Cybersecurity Trends

Edizione italiana, N. 1 / 2018

- Industria 4.0 e cybersecurity

INTERVISTE VIP:

- Aldo CAZZULLO
- Alessandro CURIONI

GLOBAL CYBER SECURITY CENTER

ISSN 2559 - 1797 / ISSN-L 2559 - 1797

Speciale Mobile Security

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

Social network e smartphone: il nuovo campo di battaglia è nelle nostre tasche

Autore: Nicola Sotira

BIO

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

Correva l'anno 2014 quando l'hashtag #AllEyesOnISIS faceva la sua comparsa in rete, peccato che non stesse annunciando il lancio di un nuovo film, ma l'invasione dell'Iraq. A questo sono seguiti video, tweet, pagine sui diversi social, una strategia di indottrinamento che ha dato voce a milioni di persone sul tema ISIS supportando, inoltre, la campagna di reclutamento dell'ISIS stesso; si stima che circa 30.000 persone di provenienza diversa abbiano raggiunto le fila dell'ISIS grazie alle campagne on-line. Per essere ancora più efficace, il cosiddetto Stato Islamico ha realizzato anche un'app per consentire ai propri fan di seguire tutti i canali in modo semplice connettendo i diversi social network.

La cosa sorprendente sta nel fatto che l'ISIS ha costruito il suo successo virale nello stesso modo in cui produttori di film e case discografiche pubblicizzano l'ultimo film di Spielberg o il nuovo album di Lady Gaga. Stessi principi e stessa strategia di marketing.

Sempre nel 2014, durante l'annessione russa della Crimea, il governo russo spese oltre 19 milioni di dollari per operazioni sui social media, come riporta sul suo blog l'analista Michael Olloway (https://thestrategybridge.org/search?q=%23WhatIsIO). Obiettivo, influenzare l'opinione internazionale creando l'immagine di una massa popolare che supporta l'annessione. Anche in questo caso il nuovo fronte non è più la montagna che ci separa dal nemico, ma lo scenario diventa globale e il terreno diventa la Rete.

Scenario che bene viene descritto dall'autore di "War in 140 Characters", David Patrikarakos: nel libro spiega come queste nuove piattaforme digitali stiano creando nuovi campi di battaglia nella nostra vita quotidiana attraverso una propaganda che riceviamo sul nostro smartphone, oggetto sempre con noi, 24 ore al giorno. Spostandoci nel 2016 vediamo che gli stessi strumenti vengono utilizzati dalla Russia per influenzare le elezioni politiche americane. In questo scenario sembra che più di 10.000 utenti di Twitter siano stati presi di mira con sofisticati malware che una volta in esecuzione assumevano il controllo del telefono e del computer della vittima. Facebook rileva che tra il giugno 2015 e il 2017 sono stati spesi oltre 100.000 dollari per promuovere post sponsorizzati legati a 470 account fasulli e che hanno stretti legami con il governo russo. Con tanto di dichiarazioni di Alex Stamos, il responsabile della sicurezza del social network. Ironico pensando a quanto venuto alla luce in questi giorni con il caso "Cambridge Analytica", l'azienda che avrebbe utilizzato impropriamente i dati di oltre 50 milioni di utenti di Facebook con lo scopo di tracciarne un profilo psicometrico da utilizzare a scopi politici ed elettorali. Sicuramente questo dovrebbe farci prendere coscienza sull'utilizzo di questi strumenti aiutandoci a comprendere che non esistono servizi gratuiti, che i nostri dati hanno un valore e che molto spesso in questo gioco il prodotto siamo noi… ■

Buona Lettura

Indice

Autore: **Marco Obiso,**

Coordinatore per la cyber security, International Telecommunications Union, Ginevra

Cari Lettori,

Se il 2017 ha visto attacchi informatici complessi e diffusi a livello mondiale, tanti quante fake news nelle testate dei media principali quasi ogni settimana, quest'anno sembra essere iniziato a un livello ancora più elevato con la scoperta di alcune vulnerabilità riguardanti la parte più vitale dei nostri dispositivi: il processore.

La sensibilizzazione, la consapevolezza, l'educazione e il rafforzamento delle capacità di resilienza e difesa nel campo della cybersecurity, rappresentano quindi, più che mai, la chiave per una vita digitale migliore, più sicura e piacevole.

L'ITU porta avanti il suo impegno in tutti i campi, coinvolgendo i suoi membri e promuovendo partnership.

Di seguito troverete un esempio di successo positivo e proattivo nel campo dell'information sharing, su minacce e soluzioni da parte degli attori di tutti i settori coinvolti: specialisti privati e pubblici, ma anche utenti privati e pubblici.

Non possiamo che complimentarci con la Swiss Webacademy e i suoi partner, per l'incremento e l'adattamento del concetto di piattaforma di dialogo sviluppata a Sibiu per l'Europa centrale, dal 2013.

La nascita, lo scorso dicembre, della piattaforma annuale dedicata all'Europa occidentale (a Porrentruy, Jura, ovvero "Cybersecurity-Svizzera") e, il prossimo maggio, della sua controparte che si terrà a Noto (Sicilia) e sarà focalizzata sull'ecosistema mediterraneo, sono eventi da classificare come necessari, oltre a quelli già esistenti.

Ai nostri giorni, molti congressi, conferenze e riunioni terminano con l'ultimo pannello dell'intervento finale. Il congresso Cybersecurity-Svizzera, invece, offre un white paper di oltre 40 pagine, tradotto in 4 lingue, che consente a tutti di cogliere la sostanza principale dei documenti di tutti i relatori presenti, portando spunti di riflessione e molte idee da sviluppare ulteriormente, come l'evento supportato dall'ITU che ha considerato elementi di sicurezza molto importanti, non esclusivamente "cyber", che hanno un impatto sul mondo digitale o che provengono da esso.

Il giorno prima della conferenza di Sibiu e degli eventi di Porrentruy, la Swiss Webacademy, in collaborazione con i dipartimenti specializzati della polizia rumena e di quella svizzera, ha stabilito un nuovo record sia europeo che svizzero riguardo al numero di bambini e adolescenti presenti alle sessioni di awareness gratuite sulla consapevolezza dei pericoli della vita digitale e le precauzioni migliori da prendere.

Pertanto, l'ITU ha deciso di aderire e co-organizzare la giornata di sensibilizzazione che la Swiss Webacademy offrirà ai bambini e adolescenti siciliani a Noto, il 9 maggio, con le prestigiose partnership della Polizia Postale e delle Comunicazioni, e della Fondazione Global Cyber Security Center di Poste Italiane.

L'educazione e la cultura sulla cybersecurity sono un must in un mondo in cui, giorno dopo giorno, l'anello più debole della linea di difesa digitale è l'uomo. Abbiamo il dovere di lavorare insieme in questo campo per offrire ai giovani le informazioni necessarie per evitare le insidie e i pericoli più comuni. ■

La sicurezza delle App mobile per la protezione del brand aziendale

Autore : Gianluca Bocci

Da qualche decennio è in corso una radicale trasformazione dei servizi offerti dalle pubbliche amministrazioni e dalle imprese private verso i cittadini e i consumatori; si è infatti passati da un modello di erogazione dei servizi di tipo tradizionale ad un modello digitale che interessa ormai tutti i settori merceologici. Se una volta si andava in libreria per acquistare un libro, oggi si utilizzano siti di e-commerce come Amazon, dove l'ordine viene effettuato online.

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.

L'attuazione dell'Agenda Digitale Italiana, con l'obiettivo di aiutare i cittadini e le imprese ad adottare le tecnologie digitali per favorire la crescita economica, rientra a pieno titolo in questa trasformazione.

Il cambiamento appena accennato è in continua evoluzione; in questi ultimi anni l'affermazione degli smartphone e dei tablet, resa possibile dallo sviluppo di App per ogni esigenza e dalla disponibilità di banda trasmissiva via via crescente, ha permesso la fruizione degli stessi servizi in un contesto di completa mobilità. Tutto ciò ha comportato notevoli vantaggi nella vita delle persone e nella crescita delle imprese, anche se entrambi hanno subito l'esposizione a nuove forme di rischio.

Analoghe considerazioni, opportunamente contestualizzate, interesseranno in un prossimo futuro molti altri domini tecnologici che si stanno affacciando prepotentemente alla ribalta delle cronache; è il caso del "Wearable Computing" che, con i dispositivi hi-tech mobili, aprirà nuove frontiere allo sviluppo di App, così come l'Internet of Things.

Per le tecnologie mobili, l'uso dilagante di piattaforme aperte come Android (oltre l'85% dell'attuale mercato utilizza questo sistema operativo) e la facilità d'introdurre codice malevolo all'interno delle App che possono essere scaricate da una moltitudine di Store, espone l'utente finale a specifici rischi che si traducono per le imprese nell'esigenza di proteggere attraverso nuovi approcci il proprio "brand".

Tale protezione deve in primo luogo basarsi su modelli di prevenzione che includano il monitoraggio di tutte le applicazioni mobile che, appartenenti o riconducibili all'impresa che intende proteggersi, sono disponibili sui canali di distribuzione considerati ufficiali (es. Google Play Store, AppleStore) e alternativi (es. Torrapk, Blackmart, ecc).

È proprio nei canali di distribuzione alternativi, dove tipicamente i controlli sono meno rigorosi, se addirittura inesistenti, che va posta la maggiore attenzione, dal momento che vi si possono trovare App potenzialmente alterate. L'utente finale, installando queste applicazioni, se pur in parte responsabile di un'azione condotta ad alto rischio, nel momento

in cui subisce la frode è indotto ad allontanarsi dal fornitore di servizi. In linea con queste considerazioni, le tecniche automatizzate per la ricerca di nuovi Store e la verifica tecnica della presenza di App malevole, rese tali, ad esempio, attraverso l'uso di metodi di repackaging, stanno assumendo un ruolo sempre più strategico nell'azione di contrasto e di prevenzione di tale fenomeno criminoso. Rafforza tale convinzione il numero crescente di App che, nel panorama del m-Commerce, annoverano sempre più spesso funzioni dispositive utilizzate per compiere transazioni economiche.

In generale la sicurezza delle applicazioni mobile dovrebbe interessare non solo il settore finanziario, ma tutti quelli che ne prevedono l'uso nei propri modelli di business. Volendo porre l'attenzione su quelli *IoT-oriented* sempre più utilizzati dalle compagnie assicurative, ricordiamo le polizze associate a servizi di smart-house, che utilizzano reti di sensori intelligenti collegate alla rete Internet attraverso la rete Wi-Fi domestica e app sviluppate ad hoc, per ricevere informazioni sullo stato dell'abitazione oppure inviare comandi. L'importanza di questa app diventa critica nel momento in cui la stessa consente l'attivazione o disattivazione da remoto dell'allarme, oppure è collegata direttamente a servizi di prima assistenza qualora uno dei sensori segnala la presenza di situazioni anomale come ad esempio fumo, fuoco, acqua, effrazioni di porte e\o vetri, etc. L'esperienza dimostra che dietro queste soluzioni si ha spesso un'infrastruttura di back-end sicura (ma non sempre), mentre ciò che lascia a desiderare è proprio la componente app.

Per una completa tutela del marchio, occorre complementare l'analisi tecnica con quella legale, in modo da avere un quadro completo che tiene conto anche delle possibili violazioni degli obblighi contrattuali e/o delle disposizioni normative vigenti che interessano di volta in volta l'App in esame.

Una possibile violazione delle disposizioni normative, che prescinde dall'alterazione del codice sorgente (originale) dell'App da parte del programmatore non autorizzato, si basa sulla tecnica combinata del framing con i servizi di mobile advertising: in sostanza l'App originale rimane inalterata, ma è manipolata per abbinarla a dei messaggi pubblicitari che potrebbero essere incompatibili con l'immagine che l'impresa desidera proiettare verso i propri Clienti.

Un programma di protezione del brand da parte di aziende la cui linea di offerta sfrutta le tecnologie mobili non può dunque prescindere dall'adottare una metodologia di monitoraggio della sicurezza delle app che almeno includa:

- la ricerca di nuovi app store oltre quelli ufficiali dove volutamente si rilasciano le proprie app;
- il censimento delle app con l'uso di tecniche di crawling avanzate (ad esempio che utilizzano oltre alle parole chiave anche le similitudini per imagine, così da poter essere utilizzate su siti che usano caratteri xxxxxxx);
- l'analisi statica e dinamica delle App che, congiuntamente, consentono di determinare il carattere malevolo delle App;
- l'analisi legale i cui risultati possono essere in generale decisivi, indipendentemente dalle rilevazioni tecniche effettuate;
- e in ultimo, ma non meno importante, la gestione delle azioni di mitigazione che possono prevedere anche la rimozione dell'App dallo Store che ne consente il download.

Pur avendo finora posto l'attenzione sui rischi introdotti con l'uso delle nuove tecnologie mobili ed in particolare quello delle App di dubbia provenienza, si desidera evidenziare come un programma "completo" per il contrasto del fenomeno della contraffazione, alterazione o uso improprio in rete dei marchi o segni distintivi di un'azienda, deve tener conto di "tutti" i possibili canali digitali che un truffatore può sfruttare e che devono pertanto essere opportunamente monitorati: sono compresi tra i canali digitali i "social network" come Facebook e Twitter, ma anche blog e mini blog, piattaforme web per il video sharing come Youtube, i quotidiani online locali, nazionali ed internazionali, e così via. Propedeutica ad un qualunque programma di protezione dei canali digitali c'è comunque e sempre la scelta oculata del dominio che deve essere registrato insieme a tutte le sue possibili estensioni ritenute strategiche per lo sviluppo del business.

Per terminare, la tutela del marchio online richiede l'impegno di risorse molto qualificate, dotate di competenze tecniche, giuridiche e di adeguati strumenti a supporto delle attività di monitoraggio in precedenza menzionate; aggiungendo a tutto questo l'esigenza di continuità che richiede un servizio di "brand protection", si comprende come spesso molte imprese potrebbero essere scoraggiate dall'avviare tali iniziative. In questi casi rimangono valide soluzioni alternative come la scelta di fornitori di servizi per la brand protection che, per dimensioni e capacità economiche, possono garantire la qualità di una prestazione così complessa ma ormai ritenuta strategica per la sopravvivenza di ogni impresa. ■

> *L'utente finale, se pur in parte responsabile di un'azione condotta ad alto rischio, nel momento in cui subisce la frode è indotto ad allontanarsi dal fornitore di servizi.*

I rischi nascosti dei sistemi di telefonia mobile

Autore: Giancarlo Butti

L'utilizzo di sistemi mobili può comportare diversi rischi per la sicurezza spesso non percepiti dalle aziende; conoscerli è invece indispensabile per poter mettere in atto adeguate misure di prevenzione e limitare, per quanto possibile, i danni.

Quando si pensa al rischio intrinseco nell'uso di un dispositivo mobile, quale ad esempio uno smartphone, si è portati naturalmente a considerare la possibile intercettazione delle comunicazioni fra i soggetti impegnati in una conversazione.

In realtà, la complessità di tali dispositivi e la ricchezza di funzionalità offerta da tali strumenti li rendono particolarmente insidiosi e tali da dover seriamente valutare l'autorizzazione del loro utilizzo da parte dei dipendenti e dei visitatori nelle aree dove si svolgono attività che richiedono un adeguato livello di riservatezza e/o privacy.

Una precauzione che stride decisamente con l'attuale realtà che vede un'imperante presenza di tali dispositivi, siano essi aziendali o privati, anche durante i momenti più importanti della vita aziendale, quali ad esempio le riunioni in merito a decisioni strategiche o dei CdA.

Dispositivi di registrazione

Un dispositivo mobile oggi è dotato di numerosi strumenti che consentono la registrazione dell'ambiente circostante:

- videocamera (spesso anche 2), con la quale è possibile effettuare riprese video comprensive di audio o effettuare fotografie, anche con un'alta risoluzione, di ambienti, persone, documenti o schermate video;
- microfoni, con i quali effettuare registrazioni audio senza che i presenti se ne accorgano.

Dispositivi di controllo ambientale

Il controllo di un ambiente mediante un cellulare può avvenire dopo averlo lasciato appoggiato su una scrivania (fatto questo considerato assolutamente normale) o mediante la registrazione audio in locale, oppure attivando una chiamata verso un dispositivo remoto dal quale effettuare la registrazione.

L'attivazione della registrazione può essere opera del proprietario del dispositivo, ma al riguardo va anche considerata la possibilità che il monitoraggio dell'ambiente tramite dispositivo mobile sia attivata tramite uno spyware da parte di terzi senza che il legittimo proprietario dello stesso ne sia a conoscenza.

L'uso dei così detti "captatori" informatici, consistenti in software installati all'insaputa della vittima, consente a chi ne controlla l'uso di attivare il microfono o le videocamere al fine di registrare conversazioni o più in generale di captare l'ambiente circostante.

Tali software consentono in realtà di avere anche il pieno controllo del dispositivo, e quindi di accedere anche a e-mail, agende, documenti presenti sul dispositivo stesso.

Recentemente il Codice penale[1] è stato modificato per permettere il lecito uso di tali strumenti da parte delle forze dell'ordine, pur limitandone in questo l'ambito d'uso ed il perimetro di controllo.

Ne consegue che non conta la buona fede o l'affidabilità dei propri collaboratori (a tutti i livelli) o anche quella di visitatori, clienti o fornitori che accedono alla propria azienda: quando si trattano temi importanti o riservati è buona cosa non avere dispositivi mobili nelle vicinanze onde evitare fughe di notizie.

Dispositivi di archiviazione

Uno smartphone può essere utilizzato come una memoria di massa.

È sufficiente collegare il dispositivo via cavo o anche in modalità wireless ad un pc (o ad un altro dispositivo mobile) per poter trasferire grandi quantità di dati, che passano così dalla rete aziendale al dispositivo privato. Tale trasferimento può essere rilevato se sono in atto sistemi di tracciatura o può essere impedito

se sono disabilitate le porte USB e non sono concessi agli utenti i privilegi per abilitare le connessioni wireless sul proprio pc di lavoro.

Tuttavia l'asportazione di dati può avvenire anche con altri sistemi non tracciabili e che non possono essere presidiati a priori, quali ad esempio la registrazione delle sessioni video mediante la videocamera del dispositivo mobile. Anche se tale pratica non è ovviamente agevole nondimeno è praticabile e, laddove le informazioni da asportare siano molto rilevanti, l'impegno richiesto in fase di acquisizione e decodifica è ampiamente giustificato.

Inutile dire che quanto viene registrato nel dispositivo sia in modo lecito, sia in modo illecito, è poi soggetto a tutti i rischi che derivano dalla possibile perdita o furto del dispositivo o dal possibile accesso illecito a tali contenuti mediante una non oculata gestione ad esempio delle connessioni wireless e USB del dispositivo stesso (anche se ovviamente difficilmente chi ha usato il dispositivo per asportare illecitamente delle informazioni non adotta tutte le precauzioni affinché questo non accada).

Dispositivo come router WIFI

Un altro possibile uso del dispositivo mobile è quello di router WiFi, con il quale collegare dispositivi aziendali non adeguatamente protetti con la rete internet.

Se i dispostivi aziendali sono contemporaneamente connessi alla rete interna si crea in tal modo una falla nella sicurezza perimetrale, non essendo la nuova connessione filtrata dai firewall e dagli altri strumenti di protezione perimetrale.

Per tale motivo, oltre che per evitare l'asportazione di file tramite connessioni wireless, sui dispositivi aziendali dovrebbero essere inibite tali connessioni.

BYOD

Anche se un crescente numero di aziende consente l'uso degli strumenti personali per finalità aziendali, non di meno tale consuetudine comporta dei rischi veramente rilevanti per l'azienda.

I problemi di sicurezza del dispositivo possono ripercuotersi sulla riservatezza delle informazioni aziendali nonostante la presenza di policy anche articolate e complete che regolino questa materia.

Anche la semplice possibilità di accedere alla posta aziendale dal dispositivo mobile, evitando quindi un alquanto rischioso accesso diretto alla rete, è tutt'altro che sicuro.

Accedere alla posta implica in genere la possibilità di scaricare degli allegati oltre ai messaggi stessi, che quindi potrebbero risiedere fisicamente sul dispositivo mobile, il cui livello di sicurezza non può essere presidiato in forma adeguata dall'azienda.

Inoltre potrebbero esserci delle oggettive difficoltà da parte dell'azienda nel garantirsi la possibilità di effettuare dei controlli sul dispositivo del dipendente.

Al riguardo le aziende dovrebbero dotarsi anche di strumenti capaci di riconoscere un dispositivo che tenta di collegarsi da remoto identificandolo come aziendale o privato e rifiutando questi ultimi.

BIO

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

Occupazione del tempo aziendale

È banale affermare che la disponibilità di un dispositivo mobile con attivi molteplici canali di comunicazione (voce, sms, mms, whatsapp…) fa sì che anche durante il normale orario lavorativo una parte del tempo sia dedicata alla relazione con la propria rete di contatti. Questo non necessariamente è un aspetto negativo in quanto la conciliazione di lavoro e vita privata è sempre più all'attenzione sia delle aziende sia del legislatore come anche la recente normativa sul lavoro agile ha evidenziato.

È opportuno quindi che le politiche aziendali non siano in tal senso ostative, in quanto non in linea con le attuali tendenze. Quello che le aziende devono fare è regolamentarne l'uso là dove siano presenti effettivi rischi per la sicurezza aziendale. ■

1 DECRETO LEGISLATIVO 29 dicembre 2017, n. 216 - Disposizioni in materia di intercettazioni di conversazioni o comunicazioni, in attuazione della delega di cui all'articolo 1, commi 82, 83 e 84, lettere a), b), c), d) ed e), della legge 23 giugno 2017, n. 103. (18G00002) (GU Serie Generale n.8 del 11-01-2018)

Nativi digitali, mettete via il cellulare e date spazio al dialogo

Intervista Vip con Aldo Cazzullo (a cura di Massimiliano Cannata)

Aldo Cazzullo

Autore: Massimiliano Cannata

"Metti via il cellulare" è probabilmente la frase che un genitore pronuncia più spesso nella società tecnologica, popolata da mirabolanti e sempre più sofisticati strumenti della comunicazione digitale. "E' record – ha scritto con la consueta sagace ironia Altan – ogni cellulare possiede un italiano". Il rapporto tra l'individuo e gli oggetti appare ormai capovolto: loro ci dominano, modificando gli asset di relazione, ma cosa ancora più grave incidendo sull'immaginario e di fatto sulle scelte e sui comportamenti soprattutto dei nativi digitali, che vivono nella Rete in una "dimensione omeopatica".

BIO

Aldo Cazzullo è inviato e editorialista del «Corriere della Sera», dove cura la pagina delle Lettere. Ha scritto più di dieci saggi sulla storia e l'identità italiana. Il penultimo, *Possa il mio sangue servire. Uomini e donne della Resistenza*, è dedicato al figlio Francesco. L'ultimo, *Le donne erediteranno la terra*, è dedicato alla figlia Rossana.

Aldo Cazzullo, editorialista del Corriere della Sera, 51 anni piemontese di Alba, ha provato a rompere il muro del *"silenzio da social"*, quello strano fenomeno per cui ciascuno di noi mentre è impegnato a vantare migliaia di *follow*, scopre di essere tremendamente solo. Sta accadendo questo ai nostri ragazzi, che si specchiano nello schermo del telefonino sul divano di casa o peggio mentre sono a scuola, novelli "narcisi" rimangono abbagliati e storditi, fuori dal mondo reale, abitano una bolla virtuale in cui le coordinate dello spazio e del tempo hanno altre regole.

Metti via il cellulare *(ed. Mondadori). Il titolo suona come una intimidazione, che rischia di cadere nel vuoto. Cazzullo, può bastare un libro, seppure di successo (più di 120mila copie vendute n.d.r.) per disciplinare il rapporto tra giovani e tecnologie?*

Certamente non basta, ma può essere un punto di inizio, un termine di riflessione che voglio sottoporre a tutte le famiglie, cominciando dalla mia. La generazione dei miei figli, Francesco che ha vent'anni e frequenta il secondo anno di Scienze Politiche alla Luiss e Rossana, che ne ha 17 e affronterà la maturità al liceo Classico Tasso di Roma, vive connessa. Il cellulare non è, come per noi, un semplice telefono, ma una protesi imprescindibile del corpo, un trampolino per gettarsi nel mare vasto, affascinante ma anche pericoloso della rete. Il punto critico sta nel fatto che ancora non abbiamo ben compreso i rischi che la navigazione *on line* comporta.

La sicurezza occupa uno spazio importante nello spazio di conversazione che hai con i tuoi figli. Il capitolo dedicato ai bulli e alle vittime dei social è molto significativo. Da poco è stata celebrata la Giornata mondiale del Safety Day "Generazioni connesse" che ha coinvolto più di 60.000 studenti in Italia, che ha insistito molto sul tema della violenza. Sembra che le aule siano diventate la "nuova trincea". Come ci si deve attrezzare per scongiurare questi pericoli?

Iniziative come queste che hanno una finalità formativa sono essenziali per incamminarsi verso un uso responsabile della rete. Va nella stessa direzione la proposta del MIUR che insieme all'Università Cattolica di Milano ha recentemente redatto il primo "Manifesto della comunicazione non ostile", nell'ambito della giornata nazionale contro il bullismo. Occorre ricordarsi che sono i valori del rispetto, della lealtà, dell'altruismo

della solidarietà l'antidoto più efficace al dilagare della violenza che domina le pagine della cronaca. Diventa perciò strategico l'impegno dei manager della security e delle istituzioni che operano senza sosta su questo terreno.

Il bullismo non è un fenomeno nuovo, perché oggi fa notizia?

Perché nel passato rimaneva confinato nella stretta cerchia della classe. Adesso è divenuto "virale", parola orribile che evoca virus, contagi, malattie. Un agente della polizia postale di Monfalcone, in occasione della presentazione del libro, mi ha spiegato che la prova d'amore che i ragazzi chiedono più frequentemente nell'era di Internet è una foto intima. Molti non resistono alla tentazione e finiscono poi col postare la foto rendendola pubblica al fine di vantarsi e in qualche caso di vendicarsi per un rapporto finito. Quando arriva la denuncia alla Polizia postale da parte delle mamme disperate, purtroppo è tardi. Da qui l'importanza della governance del rischio e delle politiche di prevenzione che devono vedere alleate lo stato e le imprese.

Il saggio elenca con puntualità i rischi e le "trappole" del digitale. Non teme di essere etichettato come un irredimibile conservatore?

Attenzione, il libro non è una predica, è un dialogo che ho intrattenuto con i miei figli, che rispondono colpo su colpo ad ogni mia osservazione. La rete per loro non è né buona né cattiva, dipende semplicemente dall'uso che ne facciamo. Per dimostrami la neutralità del mezzo mio figlio Francesco mi ha raccontato la storia di Montolivo, il giocatore del Milan e della nazionale, che è stato lontano dai campi parecchi mesi per la frattura riportata ad una gamba. Nel periodo della convalescenza ha ricevuto minacce e insulti via web, "devi morire" è stata l'intimidazione più "elegante". Il calciatore ha risposto mandando una carezza anche a quelli che gli hanno augurato le cose peggiori, disarmando e sconfiggendo, in maniera intelligente, la schiera organizzata degli odiatori.

"I nuovi servi della gleba digitale"

In questo contesto, ricco di luci e ombre difficile dar torto a Claudio Magris che sul Corsera ha parlato dei nuovi* "servi della gleba digitale" *se, come rivelano le ultime statistiche, tocchiamo il nostro cellulare più di 2600 volte al giorno. Qual è il suo parere in merito?

Il cellulare crea dipendenza, lo sappiamo tutti. Ogni secondo ci troviamo a controllare se per caso ci ha scritto qualcuno, con un danno notevole sul piano dell'economia dell'attenzione A scuola i ragazzi, anche se seduti nello stesso banco, conversano utilizzando le faccine, perché hanno perso l'abitudine a guardarsi negli occhi. Sono tutti segnali che fanno riflettere e che devono indurci a mutare atteggiamento. Dopo l'euforia è venuto forse finalmente il momento di esercitare il pensiero critico.

Per esercitare questa riflessione Lei ha scelto la forma epistolare nella tessitura del volume, che ripercorre secondo canoni ovviamente rimodulati, la grande tradizione della nostra letteratura, da Petrarca a Foscolo, per citare i grandi. Il suo messaggio non rischia di perdersi in una "babele digitale" densa di messaggini, chat, popolata da miliardi di* tweet *al giorno?

Nella costruzione del libro ho ripercorso una forma classica, mediata però dalle nuove tecnologie. Francesco e Rossana interloquiscono con me usando molto spesso Whatsapp, questo dà una struttura molto aperta a un dialogo in divenire, che deve proseguire nelle famiglie e nelle scuole, solo così il messaggio potrà sfidare la babele digitale cui lei faceva riferimento. Ritengo che sia essenziale mettere le generazioni a confronto, è importante che tornino a parlarsi genitori e figli, nonni e nipoti, insegnanti e allievi. Nessuna concessione da parte mia al "neoluddismo", semmai il bisogno di una consapevolezza maggiore. Detto in sintesi: non possiamo buttare via un oggetto che fa parte delle nostre vite, quello che dobbiamo fare è cercare di convincere i ragazzi a farne piuttosto un uso più avveduto.

Facebook *con due miliardi ha più seguaci del cristianesimo ed ha una dimensione vasta una volta e mezzo l'Islam. Siamo di fronte a una platea che supera potenzialmente la forza di trascinamento di due grandi religioni monoteiste. Sarà per questo che ha preso piede il PASN (partito anti social network), che annovera tra i sostenitori nomi famosi, tra cui anche Chamath Palihapitiya, che proprio di* Facebook *è stato dirigente e che anche nelle aziende si comincia a parlare di "diritto alla disconnessione"?*

Qualcosa sta avvenendo, è scattata una molla, un processo di riconversione, che potrebbe stupire a tutta prima, ma che è spiegabile. Sono diverse le questioni sul tappeto che dobbiamo governare legate all'innovazione. Ricordiamoci che il cellulare e la rete portano a una frantumazione della cultura. Tutto quello che l'uomo ha dipinto, pensato composto scritto negli ultimi secoli viene letteralmente fatto a pezzetti e gettato nel web, tutto diventa leggero e volatile, come si trattasse di coriandoli. Il Novecento è stato prima il secolo del cinema e nella seconda metà della televisione oltre che dei giornali. L'Ottocento era stato il secolo del romanzo, pensiamo ai grandi scrittori russi Tolstoj, Dostoevskij, agli autori francesi quali Balzac, Flaubert. E se volessimo andare ancora più a ritroso fino al Settecento, possiamo ritroviamo il teatro di Molière e di Goldoni. Giacimenti culturali immensi che rischiamo di seppellire nell'oblìo.

La rete non dovrebbe amplificare la trasmissione di questo enorme patrimonio?

Solo superficialmente perché di fatto polverizza i contenuti delle grandi opere dell'ingegno. Lo dimostra il fatto che in pochi oggi comprano un dvd, ancor meno giornali e libri, per non parlare del teatro e del cinema. Il modello di fruizione è quello di *youtube*, che impegna pochi minuti.

I suoi figli non hanno avuto nulla da ridire?

Altro che. Sono stati pronti a ribattere: "Guarda papà che se vai a vedere la Quinta di Beethoven diretta da Abbado, ha più di 170mila visualizzazioni, i giovani senza Internet che non ne saprebbero nulla...". Peccato però, ho risposto, che il pezzo pop sud coreano, il balletto *Gangnam Style*, definito ballo ufficiale sabor dei caraibi, conta circa tre miliardi di link.

La libertà e la gratuità sono delle opportunità indubbie, che rendono universalmente accessibile il sapere. Non è un vantaggio oggettivo?

Nulla è veramente gratis. C'è sempre un prodotto che viene comprato e venduto, quel prodotto siamo noi. La rete conosce tutto: sa dove andiamo in vacanza, cosa compriamo, i nostri gusti e le preferenze. Esiste un'enorme quantità di dati, una ricchezza enorme che la rete ha accumulato destinata a essere controllata nelle mani di pochi padroni del mondo che non sono certo benefattori. All'ultimo Forum Economico Mondiale è emerso proprio il tema dello sviluppo digitale come questione cruciale del prossimo futuro. L'Europa dovrà fare delle scelte delicate in tema di privacy, riservatezza e gestione dei *Big Data*, che sono la materia prima del XXI Secolo. Imprese e stati su questo terreno rappresentano interessi confliggenti, gli scenari che si stanno prospettando in questa direzione sono molto delicati e non certo rassicuranti.

La necessità di una governance dell'innovazione

Proviamo a rimanere sui temi della* governance *dell'innovazione. La Comunità Europea a maggio varerà una Carta per difendersi dall'intelligenza artificiale. Quella dei robot in questo mondo popolato di* app *è la sfida nella sfida?

La rivoluzione digitale sta incrociando un'altra grande rivoluzione del nostro tempo, che è la rivoluzione dell'intelligenza artificiale. Siamo nell'era della riproducibilità tecnica della vita, per cui l'uomo crea l'uomo o almeno ha l'illusione di farlo. Robot e clonazione esprimono la forza di un cambiamento fino a ieri inimmaginabile. Avremo uomini "nuovi" che avranno come cervello il computer e come memoria la rete, sapranno molte più cose e probabilmente saranno più intelligenti di noi. Rimane perciò fondamentale che il dominio della tecnologia rimanga saldamente nelle mani dell'uomo e non viceversa.

La scrittura corale di questo libro è un'esperienza che ha determinato un cambiamento nell'ambito dei rapporti con i suoi figli?

Si è aperta tra noi una finestra più ampia di dialogo e di confronto. Ho notato inoltre che Francesco e Rossana usano il cellulare un po' meno e un po' meglio, nel contempo credo di essere riuscito a comprendere appieno l'importanza che ha quest'oggetto per loro. Credo che sia forse ancora più importante avere innescato una comunicazione molto forte tra nonni e nipoti. L'amore a cerchio di vita tra le generazioni è una cosa meravigliosa, che non deve essere spezzata. Vale lo stesso ragionamento per il meccanismo di trasmissione della memoria, che sembra essersi perso, lacerato dalla dittatura del presente imposta dalla Rete. Il passato è come se non esistesse. La seconda guerra mondiale diventa come la seconda punica, la distanza di secoli non ci appartiene, perché quello che hanno sperimentato altre civiltà e altri popoli non esiste per noi.

Per insegnanti, ma anche per i genitori una difficoltà in più. In conclusione Le chiedo: come va affrontata?

Con determinazione. *"Essere stati è la condizione per essere"* sosteneva un grande storico degli Annales come Fernand Braudel. Sia a scuola che in famiglia bisogna riattivare la molla fondamentale della memoria. I racconti dei nonni sono interessanti oltre che fondamentali proprio perché servono a innestare le difficoltà dell'oggi in un contesto storico, attraverso una trama di connessioni spazio temporali che i ragazzi non possono ignorare. Ricordiamoci che ogni generazione ha avuto le sue guerre da affrontare. Quella dei nostri figli deve essere combattuta e vinta contro la sfiducia e la rassegnazione. Per avere successo occorrono armi morali, più che materiali, e una robusta attrezzatura culturale. ■

Dopo industria 4.0 È venuta l'ora di lanciare il piano security 1.0

Intervista VIP ad Alessandro Curioni

Alessandro Curioni

Autore: Massimiliano Cannata

In un universo completamente interconnesso la debolezza di una componente si traduce immediatamente nella debolezza di tutti. Il tema del prossimo futuro, spiega nell'intervista ***Alessandro Curioni***, editore e imprenditore, esperto di sicurezza informatica, sarà legato alla protezione delle infrastrutture critiche e alla relazione che molte di esse avranno con il mondo dell'*Internet of Things*. Fondamentale l'aspetto culturale ed educativo: perciò occhio ai nativi digitali, senza perdere di vista gli utenti più maturi ormai proiettati in una dimensione digitale che devono imparare a vivere e conoscere.

Partirei da una sua riflessione che riassume bene la filosofia dei suoi ultimi interessanti saggi:* "Questa casa non è un hashtag!" *e* "Come pesci nella rete": *"Informatica e sicurezza sono cose diverse. La prima dipende da quanto ne sai, la seconda da chi sei". In sintesi possiamo spiegare il senso di questa affermazione?

Immaginiamo due persone al volante di un'auto. La prima è un formidabile pilota e meccanico, esperto in guida acrobatica, ma forte delle sue abilità tende a non rispettare il codice della strada. La seconda è un normale guidatore e conosce lo stretto indispensabile del funzionamento del veicolo, ma è molto attento alla segnaletica e ai limiti di velocità. Quale dei due potrebbe causare un incidente? Credo che la risposta sia scontata. Il rapporto tra sicurezza e informatica non è poi tanto diverso. Chi si occupa della prima deve sapere con esattezza cosa la tecnologia è in grado di fare ma deve avere un approccio che potrei riassumere parafrasando una celebre frase del protagonista del film Blade Runner a proposito dei replicanti: *"l'informatica è come ogni altra macchina: può essere un vantaggio o un rischio. Se è un vantaggio non è un problema mio"*.

Gli esperti che operano nella security sia nella sfera pubblica che privata sono consapevoli di questa sottile ma fondamentale differenza?

Sul fatto che questa differenza sia trasparente agli esperti di security non sono tanto convinto perché troppo spesso tendono ad avere un approccio basato semplicemente sulle soluzioni tecnologiche, dimenticandosi i temi dell'organizzazione e soprattutto le esigenze degli utenti.

Il* monaco Tze *deve leggere* "i segnali del Tutto, perché la sicurezza diventa il viaggio più che il punto d'arrivo". *La scelta di una figura così eccentrica per essere protagonista in un saggio sulla sicurezza, da quale esigenza è stata dettata?

È un richiamo all'importanza dell'astrazione, che ci deve portare non all'infallibilità che di fatto è impossibile, ma a non commettere gli stessi errori. Imparare la lezione che ci viene inflitta ogni volta che sbagliamo significa

BIO

Alessandro Curioni, editore, imprenditore e giornalista. Nel 2003, dopo due anni di studio, pubblica per Jackson Libri il volume *Hacker@tack,* dedicato alla sicurezza informatica. Nel 2008 fonda DI.GI. Academy, azienda specializzata nella formazione e nella consulenza nell'ambito della sicurezza informatica. Nel 2015 riprende la sua attività pubblicistica per diverse testate cartacee e on line. Nel 2016 esce per Mimesis *Come pesci nella Rete – Guida per non essere le sardine* di Internet, un manuale che incontra l'interesse di numerose testate giornalistiche e che, nell'agosto dello stesso anno, figura tra i dieci saggi più venduti secondo la classifica settimanale de "La Lettura".

ricavare dal particolare una verità generale, che vuol dire produrre una regola astratta che poi andremo ad applicare in altre circostanze. Come dire… *"Il Tutto è l'Uno, ma anche l'Uno è il Tutto".*

Quanto è importante trovare il giusto modulo narrativo per attuare un progetto di formazione efficace e per entrare nell'universo articolato e complesso della sicurezza?

Il problema è sempre quello di arrivare alla testa e al cuore delle persone, quindi riuscire a fare in modo che il tema della sicurezza sia percepito in primo luogo come un problema personale. Il linguaggio deve essere semplice, perché se è vero che piace a tutti utilizzare la tecnologia, risulta quanto mai noioso approfondirne la conoscenza. In particolare è utile far sì che la lettura, per un libro, o l'ascolto, nel caso di un corso, possa diventare un'esperienza da ricordare. Credo molto nell'ironia sia nel caso in cui il messaggio è scritto, sia quando mi trovo a tenere dei corsi in aula. In fondo una risata fissa il ricordo ancor meglio che una bacchettata sulle mani, con il vantaggio che non fa male.

Il bisogno di una Governance globale della sicurezza

La sicurezza è considerato il valore numero uno. Semplici risparmiatori, utenti privati, aziende, istituzioni, gli stessi partiti politici sono preda di attacchi informatici. C'è una categoria che rischia più di altre?

Come nella vita ogni vittima ha il suo criminale. Se il singolo utente trova nei *malware* la propria nemesi, aziende e istituzioni sono oggetto di attacchi più articolati. Non è diverso dal rapporto tra la microcriminalità, dedita a borseggi e piccole truffe, e quella più organizzata, come le bande di rapinatori e truffatori. Poi esiste un mondo dell'information *warfare*, dove operano i manipolatori dell'opinione pubblica, e quello ancora più oscuro del cyber warfare, in cui gli Stati combattono la loro guerra virtuale, ma neppure tanto, attraverso gruppi mercenari. Ognuno è esposto a diversi rischi e questo dovrebbe stimolare un sistema di *governance* della sicurezza se non mondiale almeno internazionale.

Quali azioni occorre mettere in campo per sviluppare una strategia globale della sicurezza informatica?

Su questo terreno i problemi sono molti, per questo ho usato prima il condizionale. Una strategia efficace potrebbe essere quella che si persegue a livello europeo che punta attraverso Regolamenti e direttive finalizzate a obbligare tutte le organizzazioni pubbliche e private ad innalzare il livello medio della sicurezza. Due esempi sono il Regolamento Europeo in materia di protezione dei dati e la direttiva NIS per la sicurezza delle reti e dei sistemi informativi. È chiaro che bisogna superare molte difficoltà per arrivare a un governo globale. In primo luogo i diversi Paesi dovrebbero condividere informazioni che non di rado riguardano temi di "sicurezza nazionale", in secondo luogo i tempi di risposta agli attacchi dovrebbero essere misurabili "in minuti" e non in giorni, terzo aspetto le operazioni dovrebbero essere coordinate da una realtà che abbia un effettivo potere di azione sovrannazionale. Questo per citare soltanto alcuni degli ostacoli più evidenti.

Dopo molti anni di impegno aziendale, è riuscito a farsi un'idea precisa delle maggiori vulnerabilità che mettono sotto scacco il business e le aziende?

Da sempre il fattore umano rappresenta la prima vulnerabilità alla quale negli anni si è aggiunto il *"time to market"*. La società dell'informazione ha esasperato i tempi entro i quali i prodotti devono essere immessi sul mercato, soprattutto quando si parla di tecnologia. Il risultato è la rimozione di tutte quelle verifiche che potrebbero rallentare lo sviluppo. Al primo posto tra questi che vengono definiti "ostacoli" le organizzazioni individuano proprio la sicurezza. I controlli richiedono tempo e talvolta producono come effetto collaterale complicazioni in quella che tutti chiamano la *user experience*. In questo modo arrivano sul mercato centinaia di sistemi vulnerabili che finiscono per essere usati in un contesto, quello della Rete, che nelle sue logiche profonde non prevede la sicurezza. Come ho scritto in uno dei miei libri: fare atterrare un Boeing 747 su un'autostrada è possibile ma non è normale, tanto quanto non è normale comprare una lavatrice on line.

Quali sono le modalità più diffuse di cyber attacchi?

Devo dire che la fantasia della criminalità informatica non conosce limiti. Tuttavia il punto di ingresso, anche degli attacchi più sofisticati, è spesso l'essere umano. Messaggi di *spear phishing* accuratamente confezionati sono molte volte il vettore principale. Chi ragiona pensando che il nemico è già nelle nostre case probabilmente avrà messo a punto le strategie più efficaci.

Quali competenze deve avere oggi un esperto di security?

Premesso che non esiste un percorso di studi che prepara a questa professione, diciamo che si tratta di un uomo o donna "capace di appartenere a due mondi" perché deve riuscire a combinare competenze umanistiche a quelle tecnologiche. Un esperto deve conoscere come funzionano i sistemi informatici e avere un'ottima conoscenza di quello che le tecnologie finalizzate alla sicurezza possono e soprattutto non possono fare. Per contro deve dimostrare altrettanta competenza in materia normativa. Per esempio deve avere cognizione di come funziona un firewall e, allo stesso tempo, non può non sapere cosa sia il regolamento Europeo in materia di protezione dei dati e quali vincoli impone.

Sta nascendo un partito anti web, molti invocano il diritto alla disconnessione. Questa improvvisa "marcia indietro" ha a che fare con il diffondersi delle truffe on line, delle frodi, dei furto di identità, e di altri fenomeni che stanno destabilizzando la tranquillità dei cittadini e degli operatori economici?

Non sono tanto convinto che sia la paura di truffe e frodi a spaventare i cittadini, se così fosse sono certo che starebbero molto più attenti, come fanno quando salgono i metropolitana e si tengono ben stretti borse e portafogli. In realtà vedo due altri elementi. Da una parte mi sembra di rivivere le polemiche attorno alla televisione che per anni è stata considerata alternativamente mezzo di manipolazione o strumento di alienazione dalla realtà. Quanto volte le mamme di un tempo intimavano ai figli: "smetti di guardare la televisione che poi diventi stupido!". Il secondo tema è un po' più sottile.

A cosa si riferisce?

A quello che chiamo "effetto Grande Fratello". Sempre più persone iniziano ad avere la sensazione che nulla di quanto facciano in Rete sia privato. Premesso che hanno assolutamente ragione, perché se si utilizzano abbastanza servizi di un operatore come Google, alla fine il sistema saprà tutto di noi. Per questi "navigatori" è difficile barattare la propria vita privata con una manciata di servizi.

Probabilmente bisognerebbe riuscire a rassicurarli, dicendo loro che possono scegliere fino a che punto spingersi nel mare di Internet. Allo stesso modo si dovrebbe lavorare sul tema della protezione dei contenuti della Rete, soprattutto da distorsioni e manipolazioni, penso alle *fake news*.

L'Italia nel suo complesso può definirsi un Paese sicuro?

L'Italia non è un paese sicuro tanto quanto gli altri per il semplice fatto che la forza della sicurezza è pari a quella del suo anello più debole. Di conseguenza in questo mondo completamente interconnesso la debolezza di uno diventa immediatamente di tutti. Il tema del prossimo futuro sarà legato alle infrastrutture critiche e alla relazione che molte di esse avranno con il mondo dell'*Internet of Things*.

Per alzare il livello di protezione degli asset strategici le istituzioni e le imprese che cosa dovrebbero fare?

Le aziende del settore energy, come anche dei trasporti e sanitarie stanno interconnettendo tramite Internet sistemi che fino a ieri erano isolati. Mi riferisco ai cosiddetti sistemi di controllo (SCADA) e ai sistemi industriali (ICS) che governano oggetti piuttosto grossi come centrali elettriche, dighe e via dicendo. Si stratta di sistemi spesso basati su tecnologie non di rado "antiche" con sistemi operativi che risalgono alla fine degli anni novanta o agli inizi del nuovo millennio, con tutte le considerazioni in materia di sicurezza che derivano. Una situazione di questo genere dovrebbe fare riflettere sull'opportunità di incentivare un piano di investimenti serio sul rinnovamento di questi sistemi. Dopo Industria 4.0, sarebbe necessario lanciare il piano Security diciamo 1.0 visto che ci troviamo di fronte a qualcosa che non è mai stato fatto.

La "trincea" della scuola e i "nativi digitali"

Guardiamo ai nativi digitali. Come si fa a imporre una dieta regolare e soprattutto sicura di cellulare e pc alle giovani generazioni che vivono dentro le nuove tecnologie?

Credo che la dieta migliore sia quella in cui si mangia un po' di tutto, ma con moderazione. Tuttavia spesso ci riferiamo a una dieta dallo *smartphone*, non è corretto, perché si tratta di un oggetto che mette insieme un intero mondo. In quella scatoletta non ci sono soltanto i social network, le chat, ma anche quello che per la generazione precedente erano lo stereo, la televisione, la macchina fotografica, la sveglia, l'enciclopedia e l'elenco potrebbe diventare ancora più lungo. Da genitore non mi preoccuperei se i miei figli hanno sempre lo *smartphone* in mano, quanto piuttosto se guardano compulsivamente il loro profilo sui social, se trascorrono le nottate in chat o se passano più di tre ore consecutive a giocare on line. Insomma la dieta dovrebbe essere selettiva. Se parliamo di sicurezza, invece, molto dipende dalla capacità dei genitori di fare in modo che i figli non li tengano allo scuro di quello che vivono oltre quel piccolo schermo.

I social hanno cambiato il profilo della rete, rendendola meno sicura. Esistono delle contromisure per invertire la tendenza?

Purtroppo temo di no, almeno non dal punto di vista tecnologico. I social sono pericolosi perché le persone disprezzano la propria privacy e non si rendono conto che tutte le informazioni che riversano in queste pubbliche piazze possono essere usate contro di loro. Non è possibile scrivere una legge che imponga a liberi cittadini cosa possono o non possono pubblicare sui social della loro vita privata. Certo esiste un regolamento che impone la protezione dei dati, ma da solo non basta. A questo tema ho dedicato un libro: "La *privacy* vi salverà la vita – Internet, social, chat ed altre mortali amenità", che spiega come siamo bravissimi a farci del male da soli anche senza bisogno dell'aiuto dei criminali.

La scuola è una trincea, come si vede dalle cronache di questi giorni. Il cyber bullismo e la violenza amplificata dal web sono fra i pericoli più gravi. Si può contrastare una deriva così pericolosa?

Il bullo c'era in passato, c'è e ci sarà sempre. Esistono oggi due problemi: l'amplificazione dell'umiliazione subita dalla vittima e l'apparente anonimato che garantisce la Rete a tanti "Leoni da tastiera". Sul primo punto poco si può fare, sul secondo invece basterebbe mostrare quanto è facile essere individuati. Non scordiamoci che su Internet è difficile trovare qualcuno soltanto se non sappiamo chi cercare. Il resto è un problema di educazione, per cui dovremmo tutti cominciare a parlare finalmente di strategie culturali.

Tutti "bambini" in cammino verso il futuro

Lei si rivolge a sua figlia più volte nel corso della trattazione. La comunicazione tra generazioni può aiutare ad alzare il livello di conoscenza reale degli strumenti digitali?

Assolutamente sì. Imparo continuamente nuove cose da mia figlia, soprattutto il modo in cui un'intera generazione utilizza le nuove tecnologie, scoprendo anche le potenzialità più nascoste. Per quanto riguarda il versante opposto spero di fare bene il mio mestiere di genitore, magari aiutandola a non commettere nel mondo del virtuale errori commessi nel mondo reale. In fondo il mondo oltre lo schermo riproduce tante delle dinamiche e delle situazioni della nostra tangibile realtà.

"Come pesci nella Rete" ***si conclude con il capitolo* "Venti anni nel futuro". "Questa casa non è un hashtag"** ***ha come epilogo una sezione titolata:*** **"Pochi mesi nel passato".** ***Vuol dire in sintesi che i giovani devono recuperare il valore della memoria e i vecchi impegnarsi a respirare un lembo di futuro?***

Diciamo che ho fatto un pensiero di questo tipo: per noi anziani il futuro è quello che per i giovani è il presente pur vivendo nello stesso momento. In fondo chi ha passato i quaranta guarda con un certo stupore alcune innovazioni tecnologiche (mia nonna avrebbe parlato delle "diavolerie" dei tempi moderni), mentre un diciottenne le considera già parte integrante del suo vissuto quotidiano. Tutto sommato sembriamo più bambini noi quando, osservando un televisore di ultima generazione, esclamiamo: incredibile! che non loro quando si impossessano del telecomando e armeggiando si lamentano: *"Bah! Che televisore avete comprato, ha quattro app messe in croce!!!"*. In modo diverso tutti noi siamo ancora veramente dei bambini. ■

La Quarta rivoluzione industriale ed il suo impatto sulle Forze Armate

Autore: Marc André Ryter

I cambiamenti tecnologici in atto costituiscono una rivoluzione globale nella misura in cui aprono delle prospettive interamente nuove. Essi avranno delle ripercussioni sul comportamento degli individui, delle collettività, delle imprese e delle più diverse organizzazioni, e avranno un impatto crescente sulla sicurezza delle società e degli individui.

Di che si tratta?

I paesi e le società civili si svilupperanno integrando o subendo le evoluzioni tecnologiche. Queste creano delle opportunità in tutti i campi della società, e potranno essere utilizzate per aumentare l'efficacia e la rapidità dei procedimenti. Tuttavia, le nuove tecnologie creeranno anche delle nuove sfide e delle nuove vulnerabilità. I paesi saranno minacciati in modo diverso e dovranno adattarsi al nuovo ambiente. Le nuove tecnologie avranno di conseguenza un'influenza diretta ed indiretta sulle sfide poste alle Forze Armate e quindi sulla loro evoluzione. Esse sostituiranno dei sistemi che sono attualmente cari e complicati. Se si combinano le opportunità nascenti con le nuove vulnerabilità che creeranno, si può prevedere che le evoluzioni tecnologiche in corso influenzeranno le relazioni fra gli Stati nel campo della sicurezza, in senso positivo e negativo. L'attuale discussione sull'introduzione delle nuove tecnologie si concentra soprattutto su due aspetti radicalmente opposti: da una parte le economie sostanziali che sembrano possibili a lungo termine e d'altra parte i costi importanti che potrebbero in partenza costituire un fattore limitante. Tanto più che si dovrà instaurare un nuovo sistema di *governance* e di controlli che comporterà anch'esso un costo. Gli aspetti legati alla sicurezza di questa evoluzione sono ancora troppo spesso assenti dal dibattito.

Lo scopo di questo articolo è di sensibilizzare sulle conseguenze di questa evoluzione e di mettere in evidenza l'impatto sulla sicurezza e sulle Forze Armate, in particolare per l'esercito svizzero, per mostrare a che punto le nuove tecnologie sono pertinenti per il suo sviluppo. In un futuro prevedibile, la maggior parte delle innovazioni tecnologiche in corso saranno integrate nel campo della difesa, indipendentemente dalla minaccia. È certo che saranno necessari degli investimenti importanti e quindi che si produrranno delle conseguenze non trascurabili sui bilanci militari.

Questo articolo non tratterà degli aspetti etici di questa evoluzione, ed in particolare della dimensione etica legata all'autonomia degli armamenti. Questa questione è trattata in un progetto specifico sulla dottrina militare dello Stato Maggiore dell'Esercito e sarà oggetto di una prossima pubblicazione[1].

La quarta rivoluzione industriale, di cui parliamo in questo articolo, è costituita contemporaneamente dalla messa in rete della produzione e dei processi, e dallo sviluppo delle nuove tecnologie a supporto. Di fatto, essa consiste nell'introduzione delle tecnologie digitali in tutte le operazioni quotidiane e nell'intensificazione dell'interazione fra uomo e macchina. Le relazioni uomo-macchina, così come quelle macchina-macchina, muteranno e vedranno aumentare nelle macchine determinate qualità sensoriali, di mobilità e intelligenza, così come specifiche competenze decisionali.

In tutto il mondo, i cambiamenti tecnologici stanno facendo progressi: l'efficienza e l'efficacia dei sistemi sono migliorate, così come il coordinamento tra i sistemi e le azioni da essi gestiti. L'analisi integrata di un gran numero di dati deve permettere di operare in maniera più flessibile

BIO

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

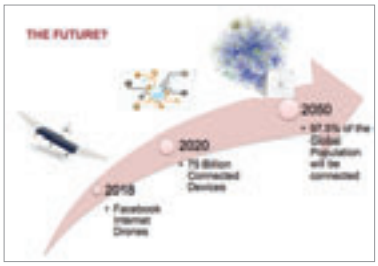


Figura 1 L'evoluzione della connettività (www.isaca.org)

Figura 2 Drone americano Instant Eye (www.usni.org)

Figura 3 Il robot LS3 (Legged Squad Support Systems) della Boston Dynamics. (www.bostondynamics.com)

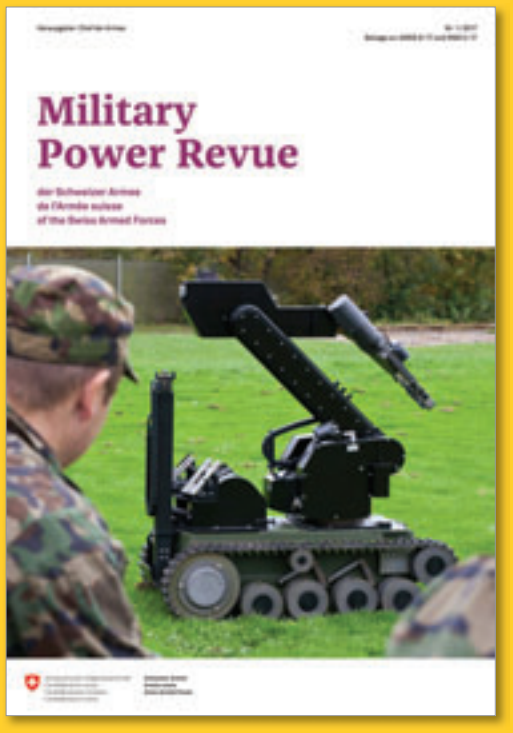
Figura 4 Transporto Tattico Multi-Utilitario (MUTT) della General Dynamics Land Systems (www.defensetech.org/2014/09/25)

Figura 5 Esempio di «LethalAutonomousRobotics» (LARS) e di robot armati autonomi (https://artselectronic.wordpress.com/2013/05/25/lars-lethal-autonomous-robotics/ewww.article36.org/statements/ban-autonomous-armed-robots)

Figura 6 Arme nello spazio (https://sofrep.com/60485/)

Figura 7 Meegaperf, casco EEG (per elettroencefalografia) della società Physip, che misura l'attività cerebrale del portatore e calcola il suo livello di stress e di stanchezza (http://hightech.bfmtv.com/produit/l-equipement-high-tech-au-servicedu-soldat-du-futur-984618.html)

Figura 8 GBU-44/E Viper Strike smartmunition (http://www.deagel.com/library/GBU-44E-Viper-Strike-smartmunition_m02012041700001.aspx)



L'articolo originale del Col. Marc-André Ryter, redatto in lingua francese, è stato pubblicato nella *Military Power Revue of the Swiss Armed Forces* (n. 1/2017, pp. 50-62). L'esercito svizzero ha accordato alla nostra pubblicazione l'onore di tradurlo in esclusiva in lingua italiana. Desideriamo porre i nostri più distinti ringraziamenti al Divisionario UrsGerber, redattore-capo della *Military Power Revue*, al Prof. Alexandre Vautravers, redattore-capo della *Revue Militare Suisse* e, last butnotleast, al Colonnello Marc-André Ryter per la sua disponibilità e per il sostegno accordatoci. Tutti i volumi della *Military Power Revue of the Swiss Armed Forces* possono essere scaricati gratuitamente dal sito dell'Esercito Svizzero: http://www.vtg.admin.ch/en/media/publikationen/military-power-revue.html

e soprattutto innovativa. L'informazione e le idee si diffondono rapidamente e su scala mondiale, senza che le persone abbiano bisogno di spostarsi. Ma questi non sono che alcuni esempi di applicazioni concrete generate dalle evoluzioni tecnologiche.

Se ci si basa sul fatto che nel 2015, l'85% delle macchine non erano ancora connesse e quasi l'80% dei dati non erano classificati e quindi non utilizzabili per generare del sapere, ci si rende conto del salto qualitativo che deve ancora avvenire.

Queste ultime si baseranno sulla moltiplicazione degli oggetti connessi e il conseguente aumento esponenziale del volume dei dati disponibili da trattare. Questo provocherà ripercussioni tali da far parlare di un cambiamento di paradigma, da cui la nozione di quarta rivoluzione industriale[2].

L'evoluzione più significativa concerne il volume dei dati che saranno generati e scambiati e la presa di controllo da parte degli algoritmi. Nel 2020, rispetto al 2015, i dati generati dalle macchine saranno 15 volte di più, e quelli memorizzati 50 volte superiori. Se ci si basa sul fatto che, nel 2015, l'85% delle macchine non erano ancora connesse e quasi l'80% dei dati non erano classificati e quindi inutilizzabili per generare del sapere, ci si rende conto del salto qualitativo che deve ancora avvenire[3]. L'intelligenza artificiale sarà sempre più necessaria se non altro per smistare la massa di dati generata. È preoccupante constatare come la questione della sicurezza non sia sufficientemente integrata in questa evoluzione, la quale implicherà necessariamente dei costi importanti, più elevati di quelli d'acquisto, quando si tratterà di aggiornare la sicurezza dei sistemi.

L'attrattiva della quarta rivoluzione industriale proviene dall'immenso potenziale di un presunto miglioramento in numerosi campi della nostra vita. Sarà quindi difficile frenare, o controllare lo sviluppo in questo campo, malgrado i rischi non ancora completamente valutati, come la possibilità per le macchine in futuro di sfuggire al controllo degli umani.

Già adesso è possibile dire che l'uso che viene fatto dei Big Data non è più sotto controllo e coloro che ne controllano una parte, in particolare il Cloud, possiedono un potere considerevole.

Ma ci sono anche altri rischi, molto più banali, che potrebbero provocare tensioni. La produzione dei sistemi legati alle nuove tecnologie richiede una gran quantità di materiali rari. Ci sarà quindi una competizione crescente per queste risorse. Inoltre, il funzionamento di questi sistemi richiede molta energia, il che ha delle conseguenze importanti e costose sullo sviluppo dell'infrastruttura energetica.

Potrebbe succedere che, a un certo punto, l'intelligenza artificiale prenda il sopravvento sull'intelligenza umana, soprattutto a causa della sua velocità d'evoluzione.

Più a lungo termine, lo sviluppo dell'intelligenza artificiale potrebbe avere delle conseguenze attualmente impreviste e imprevedibili. Potrebbe succedere che, a un certo punto, l'intelligenza artificiale prenda il sopravvento sull'intelligenza umana, soprattutto a causa della sua velocità d'evoluzione. Questo argomento, studiato sotto l'etichetta della *singolarità tecnologica*, non è tuttavia affrontato in questo articolo.

Di quale evoluzione tecnologica si parla?

Si tratta di distinguere le tecnologie dalle loro applicazioni. Di seguito sono elencate le tecnologie attualmente prese in maggiore considerazione fra quelle associate alla quarta rivoluzione industriale. Sono soprattutto di stampo civile, ma hanno un impatto sulla sicurezza per il fatto che possono essere applicate alle Forze Armate, alla conduzione della guerra e in maniera più generale possono essere utilizzate per nuocere:

- Intelligenza Artificiale;
- Internet of Things;
- Robot di nuova generazione;
- Big Data;
- Biologia sintetica;
- Sostanze nootropiche;
- Stampe in 3D o 4D;
- Calcolatori quantistici;
- Tecnologie neuromorfiche;
- Energie rinnovabili, prodotte in loco;
- Nanotecnologie.

Alcune di queste tecnologie sono già utilizzate nelle Forze Armate, mentre per altre deve essere ancora sviluppata una possibile applicazione. La combinazione di queste tecnologie può aprire nuovi orizzonti e mostrare possibili utilizzi al momento ancora ignoti. Klaus Schwab cita per esempio le possibilità di agire direttamente sul sistema nervoso dei combattenti[4].

Per il momento la discussione sui nuovi equipaggiamenti utilizzabili sui campi di battaglia porta alle seguenti applicazioni:

- Droni;
- Robot di combattimento;
- Veicoli autonomi;
- Armi autonome;
- Armi nello spazio;
- Esoscheletri e altri equipaggiamenti che servono a migliorare i risultati dei combattenti;
- Munizioni intelligenti;
- Sostanze che permettono di migliorare l'efficacia dei combattenti;
- Armi cibernetiche[5];
- Armi biologiche e chimiche[6].

È dunque importante seguire l'evoluzione di queste tecnologie e delle loro potenziali applicazioni al fine di dedurre quali sono suscettibili di essere utilizzate da un avversario e quali dovrebbero essere introdotte nell'armata svizzera o perlomeno dovrebbero essere prese in considerazione.

Soprattutto, occorrerà sviluppare adeguate contromisure, per proteggere i nostri soldati e la nostra popolazione in una duplice ottica: prima di tutto bisognerà riuscire a contenere e tenere sotto controllo la diffusione e la capacità di nuocere di queste nuove tecnologie, in particolare di quelle *dual-use*. In seconda battuta, ci si dovrà accertare che i nostri flussi decisionali e i processi per l'introduzione di nuovi materiali siano abbastanza rapidi e flessibili da permetterci di sviluppare e implementare le opzioni selezionate in maniera tempestiva quando dovesse rendersi necessario.

Secondo l'Agenzia Europea della Difesa, ci sono attualmente quattro fattori in rapida evoluzione di cui tenere conto nelle riflessioni sullo sviluppo tecnologico delle Forze Armate:

- La competizione globale per la superiorità tecnologica;
- La nascita di nuovi campi convergenti di conoscenze e di tecnologie;
- I cicli di innovazione sempre più rapidi;
- L'importanza crescente degli investimenti privati sull'innovazione[7].

La combinazione di questi quattro fattori è già una realtà e costituisce il vero carattere rivoluzionario dell'evoluzione tecnologica.

La quarta rivoluzione industriale ed il suo impatto sulla sicurezza

La quarta rivoluzione industriale è come una moneta, a due facce. Da un lato, i progressi tecnologici aprono prospettive positive di sicurezza, maggiore inter-operabilità fra i sistemi, riduzione dei costi, migliore efficacia e rapidità. Questo porterà benefici sia ai settori civili sia a quelli militari e permetteranno una migliore preparazione per situazioni extra-ordinarie, con o senza l'impegno delle Forze Armate. Dall'altro, questi progressi tecnologici implicano anche una gamma molto larga di vulnerabilità e quindi di possibili turbative e manipolazioni. A questo si aggiunge il fatto che il rischio di errori umani a causa della crescente complessità è sempre più elevato. In effetti, la gestione di questi nuovi rischi necessita risorse e competenze spesso nuove e quindi implica un aumento significativo delle interdipendenze. Per le Forze Armate, questo significa una maggiore interdipendenza fra le componenti, ma anche e soprattutto verso l'esterno.

Inoltre, la gestione dei nuovi rischi genera un onere pesante per gli utenti perché si tratta di prevenire incidenti che avrebbero gravi conseguenze per le società.

L'iper-connettività avvantaggia in questo modo gli attori non-governativi e aumenta le loro possibilità di azione, come anche il loro utilizzo quali intermediari.

Schwab parla di un'evoluzione che va verso quella che chiama l'iper-connettività[8]. A suo parere, questa iper-connettività accrescerà ancora le ineguaglianze nel mondo, e quindi le frazionerà ancora di più. Come è stato già dimostrato, questi fenomeni creano condizioni favorevoli per gli estremismi di ogni sorta e contribuiscono a rinforzare la minaccia contro gli Stati e le società. L'iper-connettività avvantaggia in questo modo gli attori non-governativi e aumenta le loro possibilità di azione, come anche il loro utilizzo quali intermediari. Allo stesso tempo, offre maggiori possibilità per compiere azioni criminali, atti di terrorismo o di ricatto, anche ad attori che posseggono risorse limitate. Si tratta qui più di un'evoluzione già in corso, che può tuttavia arrivare a delle conseguenze ben più minacciose di quelle attualmente note.

L'ampio utilizzo dei social media per diffondere propaganda che scredita le istituzioni statali può provocare significativi disordini sociali, e tuttavia si tratta di un'arma a doppio taglio che può essere utilizzata allo stesso modo dai governi.

Numerosi rischi legati all'evoluzione tecnologica possono rimettere in discussione il funzionamento delle società, e costituiscono quindi minacce esistenziali. Il loro potenziale distruttivo è molto alto e genera una sensazione di vulnerabilità. I rischi sono spesso collegati alla memorizzazione dei dati ed ai controlli necessari che ne derivano. I dubbi riguardano cosa viene fatto con i dati accumulati, quali siano le possibilità che vengano utilizzati in maniera illecita o disonesta, aumentando la quantità di informazioni diffuse in rete.

Inoltre, non è sempre semplice definire quali fondamenti giuridici si applichino, soprattutto quando non si sa nemmeno precisamente dove si trovino i dati raccolti *(cloud)*, a chi essi appartengano, chi può consultarli, utilizzarli o modificarli e soprattutto quando le connessioni fra di essi sono poco chiare. Bisogna prevedere la possibilità di correggere o eliminare le informazioni incorrette e prevenire in tutti i modi possibili un uso fraudolento. Tante questioni essenziali che al momento non sono ancora regolamentate. E quando si sa che la gestione dei database e lo sviluppo dei programmi per farlo sono già automatizzati e si basano sull'intelligenza artificiale[9], si comprende appieno quale sia la posta in gioco riguardo i Big Data.

Inoltre, non è sempre semplice definire quali fondamenti giuridici si applichino, soprattutto quando non si sa nemmeno precisamente dove si trovino i dati raccolti *(cloud)*, a chi essi appartengano, chi può consultarli, utilizzarli o modificarli e soprattutto quando le connessioni fra di essi sono poco chiare.

Gli studiosi si stanno al momento concentrando su tre principali categorie di rischio[10]. In primo luogo tutti i rischi legati ad una programmazione incompleta delle macchine e che spingerebbero i robot dotati di un'intelligenza artificiale a non svolgere correttamente la missione inizialmente prevista. Avremmo a che fare in questo caso con degli effetti collaterali negativi. In secondo luogo, i robot potrebbero eseguire la loro missione fino ad un punto che non era stato previsto. Questi effetti di saturazione porterebbero con sé comportamenti potenzialmente pericolosi. Infine, l'intelligenza artificiale implica una certa autonomia delle macchine, che potrebbero andare al di là di ciò che era stato pensato, anche stavolta con effetti negativi. Queste derive dell'autonomia costituiscono senza dubbio il pericolo maggiore per delle macchine che hanno una capacità di apprendimento autonomo.

La prossima sfida consiste nella selezione e verifica delle informazioni. Già oggi, possono essere create intenzionalmente e distribuite molto rapidamente su larga scala quelle note come *fake news*, spingendo a comportamenti irrazionali. Diventa sempre più facile manipolare le folle e alimentare proteste da parte di manifestanti persuasi della loro buona fede.

Figura 9 Sistema MS-177 *multi-spectral imaging* (MSI) con sensori per il prelievo di informazioni a lungo raggio, sorveglianza e riconoscimento (ISR), montato su di un NorthropGrumman RQ-4B Global HawkUnmanned Aircraft System (http://www.unmannedsystemstechnology.com/2016/07/utc-aerospace-systems-to-integrate-isr-sensor-onto-global-hawk-uas/)

Queste *derive dell'autonomia* costituiscono senza dubbio il pericolo maggiore per delle macchine che hanno una capacità di apprendimento autonomo.

È sempre più alto il rischio che la sicurezza dell'individuo venga rimessa in questione dall'impossibilità di accesso a servizi essenziali per tutto ciò che è ancora considerato superfluo ma che è in realtà vitale. Interventi di manipolazione sui sistemi di distribuzione dell'acqua, dell'elettricità o degli idrocarburi, possono creare rapidamente delle situazioni di pericolo. L'interruzionedelle comunicazioni, dell'approvvigionamento di cibo, della rete sanitaria o del traffico aereo, stradale o ferroviario può mettere in pericolo il funzionamento di intere società.

L'evoluzione tecnologica comporta ancora altri rischi che possono essere sfruttati per nuocere e sono per questo significativi da un punto di vista militare. La veloce evoluzione degli hardware e dei software dà vita a una potenziale vulnerabilità legata alla necessità di mantenerli sempre aggiornati, pena una rapida obsolescenza, e questo naturalmente alimenta la dipendenza dei consumatori dai fornitori.

Un'altra vulnerabilità proviene dalla complessità crescente delle reti e dall'impossibilità di proteggerle completamente, in particolare dall'hacking. Questa quasi-impossibilità spinge sempre più organizzazioni, governative e non, a operare su reti chiuse[11].

Riassumendo, le aziende dovranno gestire i rischi derivanti dalle evoluzioni tecnologiche al fine di garantire la loro sicurezza ed in particolare la pace sociale. È difficile prevedere le conseguenze di una automatizzazione ad oltranza e la perdita dei posti di lavoro per gli umani che ne possono derivare.

Implicazioni sulla difesa e le Forze Armate

L'utilizzazione crescente da parte delle Forze Armate delle tecnologie di punta non costituisce in sé una cosa nuova. La nozione di guerra in rete *(network centric warfare/network enabled operations)* è già parte del panorama mentale delle Forze Armate nella maggior parte dei paesi, a diversi livelli, da numerosi anni. Inizialmente, l'obiettivo era quello di collegare fra loro le diverse componenti delle Forze e di mettere a disposizione dei militari collegamenti rapidi e molteplici con differenti tipi di sensori (droni, satelliti, ecc).

Poiché il settore della difesa non è più lo stimolo principale delle evoluzioni tecnologiche, esso dovrà adattarsi alle innovazioni provenienti dall'industria civile.

Le evoluzioni in corso richiederanno un adeguamento da parte delle Forze Armate, perché siano in grado di far fronte a possibili sorprese strategiche. Poiché il settore della difesa non è più lo stimolo principale delle evoluzioni tecnologiche, esso dovrà adattarsi alle innovazioni provenienti dall'industria civile. Tale adattamento riguarderà il *core* della capacità di difesa, e non costituirà più semplicemente un'evoluzione di quanto in essere. In questo modo, verrà superato l'attuale modello C4ISTAR, e sarà il controllo dell'informazione a stabilire e consentire di conservare la superiorità operazionale[12].

La capacità di scegliere e di decidere meglio e più rapidamente dell'avversario, non cadendo vittime di false informazioni e manipolazioni di sistemi, è dunque centrale.

Figura 10 Alcune possibilità di migliorare le capacità dei soldati (http://www.defenseone.com/technology/2015/10/talking-helmets-robot-built-bases-army-peers-future-3d-printing/122551/)

Figura 11 Sempre più informazioni potranno essere integrate nell'immagine del campo di battaglia (http://armypress. dodlive. mil/2016/09/26/big-data-war-games-necessary-forwinning-future-wars/ - consultato li de 01. 03. 2017)

La superiorità nell'ambito dell'informazione deve permettere di assicurare alcuni vantaggi sul campo, quali la capacità di sorprendere l'avversario, la disponibilità e l'adeguatezza dei mezzi, la rapidità dell'azione o la flessibilità della reazione. Essere in grado di effettuare la scelta migliore fra diverse opzioni, e di concentrare i mezzi nel momento e nel luogo corretti,resteranno fattori operativi decisivi. La capacità di scegliere e di decidere meglio e più rapidamente dell'avversario, non cadendo vittime di false informazioni e manipolazioni di sistemi, è dunque centrale. Sono in via di sviluppo e presto saranno introdotti nelle Forze Armate, nuovi sistemi capaci di connettere i sensori, i centri decisionali e di controllo, e quelli di automazione degli armamenti. Inoltre, saranno connessi anche i sistemi che permettono una valutazione costante della situazione al fine di migliorarne l'esecuzione. Tuttavia, anche se le reazioni sono più rapide e più precise, l'automatizzazione della decisione in campo militare ed il fatto che delle macchine possano essere programmate per combattere in maniera autonoma rimangono temi sensibili, soprattutto per le evidenti implicazioni etiche.

Sempre più, le innovazioni derivate dalla ricerca civile si ripercuotono nell'ambito militare con i loro rischi e le loro nuove vulnerabilità. C'è quindi un'inversione completa con il passato, a causa dei costi della ricerca, dello sviluppo, della produzione e della gestione. Tuttavia, le tecnologie riprese nel campo militare sono in linea di principio adattate per aumentare la loro sicurezza, oltre alla loro affidabilità e resistenza.

Dal punto di vista militare, molti aspetti devono essere presi in considerazionein modo prioritario. L'evoluzione delle tecnologie permetterà un maggiore utilizzo, sia quantitativamente che qualitativamente, di nuove dimensioni, in particolare lo spazio e le profondità marittime. Poi, l'analisi di più informazioni in tempi più rapidi creerà un vantaggio permettendo di modificare in corsa le azioni tattiche e la conduzione delle operazioni inter-forze. Ci sarà anche un miglioramento sensibile della comprensione del campo di battaglia *(battle space awareness)*, che sarà basato su una maggiore trasparenza, malgrado le contro-misure che saranno immancabilmente sviluppate. I sistemi saranno in grado di riconoscere più facilmente posizioni, dispositivi e spostamenti di truppe. Saranno, infine, migliorati il sostegno e il coordinamento, le munizioni diventeranno più intelligenti, con meno danni collaterali. Ciò sarà particolarmente vantaggioso nelle aree urbane e nell'utilizzo di una strategia ibrida, dove civili e combattenti saranno mescolati fra loro e quindi difficili da distinguere.

Però ci saranno anche delle conseguenze negative. Un avversario avrà più possibilità di influenzare e disturbare la condotta militare dell'altro, a tutti i livelli. Potrà agire sui suoi sensori, che sono sempre più numerosi, sulle sue reti di comunicazione, come anche sui sistemi di guida o sui fornitori esterni da cui dipendono sempre più le Forze Armate. L'avversario potrebbe riuscire ad accedere alle informazioni-chiave e di modificarle al fine di creare una falsa immagine della situazione. La protezione adeguata dei sistemi costituirà dunque un'assoluta necessità, con la consapevolezza che basta un solo errore di utilizzo ad aprire un varco all'avversario. Per rinforzare questa protezione, sarà inevitabile ricorrere alle tecnologie di verifica *(crosscheck)* basate sull'intelligenza artificiale. A causa della complessità dei loro sistemi, che collegheranno numerose attrezzature ed implicheranno numerosi programmi, con connessioni e punti di accesso multipli, le applicazioni militari saranno particolarmente vulnerabili ai più svariati malfunzionamenti ed interruzioni.

L'introduzione di nuove tecnologie diventa necessaria e addirittura inevitabile poiché la quantità di informazioni disponibili per prendere una decisione giusta è aumentata in maniera esponenziale. L'uso di strategie ibride crea anche un maggiore bisogno di informazioni, poiché diventa più difficile sapere ciò che accade. È necessaria

un'immagine più accurata del campo di battaglia per identificare continuamente le nuove esigenze di informazione. La domanda che si pone è se tutte le informazioni disponibili potranno essere analizzate nei tempi necessari, e se le informazioni rilevanti potranno essere identificate all'interno di un *cloud* formato da un numero quasi infinito di dati. Il rischio di perdersi nei dettagli è molto elevato, come quello di non essere più in grado di distinguere le informazioni e di ricorrere ad un'automatizzazione della separazione dei dati che potrebbe essere fallace.

L'introduzione di nuove tecnologie diventa necessaria e addirittura inevitabile poiché la quantità di informazioni disponibili per prendere una decisione giusta è aumentata in maniera esponenziale.

La digitalizzazione avrà un impatto maggiore su tutte le fasi del ciclo OODA (osservare, orientare, decidere, agire[13]), poiché le nuove tecnologie sono trasversali a ciascuna delle fasi[14]. In particolare, l'osservazione sarà fatta integrando ancor più dati, l'orientamento sarà basato sulla simulazione, la decisione sui numerosi strumenti a supporto e l'azione su quanto raccolto fino a quel momento. Inoltre, le conseguenze del miglioramento della comunicazione, dello scambio e del trattamento di informazioni arriveranno fino alle linee di approvvigionamento.

La "biosfera", cioè ciò che succede all'interno dei corpi dei combattenti, diventerà sempre più uno spazio da prendere in considerazione nel contesto militare.

Le nuove tecnologie non si applicheranno solamente alle macchine, ma anche ai soldati, che potrebbero vedere le proprie capacità di combattimento migliorate da misure tecniche e chimiche. I progressi biologici permetteranno una migliore resistenza al dolore, alla paura e allo stress. La "biosfera", ovvero ciò che succede all'interno dei corpi dei combattenti, diventerà sempre più uno spazio da prendere in considerazione nel contesto militare.

L'introduzione di robot nelle Forze Armate, come anche in campi non-militari, deve prima di tutto liberare i soldati dai compiti pericolosi, sporchi e ripetitivi[15], là dove le necessità di controllo e comando sono limitate, se non assenti. Certo, i robot hanno il vantaggio di non essere sensibili alla fatica, garantiscono una migliore precisione e hanno più forza degli umani, ma hanno anche bisogno di tecnici per la loro manutenzione e hanno dei limiti quando si tratta di reagire di fronte ai cambiamenti, che in fase di combattimento può risultare estremamente limitativo. Di conseguenza, i robot offrono delle ottime prospettive soprattutto nel campo della logistica, (in particolare per la manutenzione) e dei trasporti. Tuttavia, possono essere contemplati altri utilizzi per dei mini-droni o dei robot di piccole dimensioni, come ad esempio per missioni di sabotaggio. Il vantaggio è che sarà possibile lanciare l'operazione affidandola ai robot o droni e le macchine potranno compierla in maniera autonoma e senza necessità di una guida. Certamente, questo genere di azioni può fallire a causa della fragilità delle macchine ed in particolare dei loro sensori, macchine da presa, microfoni, GPS, ecc. , o anche dei loro motori.

Le innovazioni tecnologiche permettono di migliorare contemporaneamente i procedimenti da seguire, le *performance* dei soldati e degli armamenti.

Queste riflessioni mostrano che esistono chiaramente due campi ben diversi interessati dall'introduzione delle nuove tecnologie nelle Forze Armate. In primo luogo, certe tecnologie permettono di migliorare le prestazioni di base e la sistemazione della disponibilità di base, automatizzando numerose funzioni. I sensori permettono di effettuare delle manutenzioni solamente quando queste ultime sono veramente necessarie. In secondo luogo, c'è il livello della vera e propria conduzione delle operazioni, giù giù fino al soldato semplice. Le innovazioni tecnologiche permettono di migliorare contemporaneamente il procedimento da seguire, l'efficienza dei soldati e degli armamenti. Dei sensori indossati dai soldati permetteranno di identificare in tempo reale le misure da prendere per garantire la massima efficacia nel combattimento e daranno delle indicazioni che costituiranno un fattore nuovo ed importante nelle decisioni. Le nuove tecnologie si dimostrano così adatte sia a supportare la gestione di numerosi siti, strumenti o macchine, sia quando si tratta di coordinare processi a diversi livelli.

A causa della sua promettente potenzialità di miglioramento, l'intelligenza artificiale sarà certamente utilizzata in maniera crescente nelle Forze Armate. Questo sviluppo si farà in funzione di cinque fattori che giocheranno tutti un ruolo-chiave:

- la rapidità del lavoro delle macchine in tutti i campi, quali l'analisi dei dati, l'allerta,la difesa nel cyber-spazio, o, ad esempio, la guerra elettronica;
- la complementarietà crescente fra l'uomo e la macchina, in particolare nel processo decisionale;
- il miglioramento delle capacità dei soldati di analizzare l'ambiente circostante e di reagire in modo adeguato;
- l'impegno combinato di uomini e macchine per aumentare l'efficienza;
- l'assunzione di sistemi di armi autonome, che saranno resistenti agli attacchi cyber ed elettronici[16].

Questo dimostra ancora una volta che la maggior parte delle nuove tecnologie avranno un ruolo centrale sia nelle Forze Armate sia in campo civile. La problematica del doppio impiego, legata a quella della proliferazione, avrà delle implicazioni importanti nel campo della sicurezza. Una sempre maggiore quantità di rilevatori e sensori richiederà la creazione di sistemi atti a unificare e organizzare questa moltitudine di dati, che a loro volta aumenteranno la necessità di protezione a vari livelli. Particolarmente sfidante sarà anche garantire la facilità di utilizzazione.

Impatto sulla dottrina ed il campo di battaglia

Appare evidente dunque che l'evoluzione tecnologica avrà delle conseguenze sulla natura dei conflitti e genererà una metamorfosi più o meno rapida del campo di battaglia. È tuttavia ancora difficile prevedere esattamente come e fino a che punto le nuove tecnologie cambieranno la maniera in cui i paesi condurranno le loro operazioni e quale sarà il loro impatto sulle guerre. In particolare, sarà sempre più difficile fare chiaramente una distinzione fra lo stato di pace e lo stato di guerra. Allo stesso modo, nei conflitti futuri sarà molto complesso distinguere fra combattenti e non-combattenti[17]. In futuro, infatti, le guerre saranno sempre più caratterizzate da una combinazione di azioni su scala locale e globale in tutte le diverse sfere di operazione. Saranno in pratica un insieme di azioni militari e/o terroristiche su una piccolissima scala con delle campagne di grande levatura, il tutto sostenuto da una propaganda trasversale. I conflitti saranno caratterizzati da una combinazione di ogni sorta di azione partendo da quelle di guerra classica fino a quelle meno convenzionali. I social network avranno un ruolo sempre maggiore, sia nel campo della propaganda e della disinformazione, sia in quello del reclutamento. Il potenziale esatto delle nuove tecnologie non si presta all'ottimismo poiché le nuove armi saranno più facili da acquistare e maggiormente dannose.

…la distinzione fra combattenti e non-combattenti sarà una sfida maggiore dei conflitti futuri

L'evoluzione delle tecnologie mira a diminuire le incertezze del campo di battaglia. Tuttavia, e malgrado lo sviluppo esponenziale della massa di informazioni disponibili a tutti i livelli, è poco probabile che l'effetto sorpresa sparisca dal campo di battaglia. Ci saranno dei limiti alle capacità di anticipare le decisioni dell'avversario, malgrado i mezzi di supporto sempre più efficienti. Le evoluzioni tecnologiche aumenteranno anche le capacitàdi sorprendere l'avversario[18], principalmente grazie alle possibilità di indurlo in errore. Così, nel campo dell'informazione, le nuove tecnologie consentiranno infatti nuovi modi per diffondere false informazioni relative alle intenzioni sulle future operazioni. Le nuove tecnologie aumenteranno la capacità di evitare la sorpresa e l'attitudine a sorprendere.

Un'altra conseguenza dell'evoluzione tecnologica sarà l'immediata disponibilità di maggiori informazioni fino all'ultimo soldato. Per esempio, sarà possibile introdurre dei droni che trasmetteranno immagini direttamente al soldato per fornire un'immagine precisa dell'ambiente circostante. Allo stesso modo, dei sensori sugli uomini e le macchine permetteranno di avere un'immagine dello stato fisico dei combattenti e delle necessità di manutenzione dei sistemi. In particolare per questi ultimi, queste indicazioni permetteranno di migliorare in modo sostanziale la loro funzionalità. Questo potrebbe rivelarsi essenziale per esempio sugli aerei da combattimento[19].

Delle questioni fondamentali si pongono in questo contesto a proposito del futuro ruolo del soldato, che nel corso di questa evoluzione potrebbe perdere la sua autonomia, insieme alla libertà di decisione sul come affrontare una data situazione.

Per quanto riguarda le formazioni, l'evoluzione nel campo militare potrebbe rimettere in discussione la *Auftragstaktik* – che lascia margine di libertà e scelta al soldato – e favorire una condotta più rigida nel senso della *Befehlstaktik* – che invece accentra il potere decisionale nei superiori in grado.

Ma, d'altro canto, se si considera la quantità di informazioni rese disponibili dalle nuove tecnologie e la facilità con cui è possibile diffonderne di false, appare evidente che il soldato dovrà conservare una facoltà di analisi e di decisioni proprie. Potrebbe anche darsi che si ponga la questione della fiducia che potranno riporre i capi militari ed i soldati nei sistemi che dovrebbero aiutarli. Così sarà necessario impegnare le nuove tecnologie per supportare i militari e non per sostituirli[20]: i sistemi automatizzati saranno semplice sostegno alle capacità analitiche del soldato, che rimarrà l'elemento centrale che interagisce con l'ambiente in cui si trova e gli attori presenti in questo quadro. Le qualità di analisi degli individui resteranno essenziali nell'ottica di garantire la resilienza di un sistema che sarà capace di adattarsi meglio all'evoluzione del combattimento.

Ma anche la natura stessa della condotta del combattimento sarà influenzata dagli sviluppi tecnologici. Si porrà la questione di sapere fino a che punto si potrà lasciare condurre il combattimento in maniera autonoma da robot o altre armi intelligenti artificiali, cioè senza che le azioni siano dirette dall'essere umano. Fin dove si può delegare la decisione di aprire il fuoco? Questi aspetti etici riguardano in primo luogo la decisione di colpire senza intervento umano, ma devono essere tenuti in considerazione anche altri aspetti, come ad esempio le misure che potrebbero prendere le macchine per assicurare la propria sopravvivenza.

La predominanza del settore civile nello sviluppo delle nuove tecnologie ha analogamente delle conseguenze. Il mercato civile, che è orientato unicamente sul profitto, progredisce in fretta e in fretta appaiono nuove possibilità. L'approccio delle Forze Armate non può modificarsi così rapidamente, né costantemente adattarsi a causa di una novità tecnologica. Bisognerà dunque ridefinire ciò che deve contenere una dottrina militare, come essa può modificarsi e soprattutto identificare le evoluzioni significative. La conseguenza sarà uno scarto crescente fra le possibilità tecnologiche esistenti ed i sistemi in uso nelle Forze Armate.

Le qualità di analisi degli individui resteranno essenziali nell'ottica di garantire la resilienza di un sistema che sarà capace di adattarsi meglio all'evoluzione del combattimento.

Globalmente, le nuove tecnologie genereranno nuovi rischi per le Forze Armate, che possono essere classificati in sei gruppi distinti:

1 In primo luogo, gli sforzi per ridurre costantemente la lunghezza del ciclo decisionale e aumentare il volume delle informazioni analizzate provoca un incremento del numero delle interazioni lungo tutta la catena di comando e aumenta dunque la possibilità di errore.

2 In seconda battuta, il vantaggio di poter reagire rapidamente al mutare della situazione implica però il rischio che i livelli più alti vengano coinvolti direttamente nelle decisioni di livello tattico.

3 Le capacità dei sistemi susciteranno aspettative sempre più elevate da parte dei soggetti decisionali, il che può comportare paralisi sistemiche per parecchie ragioni. Prima di tutto, nel caso in cui nessuna decisione venga presa poiché si aspettano sempre delle informazioni complementari; poi, se nessuno decide, rimanendo in attesa di istruzioni. Infine, nel caso in cui i sistemi diano delle indicazioni giudicate insufficienti.

4 I sistemi di trasmissione dati si indeboliscono a causa dei volumi da trasmettere, il che genera interruzioni e un rallentamento generalizzato dei cicli di decisione.

5 Le informazioni corrette non possono più essere identificate nella mole dei dati a disposizione.

6 L'aumento del volume dei dati e delle informazioni disponibili, aggiunti alla moltiplicazione degli interventi di parti in causa sempre più numerose, può facilmente generare il caos.

La possibilità di vedere paesi o attori affrontarsi su un campo di battaglia unicamente attraverso l'intermediario di robot è qualche volta evocata da alcuni autori[21]. Tuttavia, esistono molte ragioni per essere cauti in tal senso. In primo luogo è difficile, nella maggior parte dei Paesi ed in particolare in Europa, immaginare larghe zone non abitate e nelle quali potrebbero svolgersi delle guerre fra robot. In seguito, anche in caso di battaglie in zone disabitate, dei combattimenti fra robot o altre macchine avranno certamente delle conseguenze per la popolazione in caso di distruzione o di danni provocati alle infrastrutture critiche.

Il cyber-spazio come campo di battaglia particolare

La necessità di trattare specificatamente del cyber-spazio deriva dal fatto che una guerra in questo ambito è spesso considerata come la minaccia principale legata allo sviluppo tecnologico in atto. La cyber-guerra e le cyber-vulnerabilità sono spesso evocate quando si parla di nuove tecnologie e del loro impatto sulla sicurezza. Settori interi della società possono essere paralizzati o messi fuori servizio attraverso delle azioni in campo cyber. Ciò è dovuto in parte al fatto che le conseguenze di attacchi cyber sono difficili da valutare, e possono persino rivoltarsi contro l'aggressore. La rilevanza di questo tema è stata dimostrata ripetutamente durante l'ultimo decennio. Alcuni governi e ministeri sono stati presi di mira direttamente, così come compagnie private di importanza vitale e strategica per il proprio paese. Sono aumentati sempre più gli attacchi nel cyberspazio, anche fra Stati. I rapporti di forza generano la creazione di frontiere erette come misura di protezione. La dimensione umana e politica rimane tuttavia essenziale nel cyberspazio poiché, al di là degli aspetti tecnici, c'è una reale giustapposizione fra strategie ed interessi che mirano a scopi concreti, dunque non più né virtuali né immateriali. Parecchi Stati, come la Cina e la Russia, cercano di imporre il loro controllo anche nel cyber-spazio e non si vergognano di utilizzarlo per il loro profitto. Quest'ultimo è diventato un campo di battaglia come il suolo, l'aria, il mare, lo spazio[22], con un potenziale che diventa sempre più evidente.

Riferendosi alla definizione di cyber-spazio come di uno spazio costituito da 3 strati distinti[23], si possono mettere in evidenza i differenti tipi di azione ostile possibili in ciascuno.

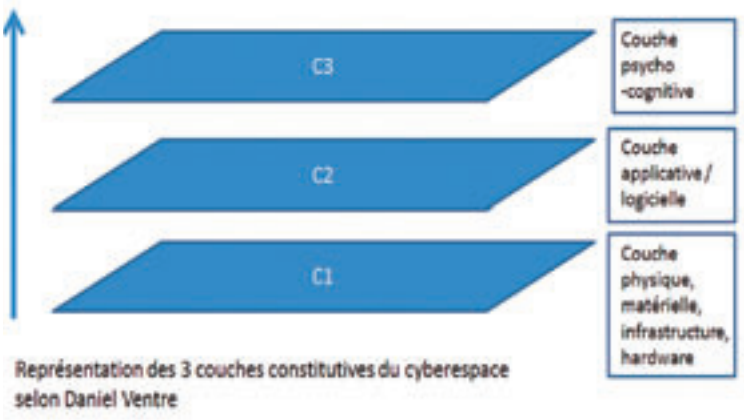


Figura 12 I 3 strati dello spazio cibernetico: strato psico-cognitivo; Strato applicativo/software; strato fisico, materiale, infrastrutture, hardware. (Daniel Ventre)

(1) Nello strato fisico, si possono considerare degli attacchi contro infrastrutture, equipaggiamenti, armamenti o reti. Èinteressante notare che, in questo strato, è particolarmente evidenteil legame fra cyber-spazio e gli altri. Un raid aereo può per esempio distruggere edifici che accolgono dei server e così bloccare l'operatività nel cyber-spazio. L'isolamento del cyber-spazio come un campo di battaglia particolare è dunque del tutto relativo. (2) Nello strato software gli attacchi si svolgono spesso attraverso l'introduzione di malware, che permettono di distruggere i sistemi ed i software dell'avversario, renderli inoperanti o prenderne il controllo. Infine, (3), nello strato cognitivo, un avversario punterà all'appropriazione o modifica dei dati accumulati o trasmessi, al fine di spingere l'avversario a prendere decisioni sbagliate. Si nota qui la quantità di azioni possibili contro le Forze Armate nel cyber-spazio e le numerose vulnerabilità che devono essere controllate. È molto difficile fissare delle priorità univoche: le possibili conseguenze nei tre strati potrebbero rivelarsi fatali per il sistema globale e praticamente tutte le azioni si configurano come indispensabili per la sicurezza militare.

Il cyber-spazio deve essere considerato come un teatro di operazioni completo, anche se spesso è utilizzato in parallelo con altri ambienti. Bisogna essere coscienti che il cyber-spazio, a causa delle possibilità che offre e dei disastri che può generare, può essere utilizzato in maniera esclusiva, anche se i benefici delle azioni si situano in altri ambiti, come l'economia. Non stupisce dunque che vengano poste delle domande in rapporto alla natura dei conflitti ed al limite a partire dal quale un Paese può sentirsi attaccato ed in posizione legittima di difendersi se è vittima di attacchi cyber. La minaccia all'economia di un Paese può in effetti essere considerata sempre più come un'aggressione bellica, a causa delle conseguenze spesso potenzialmente molto simili a quelle di un conflitto classico. La crescita della connettività che mette sempre più oggetti in rete non fa che rinforzare questo rischio. Il dominio degli Stati Uniti in questo spazio, e la sorveglianza che possono esercitare, spinge sempre più Stati a voler disporre di proprie infrastrutture al fine di poterle controllare, filtrare e all'occorrenza bloccare.

Il cyber-spazio deve essere considerato come un teatro d'operazione completo, anche se spesso è utilizzato in parallelo con altri ambienti.

Altri attacchi sono più chiaramente identificabili. È il caso di quando interferiscono con ambiti civili, al punto di minacciare il corretto funzionamento della società. Le reti in continua crescita nelle società moderne diventano sia obiettivi sia vettori di attacchi. Infine, come nel caso di un attacco convenzionale, è la sicurezza della popolazione che viene messa in pericolo. Una guerra nel cyber-spazio può così portare alla vittoria attaccando le infrastrutture civili critiche nei campi dell'approvvigionamento energetico (acqua, gas, elettricità), della salute, del traffico stradale, ferroviario e aereo, e di beni in generale. È quindi prevedibile che certi paesi reagiranno a degli attacchi cyber, laddove l'aggressore può essere identificato, attraverso le azioni militari convenzionali. Durante dei conflitti aperti, le armi cyber sono utili, nella misura in cui permettono di disturbare o manipolare i sensori, le comunicazioni e quindi il processo decisionale.

…ricordiamo ancora che ilcyber-spazio è lo spazio d'elezione per l'utilizzodell'intelligenza artificiale, poiché da sola essa può gestire a suo vantaggio la moledi informazioni che vi si trovano ed utilizzare l'immensa rete costituita da internet.

In tutti i casi, per un aggressore il vantaggio principale di utilizzare il cyber-spazio viene dalla difficoltà per il suo avversario di riconoscere che è attaccato e di identificare l'autore dell'attacco. Un aggressore può così essere non soltanto uno Stato o un gruppo armato, ma anche un pirata isolato, un gruppo terrorista con mezzi limitati, una micro-cellula di attivisti di ogni genere, o ancora dei gruppi criminali motivati unicamente dal guadagno. Può agire ovunque ed istantaneamente. Di fatto il cyber-spazio permette ad ogni individuo che per una ragione o un'altra è in disaccordo con uno Stato di combatterlo e di causare dei danni importanti. La flessibilità del cyber-spazio permette ad ogni attore o ad ogni utente di costruire "il suo spazio in funzione della sua utilizzazione, delle sue rappresentazioni, dei suoi interessi".[24] È molto difficile riconoscere un atto di guerra che mira a nuocere ad un paese e alla sua popolazione e a distinguerlo da un atto criminale.

In conclusione, ricordiamo ancora che il cyber-spazio è lo spazio d'elezione per l'utilizzo dell'intelligenza artificiale, poiché da sola essa può gestire a suo vantaggio la massa di informazioni che vi si trovano ed utilizzare l'immensa rete costituita da internet.

Conclusioni e conseguenze

L'introduzione delle nuove tecnologie, che globalmente costituisce la quarta rivoluzione industriale, implica anche dei rischi e delle opportunità, sia per il campo civile sia per quello militare. Il ruolo e l'equipaggiamento delle Forze Armate, oltre che la diversità degli strumenti nel senso più ampio, devono evolvere. Il volume dei dati scambiati e da analizzare ("info-obesità"[25]) al fine di dedurne un sapere utilizzabile potrebbe costituire un limite allo sviluppo e all'introduzione delle nuove tecnologie in generale, e in seno alle Forze Armate in particolare. La manutenzione potrebbe creare dei limiti, anche se potrebbe essere anch'essa almeno in parte automatizzata.

Dei paesi che non sono super-potenze o che non sono membri di alleanze militari, come la Svizzera, non avranno le risorse per seguire continuamente il ritmo delle evoluzioni tecnologiche ed introdurre dei sistemi complessi nelle loro Forze Armate.

I costi costituiscono senza dubbio il limite più importante. Pochi paesi potranno finanziare delle Forze Armate che dispongano di tutti questi nuovi sistemi.[26] Dei paesi che non sono superpotenze o che non sono membri di alleanze militari, come la Svizzera, non avranno le risorse per seguire continuamente il ritmo delle evoluzioni tecnologiche ed introdurre dei sistemi complessi nelle loro Forze Armate. La loro dipendenza dalla ricerca e dal sostegno del settore privato andrà aumentando piuttosto che diminuire. Queste limitazioni non cesseranno di esistere, anche se l'*Internet of Things* ridurrà almeno in parte i costi in numerosi campi, e migliorerà l'efficacia dei mezzi impegnati, sia nelle missioni di sostegno sia in quelle di combattimento. La protezione dei sistemi ed il bisogno di specialisti genereranno costi importanti, ciò che potrebbe portare a un gioco a somma zero, in cui i guadagni in efficacia e la riduzionedel numero dei sistemi potrebbero essere controbilanciati dall'aumento dei costi dei materiali e del personale.

L'importanza del ruolo dell'essere umano, e quindi la necessità di mantenerne inparte l'intervento, è un tema centrale e determinante.

L'impatto della crescente messa in rete delle macchine, soprattutto se queste ultime dispongono di una certa autonomia, rimane per il momento difficile da valutare. L'importanza del ruolo dell'essere umano, e quindi della necessità di mantenere in parte l'intervento umano, è un tema centrale e determinante. Parecchi autori concordano sul fatto che l'intervento ed il lavoro umano continueranno ad avere tutta la loro importanza, anche nel campo della raccolta dei dati e del loro caricamento nei sistemi.[27] Non potrà essere tutto automatizzato. Si tratterà di definire degli spazi specifici nei quali le macchine possono agire in maniera autonoma, ed altri in cui l'intervento dell'essere umano rimane indispensabile. Si porrà senza dubbio la questione di sapere se è opportuno dare alle macchine il potere di correggere certe decisioni degli esseri umani quando esse giudicheranno che si tratta di un errore. In questo caso, la macchina prenderà in qualche sorta il controllo totale dell'azione.[28]

Nondimeno, la capacità della difesa di integrare e controllare lo sviluppo delle nuove tecnologie sarà la chiave della sicurezza nel futuro. Questo sviluppo, come con gli antichi sistemi d'armi meno sofisticati, si dipanerà così su due assi opposti: le nuove tecnologie saranno utilizzate da un lato per migliorare l'efficacia e dall'altro per migliorare la protezione. La capacità di distruggere e la capacità di sopravvivere conserveranno le loro importanze rispettive ed il progresso tenderà a metterle in una situazione di parità. Le nuove tecnologie trarranno vantaggio dagli sforzi militari, che le renderanno più affidabili e più resistenti.

La dimensione umana rimarrà quindi una posta in gioco essenziale, anche per la Svizzera. Ci vorranno sempre più specialisti per gestire e manutenere le macchine, anche se queste ultime avranno un grado elevato di autonomia. Sarà anche necessario un numero maggiore di persone capaci di interpretare i dati. Nel caso di una milizia come l'armata svizzera, si pone la questione di sapere se si potrà trovare il numero necessario di specialisti civili soggetti al servizio militare, se si avrà la capacità di formarli secondo necessità o se si dovrà procedere ad una professionalizzazione del settore.

Alla fine, si porrà la questione dell'importanza dell'intuizione nel processo decisionale. Essa non potrà essere sostituita da processi automatizzati, anche se l'intelligenza artificiale avrà la capacità di apprendere dalle esperienze passate.

Nel caso di una milizia come l'armata svizzera, si pone la questione di sapere se si potrà trovare il numero necessario di specialisti civili soggetti al servizio militare, se si avrà la capacità di formarli secondo necessità o se si dovrà procedere ad una professionalizzazione del settore.

Bisognerà anche considerare la possibilità di attacchi cyber e come rispondere, in maniera proporzionata, quando l'attacco è accertato. La conseguenza logica è che bisogna disporre di una capacità offensiva in questo settore. Il dibattito sulla possibilità di rispondere ad un attacco cyber con delle azioni nel campo convenzionale mostra quanto siano interlacciate le relazioni fra i diversi spazi.

Non bisogna dimenticare che le evoluzioni tecnologiche saranno vantaggiose anche per attori non-governativi, principalmente a causa della miniaturizzazione e del calo dei costi che prevedibilmente ne deriverà. Ciò aprirà nuove prospettive per questi attori, e quindi necessiterà di una risposta degli Stati, vale a dire dovranno essere individuate le possibili reazioni alle nuove vulnerabilità. La cooperazione fra le industrie civili e militari, e fra le nazioni, diventerà una caratteristica centrale dello sviluppo delle Forze Armate, sia per ragioni di bilancio che tecnologiche.

L'evoluzione verso una maggiore digitalizzazione, in particolare nelle Forze Armate, sarà favorita da quattro fattori principali. In primo luogo (1) ci sarà il calo dei prezzi dei sensori e captatori di ogni genere, e anche la riduzione delle loro dimensioni. In seguito (2), la crescita della connettività con delle reti sempre più interconnesse e sempre più competitive fornirà la base necessaria a questo sviluppo. Ci sarà anche (3) una miniaturizzazione degli apparecchi di stoccaggio e di trattamento dei dati. Infine, bisognerà contare (4) su nuovi programmi che permetteranno di trattare i dati al fine di identificare le azioni adeguate e metterle in atto.

Ma, d'altro canto, ci saranno anche cinque fattori che limiteranno senza dubbio l'espansione delle nuove tecnologie sul campo di battaglia: (1) le condizioni metereologiche, (2) la distinzione fra combattenti e non-combattenti, (3) la pirateria/sabotaggio informatico, (4) la velocità dello sviluppo dei sistemi che provocherà dei problemi fra le diverse versioni dei prodotti e (5) gli atri rischi implicati.

Questi limiti provengono dal fatto che l'iper-connettività può generare degli errori, e bisognerà quindi elaborare dei meccanismi di controllo per prevenirli.

L'utilizzo delle nuove tecnologie da parte delle Forze Armate implica che queste ultime siano esposte agli stessi rischi della società civile. Il controllo dell'intelligenza artificiale rappresenterà la sfida centrale, poiché le macchine potranno agire con azioni liberamente pensate. In particolare la distinzione fra amici e nemici rappresenterà una sfida che sarà difficile da delegare alle macchine.

Riassumendo, per l'armata svizzera, tre sono le tappe fondamentali che dirigeranno l'integrazione delle nuove tecnologie:

- La definizione dei bisogni al fine di ottenere valore aggiunto;
- L'identificazione delle soluzioni possibili in rapporto alle tecnologie esistenti o in sviluppo;
- L'adattamento delle tecnologie scelte agli ostacoli nell'utilizzo militare, in particolare nel campo della sicurezza.[29]

Durante tutto questo processo, bisognerà ancora integrare la problematica della compatibilità fra macchine e programmi di generazioni differenti e che potrebbero entrare in conflitto. È probabile che l'armata svizzera non potrà, per ragioni finanziarie principalmente, seguire ogni tappa tecnologica e adattare costantemente l'insieme dei suoi mezzi. Ci sarà quindi un adattamento ed un'integrazione progressiva di nuove tecnologie collaudate, come ciò che si fa già con gli FA-18, che possono essere almeno in parte considerati come dei computer volanti. Altre applicazioni possono essere prese in esame nell'automatizzazione di certi sistemi d'armi, secondo un modello similare. ■

1 Martin Krummenacher : « Letale autonome Waffensysteme - FluchoderSegen ? EthischeBetrachtungenundsozialtechnischeVergleiche » (Arbeitstitel).
2 Vedi : Bloem, Jaap, van Doorn, Menno, Duivestein, David, Maas, René e van Ommeren, Erik : « The Fourth Industrial Revolution : Things to Tighten the Link Between IT and OT », VINT Research Report 3, Groningen, 2014,p.4.
3 Tutte questecifre si ritrovano in Wind River Systems : The Internet of Things for Defense, White Paper, 10/2015, p.3.,disponibile su http://events.windriver.com/wrcd01/wrcm/2016/08/WP-IoT-internet-of-things-for-defense.pdf (consultato il 21.03.2016).
4 Vedi: Schwab, Klaus, « The Fourth Industrial Revolution », WEF, 2016, pag. 88.
5 Le possibilità di questearmi sono spiegatesegnatamentenell'articolo di Freedberg, Sydney J. Jr, « Wireless Hacking in Flight : Air Force Demos Cyber E-130 », disponibile su http://breakingdefense.com/2015/09/wireless-hacking-in-flight-air-force-demos-cyber-ec-130/, consultato il 21.03.2017.
6 Per unavisione di insieme edunaanalisidettagliata di tutte le nuove tecnologie che rilevano del campo della sicurezza, riferirsiall'opera di Ladetto, Quentin : « Technologiefrüherkennung: Trends und Potenziale2015-2025 », armasuisseWissenschaft + Technologie, Thun,2015.
7 Vedi : « The next industrial (r)evolution : Wat implications for the security and defencesector ? », in EuropeandefenceMatters, EuropeanDefence Agency, Nr.10/2016, p. 13.
8 Vedi: Schwab, Klaus, « The Fourth Industrial Revolution » WEF, 2016, p. 80.
9 Vedi : Tuck, Jay: « Evolution ohne uns »,Kulmbach, PlassenVerlag, 2016, p. 32.
10 Citato da Demeure,Yohan : « Les risques liés à l'intelligence artificielle enfin pris au sérieux », Science et Vie, 05.07.2017, p.2.
11 Anche se il caso STUXNET ha dimostrato che un taglio completo delle reti con l'esterno (air gao) non costituisce più una protezione assoluta..
12 Vedi : Goetz, Pierre et Cahuzac-Soave, Olivia : « Impact de la numérisation sur l'exercice du commandement », Compagnie Européenne d'Intelligence Stratégique (CEIS). Les notes stratégiques, décembre 2015, pp. 11-12.
13 Observer, Orienter, decider, agir nel testo originale
14 Vedi: Goetz, Pierre e Cahuzac – Soave, op.cit. pp. 14-15.
15 Vedi : Bloem, op. cit , p. 13. Egli parla della capacità dei robot di occuparsi di tuttociòche è coperto dalle 3 D : « dirty, dangerous and dullwork ».
16 Vedi : Hwang, Jennie S. : «The Fourth Industrial Revolution (industry 4.0) : Intelligent Manufacturing», SMT Magazine, July 2016, p. 14.
17 Vedi : Schwab, Klaus, « The Fourth Industrial Revolution », in ForeignAffairs, December 2015.
18 Vedi : Hémez, Rémy : « L'avenir de la surprise tactique à l'heure de la numérisation », études de l'Ifri, N0 69, Juillet 2016, pp.25-27.
19 Vedi : Mariani, Joe, Williams, Brian and Loubert, Brett : « Continuing the march : The past, present, and future of the IoT in the military », Deloitte UniversityPress, 2015, pp. 11-13.
20 Vedi : Wood, Colin, D.. «The Human Domain and the Future of ArmyWarfare : Present as Prelude for 2050», in Small Wars Journal, August 2016, p. 3.
21 Per esempio da Swab , Klaus, « The FourthIndustrialRevolution, WEF , 2016, p. 85.
22 Vedi : Cattaruzza, Amaël e Sintès , Pierre : « Geopolitique des conflits », Edition du Bréal, Mesnil-sur-l'Estrée, 2016, p. 148.
23 Vedi : Ventre , Daniel : « Le Cyberespace : définition, représentation », Revue de Defence Nationale, Juin 2012, No 751, p. 36.
24 Vedi : Cattaruzza, Amaël e Sintès, Pierre, op. cit. p. 152.
25 Vedi : Hémez, Rémy, op. cit. p. 27.
26 Bloem stima che fra il 2013 ed il 2016, quasi 95.000 robot di nuova generazione sono stati immessi nel mercato, per un costo totale di 14 miliardi di dollari (cioè quasi 150.000 dollari l'uno). In Bloem, op, cit., p. 14.
27 Per esempio Zheng, Denise E. e Carter, William A. : « Leveraging the Internet of Things for a More Efficient and Effective Military », Center for Strategic and International Studies (CSIS, Report of the CSIS Strategic Technologies Program, September 2015, p.19.
28 Vedi : Haski, Pierre : « Faut-il avoir peur de l'intelligence artificielle », Nouvel Observateur, 26.08.2016, p. 7.
29 Adattato da Goetz, Pierre e Cahuzac-Soave, op, cit., p. 34 .

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

GDPR per l'Advanced Analytics: Riflessioni

Autore: Marco Schonhaut

I dati sono l'oro del terzo millennio e, come è stato per la corsa all'oro, oggi si assiste ad una profusione di carovane speranzose e vogliose di trarre dalle vene dell'informazione il maggior profitto possibile. Le leggi stilate dall'Europa (GDPR – General Data Protection Regulation) e i relativi accordi con gli Stati Uniti (il Privacy Shield) volte alla regolamentazione sull'uso dei dati personali e alla corretta applicazione dei principi di privacy, vengono da molti viste come una fastidiosa imposizione che rallenterà i potenziali è già di per sé faticosi investimenti sulle nuove possibilità offerte dal digital automation, machine learning e dall'intelligenza artificiale per ottimizzare il business in modo sempre più maniacale.

In verità il proposito più profondo di queste leggi è di correre al riparo contro una malacreanza ormai instillata nel vivere quotidiano che banalizza il valore reale dei dati considerandoli beni di consumo usa-e-getta da scambiare senza riflettere, come ai tempi del colonialismo in cui le popolazioni indigene barattavano pietre preziose o la propria libertà in cambio di collane di perline.

Ognuno di noi dovrebbe iniziare a concepire ed approcciare queste leggi non come un obbligo da mettere in pratica ma come un lascito costituzionale per la società del futuro, per far sì che questa resti un mondo civile con delle fondamenta salde dove le aziende, sempre più solide, siano una naturale espressione di esso.

Non è un caso che il testo della GDPR sia composto più da principi che da regole: le regole infatti al più si rispettano, ma i principi si sposano.

In sostanza la regolamentazione europea una volta letta e capita può essere "distillata" in tre essenziali linee guida:

RISPETTA I DATI PERSONALI
USALI SOLO PER IDENTIFICATE FINALITÀ UTILI O NECESSARIE
TRATTALI IN MODO CONSAPEVOLE ED EFFICIENTE

Le informazioni, essendo immateriali, vengono astutamente o inconsciamente considerate come terra di nessuno. Qualcuno filosoficamente ipotizza che nel momento in cui vengo a conoscenza di un'informazione essa diventa anche mia perché la detengo. I dati invece sono beni alla stessa stregua di ogni altro bene materiale che possediamo di cui conosciamo il valore e la fragilità.

Per i dati personali vale lo stesso concetto: sono un bene personale di nostra proprietà. Non è un caso che si usi il termine "prestare il consenso" all'uso dei dati. Le nostre informazioni personali vengono prestate, non regalate! Quando vi chiedono in prestito un libro, vi aspettate che esso vi venga restituito integro una volta letto, se deve essere usato per scopi diversi ed inusuali dalla normale lettura, per ritagliarci le illustrazioni per una ricerca o come zeppa sotto una gamba del tavolo ad esempio, vi aspettate che vi venga detto al momento della richiesta del prestito per valutare se autorizzare o meno la cosa.

L'utilizzo dell'informazione ha subito negli ultimi decenni una rapida evoluzione che a ben vedere porta con sé la ricerca alchemica di attribuire ad essi "poteri magici": se al principio i dati venivano utilizzati a scopo "descrittivo", per comprendere meglio cosa fosse accaduto fino ad oggi, quindi per una finalità culturale, l'evoluzione delle tecniche e dei mezzi di gestione del dato ha portato il focus verso la capacità di guardare al futuro e fornire un'indicazione precisa di cosa può succedere fino a suggerire quali azioni intraprendere per modificare il domani stesso in funzione dei nostri obiettivi.

Non sono forse questi gli stilemi della magia: arte divinatoria e possibilità di condizionare il futuro a piacimento?

Tutto questo è molto potente, ma non è di per se stesso un male! Se grazie all'informazione fossimo in grado di prevenire epidemie e attentati terroristici, o ancora di gestire al meglio il traffico e il degrado delle città, o perfino

suggerire una vita più sana ad ogni cittadino che voglia un consiglio a riguardo; se potessimo avere tutto questo, pochi di noi non autorizzerebbero l'uso dei nostri dati per contribuire al progresso comune verso un mondo migliore.

Ad oggi tuttavia manca la fiducia che i nostri dati personali siano utilizzati per scopi di benessere comune e in questo modo il cittadino cerca di difendersi a priori da chi chiede correttamente il consenso al loro utilizzo, lasciando spazio solo a realtà che sottraggono dati con l'inganno.

Sfruttare senza riguardi e mungere fino all'ultima goccia tecniche potenti in grado di fare breccia nella nostra parte limbica del cervello e indurci a comportamenti non desiderati basati sulla profonda conoscenza delle nostre abitudini, non rappresenta un investimento a lungo termine ed è un percorso che può condurre ad una società paradossale dove vivremo una vita di puro lavoro per poterci permettere qualcosa che non ci serve ma che vogliamo misteriosamente senza domandarci più che cosa ci rende felici, cosa è importante e qual è il senso della nostra vita stessa.

Porsi come azienda l'obiettivo di contribuire a creare una società migliore fornendo prodotti e servizi a supporto della società stessa, è un percorso più lungo e difficile; per questo ha bisogno di un supporto e una guida. La GDPR, ostacolando i competitori scorretti, viene in aiuto dei virtuosi per dare loro più spazio nel mercato e fornendo loro delle utili e chiare linee guida su come avere cura dell'informazione al fine di focalizzarsi solo verso chiari obiettivi investendo in efficienza e sostenibilità per i progetti da avviare.

Avere cura del dato significa che è necessario tracciare dove, come e chi lo usa facendo il possibile per evitare falle nel processo prefissato. Tutto questo tradotto in un concetto unico si chiama "Data Governance". Una volta messa in pratica una politica di data governance sarà un orgoglio essere in grado di comunicare a noi proprietari dell'informazione con quanta attenzione vengono trattati i nostri dati e questo scatenerà un circolo virtuoso per cui saremo sempre più lieti e fiduciosi di affidarli nelle giuste mani.

Immaginiamo una società interconnessa, dove ad esempio abbiamo i semafori intelligenti guidati in modo interconnesso grazie a informazioni previsionali di traffico e dove macchine con autopilota girano per la città al nostro posto in cerca di un parcheggio per poi venirci a prendere su nostro comando. Se le società che gestiscono i nostri dati lo facessero in modo approssimativo e senza cura, persone non autorizzate potrebbero sapere le nostre abitudini a fini di lucro o truffa, potrebbero persino far impazzire i trasporti a guida autonoma causando incidenti di massa in meno di un secondo.

BIO

Marco Schonhaut, laureato in Ingegneria Elettronica presso l'Università degli Studi di Bologna, ha avuto una "rivelazione" seguendo il corso di Sistemi Informativi I nel lontano 1995. Da allora non ha più abbandonato la specialità legata all'analisi ed alla gestione dei dati. Presso il CINECA (Centro di calcolo interuniversitario dellíltalia Nord-orientale), dopo una borsa di studio sul tema ì Sistemi di Data Warehouse e On-line Analitycal Processing (OLAP)", ha contribuito allo sviluppo del "dlab", laboratorio di Data Warehouse per lo studio e la promozione delle nuove tecnologie di analisi dati in Italia, svolgendo il ruolo di Project Manager e Ricercatore. Dopo un'esperienza di successo come imprenditore in cui ha fondato insieme ad altri 3 soci e fatto crescere Iconsulting Srl, una società di consulenza informatica nel campo della Business Analytics, ha proseguito la propria carriera in autonomi come libero professionista per esplorare tutti i diversi aspetti legati all'informazione collaborando con diverse società di consulenza e fornendo consulenza per grandi gruppi aziendali internazionali. Nel proprio percorso ha svolto il ruolo di formatore tenendo seminari e corsi presso l'Università di Bologna, CUOA Foundation, SMAU.
Nell'ambito dello Sviluppo SW ha progettato e sviluppato un SW di Performance Management per Xtel Spa, ha seguito come Quality Assurance Officer lo sviluppo di una suite di prodotti Software denominata CCM (Customer and Channel Management) per il gruppo DSM Spa volta alla pianificazione di processi di business lato Trade Marketing per aziende del Largo Consumo, ha progettato e sviluppato in autonomia e per terzi applicazioni per smartphone in ottica business. Da alcuni anni collabora attivamente con Iconsulting Spa, svolgendo il ruolo di Advisor strategico per investimenti su Enterprise Data Architecture e nell'ultimo anno ha approfondito i temi di Data Governance e Data Management legati agli aspetti di privacy e di GDPR.

A conclusione di questa riflessione, l'Europa sta cercando, con la GDPR e tante altre iniziative, dei mezzi per riportare in auge la serietà professionale favorendo un cambiamento positivo per una società migliore dove gli imprenditori possano mirare i propri sforzi verso il progresso in modo più consapevole e sostenibile per se stessi e per gli altri. Se cercheremo di sfruttare questa occasione al meglio possiamo ancora sperare di non abbassare lo sguardo davanti al viso di nostro figlio che ci sorride implorando di poter ricevere il testimone per un futuro ancora "umano" e governabile. ■

Kaspersky Lab: le minacce finanziarie nel 2017

Autore: Giampaolo Dedola

Lo scorso anno è stato un periodo di cambiamenti per il mondo delle minacce finanziarie durante il quale abbiamo osservato mutamenti sia nelle tattiche utilizzate che nei target colpiti dagli attaccanti. In generale le minacce in questo contesto sono molteplici, si presentano in varie forme, e possono essere suddivise in due gruppi: le minacce che mirano agli utenti e quelle che colpiscono gli istituti stessi.

BIO

Giampaolo Dedola è un ricercatore del Global Research and Analysis Team (GReAT) di Kaspersky Lab.
Prima di entrare in Kaspersky Lab ha lavorato nel Security Operation Center (SOC) di Telecom Italia in qualità di principal malware analyst e analista forense. In particolare era inserito all'interno del team di Incident Response dove si occupava della gestione degli incidenti critici.
In questi anni ha sviluppato competenze nella gestione degli attacchi DDoS e ha partecipato a esercitazioni di sicurezza quali "Cyber Italy" e "Cyber Europe". Precedentemente ha lavorato come analista di sicurezza nel gruppo Finmeccanica ed ha contribuito all'"Italian chapter" dell'organizzazione Honeynet Project in qualità di analista malware e sviluppatore.

Minacce Utenti

Phishing

Nella prima categoria troviamo attacchi ben noti e relativi ad azioni quali il phishing. Questa è una delle attività criminali più comuni in quanto non richiede elevate competenze tecniche e rimane sempre proficua. Per queste ragioni, il *financial phishing* continua ad essere una minaccia in costante crescita, che negli ultimi tre anni ha fatto registrare una variazione che va dal 34.33% del 2015 al 53.82% del 2017.

Di particolare interesse l'aumento di attenzione dei "phisher" verso le *cryptocurrency*. Quest'ultime sono sempre più presenti nelle nostre vite e gli attaccanti colgono l'occasione per realizzare attacchi di phishing che mirano alla sottrazione dei "wallet" digitali o al dirottamento di transazione attraverso la modifica dell'indirizzo del destinatario.

Banking malware

I *malware,* ed in particolare i *trojan*, specializzati nel furto di dati finanziari, sono sempre stati una delle minacce principali, ma nel corso degli ultimi anni hanno subito una decrescita. Nel corso del 2017 abbiamo osservato una riduzione di circa il 30% delle "detection", circa 300 mila utenti attaccati in meno. Questo fenomeno è dovuto al fatto che gli strumenti storicamente utilizzati per queste attività, quali ZeuS e SpyEye, iniziano ad essere obsoleti, ed inoltre gli attaccanti, sempre più frequentemente, rivolgono la propria verso il furto di *cryptocurrency* o attività di *mining*, considerate più profittevoli.

Minacce Istituti finanziari

Se alcune tipologie di attacchi verso gli utenti mostrano segni di decrescita, dall'altra parte, gli attacchi contro gli istituti finanziari sembrano essere in costante crescita. Le azioni contro strutture quali le banche sono svariate e mirano principalmente alla sottrazione di denaro, ma anche al furto di dati sensibili, che, spesso, possono essere rivenduti per cifre considerevoli.

ATM jackpotting

Uno dei target più comuni sono i soldi contenuti all'interno degli ATM e gli attaccanti cercano sempre nuovi modi per ottenerli. Per questo motivo quella parte di mercato criminale che si occupa di vendere software e servizi cerca di sfruttare l'interesse di malintenzionati, vendendo *malware* creati appositamente per fare *jackpotting*, ovvero svuotare i contanti presenti nelle cassette degli ATM.

Un esempio è "Cutlet Maker", un *malware* comparso nel 2017 e venduto in alcuni market della *Darknet* per circa 5000 dollari.

Lo strumento consentiva di svuotare un ATM attraverso una comoda interfaccia grafica e veniva venduto insieme ad una guida che aiutava l'utente *step-by-step*.

(Continua a pagina 30)

L(')abile confine

BYOD (Bring Your Own Device): come tutelare la sicurezza dei dati quando la sfera privata e quella lavorativa si sovrappongono.

Autore: Viviana Rosa

Sembra passato un secolo e invece sono solo pochi lustri da quando il cellulare aziendale era considerato uno status symbol, il riconoscimento di un ruolo all'interno dell'azienda. Chi riceveva in dotazione il cellulare aziendale sembrava detenesse un potere: una sorta di piccolo scettro elettronico del comando.

Adesso, invece, la tendenza in quest'ambito prevede la pratica del BYOD *(Bring Your Own Device)* o meglio del BYOT *(Bring Your Own Terminal)* ossia di qualsiasi cosa venga in mente al dipendente di portare in azienda per essere utilizzato a fini della produttività personale.

Negare l'esistenza di questo fenomeno o dichiarare di essere contrari non serve e probabilmente è anche controproducente; la verità è che i dipendenti (o i loro capi) introducono da tempo i propri dispositivi, più o meno conformi, nella rete aziendale con o senza il vostro permesso. Lo studio, neanche recente, condotto da Forrester sugli operatori dei servizi informativi negli Stati Uniti ha rivelato che ben oltre il 40% di essi si sta già muovendo con la tecnologia prima delle autorizzazioni formali o dell'istituzione di policy aziendali.

Il confine tra lavoro e tempo personale così diventa sempre più labile e permeabile abbattendo i muri fisici dell'ufficio ed espandendo l'orario del lavoro. Gli impiegati comprano gli apparecchi che preferiscono e l'organizzazione paga il conto. Sembra una situazione ideale, ma la sicurezza della rete aziendale e in definitiva quella dei dati aziendali come viene garantita?

Violazioni di dati e altri incidenti possono essere molto costosi, soprattutto in prospettiva, quando dal 25 maggio p.v. con il nuovo *Regolamento della Privacy* le perdite di dati potranno essere sanzionate molto più severamente di adesso.

Il BYOT oggi è veramente un beneficio per le organizzazioni come appare?

Le opportunità che offre sono molteplici: flessibilità del lavoro, soddisfazione dell'utente, aumento della produttività, relativo risparmio sull'acquisto e sul mantenimento dei dispositivi. Nell'altro piatto della bilancia ci sono i rischi dovuti alla possibile perdita di dati, legati principalmente al fattore umano, l'anello più debole per quanto riguarda Information Security.

Ma ritornando alla visione più tecnica del problema, diversamente dai dispositivi ICT di proprietà dell'organizzazione, i dispositivi personali (POD) sono dispositivi ICT di proprietà di dipendenti o di terze parti (quali fornitori, consulenti ecc.). Impiegati autorizzati e terze parti intendono utilizzare i loro POD per motivi di lavoro, ad esempio facendo e ricevendo telefonate al lavoro e messaggi di testo sui propri cellulari personali, utilizzando il proprio tablet per accedere, leggere e rispondere alle email di lavoro o lavorare da casa. Il BYOD pertanto è associato a una serie di rischi per la sicurezza delle informazioni quali:

- perdita, divulgazione o danneggiamento dei dati aziendali sui POD;
- incidenti che coinvolgono o compromettono l'infrastruttura ICT aziendale e altre risorse informative (ad esempio infezione da malware o hacking);
- non conformità rispetto leggi, regolamenti e obblighi applicabili (ad esempio privacy o pirateria);
- diritti di proprietà intellettuale per informazioni aziendali create, archiviate, elaborate o comunicate sui POD durante l'attività lavorativa.

Ecco che, come in qualsiasi altro progetto, la definizione di una linea guida aziendale deve precedere l'implementazione della tecnologia, persino nel cloud. Sì, perché cloud e BYOD sono, nelle organizzazioni più evolute, intimamente connessi. Probabilmente una buona policy dovrà tenere conto di alcuni fattori quali:

- **La tipologia dei dispositivi.** Quali dispositivi mobili saranno supportati? Solo alcuni dispositivi che garantiscano un doppio dominio (aziendale e personale) o qualunque dispositivo desideri il dipendente?

(Continua a pagina 30)

BIO

Viviana Rosa ricopre il ruolo di Commercial Director in BSI Group Italia, azienda nella quale entra nel 2010, e per la quali si occupa della strategia commerciale e marketing oltre che dell'introduzione di nuovi prodotti nel settore della Sicurezza e del Risk Management. Durante la sua carriera professionale, per diversi anni, ha ricoperto ruoli di rilevanza internazionale seguendo importanti progetti di comunicazione, marketing e vendite per realtà di svariati settori, instaurando solidi rapporti con gli stakeholder di riferimento, comprese le amministrazioni pubbliche e gli enti governativi. Laureata in Lingue e Letterature Straniere presso l'Università Cà Foscari di Venezia ha ottenuto una specializzazione post laurea in Multimedia Content Design presso la Facoltà di Ingegneria di Firenze e ha studiato Foundation of Management a Londra presso l'ILM - Istituto di Leadership Management.

Kaspersky Lab: le minacce finanziarie nel 2017

(Prosegue da pagina 28)

APT (Advanced Persistent Threats)

Gli attaccanti non mirano però solo al singolo ATM, alcuni hanno migliorato le proprie capacità tecniche e sono in grado di lanciare attacchi direttamente alle infrastrutture informatiche interne alle aziende.

Le statistiche del 2017 mostrano che negli attacchi verso gli istituti finanziari solo il 27% delle azioni mirano agli ATM mentre nel 65% dei casi gli obiettivi sono gli *endpoint* ed i server dell'infrastruttura.

I criminali utilizzano le APT per inserirsi all'interno delle reti bancarie, prenderne il controllo e rubare denaro attraverso transazioni SWIFT non autorizzate, modifica dei database contenenti il saldo contabile degli utenti, oppure compromissione degli ATM con malware in grado di fare *jackpotting*. In passato abbiamo osservato operazioni APT come Carbanak, Metel, GCMAN. Abbiamo osservato gruppi come Lazarus, che già utilizzavano questo tipo di attacchi per attività di spionaggio o sabotaggio, iniziare ad utilizzare le proprie capacità per raccogliere capitali colpendo varie banche in tutto il mondo.

Il 2017 ha confermato la presenza di questo tipo di attacchi, durante il quale abbiamo osservato ulteriori campagne contro varie organizzazioni finanziarie e realizzate da nuovi gruppi quali, ad esempio, Silence.

I sistemi utilizzati dagli attaccanti per infiltrarsi all'interno dei sistemi sono molteplici. Nel 23% dei casi utilizzano le classiche mail di *spear-phishing* con allegato malevolo. Nel 15% dei casi utilizzano tecniche di *social engineering* per acquisire informazioni quali le credenziali di accesso o portare un dipendente ad effettuare delle azioni dannose. Nell'8% dei casi utilizzano attacchi di tipo *watering hole*, oppure sempre nell'8% dei casi gli attaccanti utilizzano attacchi di tipo *supply chain*.

Cosa fare?

Le minacce finanziarie si presentano in svariate forme che mutano costantemente e per fronteggiarle correttamente bisogna strutturare una difesa multilivello composta da soluzioni per la prevenzione delle frodi, sistemi di difesa evoluti per gli *endpoint*, prodotti specifici per la protezione da attacchi mirati e di tipo APT e soprattutto attività di "threat intelligence".

Particolare attenzione va data a quest'ultimo aspetto in quanto solo l'acquisizione di informazioni di qualità relative alle attività di attacco ed ai trend delle minacce ci può consentire di rispondere in maniera efficace alle evoluzioni degli attacchi. ■

L(')abile confine

(Prosegue da pagina 29)

- **Conformità.** Quali norme disciplinano i dati che l'organizzazione deve proteggere? La norma HIPAA *(Health Insurance Portability and Accountability Act)*, ad esempio, richiede la crittografia nativa su tutti i dispositivi che contengono i dati in oggetto. E la ISO 27001, o la NIST 800-46?
- **Protezione.** Quali misure di protezione sono necessarie (protezione dei passcode, dispositivi jailbroken/rooted, applicazioni anti-malware, crittografia, limitazioni relative ai dispositivi, backup iCloud)? E sulla base di quale Risk Assessment vengono individuate le contromisure di sicurezza efficaci?
- **Applicazioni.** Quali applicazioni sono vietate? Scansione IP, condivisione di dati, Dropbox, social network? Da dove dovranno venire scaricate quelle ammesse?
- **Accordi.** Esistono accordi aziendali e sui criteri di utilizzo (AUA, *Acceptable Usage Agreement*) per i dispositivi dei dipendenti con dati aziendali?
- **Servizi.** A quale tipo di risorse/e-mail possono accedere i dipendenti? Alcune reti wireless o VPN? CRM?
- **Privacy.** Quali dati vengono raccolti dai dispositivi dei dipendenti? Quali sono i dati personali che non verranno mai raccolti? Geolocalizzazione? gestione da remoto del terminale?

Il BYOD in definitiva è una best practice emergente per concedere ai dipendenti la libertà di lavorare sui propri dispositivi riducendo al contempo l'elevato onere finanziario e gestionale che grava sul personale IT. Bisogna tuttavia ricordare che BYOD non sarà mai in grado di garantire una gestione semplificata abbinata a un risparmio dei costi senza un'accurata policy aziendale, un'attenta analisi dei rischi e un'efficace piattaforma di gestione (MDM, *Mobile Device Management*).

Dal punto di vista regolatorio vale la pena ricordare, in campo internazionale il Data Protection Act 1998 (DPA), che richiede che il responsabile del trattamento dei dati debba adottare misure tecniche e organizzative adeguate contro l'elaborazione non autorizzata o illecita di dati personali e contro la perdita accidentale o la distruzione o il danneggiamento di dati personali.

In ambito ISO, standard fondamentale è rappresentato dall'ISO 27001:2013 e dalla linea guida in tema di networking security, ISO 27033-6.

Da non dimenticare il contributo di ENISA sulla *Consumerization of IT* relativamente a strategie di mitigazione del rischio e buone pratiche, analizzando gli sviluppi BYOD e fornendo sei messaggi chiave per garantire che "portare il proprio dispositivo" non porti anche rischi imprevisti.

La strategia BYOD dunque può essere positiva sia per le imprese che per i lavoratori. Con i dovuti accorgimenti (pianificazione, adeguati investimenti, educazione dell'utente e tecnologie avanzate) si trasforma in un sistema "win to win" dove ognuno ha i suoi vantaggi e si ritiene soddisfatto, riuscendo a disinnescare le potenziali minacce; perchè come diceva il filosofo Zygmunt Bauman: "I confini dividono lo spazio; ma non sono pure e semplici barriere. Sono anche interfacce tra i luoghi che separano. In quanto tali, sono soggetti a pressioni contrapposte e sono perciò fonti potenziali di conflitti e tensioni." ■

Bibliografia

"Sfogliando" **Luciano Floridi, *La quarta rivoluzione***, Raffaello Cortina editore (autore: Massimiliano Cannata)

Una rivoluzione epocale al servizio dell'uomo

Reale e virtuale sono categorie dell'essere che non è più possibile separare, il mondo in cui viviamo è, infatti, il risultato della densa contaminazione tra questi due ambiti. Questo fitto intreccio ha un nome, "infosfera", e sarà l'habitat dell'*homo technologicus*, non ancora *Homo Deus* per usare la definizione di Yuval Noah Harari coniata nel saggio, edito in Italia da Bompiani e divenuto ben presto *best seller* mondiale, ma discendente diretto della specie *sapiens sapiens*. Abbiamo evidentemente conquistato un grado più avanzato nella scala evolutiva, ma abbiamo ancora da risolvere tanti "grattacapi". L'ecosistema digitale in cui siamo immersi richiede un investimento continuo in conoscenza, metodo di ricerca, capacità di previsione, nessuna posizione di rendita è ammessa, senza solide armi culturali per nessuno ci saranno chances di successo.

Questa la tesi di fondo che Luciano Floridi, direttore di ricerca e docente di filosofia ed etica dell'informazione presso l'Università di Oxford, argomentata nel saggio: *La quarta rivoluzione* (ed. Raffaello Cortina). La contemporaneità è segnata dal prepotente sviluppo della tecnoscienza, rispetto a cui è inutile esercitare un atteggiamento scettico. "Non ha senso chiedersi – spiega lo studioso – se l'acqua sia dolce o salata, quando siamo nel mare di Internet, bisogna imparare a nuotare. Non possiamo permetterci di rimanere ai margini di una rivoluzione così profonda e radicale, piuttosto i nostri sforzi devono essere volti ad acquisire una *mentalità digitale*, altrimenti, e lo dico da italiano, saremmo destinati ad occupare posizioni di retroguardia". Il nostro Paese è chiamato in causa dallo studioso, che ricorda come a dispetto della propaganda continuiamo ad essere fanalino di coda a livello europeo nella diffusione di alcune importanti *best practices* come i pagamenti on line, gli acquisti in rete, l'utilizzazione dei big data e dei servizi bancari disponibili sul web.

È molto grave non avere imparato nulla dal passato. La potenza dell'innovazione tecnologica "già altre volte nella storia con l'avvento di Copernico, Darwin e Freud, aveva sottratto la centralità dell'uomo nella storia. Con la rivoluzione informatica lo scossone è stato ancora più forte, perché l'individuo non è protagonista nemmeno nella gestione dell'informazione e della comunicazione". Bisognerà sapersi adattare ai cambiamenti in atto, facendo maturare tutte le abilità intellettuali di cui si è capaci. Dovremmo finalmente acquisire la consapevolezza che l'innovazione non va ostacolata con cecità, va piuttosto regolata con intelligenza, perché sia in grado di sprigionare tutta la sua forza di trasformazione al servizio dell'umanità.

Due termini chiave: Iperstoria e Infosfera

Il salto di paradigma dall'industriale al digitale presenta implicazioni di natura tecnico-economica ed etico-sociale di vasta portata, con cui bisogna misurarsi. C'è insomma bisogno di mettere in campo una filosofia, intesa come elaborazione di un pensiero sistematico per comprendere la natura stessa dell'informazione, per prevedere e gestire l'impatto etico dell'ICT su di noi e sul nostro ambiente, per migliorare le dinamiche di sviluppo della *web society* e, non ultimo, per individuare un percorso di senso, nel solco di una globalizzazione contrassegnata da molte contraddizioni. Nell'ambito di questo scenario straordinariamente articolato Floridi introduce i due termini chiave della sua riflessione teorica: l'*iperstoria* e l'*infosfera*. Sulla seconda ci siamo già soffermati in apertura, quanto all'iperstoria va detto che esprime la concezione di chi, si tratta ormai della maggioranza, vive in una società che non usa semplicemente l'ICT per conservare e trasmettere dati, ma come strumento essenziale per avviare il motore della crescita. Tale posizione presuppone un approccio del tutto inedito con l'universo digitale. La rielaborazione e l'interazione, fattori non presenti nell'epoca analogica, sono ora parte sostanziali dell'*infosfera*, che spinge l'individuo e l'utente a confrontarsi con agenti non necessariamente umani. "In altri termini – commenta l'autore – può accadere sempre più spesso che la nostra interfaccia sia rappresentata da un software, molto più lesto e abile ad esprimere preferenze e interessi di quanto lo siamo noi". Questo agente portatore di un'intelligenza artificiale, chiamiamolo pure robot, saprà giocare d'anticipo, selezionando e ordinando gli elementi in movimento, persino saprà prevenire le nostre richieste, condizionando scelte e decisioni, piccole o grandi che siano. Facile immaginare quali saranno le conseguenze non solo sul delicato terreno del rapporto uomo-macchina, ma più in generale sul piano degli equilibri psicologici ed esistenziali.

Verso un capitalismo dal volto umano

Siamo ormai oltre il meccanismo di causa-effetto, il digitale procede per link, sulla base di uno schema reticolare, costituito da nodi e intrecci, che richiede apertura mentale, elasticità e riconoscimento dell'altro. È, di fatto, la relazione il punto focale della web community, tutto il contrario della chiusura egocentrica, iconizzata nella logica dei *selfie* tanto praticati. Il prezzo che abbiamo pagato lo si può valutare a partire dall'avvitamento di una visione dello sviluppo fondata sulla finanziarizzazione dell'economia, che ha promosso avidità e ignoranza, generando una crisi interminabile che ha tolto serenità e sicurezza a tutto il mondo Occidentale.

Da dove ripartire dunque? Dalla prospettiva di un capitalismo inclusivo capace di puntare sugli alfabeti digitali per migliorare la qualità della vita e del lavoro, oltre all'effettivo livello di benessere delle organizzazioni produttive. Solo a queste condizioni si potrà compiere una "migrazione virtuosa" dallo spazio fisico newtoniano al nuovo orizzonte immateriale, edificato sulla condivisione di saperi, idee e informazioni. Questo particolare "serbatoio", l'infosfera appunto, non è altro che un immenso patrimonio da spendere al servizio della convivenza pacifica e del progresso, uno spazio comune che va preservato a vantaggio di tutti. ■

Bibliografia - Cybersecurity Trends

"Sfogliando" **Roberto Panzarani** ***Costruire Communities. Come cambierà il futuro del capitalismo, dell'economia, della società e del lavoro***, ed. Lupetti (autore: Massimiliano Cannata)

Il nuovo capitalismo delle *communities*

Roberto Panzarani, docente di *Innovation Management* presso il Crie *(Centro de Referência em Inteligência Empresarial Universidade Federal)* di Rio de Janeiro, individua nel suo ultimo lavoro: *"Costruire Communities. Come cambierà il futuro del capitalismo, dell'economia, della società e del lavoro"* (ed. Lupetti) un estremo spazio relazionale del possibile, un ultimo approdo insomma per il modello capitalistico, che in Occidente ha mostrato la corda in questi anni di crisi. "Se il 2008 – spiega l'autore – ha segnato l'inizio della crisi economica e ha mostrato che il neoliberismo è attualmente un modello saturo perché non più in grado di gestire le richieste di un mercato globale sempre più mutevole e incontrollabile e di una classe politica allo sbando, ciò che bisogna fare è cambiare il paradigma, ora e non domani. Le vecchie regole non risultano più valide, questo è il momento in cui dobbiamo inventarne di nuove. L'importante è avere chiara una direzione. E la direzione è quella della rinuncia alla cieca economia del consumo, per giungere a uno scambio sostenibile".

Lo studioso segue la scia di grandi pensatori, dal filosofo francese Jaques Attali al Nobel Amartya Sen, che hanno messo al centro del loro impegno la promozione dei valori della responsabilità e dell'etica sociale in economia. In un mondo di disuguali il messaggio che arriva da questo filone di ricerca risulta ancora più importante. Basta fare parlare i numeri. Nel mondo otto uomini, da soli, posseggono 426 miliardi di dollari, la stessa ricchezza della metà più povera del pianeta, ossia 3,6 miliardi di persone. Ed è dal 2015 che l'1% più ricco dell'umanità possiede più del restante 99%. L'attuale sistema economico favorisce l'accumulo di risorse nelle mani di un'*élite* super privilegiata ai danni dei più poveri (in maggioranza donne). L'Italia non fa certo eccezione se, stando ai dati del 2016, l'1% più facoltoso della popolazione ha nelle mani il 25% della ricchezza nazionale netta.

Sono alcuni dei dati sulla disuguaglianza contenuti nel rapporto *"Un'economia per il 99%"* della Ong britannica Oxfam, diffusi alla vigilia del World Economic Forum di Davos, in Svizzera, nel gennaio del 2017 e richiamati nel saggio di Panzarani. Il trend porta alla facile deduzione che nei prossimi venti anni, cinquecento persone trasmetteranno ai propri eredi 2.100 miliardi di dollari: è una somma superiore al Pil di una grande nazione come l'India, Paese in cui vivono 1,3 miliardi di persone. Vuol dire che i mega Paperoni dei nostri giorni si arricchiscono a un ritmo così spaventosamente veloce che potremmo veder nascere il primo trillionaire (ovvero un individuo con risorse superiori ai mille miliardi di dollari) nei prossimi venticinque anni.

Il grave *gap* formativo

Di fronte a tutto questo non si può stare a guardare. L'Italia sembra aver curiosamente scelto di "negare" l'innovazione. Un atteggiamento miope che non piace per nulla all'autore. "Se non vogliamo che il nostro destino sia segnato occorre cambiare marcia. Un indice di grave superficialità emerge dagli investimenti nella formazione, che appaiono in netto calo. Dal 2009 al 2015, secondo la ricerca Cranet 2015, le giornate medie dedicate alla formazione erano passate da tre a cinque. Anche i fondi utilizzati avevano subito un incremento rilevante: la percentuale del costo retributivo annuo investito era passato da <=1% nel 59% delle aziende private nel 2009 a oltre l'1% nel 63% delle aziende nel 2015, con un 23% di aziende che dedicava anche più del 3% del costo retributivo annuo agli investimenti in formazione. Ma dopo questa impennata, le imprese hanno scelto di disinvestire, con il risultato che nel 2016 le aziende che si sono servite di formazione sono scese al 20,8%, significa che le persone che hanno partecipato ad almeno un corso di formazione o aggiornamento professionale sono state 240 mila in meno rispetto al 2015."

La *sharing economy* nell'era dell'accesso e della condivisione potrà dare una spinta al sistema, a patto che le organizzazioni aziendali si dimostrino ancora una volta all'altezza. "L'errore più grande – precisa l'autore – sarebbe quello di 'burocratizzare l'innovazione'. Non è sufficiente progettare un dipartimento ad hoc, uguale a tanti altri settori dell'azienda, perché si deve creare una vera e propria mobilitazione, un coinvolgimento delle persone, che sappia trascinare emotivamente ogni dipendente".

La *sharing economy* porta con sé una nuova organizzazione della domanda e dell'offerta, in cui le persone contano finalmente molto di più. Occorre maturare la consapevolezza che in questo nuovo modello economico non varrà più la distinzione tra produttori e consumatori, perchè si va definendo un modello *peer* in cui soggetti di pari dignità si scambiano beni e servizi sulla base di reciproche promesse, che si tramutano in penalità nel caso in cui non vengano mantenute.

Le communities nel mondo

Il volume si chiude con alcuni esempi di *communities* nel mondo, dal caso della Nespresso che nel 2003, con la collaborazione di Rainforest Alliance, ha avviato il Programma AAA per una qualità sostenibile del suo caffè, che ha coinvolto i coltivatori della Colombia, all'Arizona, terra in cui è attecchito il sogno ipertecnologico di Bill Gates: Belmont, una *smart city* sostenibile e digitale che sorgerà vicino Phoenix. Il numero uno di Microsoft ha finanziato con 80 milioni di dollari la realizzazione di questa realtà nel bel mezzo del deserto, per la costruzione di un hub ipertecnologico desinato a rivoluzionare l'idea di città. Altra esperienza interessante ricordata nel libro riguarda la comunità di Arcosanti, fondata nel 1970 dall'architetto Paolo Soleri, ex allievo di Frank Lloyd Wright. Un villaggio che, in tempi non sospetti, ha tentato e tenta ancora di concretizzare l'idea di un ritorno a una vita più sostenibile e collettiva. Ad Arcosanti oggi vivono circa cento persone stabilmente, il sito è frequentato annualmente da almeno 50mila visitatori, fra turisti, studenti e ricercatori. Si tratta di nuove realtà che cominciano a prendere piede. Non sarà facile diffondere questa nuova cultura del business, ci sarà bisogno di rafforzare a tutti i livelli la preparazione manageriale e professionale oltre che di una classe dirigente adeguata, senza di cui sarà praticamente impossibile affrontare con qualche ragionevole *chances* di successo i profondi cambiamenti che ci aspettano. ■

CyberSecQuiz

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

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

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

CYBERSECURITY
- MEDITERRANEAN -
CONGRESS
1ª Edition

BROUGHT TO YOU BY: swiss webacademy AND CITTA' DI NOTO PATRIMONIO DELL'UMANITA'

UNDER THE AEGIS OF: ITU

UNDER THE HIGH PATRONAGE OF: Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra
Ambasciata di Svizzera in Italia

IN COLLABORATION WITH: Global Cyber Security Center

IN PARTNERSHIP WITH:

10th & 11th of May, 2018 , Noto, Sicily

Your window towards the multiple and diverse Mediterranean cyberscurity ecosystems

**PSD2, GDPR, Mobile devices vulnerabilities and threats,
Transports security, Business and Industry 4.0, and much more...**

www.cybersecurity-mediterranean.it