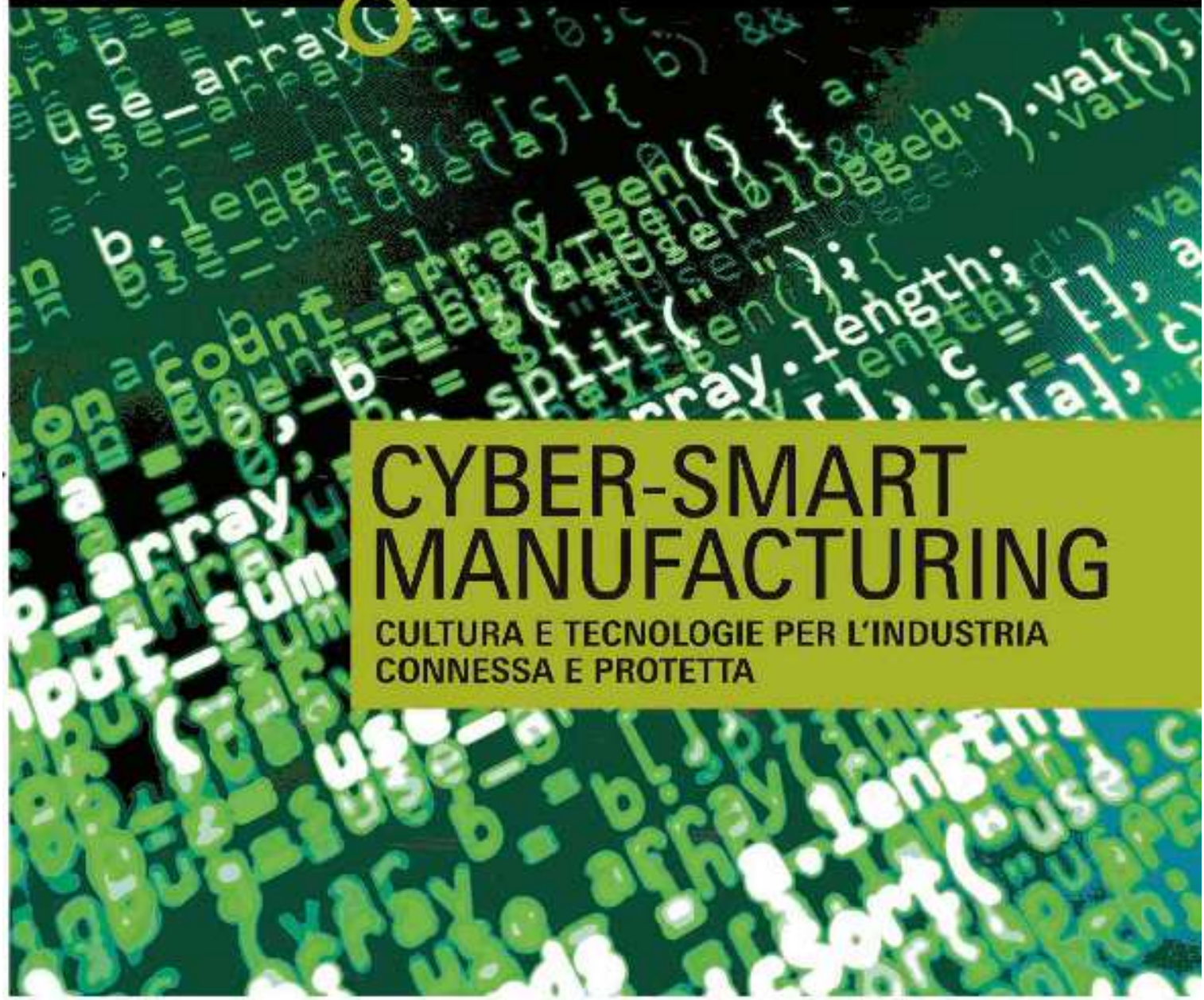
KRISTOFER SWANSON
Vice President and Practice Leader, Forensic Services
Charles River Associates
Chicago, IL

TIM WATSON
Director of the Cyber Security Centre
Warwick Manufacturing Group
Coventry, UK

SKYTOP STRATEGIES *www.SkytopStrategies.com*

ICS FORUM
Industrial CyberSecurity

MILANO
30 GENNAIO 2018
Grand Visconti Palace



CYBER-SMART MANUFACTURING

CULTURA E TECNOLOGIE PER L'INDUSTRIA CONNESSA E PROTETTA

PER INFORMAZIONI
espositori@icsforum.it
visitatori@icsforum.it

www.icsforum.it

In collaborazione con
INNOVATION Post

Organizzato da
messe frankfurt