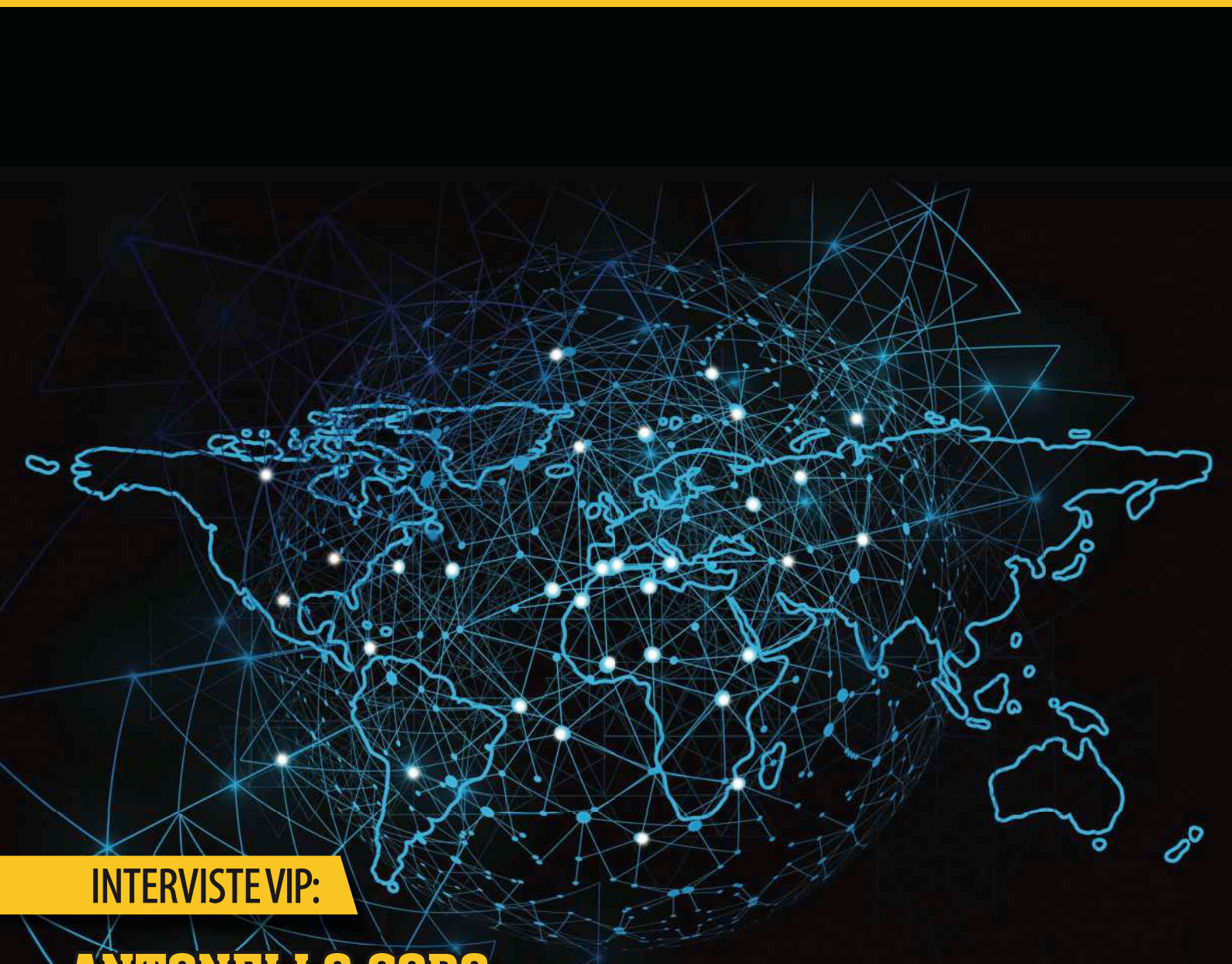
Cybersecurity Trends

Edizione italiana, N. 1 / 2020



INTERVISTE VIP:

ANTONELLO SORO
MARCO RAMILLI
PASQUALE PREZIOSA

GLOBAL CYBER SECURITY CENTER

ISSN 2559 - 1797 / ISSN-L 2559 - 1797

Folder centrale: CYBER SECURITY E GEOPOLITICA

Global Cyber Security

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

Information Sharing
Creazione di modelli di information sharing pubblico - privato

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

Sensibilizzazione
Campagne di sensibilizzazione multi-livello

Formazione
Attività di formazione e corsi di specializzazione e master

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

GLOBAL CYBER SECURITY CENTER

Indice

Si può fare?

Autore: Nicola Sotira

Oggi sembra quasi la "normalità" parlare di misure di emergenza, di pandemie, COVID-19; una situazione emergenziale che comincia pubblicamente a fare capolino il 30 Gennaio con due turisti cinesi che risultavano positivi. Da qui i numeri crescono e i nostri occhi si dovranno abituare a vedere tutto sotto una nuova luce. Come sottolinea molto chiaramente anche il rapporto del MIT del 17 marzo, per fermare questa pandemia dovremo cambiare tutte le nostre consuetudini, il modo in cui lavoriamo, facciamo attività fisica, acquisti, educhiamo, scuole, socializziamo e non ultimo viaggiamo.

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.

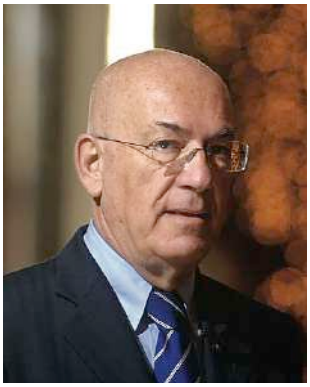
Alcune di queste trasformazioni potrebbero diventare permanenti? Sino a poco tempo fa lo *smart working* sembrava appartenere solo ad alcune nicchie di lavoratori, oggi è stato adottato su larga scala e con grande soddisfazione delle aziende, in particolare per quelle che operano nel settore servizi. Abbiamo quindi scoperto che si può fare, che la nostra giornata lavorativa può essere scandita da riunioni attraverso piattaforme di collaborazione senza che la qualità del lavoro ne venga inficiata. E cosa succederà alle scuole, alle università? Ci ricordiamo le immagini dei notiziari che ci proponevano aule piene e scarsità di locali? Quasi anacronistico oggi, e non voglio nemmeno toccare il tema delle costose manutenzioni ancora da effettuare e/o la costruzione di nuovi spazi. In questo frangente le scuole hanno avviato sessioni on-line ed il tema e-learning è stato sdoganato in pieno. Niente più aule affollate e tutti possono seguire le lezioni da casa e interagire con il docente via chat o form online. Anche le centraline e le immagini satellitari rilevano una diminuzione dell'inquinamento, altro elemento che ci fa riflettere su come un modello di crescita diverso può coniugare sviluppo insieme a sostenibilità ambientale. Il digitale si sta dimostrando sempre più rilevante e abilitante nel cambiare le regole del gioco, nella produzione, nel ciclo di vita delle aziende, ma anche per la gestione del tempo libero in tempi di socializzazione forzatamente ridotta come gli attuali. Non solo, abbiamo anche dematerializzato la ricetta medica, in questa emergenza sarà possibile richiedere il rilascio dematerializzato via email e persino via WhatsApp. Stiamo usando Big Data e tecniche predittive nel campo sanitario, si parla di utilizzo di App per poter monitorare la diffusione della pandemia, si pensa a implementazioni di telemedicina e quindi, si può fare!

Il mondo è cambiato molte volte e questa pandemia cambierà ancora le nostre vite. Tutti noi dovremo adattarci a un nuovo modo di vivere dopo questa esperienza. Ma come per tutti i cambiamenti, cerchiamo di prendere gli aspetti positivi per fare un salto e accelerare una vera metamorfosi digitale, certamente includendo tutti gli aspetti di sicurezza e privacy, che migliori la nostra qualità di vita.

Il meglio che possiamo sperare è che la profondità di questa tragedia non solo costringa tutti i paesi a ripensare le tematiche sociali che hanno generato disuguaglianze, ma attui quei cambiamenti che possono andare oltre questo tempo di emergenza. ■

Tecnologia e diritto devono allearsi per una corretta governance digitale

Intervista VIP a Antonello Soro, Presidente dell'Autorità garante per la protezione dei dati personali



Autore: Massimiliano Cannata

"Nel 2019 il *cybercrime* è cresciuto del 17% a livello mondiale rispetto alle cifre del 2018: anno già definito, per quel che riguarda l'Italia, il peggiore per la sicurezza cibernetica. Gli esperti hanno tracciato preoccupanti previsioni sui possibili rischi e sulle tendenze per il 2020, delineando un orizzonte fatto di attacchi sempre più sofisticati".

BIO

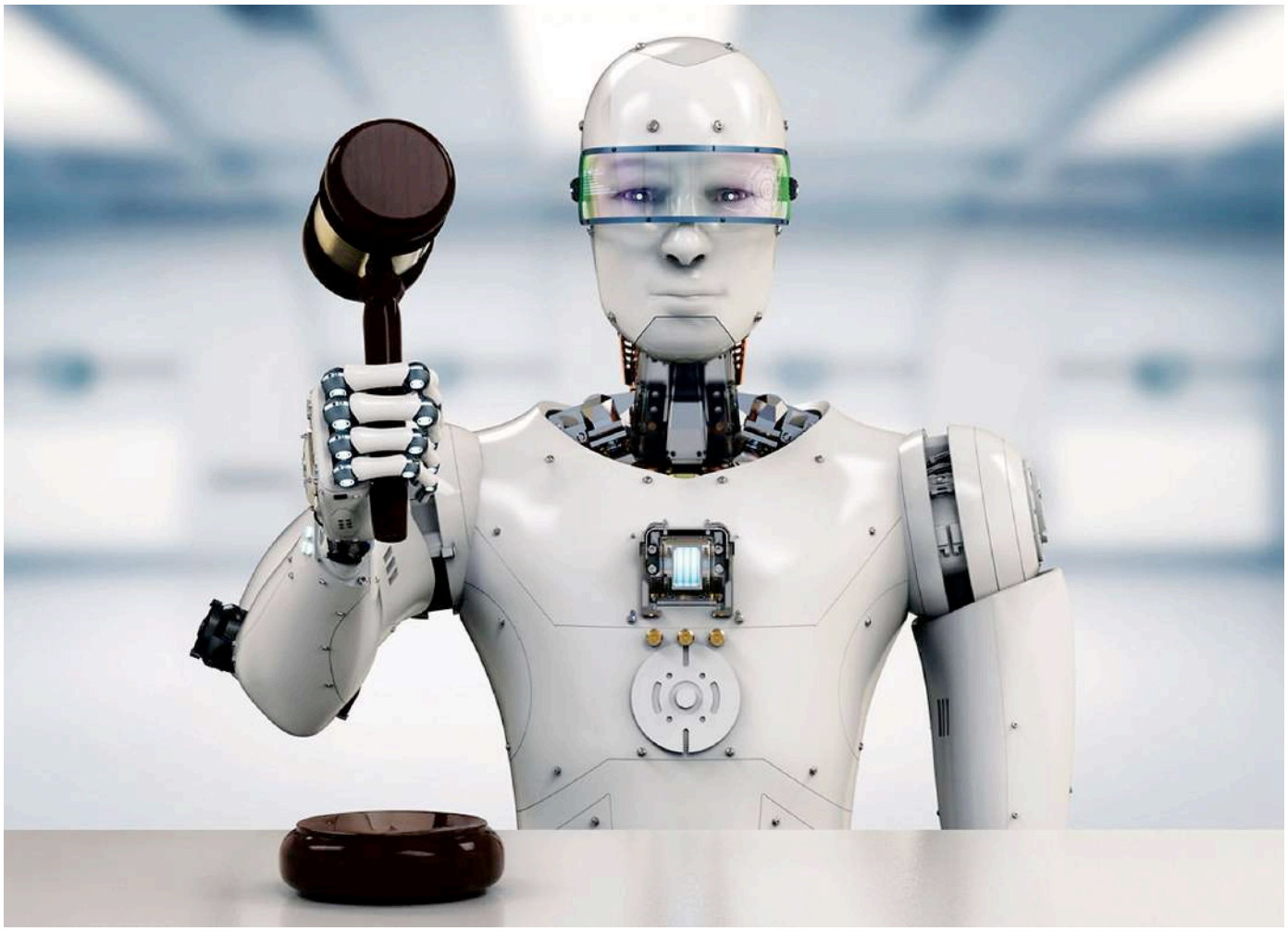
Presidente dell'Autorità Garante dal 19 giugno 2012, Antonello Soro è stato Vice Presidente dei Garanti privacy europei (WP art. 29) dal 26 novembre 2014 al 12 dicembre 2016. Primario Ospedaliero, è stato sindaco di Nuoro e consigliere regionale della Sardegna e nel 1994 viene eletto deputato. Dal 1998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

Presidente Soro questo il messaggio che è arrivato dalla 14° giornata europea dedicata alla protezione dei dati personali. A quali scenari dobbiamo preparaci?

La sicurezza della dimensione cibernetica è costantemente esposta a minacce sempre più "ibride", tali da configurare una sorta di cyber guerriglia permanente. Nei mesi scorsi, la Polizia Postale ha portato alla luce quello che parrebbe configurarsi come il più grave attacco alle banche dati istituzionali finora realizzato, con tecniche di *phishing* che consentivano l'accesso a sistemi informativi tra i più rilevanti per il Paese, dai quali estrarre dati da rivendere ad agenzie investigative e di recupero crediti. E' un fatto emblematico che la dice lunga sui trend evolutivi di un fenomeno come quello del *cybercrimine* che richiede, per poter essere arginato, competenza, tempestività e immediata capacità di risposta.

Questo numero di* Cybersecurity Trends *è dedicato al rapporto tra Cyber Security e geopolitica. Come vede questo delicato binomio?

Gli attacchi informatici sono divenuti anche mezzi d'ingegneria bellica. Basta pensare ai recenti avvenimenti in Medio Oriente, anticipazione di quel che sarà il paradigma dello scontro militare nei prossimi anni: droni armati e attacchi informatici utilizzati quali vere e proprie armi, dotate di una potenza straordinariamente maggiore. Quella cibernetica è la dimensione su cui si sposta sempre più la dinamica dei conflitti, palesi o latenti, tra Stati e tra soggetti, operata attraverso dati e sistemi informativi. Per altro stiamo

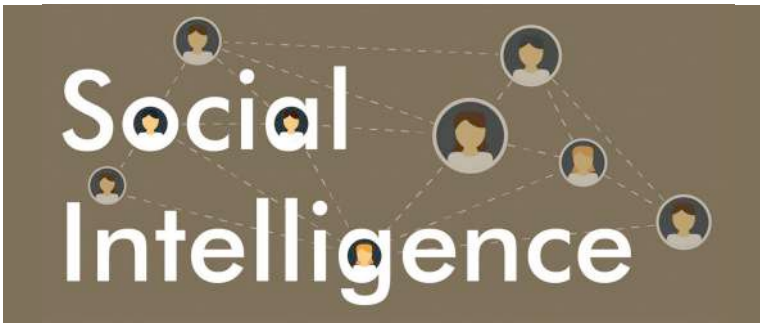


parlando dell'unica dimensione della sicurezza e della difesa sostanzialmente priva di un'adeguata cornice di diritto internazionale. Un'efficace strategia di prevenzione dei rischi cibernetici presuppone, infatti, la consapevolezza dei fattori su cui si basano, rispettivamente, azione e reazione: la tecnologia e il diritto.

Il diritto deve essere al servizio dell'uomo, ma troppo spesso ce ne dimentichiamo…

Il diritto è l'unica risorsa capace di mettere la tecnica al servizio dell'uomo, della libertà, della sicurezza. Sarebbe per altro auspicabile un'alleanza tra tecnologia e diritto che può rappresentare l'architrave di una risposta democratica e lungimirante alle nuove minacce del digitale, minacce fortunatamente controbilanciate dalle straordinarie potenzialità di questi mezzi. Questo presuppone anzitutto il massimo equilibrio tra le discipline deputate a governare il rapporto tra le libertà e il lato oscuro della tecnica, ovvero quella di protezione dati e quella a tutela della sicurezza cibernetica.

E' corretto definire la* cyber security *come l'altra faccia della Privacy, come ha ricordato introducendo il dibattito Arturo di Corinto?



Tra protezione dei dati e tutela della sicurezza informatica intercorre un rapporto indubbiamente complesso, ma che tra antagonismi e inattese sinergie, dice moltissimo di una società in cui l'esibizione incontenibile della vita privata riflette una crisi profonda di fiducia e coesione sociale: elementi - questi - su cui in passato si fondava un'assai diversa percezione tanto della sicurezza quanto della libertà. Occorre ricordare a questo proposito che la tutela della sicurezza cibernetica ha legittimato limitazioni incisive della privacy, in nome del contrasto a minacce tanto immanenti quanto pulviscolari, con il ricorso a strumenti investigativi spesso di tipo massivo. *Social* e *signal intelligence*, sorveglianza strategica, *data mining*: sono solo alcune delle forme che può assumere l'azione di prevenzione, che estende il suo raggio di intervento quanto più la società iperconnessa alimenta continui flussi informativi.

La *cyber security* come diritto dell'uomo

Al rapporto tra democrazia e potere dei dati ha dedicato un interessante saggio* (Libertà algoritmi e umanesimo digitale, ed. Baldini e Castoldi n.d.r.). *Sotto il profilo degli equilibri demo-cratici, come va bilanciato il rapporto tra sicurezza e tutela della privacy?

La potenza della tecnologia e le caratteristiche della minaccia cibernetica sempre più evoluta implicano un aumento dello spettro dell'azione investigativa. Questo, come giustamente lei sottolinea nella domanda, non può che avere degli effetti sotto il profilo delle libertà e degli equilibri democratici. Dobbiamo pensare che, nel nostro Paese, i gestori conservano, ogni giorno, circa 5 miliardi di tabulati di traffico telefonico e telematico per fini di contrasto, nell'ambito di una massa così enorme di dati non è certo facile rinvenire quelli utili. Detto in altri termini: se stendendo così a dismisura il pagliaio può ancora essere ragionevole pensare di poter trovare l'ago?

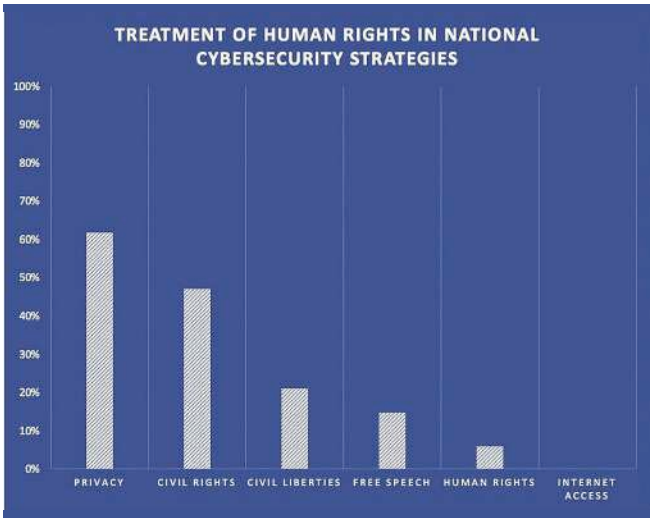
La collaborazione dell'Autorità Garante con il DIS (Sistema di informazione per la sicurezza della repubblica n.d.r) è un punto certamente qualificante sul fronte della protezione dei dati. Può spiegare in che senso?

Il protocollo d'intenti siglato con il Dis nel 2013, è stato dettato dalla precisa esigenza di definire un parallelismo tra un'estensione dei poteri degli Organismi e un adeguato corrispondente aggiornamento delle funzioni di garanzia dell'Autorità. A dimostrazione della delicatezza del problema anche il legislatore europeo si è mosso, instaurando una significativa simmetria tra protezione dati e sicurezza cibernetica, che appare evidente nella definizione di alcuni istituti che accomunano il Regolamento, la direttiva NIS e lo stesso regolamento 2019/881 sulla *cybersecurity*.

Dal suo intervento è emerso in maniera netta come la* cyber security *debba essere considerata come un diritto dell'uomo nella società delle reti, in quanto sfera che chiama in causa i diritti inviolabili di espressione, movimento, partecipazione, relazione. E' una interpretazione corretta?

E' corretta se si considera che in un'economia e una società fondata sui dati, proteggere questi significa tutelare ad un tempo i singoli e la collettività. Nel contesto della società digitale in cui ciascun oggetto di uso quotidiano può rappresentare il canale d'ingresso di potenziali attacchi informatici e in cui quindi le fonti di rischio si moltiplicano a dismisura, è indispensabile fare della protezione dei dati, dei sistemi e delle infrastrutture l'obiettivo prioritario delle politiche pubbliche, perché da questo dipende la tutela della persona ma anche la sicurezza nazionale.

La crescente complessità dei sistemi genera, infatti, vulnerabilità sfruttate per attacchi informatici che possono paralizzare reti di servizi pubblici essenziali, canali di comunicazione istituzionali di primaria importanza, con un impatto, dunque, molto forte sulla vita pubblica. Nel *"capitalismo della sorveglianza"*, in particolare, i rischi sono ancora più alti se pensiamo che le minacce, come nel caso del terrorismo, non sono più prevedibili avendo un carattere "pulviscolare" e in continua evoluzione. La difesa diviene così asimmetrica anche perché le catene, più complesse, su cui si articolano i flussi informativi presentano una molteplicità crescente di anelli deboli.



Treatment of Human Rights in national Cybersecurity Strategies, © Scott Shackelford, Should Cybersecurity Be a Human Right? Columbia Law School

In questa prospettiva lo spazio cibernetico diventa bene comune, tema molto caro a Stefano Rodotà. Cosa vuol dire in concreto?

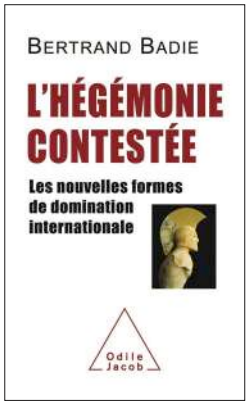
Le sinergie che caratterizzano il rapporto tra protezione dati e cyber security, per quanto ho cercato di spiegare in questa conversazione, non sono soltanto normative ma attengono a un livello più profondo e strutturale, perché tendono entrambe alla protezione della realtà digitale, dei dati e i dei sistemi considerati non isolatamente, ma nelle loro reciproche inferenze. Per questa ragione la sicurezza cibernetica è stata definita bene comune, la cui tutela avvantaggia tutti, proprio perché attiene a una realtà, quale quella digitale, fondata sull'interdipendenza di dati, sistemi, soggetti.

L'importanza di un'innovazione democraticamente sostenibile

L'intelligence geopolitica *dei dati e la spinta verso l'egemonia tecnologica, che molti stati hanno messo in atto può determinare un mutamento degli equilibri politici ed economici a livello mondiale?*

La domanda è complessa e implica più livelli di analisi. Rimanendo al tema di questa intervista occorre sottolineare come la stretta dipendenza della sicurezza della rete da chi ne gestisca i vari snodi e "canali" stia di fatto facendo emergere il tema della "sovranità digitale", da declinarsi non in chiave nazionalistico-autarchica,

quanto piuttosto nell'ottica di una *governance* della dimensione digitale, che oggi esprime un'identità giuridica e politica. Detto in sintesi: dal momento che le minacce sono globali, credo che l'obiettivo debba essere la complessiva assunzione di responsabilità pubblica rispetto a un interesse, quale la sicurezza cibernetica, da cui dipende in primo luogo l'indipendenza dei Paesi e che deve sempre più declinarsi in chiave sovranazionale, spostando, proprio come è stato per la protezione dati, il proprio orizzonte su una prospettiva quanto meno europea.



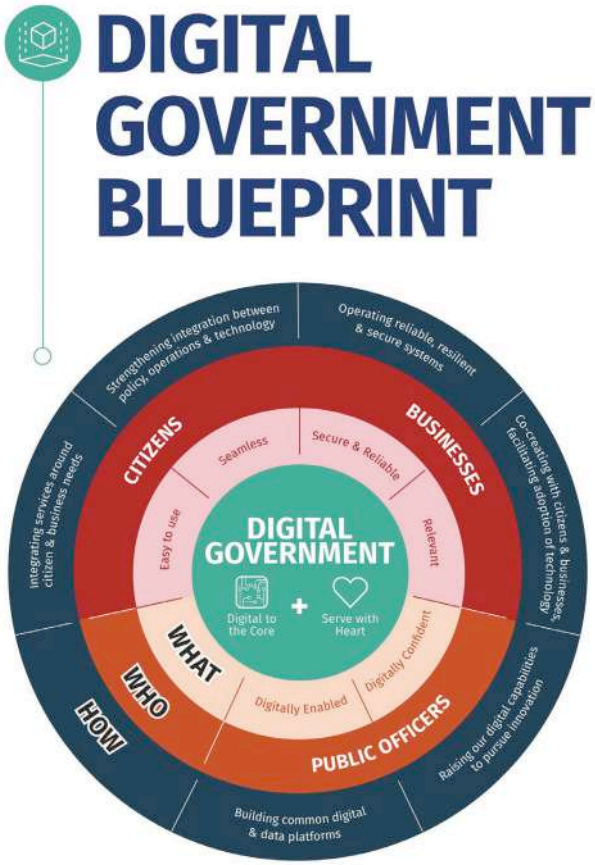
Il politologo francese* Bertrand Badie *in un celebre saggio parla di fine dei territori e del declino del* "Leviatano" *di Hobbes. In maniera, per certi aspetti imprevedibile, non Le pare che si stia facendo strada, insieme all'orizzonte di una diversa concezione della sovranità, cui lei faceva prima cenno, il pericolo di un "neoimperialismo digitale" fondato sul controllo dei dati e delle informazioni?

In uno spazio "defisicizzato" come la rete la sovranità va declinata in forme nuove, meno legate al tradizionale criterio di territorialità e più attente, invece, alla capacità degli Stati di rendere effettiva la tutela dei diritti e la stessa forma democratica, di fronte a sempre nuove spinte illiberali. Sono significativi, in tal senso, i rischi cui un uso manipolativo dei dati personali, anche da parte di potenze estere, può avere sulla sovranità nazionale e sulle scelte politiche essenziali che ne determinano l'esercizio. La vicenda *Cambridge Analytica,* per citare un caso sicuramente eclatante, ha dimostrato come il cosiddetto *"microtargeting"* basato sulla profilazione dei cittadini e la conseguente propaganda elettorale, mirata in base al tipo di elettore stilato dall'algoritmo, possa determinare un pesante condizionamento del processo di formazione del consenso, che risulta gestibile da potenze straniere per orientare a loro favore il risultato elettorale. Sta accadendo che la competizione sempre più forte per l'egemonia tecnologica cela, oggi, una più stretta connessione con le dinamiche geopolitiche, suscettibile di coinvolgere in maniera determinante profili di sicurezza nazionale. Il rischio di un "neo imperialismo digitale" cui lei faceva riferimento è stato colto ed evidenziato dalla preoccupazione espressa dal Copasir a fronte di quella che appare come un'evidente debolezza delle legittime esigenze di cyber security, sempre più sopravanzate dalla forza schiacciante di interessi commerciali che la fanno da padrone, limitando di fatto la libertà degli utenti e persino l'esercizio della sovranità da parte degli stati nazionali.

L'Europa, nella complessa partita di una governance globale del digitale?

l'Europa ha reso la protezione dati un fattore identitario, ritrovandovi, proprio in un momento in cui riaffiorano le spinte divisive, quell'aspirazione federale così ostacolata in altri campi, tale da segnare un vero e proprio divario transatlantico nella gestione del rapporto tra tecnica e diritti, economia e libertà. Questa vocazione unitaria, che purtroppo spesso latita in altri ambiti, ha permesso di superare i particolarismi che spesso privano il diritto del suo necessario *"sguardo lungo",* ha consentendo a questa disciplina di divenire il fronte più avanzato di una *governance del digitale*, in grado di spingersi verso una vera e propria costituzione per l'algoritmo, a cui poi molte altre normative (anche extraeuropee) hanno attinto.

In prospettiva penso che si renderà quanto mai necessario aggiornare l'agenda politica, mettendo al centro idee e progetti per governare la società digitale, al fine di garantire i diritti e le libertà in questa nuova dimensione della vita rispetto a cui la protezione dati è da considerarsi come una imprescindibile bussola. ■



Digital Governance : Il concetto sviluppato da Singapore

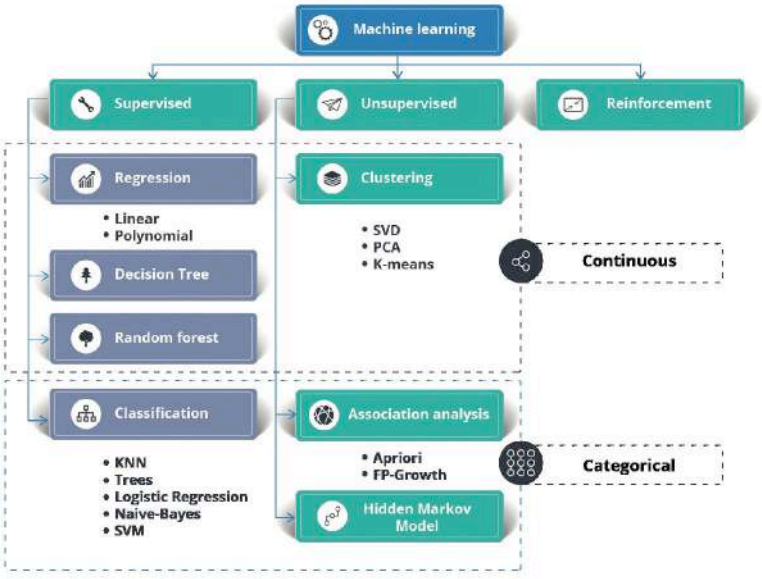
La cybersecurity? Un diritto inalienabile nell'era digitale

Intervista VIP a Marco Ramilli

Autore: Massimiliano Cannata

Marco Ramilli è tra i massimi esperti a livello internazionale di Cybersecurity. Basta riassumere alcuni passaggi della mission di Yoroi, l'azienda di cui è CEO e fondatore, per comprendere alcuni aspetti essenziali di quella che non è tanto un organigramma aziendale quanto una precisa filosofia di vita: *"Nostro compito è proteggere i vicini dalle minacce del cyber spazio che è un bene comune in cui gli esseri umani si trovano ad affrontare macchine, ma anche altri esseri umani".* C'è dunque una contaminazione continua tra tecnologi e umanisti, per cercare di costruire un itinerario di crescita veramente a misura d'uomo. Tutto è in continua evoluzione, tutto scorre come sosteneva Eraclito alle origini della filosofia occidentale, nessuna pretesa di massima sicurezza, sarebbe utopia, piuttosto con umiltà socratica occorre operare come se "l'edificio che stiamo costruendo dovesse durare per sempre", ricordandoci che la "difesa appartiene agli umani" e che il bisogno di un approdo al riparo delle minacce ambientali e di riduzione del rischio è nel DNA degli individui, che fin dalle prime forma di aggregazione sociale hanno cercato di edificare un luogo sicuro adatto alla prosecuzione della specie.

Ing. Ramilli, Cybersecurity e Intelligenza Artificiale come si può declinare oggi questo delicato binomio, che è da sempre al centro delle sue attenzioni di manager e studioso?



Machine learning algorithms ©Edureka

BIO

Marco Ramilli è un esperto internazionale di sicurezza informatica, imprenditore, scrittore e white-hat hacker. Ramilli ha conseguito il dottorato di ricerca in Information Communication Technology presso l'Università di Bologna, facendo studi all'Università della California a Davis. Durante il suo dottorato di ricerca ha lavorato per il Governo degli Stati Uniti (NIST) dove ha svolto intense ricerche sulle tecniche di evasione del malware e sulle metodologie di penetration testing per migliorare i sistemi di voto elettronico statunitensi. Nel 2015 ha deciso di fondare Yoroi: un innovativo Managed Cyber Security Service Provider, sviluppando uno dei più sorprendenti centri di difesa per la sicurezza informatica che abbia mai sperimentato. Oggi Ramilli guida alcuni dei più talentuosi hacker etici con una missione unica: difendere le organizzazioni pubbliche e private nello spazio digitale. Ramilli crede fermamente nel ruolo dell'umanità nell'era digitale. Spesso ricorda il suo credo: «*La difesa appartiene agli umani*".

Il crescente numero di attacchi informatici e l'aumento della rispettiva complessità porta qualsiasi analista a saturare velocemente la propria capacità produttiva. Algoritmi di intelligenza artificiale (nel caso specifico di *machine learning*) come per esempio: regressioni lineari, alberi decisionali e SVR (*support vector regression*) aiutano l'analista nel comprendere se un dato artefatto possa risultare malevolo o benevolo. Inoltre grazie ad algoritmi di *clustering*, come per esempio k-means, Modelli bayesiani e GMM (*Gaussian Mixture Model*) è possibile incrementare notevolmente la capacità di investigazione e di risposta ad un incidente. Tali strumenti offrono aggregazioni ed al contempo *"divisioni di insieme"* molto definite ed utili per chi deve comprendere cosa sia accaduto e sviluppare una risposta.

Possiamo affermare che se governati dall'uomo gli strumenti sofisticati della tecnologia offrono straordinarie possibilità, in caso contrario sono guai?

Questa è una regola aurea che bisognerebbe sempre tenere a mente, altrimenti ci troveremmo di fronte a uno sviluppo senza progresso. In particolare se ci soffermiamo sulle potenzialità dell'intelligenza artificiale, oggi al centro del dibattito scientifico e culturale, bisogna dire che ogni analista nel suo lavoro è come "amplificato" o potenziato da questa "protesi" o, se preferiamo vedere tutto in un'ottica differente, possiamo dire che l'Intelligenza Artificiale ci consente di filtrare numerosi eventi che potrebbero risultare "falsi positivi", esaltando quelli più anomali e quindi interessanti sotto il profilo della *cybersecurity*.

Big data,* analytics *sono competenze che possono aiutare i security manager?

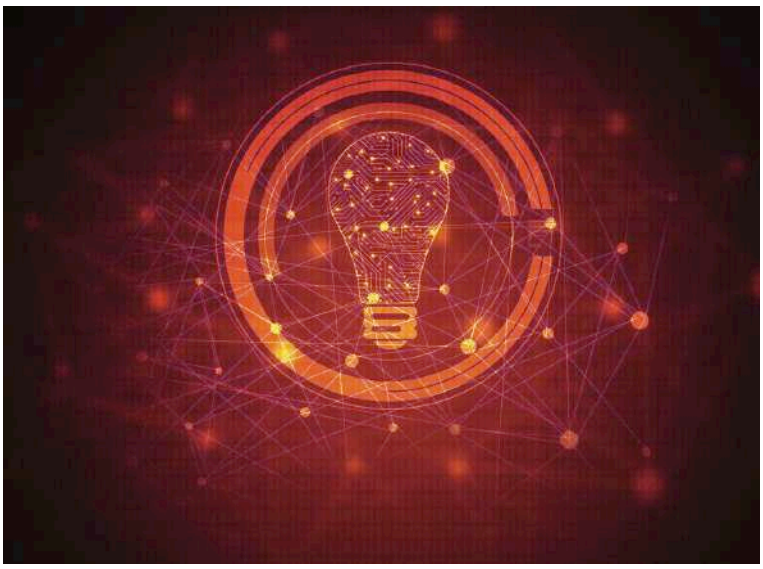
Sono anche questi strumenti importanti, che possono aiutare notevolmente nell'analisi di quantità importanti di dati rintracciabili al di fuori del perimetro organizzativo dell'azienda. Faccio un esempio per capirci: se si raccolgono dati attraverso l'uso di OSINT (*Open Source Intelligence*, fonti aperte alla libera consultazione n.d.r) è possibile con l'ausilio dei *big data analytics* estrarre trends ed informazioni utili che possono essere sfruttati dalle organizzazioni produttive con un indubbio vantaggio. Senza questi ausili sarebbe impossibile sfruttare questa tipologia di fonti per la bassa qualità informativa che connota questi "contenitori".

Quali profili di rischio bisogna analizzare per fronteggiare attacchi informatici sempre più subdoli e per questo difficili da individuare e neutralizzare?

Pensare di proteggere la propria organizzazione in maniera costante e totale risponde a una visione utopistica e, a mio giudizio, scarsamente produttiva. Come se pretendessimo che i nostri figli non si ammalassero mai o che nessuna influenza li possa mai toccare. Non è questo il modo corretto di difendere un organismo biologico o informatico che sia (la metafora scelta da Ramilli pare quanto mai opportuna in tempo di coronavirus n.d.r), perché se anche fosse possibile mantenerlo in isolamento perenne, non svilupperebbe mai gli anticorpi necessari per condurre una vita normale.

Quale strategia occorre dunque seguire?

E' necessario modificare il nostro modus operandi affinché si passi da un'astratta pretesa di "protezione" assoluta a una più pragmatica e concreta



strategia di "difesa". In questa prospettiva, che ammette la relatività della sicurezza, è assolutamente prioritario comprendere quali sono le funzionalità e/o i settori maggiormente a rischio dell'organizzazione, al fine di elaborare una risposta puntuale e strutturata in grado di neutralizzare le molteplici minacce emergenti.

Il "furto dei dati" come ha anche sottolineato il Garante Antonello Soro nella recente giornata europea della privacy, è l'emergenza di questa particolare fase dello sviluppo della società digitale, tanto da giustificare la definizione di "capitalismo della sorveglianza" per definire questo cambiamento d'epoca. E' d'accordo con questa visione?

Il dato è indubbiamente la nuova unità di misura sulla quale si costruirà l'economia del futuro. Possedere dati significa avere informazioni preziose, che se trattate in modo adeguato possono generare conoscenza, che non dimentichiamo è divenuto il quarto fattore della produzione che si aggiunge alla terra, al capitale e al lavoro. Acquisire know-how consente, infatti, di implementare nuove tecnologie, di adire a mercati competitivi, di risolvere problemi inerenti la salute e la qualità della vita, di proteggere dati, di tutelare insomma quello che Rodotà definiva la sfera del "corpo elettronico".

I CERT che funzione possono svolgere in quanto frontiere avanzate della sicurezza?

CERT, CSIRT e SOC, pur essendo entità differenti tra loro con compiti specifici ma assolutamente coerenti hanno un importante ruolo nella difesa degli asset. Entrando più nello specifico possiamo dire che hanno il compito di monitorare ed individuare possibili minacce e attacchi in essere e, a seguito di una azione di *incident response,* sono in grado, (ogni team con modalità differenti) di supportare le organizzazioni aziendali, finalizzando azioni e comportamenti alla mitigazione, se non al blocco, degli attacchi.

Vi sono elementi di differenziazione nelle metodologie di intervento che caratterizzano l'attività di CERT che operano nei più svariati contesti?

Ogni gruppo di lavoro ha un focus differente, tra chi opera sull'analisi delle minacce globali al fine di posizionarsi al meglio nell'ottica dell'anticipazione degli attacchi, chi effettua azioni puntuali finalizzate al blocco delle minacce in essere e infine chi ha il compito della gestione più organizzativa che tecnica delle potenziali intrusioni o manomissioni degli asset digitali. I team migliori sono quelli "ibridi", fondati sulla contaminazione di profili e competenze, capaci di operare con il debito distacco dalle organizzazioni

La mappa interattiva dell'ENISA che elenca, per ogni paese, i vari CERT/CSIRT attivi (www.enisa.europa.eu/topics/csirts-in-europe/csirt-inventory/certs-by-country-interactive-map)

aziendali. Una squadra che sa operare su più realtà organizzative infatti, ha la possibilità di analizzare una molteplicità di scenari e quindi di creare una *expertise* di previsione e risposta agli incidenti certamente superiore rispetto a chi si focalizza solo su ambiti di intervento molto specifici. Per questa ragione sono i CERT Nazionali e i CERT/CSIR/SOC *"multi-corporate"* che possiedono un punto di vista privilegiato nell'orizzonte variegato della cybersecurity.

Può illustrare ai lettori di Cybersecurity Trends i tratti distintivi del modello organizzativo e di difesa che Yoroi, l'azienda che Lei guida, ha sviluppato per andare incontro alle esigenze delle imprese e attuare una corretta "igiene cibernetica"?

Yoroi ha sviluppato una tecnologia capace di individuare e gestire un attacco informatico al fine di massimizzare l'operato degli analisti, focalizzando e guidando le loro azioni attraverso strumenti di AI e piattaforme di *detection* dinamiche. In particolare Y. Si preoccupa di implementare la tecnologia di cui dispone, mentre è il SOC che opera nell'organizzazione aziendale che elabora le strategie di difesa. Entrando più nel dettaglio va detto che attraverso i nostri analisti di secondo livello (esperti di gestione di incidenti) e di terzo livello (esperti di analisi Malware e di attribuzione) offriamo un aiuto periodico alle organizzazione nel momento in cui si manifestano bisogni di sicurezza. Si viene così a creare un rapporto molto stretto tra "samurai" (yoroi) e *"soc operator"* (organizzazione e modello di

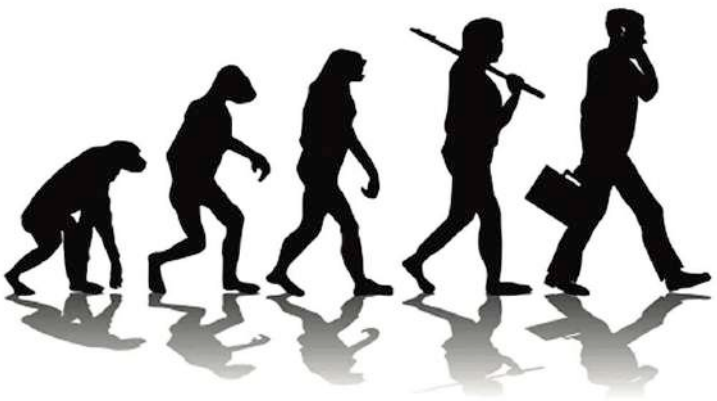
difesa) che ha come finalità il miglioramento continuo dell'organizzazione e dei livelli di collaborazione, che possono innalzare la performance di tutta la squadra coinvolta.

Profili, competenze, tecnologie sono questi i punti di forza di Yoroi. A quali target vi rivolgete?

Intendiamo formare i nostri "samurai" al nostro interno cercando di offrire un percorso strutturato per aiutarli nella crescita professionale. La tecnologia che siamo in grado di implementare guida gli analisti in un processo standard, finalizzato alla riduzione degli errori, riferibili sia all'attribuzione, che alla gestione degli incidenti. Sono in particolare due le tipologie di target aziendali cui ci rivolgiamo: il primo si riferisce alle medie imprese cui offriamo supporto tecnologico insieme a una gamma di servizi integrati. Mettiamo in campo tecnologie e capitale umano quali componenti imprescindibili per la gestione degli incidenti informatici; il secondo target è fatto di grandi player, costituiti da gruppi strutturati, cui offriamo principalmente tecnologie e servizi di alto livello. Di norma queste realtà hanno al loro interno un SOC articolato, che possiede delle competenze distintive per la gestione dell'*Incident Response,* che sfrutta le tecnologie e i servizi che Yoroi mette a disposizione.

Il fattore umano, a detta di molti studiosi e osservatori, rimane il punto debole.* Awareness *è una delle parole chiave del nostro tempo. Come va attuata e con quali linguaggi perché possa risultare realmente efficace?

Non sono d'accordo con l'affermazione che il fattore umano rappresenti sempre l'anello debole della catena. Quello che è debole diventa, infatti, punto di forza. Se per debole intendiamo ingenuo ed emotivo, dobbiamo considerare che questi ingredienti sono anche punti di forza, in quanto rientrano in quella sfera dell'irrazionale che offre una chiave interpretativa e di individuazione delle nuove minacce, che va al di là del noto, del prevedibile e del conosciuto. La componente irrazionale ci permette, come ci hanno insegnato molti filosofi, di comprendere comportamenti che sfuggono alla logica deterministica, di stampo e derivazione cartesiana fondata su uno schema rigido di previsione e controllo. La svolta epistemologica cui diamo, per convenzione, l'etichetta di pensiero complesso, come è noto, ha mandato in soffitta ogni visione deterministica, aprendo il campo dell'analisi a quei sistemi lontani dall'equilibrio in cui regna l'incertezza, ma che sono il sale della vita e di quella creatività che da sempre è la molla vincente dell'innovazione sociale, dello sviluppo umano e del vero progresso. ■



Tecnologia e sicurezza: come cambiano gli scenari geopolitici

Intervista VIP a Pasquale Preziosa

Autore: Massimiliano Cannata

Cyber security, sviluppo tecnologico, equilibri geopolitici sono fattori sempre più interconnessi. Il generale Pasquale Preziosa, già capo di Stato maggiore dell'Aeronautica militare, in questa intervista per Cybersecurity Trends fa vedere molto bene quanto la decisione politica dipenda oggi più che mai dalla forza economica e dagli investimenti in ricerca e innovazione.

Dalla sua disamina emergono chiaramente le difficoltà attuali dell'Europa a ritagliarsi un ruolo politico militare in uno scenario che sarà presto dominato dall'ipersonico, con la conseguenza che nel prossimo futuro, l'organizzazione di difesa della NATO, basata sul sistema antimissile americano e sulle forze convenzionali, potrebbe non bastare a garantire pace e sicurezza all'Occidente. Intanto Cina e Russia…

Generale come ha spiegato dettagliatamente in un recente editoriale apparso sulla rivista* Formiche *il primo fattore destinato a far saltare il banco degli equilibri tra le potenze a livello globale è rappresentato dall'ipersonico. Quali scenari si aprono sul fronte della sicurezza internazionale?

Partirei da un'evidenza di fondo. L'equilibrio mondiale si è sempre basato su un bilanciamento di potere tra i grandi stati che influenzano i *follower*. Alla fine della Guerra Fredda abbiamo avuto solo una grande superpotenza gli USA, in uno scenario che si è ben presto evoluto, in un sistema multipolare, che ha visto la progressiva crescita di influenza dei BRIC, con la Cina in testa, nazione capace di svilupparsi a dispetto delle crisi economiche, che sta ora competendo con l'Occidente. I dati del PIL sono 12 trilioni di $ i livelli della Cina, contro i 20 trilioni di $ degli USA, con la concreta possibilità che questo divario venga, nel giro di pochi anni, colmato, dimostrano la forza che potenzialmente, il "celeste impero", è in grado di esercitare nello scacchiere internazionale.


Tra Usa e Francia, la sfida nucleare per l'Europa. L'opinione del gen. Preziosa

Pasquale Preziosa JAMES BOND

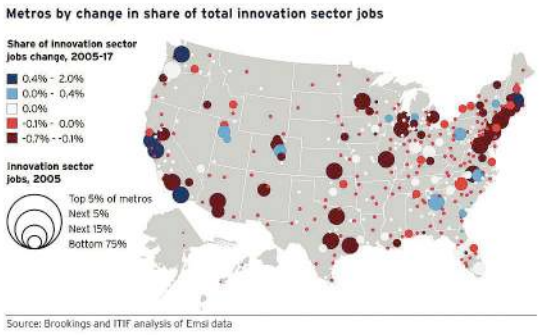
Il rischio di una nuova corsa al nucleare nell'analisi del generale Pasquale Preziosa, già capo di Stato maggiore dell'Aeronautica militare. Il Vecchio continente, in sinergia con Stati Uniti e Nato, deve recuperare terreno nel dibattito globale, scosso dagli avanzamenti ipersonici di Cina e Russia

Una forza che presenta una matrice soprattutto economica, non crede?

Ma che diventa inevitabilmente anche politico - militare. Politica ed economia sono due facce della stessa medaglia. Informazione, diplomazia, intelligence, attività militare sono componenti strettamente correlate alla capacità economica che si traduce in offerta politica. A questo fattore si aggiunge la componete tecnologica, pilastro essenziale nel gioco degli equilibri della società digitale. Ma il quadro non è ancora completo…

A cosa si riferisce?

Al sistema formativo. Quello USA, da sempre di alto livello, ha consentito a chi frequentava le università oltre oceano di entrare in automatico nella setta degli innovatori, apportando floridezza alla nazione americana e a tutte quelle realtà che vi gravitano attorno. Anche in



Industrie classiche sostituite da innovation clusters negli Stati Uniti d'America © Vox

questo campo la Cina sta facendo passi avanti importanti, è divenuta attrattiva per molti giovani, sviluppando alcuni ambiti di competenza soprattutto *nell'high* tech ed è facile prevedere che quando saranno superate le naturali barriere linguistiche ancora esistenti, la concentrazione di cervelli e know-how daranno un'ulteriore spinta a questo immenso Paese.

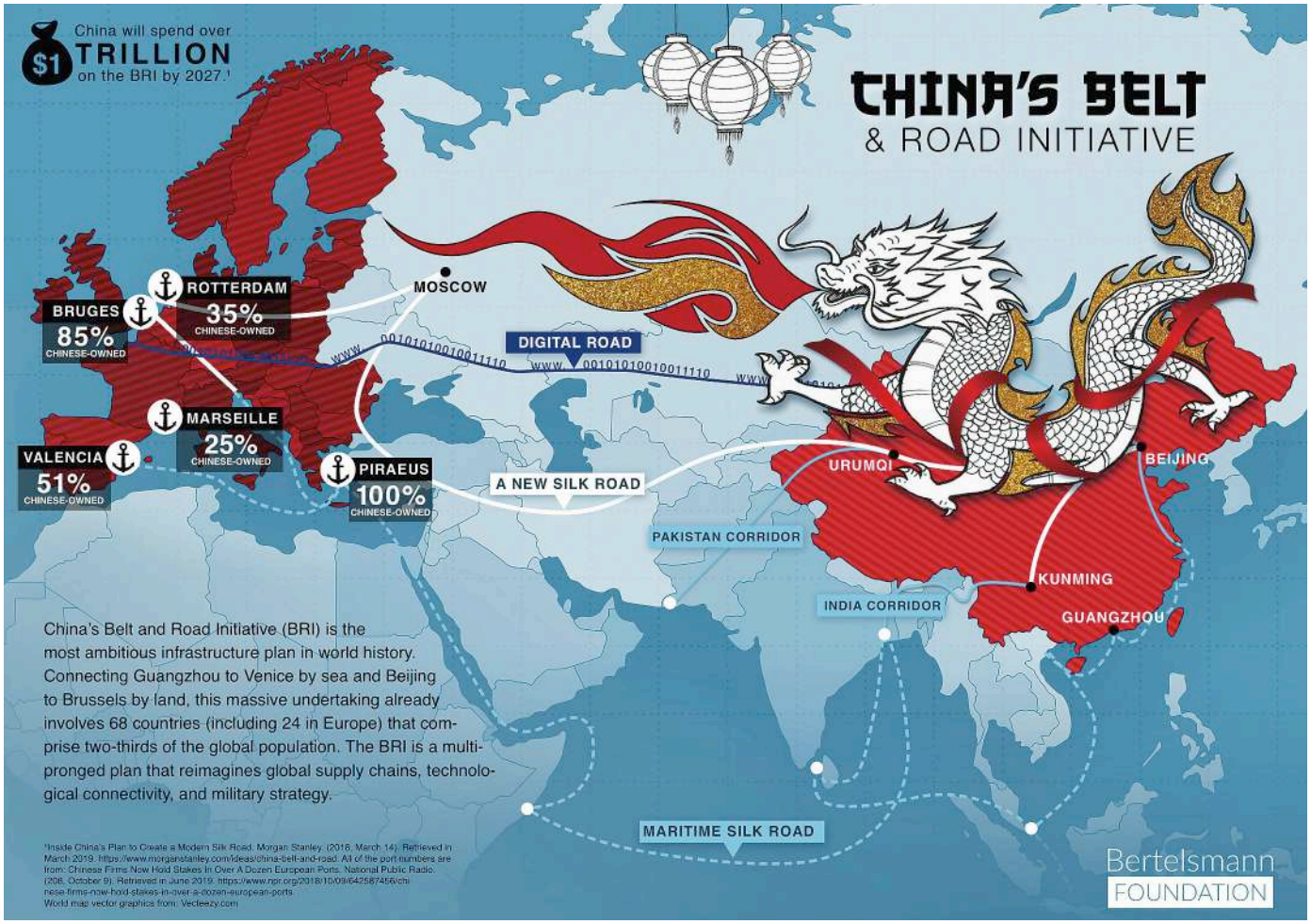
La via della seta *e l'offerta politica della Cina*

Sospinta da dati macroeconomici di segno positivo, l'offerta politica della Cina da quali aspetti è caratterizzata?

La risposta si può in sintesi chiamare *"China's Belt and Road strategy"*, o via della seta se preferisce, una delle più ambiziose iniziative geopolitiche. Basta vedere il livello di investimenti infrastrutturali in Africa, ma anche in Europa per capire la posta in gioco. Non occorre neanche andare troppo lontano, proviamo a osservare il porto di Trieste, tradizionale cerniera di collegamento tra Oriente e Occidente. I cinesi hanno messo pesantemente le mani sulla città di Svevo, ovviamente con i loro modi, la loro sensibilità e i loro linguaggi. Non dimentichiamo che siamo di fronte a un paese che ha un regime politico non democratico con cui venire a patti, e ciò può presentare profili di rischio da non sottovalutare.

Fenomeno difficile da evitare, quando è soprattutto l'economia a dettare l'agenda. Tornando alla via della seta, quale partita si sta giocando?

E' in gioco molto più che il controllo di un canale commerciale, seppur strategico. L'infrastruttura in questo caso serve da cavallo di troia per proporre prodotti, equipaggiamenti militari e quindi per promuovere l'industria cinese, che sta raggiungendo livelli qualitativi comparabili con gli



China's Belt and Road Initiative. Infografica © Bertelsmann Foundation

standard americani. Quello che ora più interessa a Xi Jinping, è il dominio regionale di un'area che comprende il mare. La libertà di navigazione è essenziale per affermare qualsiasi dominio. Quello che è avvenuto a Pearl Harbour tra Giappone e USA nel 1941 dovrebbe averci insegnato qualcosa in merito. Bisogna inoltre tener presente che il commercio euroasiatico ha un valore stimato di circa 2 trilioni di $ all'anno, più del doppio del volume transatlantico e molto più significativo di quello transpacifico. Dopo i flussi commerciali, seguiranno quelli finanziari per poi avviare quelli culturali e di influenza politica. Chi porterà a termine l'unione infrastrutturale euroasiatica avrà, dunque, una maggiore possibilità di influenzare politicamente gli altri.

L'ipersonico *game changer* nei rapporti di forza

Il mondo è cambiato. E' il fattore tecnologico, come accennava all'inizio della nostra conversazione, a fare (parafrasando Gramsci) la differenza tra nazioni egemoni e nazioni subalterne?

Certamente, e la Cina dimostra di saperlo bene, tanto che in collaborazione con la Russia ha sviluppato la tecnologia dell'ipersonico, sfruttando il "cavallo spaziale". La Russia come la Cina è una potenza militari con le quali bisogna dialogare per trovare i giusti punti di incontro per abbassare le tensioni e innalzare la cooperazione per il bene di entrambe le comunità. Putin ha dichiarato pochi giorni fa, che ha creato un sistema offensivo mai visto al mondo *"the hypersonic offensive system"* che può volare fino a 27 volte la velocità del suono, per mantenere la stabilità strategica tra le super potenze, creando le condizioni di deterrenza più elevate per la Russia. Questi salti in avanti, vengono percepiti dagli analisti come una nuova corsa agli armamenti anche nucleari. Anche la Cina, dal canto suo ha dichiarato di possedere capacità ipersoniche da non trascurare, allineandosi alla Russia. Gli USA, in risposta ai nuovi traguardi russo-cinesi, il 2 marzo hanno lanciato lo studio chiamato *"Industrial base for hypersonic weapons"* per bilanciare la capacità tecnologica dichiarata dalla Russia.

L'ipersonico è un aspetto molto delicato, su cui pochi si sono ancora soffermati. Cosa dobbiamo aspettarci?

Che, come avevo già sottolineato in un convegno internazionale di circa sei anni fa, l'ipersonico è il vero *game changer* degli equilibri militari del pianeta perché avrebbe reso insufficiente il livello di deterrenza USA basato, principalmente, sull'architettura antimissile. Attraverso questa tecnologia ipersonica applicata non solo nel campo delle testate nucleari, ma anche nel settore degli armamenti che si muovono nell'atmosfera, la Cina e la Russia hanno spinto la loro potenza e soprattutto la loro influenza su aree del mondo geograficamente molto lontane.

BIO

Il Generale Pasquale Preziosa è nato a Bisceglie (BA) il 21 marzo 1953. Si è arruolato in Aeronautica nel 1971 con il corso «Marte III» dell'Accademia Aeronautica. Nel 1982 si è qualificato istruttore di volo su Aviogetti e nel 1983 si è qualificato istruttore di volo sul velivolo Tornado presso la base inglese di Cottesmore. Dal 1985 all'agosto 1987, ha ricoperto l'incarico di Capo Ufficio Operazioni del 36° Stormo e, dall'agosto 1987 al settembre 1988, ha ricoperto l'incarico di Comandante del 156° Gruppo del 36° Stormo. Nel periodo luglio 1989 – gennaio 1992 ha svolto l'incarico di Aiutante di Volo. Promosso Colonnello nel dicembre 1991, è stato successivamente assegnato allo Stato Maggiore dell'Aeronautica in qualità di Capo della 2ª Sezione dell'Ufficio Pianificazione Generale Programmazione e Bilancio. Nel 1993 ha frequentato il «Defense Resources Management Course» negli Stati Uniti d'America. Dal 12 settembre 1994 al 9 settembre 1996 ha ricoperto l'incarico di Comandante del 36° Stormo. Dal settembre 1996 al 31 ottobre 1997 ha assolto l'incarico di Capo del 2° Ufficio dell'Ufficio Pianificazione Generale Programmazione e Bilancio dello SMA. Dal 1° novembre 1997 al 23 luglio 1998 ha espletato l'incarico di Capo del 2° Ufficio del Reparto Pianificazione Generale dello SMA e dal luglio all'ottobre 1998 quello di Vice Capo del citato Reparto. Il 1° gennaio 1999 è stato promosso Generale di Brigata Aerea e, dal 23 agosto 1999 al 3 dicembre 2001, ha ricoperto l'incarico di Capo dell'Ufficio del Capo di Stato Maggiore dell'Aeronautica Militare. Il 4 dicembre 2001 ha assunto l'incarico di Vice Capo Reparto del 3° Reparto dello SMA e, nel periodo dal 15 giugno 2002 al 30 luglio 2002, ha operato presso la cellula di risposta «Enduring Freedom» in Tampa (USA) con l'incarico di Italian Senior National Representative. Il 30 agosto 2003 ha assunto l'incarico di Addetto per la Difesa e la Cooperazione per la Difesa in Washington D.C.. Il 1º gennaio 2005 é stato promosso al grado di Generale di Divisione Aerea. Dall'11 settembre 2006 al 14 febbraio 2008 ha ricoperto l'incarico di Capo Ufficio Generale Pianificazione Programmazione e Bilancio dello Stato Maggiore Difesa. Dal 15 febbraio 2008 al 4 ottobre 2009 ha ricoperto l'incarico di Capo del III Reparto dello Stato Maggiore Difesa. Il 22 giugno 2009 è stato promosso Generale di Squadra Aerea e dal 5 ottobre 2009 è a disposizione del Capo di Stato Maggiore AM per incarichi particolari. Dal 6 dicembre 2011 al 24 febbraio 2013 ha ricoperto l'incarico di Capo di Gabinetto del Ministro della Difesa. Dal 25 febbraio 2013 al 29 marzo 2016 ha assunto l'incarico di Capo di Stato Maggiore dell'Aeronautica. Nel marzo 2020, il Generale Pasquale Preziosa è stato eletto Presidente dell'EURISPES, Osservatorio Sicurezza.

Il risultato è che attualmente la Cina può esercitare deterrenza per il dominio del mar cinese meridionale.

Intanto una emergenza inaspettata si è fatta strada. Un virus biologico e non informatico sta mietendo vittime generando grande paura e mettendo in evidenza le crepe di una governance della globalizzazione contraddittoria. Cosa dobbiamo aspettarci?

Il diffondersi dell'epidemia costringerà a rivedere i piani di sviluppo e le priorità di tutti i paesi compresa la Cina, la quale aveva affermato che avrebbe raggiunto la "dominance" dell'intelligenza artificiale nel 2030. Putin dal canto suo aveva già tracciato il nesso tra la "dominance" nell'intelligenza artificiale e l'egemonia sui trend di sviluppo di una "nuova rivoluzione industriale". Per la parte USA, il Gen. Jack Shanahan, alla National Security Commission on Artificial Intelligence (AI) USA ha sottolineato che le future battaglie saranno caratterizzate da "algoritmi contro algoritmi", e il miglior algoritmo sarà il vincitore. È evidente che le vecchie catene di comando e controllo militari non sono più sufficienti e che senza tecnologia applicata alla sicurezza non si va da nessuna parte.

Va, inoltre, precisato, che la diffusione del coronavirus comporterà coseguenze, come danni sociali economici e finanziari che si manifesteranno in molte aree del mondo nella loro piena essenza solo a ridosso della prossima estate.

E l'Europa, in questa dinamica, sta solo a guardare?

L'Unione europea con i suoi 16/18 trilioni di $ di PIL potenziali, presenta le sembianze di un grosso concorrente sia per gli USA sia per la Cina, ma anche per la stessa Russia che, pur non avendo stessi indici di produttività, rimane un'importante potenza militare. Oggi l'Europa deve recuperare forza e autonomia, iniziando a costruire il Pilastro della sua difesa all'interno della NATO. Qualche segnale di una nascente industria europea della difesa si comincia a intravedere basti pensare all'impegno di Fincantieri a fianco della francese Novartis. Più in generale sarebbe opportuno che gli stati nazionali collaborassero in un progetto armonico, che consentirebbe, grazie alle economie di scala, di ridurre i costi e di rafforzare la rendita degli investimenti, migliorando i fattori della competitività internazionale.

Il nuovo campo di battaglia per l'Europa, per un suo possibile rinascimento, è rappresentato dalla delibera del Parlamento europeo del 15 gennaio u.s. che ha dato via libera alla "Conferenza sul futuro dell'Europa 2020-2029" su proposta franco-tedesca.

Il rapporto UE e Russia verso un nuovo paradigma

Lei faceva riferimento all'impegno francese nel campo nucleare e al potenziale antagonismo che potrebbe nascere con gli USA. E' una prospettiva che deve preoccuparci?

Per esercitare a pieno la sovranità, secondo il Principe del Macchiavelli servono sia il "soldo" sia la "spada"; in Europa, quindi, il pilastro militare dovrebbe affiancare quello finanziario.

Costruito il pilastro militare europeo all'interno della Nato, dovrà esser presa in considerazione la componente nucleare francese, anche se modesta nelle quantità e non aggiornata alle nuove tecnologie ipersoniche. L'offerta francese per il nucleare europeo non ha, però, visto la condivisione nè della Germania nè degli USA.

Sotto il profilo politico, l'approfondimento del tema della difesa europea, vede oggi gli USA impegnati nelle prossime elezioni di novembre, la Merkel in Germania in affanno di consensi, la Francia con problemi di politica interna e altri paesi distratti da altre esigenze.

In questo contesto sociopolitico confuso e frammentato, la volontà francese di andare avanti con un esercito europeo, che peraltro, risale alla tradizione di De Gaulle, fatica a farsi strada.

L'Europa posta di fronte alle ultime emergenze, il coronavirus da un lato e i migranti che stanno letteralmente assalendo la Grecia dalla Turchia sono due capitoli entrambi molto caldi e difficili da trattare, non riesce a dare risposte univoche. Quali sono le ragioni di tale incertezza?

L'Unione europea basa la sua azione politica sui concetti di libertà, solidarietà e sussidiarietà.

Ogni Paese è responsabile di attuare, in primis, le azioni ritenute necessarie per fronteggiare i problemi che si presentano ai confini, chiedendo interventi comunitari quando risultano insufficienti quelli nazionali. Gli interventi dell'Unione sono in accordo con le regole già stabilite all'unanimità, che con i recenti scenari di crisi, mal si conciliano con le soluzioni attese dai singoli paesi.

La Conferenza sul futuro dell'Unione europea ha il compito di elaborare nuove regole e procedure. Intanto la Turchia ha deciso di aprire le frontiere ai rifugiati presenti in loco per perseguire i propri obiettivi di politica interna.

L'azione sta avendo un grande impatto sulla Grecia e come conseguenza sull'Unione europea.

Una risposta dovrà pure arrivare dall'UE e in tempi brevi, non crede?

La Commissione europea è all'opera per cercare soluzioni al grave problema creatisi.

Purtroppo, l'UE, non avendo terminato l'opera di completamento con il pilastro militare e di politica estera, si ritrova monca e solo col pilastro monetario. Peraltro, la Turchia oggi esprime una leadership forte che vuole affermarsi quale potenza mediterranea e mediorientale.

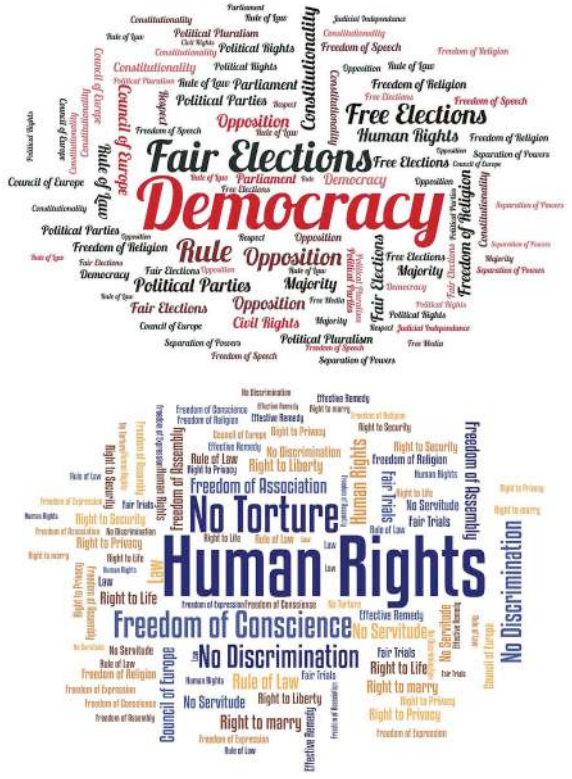
Le grandi potenze, al momento, evidenziano altre priorità e contrarietà al completamento del progetto europeo, che percepiscono erroneamente, solo come concorrente e non come una unione cooperante. Le due crisi, che sono accomunate dal fatto che non presentano soluzioni a breve termine, sanitaria da una parte e sociale dall'altra legata alle migrazioni, hanno portato il livello di "sofferenza" dei paesi europei a livelli molto alti.

I paesi dell'Est, ultimi arrivati nella casa comune, che gravitavano nella vecchia aria di influenza sovietica, avranno un ruolo nel progetto di una nuova industria della difesa europea?

I paesi dell'Est non hanno, per ovvie ragioni, maturato la cultura della vecchia Europa della CECA, sono stati abituati a percepire la UE come fonte di aiuti finanziari e hanno considerato e collocato la NATO quale baluardo per la difesa dalla Russia. Occorrerà aiutare questi popoli a maturare una più profonda coscienza di appartenenza all'Unione. Questo salto di visione deve essere accompagnato da una rivisitazione del rapporto con la Russia, che deve andare oltre i canoni ormai superati della guerra fredda. Un nuovo paradigma deve insomma farsi strada, nei rapporti tra l'Europa e la Russia, senza fraintendimenti.

Cosa intende dire?

Che i valori europei non possono essere sacrificati. Vi sono altre culture e altre visioni della democrazia con cui si dovrà venire a contatto, per rendere più solido il progetto dell'UE. Rispettiamo l'identità di questi paesi, senza necessariamente condividere valori che non fanno parte del tessuto profondo della costituzione europea, che riflette l'impegno e il sacrificio di padri fondatori che hanno lottato per affermare la libertà e la pace, dopo il grande incendio di un conflitto mondiale che aveva portato morte, povertà e distruzione. ■



I valori fondamentali dell'Europa
©Europewatchdog, Council of Europe

Italia sotto scacco. La sicurezza, un bene di rilevanza sociale.

Autore: Massimiliano Cannata

Il mondo sottosopra, l'assalto di un microorganismo ha gettato nel panico l'Italia. La penisola "chiude per virus" come molti giornali hanno titolato. L'ora più buia è arrivata con la scuola che chiude i battenti (fatto senza precedenti) "diventando – come ha scritto Ezio Mauro in un recente editoriale apparso su Repubblica – "il simbolo principale di una società presa in ostaggio". Anche il mondo del calcio (cosa sempre eclatante alle nostre latitudini) si arrende. Stop alle cerimonie religiose, con il papa costretto a un inedito "angelus sotto vetro", proferito dalla biblioteca vaticana. Una quaresima di grande penitenza per tutti ma senza liturgia, un ulteriore gioco di contrasti in questa strana apnea, che gonfia l'ansia collettiva.

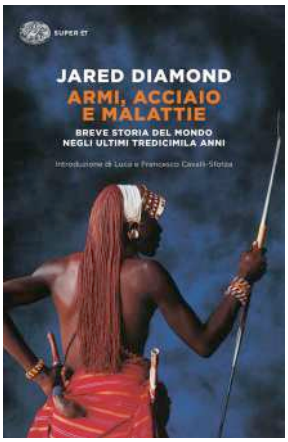
E' arrivato il momento di un reset, non informatico come il linguaggio dell'ICT oggi molto alla moda suggerirebbe, ma un reset mentale e psicologico che ci riguarda tutti, perché tocca quel filo sottile che lega libertà e sicurezza. "L'avanzare dell'epidemia – commenta lo scrittore **Antonio Scurati** – polarizza agli estremi, nell'era di Internet sembra che non sappiamo vivere senza un'apocalisse all'orizzonte. Passiamo continuamente dall'inezia al panico, dalla facezia comica al melodramma, quando occorrerebbe recuperare un "codice culturale" capace di elaborare un equilibrato e sano rapporto con la morte e con la vita, per bilanciare azioni e comportamenti". "Siamo al *Crash test* di una civiltà – come non dare ragione ad **Alessando Baricco** che ha dedicato un saggio di successo, *"The game"* in cui ha indagato a fondo gli aspetti di quel *"salto ontologico"* dagli atomi ai bit, che segna la condizione dell'uomo nella contemporaneità. "Attenti però, il Game - puntualizza lo scrittore - è solo il nostro piano B, perché il piano A rimane la vita reale, fatta da un mondo più poroso, attraversato da paure a tutte le latitudini".

"Armi, acciao e malattie"

"Adeguatezza e proporzionalità" si è appigliato a questi concetti in diverse occasioni in queste difficili settimane il premier cercando di trovare la quadra e una strategia di contenimento efficace dell'epidemia. Ora è il momento di esercitare appieno il senso di una responsabilità individuale che si traduce in bene collettivo, in solidarietà realmente vissuta. "Dobbiamo mettere in atto una fenomenologia dell'ascolto e un'etica di riconoscimento dell'altro – l'invito del gesuita **Stefano del Bove**, formulato nel bel saggio *Valori/Comportamenti* che apre le schede del *Rapporto Italia Eurispes 2020* va accolto in pieno, perché può essere un "vaccino" prezioso e un argine efficace a contenere il profondo senso di disorientamento che è facile prevedere segnerà le nostre vite nel prossimo futuro.

BIO

Massimiliano Cannata (Palermo, 1968), Filosofo, giornalista Professionista, autore televisivo, svolge attività di consulenza nell'ambito della comunicazione d'impresa. Membro del Comitato scientifico di "Anfione e Zeto", collabora con "Technology Review", "L'impresa", "Il Giornale di Sicilia", "Centonove Press". E' autore di numerosi saggi sui temi della social innovation, della formazione, dello sviluppo organizzativo e manageriale.



Il "mostro" ci minaccia nessuno lo conosce ancora a sufficienza, soprattutto poco sappiamo sulle sue capacità di resistenza e di sviluppo. La storia dell'umanità è segnata dalla continua lotta contro il male, che ha assunto in particolari momenti i contorni dell'apocalisse. *"Armi, acciaio e malattie"*. Non può non venire alla mente il celebre scritto del biologo e antropologo statunitense **Jared Diamond** che ha provato a riassumere il percorso evolutivo dell'umanità negli ultimi "tredicimila anni" racchiudendolo in un trinomio, attorno a cui l'Occidente ha organizzato un progetto egemonico oggi entrato in crisi, di pari passo al declino della modernità con la sua pretesa di previsione e controllo, alimentata da sorti "magnifiche" e progressive.

La sicurezza richiede una governance integrata

"In uno scenario di iperconnettività in rapida crescita, nel contesto emergente delle *smart city*, la sicurezza è una questione di rilevanza sociale. Quello che stiamo vivendo è una sorta di stress test non solo per l'Italia, ma anche per l'Europa, che richiede una *governance* integrata fatta di competenze, mestieri, visioni e sensibilità diverse. Non può esistere un unico protocollo atto a garantire la sicurezza assoluta, occorre sviluppare un lavoro costante di collaborazione che deve vedere fianco a fianco competenze tecniche e decisore politico, nel

superamento della vecchia distinzione tra pubblico e privato", commenta **Nicola Sotira** tra i massimi esperti di *Cyber Security* direttore generale della Fondazione no-profit GCSEC e del CERT di Poste italiane, per mestiere abituato a muoversi sulla frontiera mobile che separa il reale dal virtuale. "E' il fattore umano l'anello debole su cui bisogna agire, bisogna innalzare i livelli di consapevolezza perché nella società del rischio, le crisi planetarie potranno avere un carattere ciclico e ripresentarsi sotto diverse sembianze, quali inevitabili conseguenze di un percorso di sviluppo straordinariamente rapido e denso di contraddizioni".

Contraddizioni su cui si sofferma **Margherita Petranzan**, direttore della prestigiosa rivista *Anfione e Zeto* che ha dedicato uno scritto "La presenza dell'assenza" al soffermandosi sul duplice sguardo su vita e morte in architettura: "In questo momento di grande emergenza - commenta l'architetto - la casa torma ad essere principio dell'abitare nella città totale, quale luogo che finalmente può aiutarci a immergerci, con l'aiuto di buone letture, nel tempo presente. Siamo stati tutti serfisti nella società delle reti, dopo aver corso sulle onde all'impazzata abbiamo fatto naufragio, adesso ci troviamo costretti ad andare nel profondo, non c'eravamo più abituati. Chi riuscirà ad emergere uscirà più

forte e anche più consapevole".

Da strada da fare ne abbiamo per ritrovare un percorso di crescita solidale e consapevole *Lo choc* planetario, sta, infatti, generando un'onda d'urto per molti aspetti superiore a quella generata dal crollo delle torri gemelle. Crollano le borse lo spread risale a livelli di guardia. "E' la crisi della globalizzazione – la tesi dell'economista ed ex ministro **Giulio Tremonti** – Il Pil di Cina, Europa e Stati Uniti scenderà parecchio oltre le previsioni. Dovranno essere ricostruite – aspetto molto delicato quest'ultimo - le filiere produttive che avevano proprio la Cina al centro, che viene meno come modello di stabilità. Il cambiamento cui siamo posti di fronte non poteva essere più brusco, e chiama in causa il ritorno della politica magari – prosegue l'analisi di Tremonti – con un piano di investimenti pubblici, chiama in causa l'Europa".

Appunto l'Europa, molti sostengono che stia brillando per la sua assenza. Questa emergenza può essere un'ottima occasione di rinnovamento per l'Europa e per l'adozione di un

approccio unico. E'l'auspicio di **Giorgio Pacifici**, sociologo del cambiamento, autore del saggio *Le maschere del male*. "Sembra che il male stia stringendo la sua morsa sull'umanità. Vi sono tante agenzie del male che operano e che prosperano ad ogni latitudine. Non so se l'Europa abbia gli anticorpi necessari (Europe è l'ultimo scritto di Pacifici realizzato con Renato Mannheimer), quello che è certo che l'offensiva di questo male oscuro possiede le sembianze di una fenomenologia del male necessario che ci sta lasciando più soli, fino a prosciugare l'orizzonte di ogni relazione possibile. Mi chiedo: Quanti giusti posson bastare per conferire a questa lotta una forza morale e spirituale, oltre che una guida culturale e intellettuale?". Difficile dare una risposta a Pacifici dalla prospettiva di un "Paese come il nostro che ci appare come un paziente malato e che avrebbe bisogno di una *ri-costruzione* e di una terapia speciale, organizzata e sistematica, fatta di cultura, rispetto, senso della storia, attenzione alla verità, obbligo di memoria", come sostiene il Presidente di Eurispes Gian Maria Fara. Una ri-costruzione quella sostenuta dallo studioso che andrebbe riletta nell'ottica della ri-fondazione dei luoghi dell'abitare attorno a cui si organizza la convivenza.

Immunizzazione e adattamento dovremo oscillare tra questi due versanti se vogliamo averla vinta è la tesi di **Gian Paolo Caprettini**, filosofo del linguaggio, docente di semiotica dei media dell'Università di Torino. La sicurezza" – ha infatti nel suo stesso tessuto etimologico e culturale una radice sfaccettata, una pluridimensionalità congenita, che la caratterizza come valore, ma anche come obiettivo, come stato d'animo, come condizione esistenziale".

I ricercatori individueranno un vaccino che ci garantirà l'immunità, la scienza fortunatamente va avanti, sono i nostri modelli di comportamento che devono mutare. Questa la "lezione" che dovremmo apprendere a valle della tormentata esperienza, che stiamo attraversando e che potrà servire a tutti in un futuro che ci vedrà diversi. ■

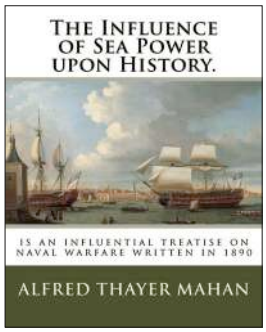
Cyberspace: un dominio da controllare?

Autore: Massimo Cappelli

Nel maggio del 2010, il Segretario statunitense della Difesa annunciò la nomina del **Generale Keith Alexander** come il primo comandante del nuovo U.S. Cyber Commander.

Nell'art. 70 della dichiarazione del luglio 2016 di Varsavia, il Consiglio Nord Atlantico afferma che il cyberspace è un nuovo dominio di conflitto: *"…Now, in Warsaw, we reaffirm NATO's defensive mandate, and recognise cyberspace as a domain of operations in which NATO must defend itself as effectively as it does in the air, on land, and at sea…."*

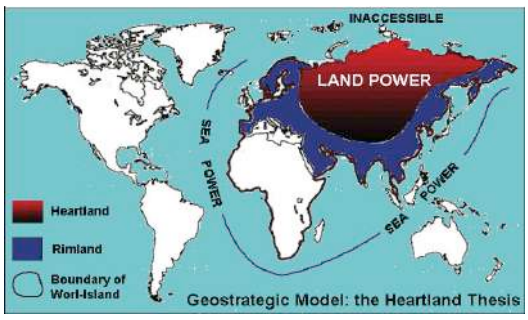
Questa nomina ha rafforzato la convinzione che il cyberspace fosse diventato un ulteriore dominio di conflitto. Già in passato ho trattato l'argomento in alcune conferenze e anche sulla newsletter della Fondazione GCSEC. Ritengo sia utile ripercorrere brevemente alcune teorie che hanno influenzato le Nazioni in passato e che potrebbero applicarsi anche al cyberspace.



L'Ammiraglio statunitense, **Alfred T. Mahan** teorizzò che, per dominare il mondo, fosse necessario prevalere sui mari con flotte ben equipaggiate. Alla fine del XIX secolo e inizi del XX secolo, i governi degli Stati Uniti, Germania, Giappone e Regno Unito, iniziarono una pesante campagna di rafforzamento navale.

Agli inizi del 900, il geografo britannico, **Sir Halford Mackinder**, sosteneva esistesse una pivot area del mondo, chiamata Heartland ("Heart of the World"), identificabile con i territori dell'Ex Unione Sovietica.

Il controllo di questa area avrebbe consentito il controllo dell'Island World, in quanto rappresentava un'area non raggiungibile dalle flotte navali.



La teoria di Mackinder è stata poi ripresa anche da Nicholas Spykman. Spykman sosteneva però che era molto più importante prendere il controllo del Rimland, regione che racchiude l'Heartland. Controllare il Rimland permetteva di controllare l'Heartland e quindi il mondo.

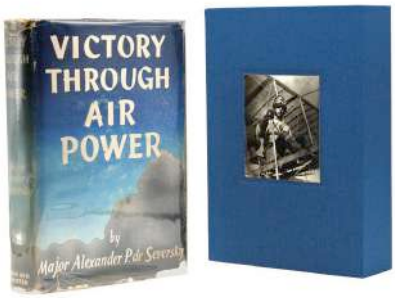
Il Presidente statunitense Truman fu influenzato da entrambe le teorie e utilizzò una strategia di *containment* nei confronti dell'Unione Sovietica.

Le teorie geopolitiche sono comunque influenzate pesantemente dallo sviluppo tecnologico. Gli avanzamenti nel campo dell'aeronautica e della missilistica e lo stesso avvento dell'era nucleare hanno portato a nuove teorie. Alla base delle teorie rimaneva pur sempre il ruolo della supremazia.

Il pilota russo, **Alexander P. de Seversky** aveva già nel 1942 evidenziato l'importanza del predominio aereo per avere il controllo del mondo. Pertanto, divideva il mondo in due grandi circonferenze il cui centro è rappresentato dai poli industriali statunitensi e sovietici e il raggio è definito dalla portata

BIO

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



dei bombardieri dell'epoca.

Il disgregamento del blocco sovietico ha messo in crisi le teorie del passato e ha cambiato le carte in tavola. La fine della Guerra Fredda ha portato alla nascita di nuove considerazioni in cui, le frontiere, seppur avessero già iniziato a vacillare come riferimento per il controllo del mondo, iniziarono ad avere sempre meno rilevanza.

Bertrand Badie ha espresso tale concetto osservando le guerre e le proteste in diverse aree geografiche in cui bandiere di diverse nazionalità sventolavano assieme, accomunate da ideologie religiose o di altra natura.

La comunicazione sempre più capillare e presente intorno a noi, ha portato alla luce affinità fra popoli diversi ma con problematiche comuni. La propagazione delle idee ha trovato nuova linfa vitale con la diffusione sempre più massiccia di Internet.

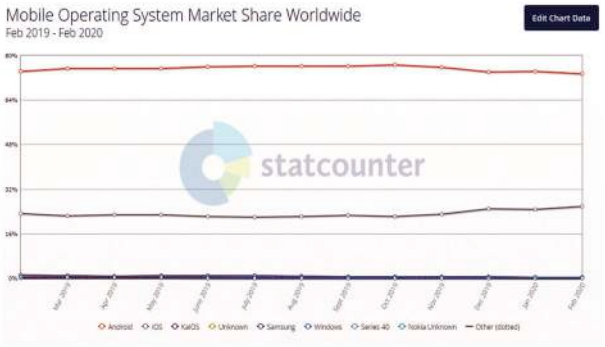
Gabriella Coleman, antropologa, ha osservato questo fenomeno nel movimento Anonymous. Il moto *"We are Anonymous"* esprime al meglio il movimento. Un movimento variegato in termini di religione, nazionalità ed etnia o estrazione sociale, alimentato da una stessa motivazione sia essa la Primavera Araba o la guerra contro Multinazionali o Agenzie governative. Di volta in volta, i partecipanti variano in base alla motivazione ed è per questo considerabile come un movimento, mai uguale, sempre diverso.

L'ascesa di Internet ha aggiunto un nuovo dominio di conflitto, il cyberspace che si aggiunge allo spazio terrestre, marittimo, aereo e spaziale.

Le teorie geopolitiche del passato prevedevano il controllo di un determinato spazio fisico per controllare il mondo. Potrebbe essere vero anche in questo caso. Se così fosse, dovremmo osservare il cyberspace per comprendere chi lo sta dominando. Lo spazio digitale è sì virtuale, ma la sua creazione e il suo sviluppo si poggia pur sempre su asset fisici e logici da cui non può svincolarsi. Pertanto, se dovessi ipotizzare chi sta vincendo la Guerra digitale dovrei comprendere chi detiene la maggioranza degli "strumenti" digitali per decretare un vincitore. La cosa non è così semplice perché parliamo di una moltitudine di attori pubblici e privati che ogni giorno sviluppano spazi virtuali da dove poter erogare servizi o vendere prodotti.

Se dovessi applicare le teorie del passato, potrei iniziare verificando il tasso di penetrazione di determinate tecnologie rispetto altre e la nazionalità di appartenenza delle stesse. Questo mi darebbe un'idea di come le varie nazioni sono presenti a livello mondiale. Solo a titolo di esempio ho cercato alcuni siti di statistica. L'esercizio è puramente esemplificativo e non ha basi scientifiche. Le stesse fonti consultate non sono state comparate né tantomeno è stata verificata l'affidabilità della fonte o l'attendibilità della notizia. Nonostante questo, sono palesi i risultati di questa prima ricerca che non penso differiscano molto dalla realtà.

Partiamo dai sistemi operativi. I sistemi operativi che dominano il mercato sono quelli di Microsoft (USA) con quote di mercato che si attestano sull'80%, seguiti da OS X (USA) con una percentuale intorno al 16-17%. La distribuzione geografica è impressionante soprattutto per Windows, raggiungendo anche Paesi come la Russia.



Sui sistemi operativi mobili, la predominanza è sempre statunitense con Android (USA) che si attesta oltre il 70% e IOS (USA) oltre il 25%.

Allo stesso modo vediamo la prevalenza dei social media statunitensi su tutti, dove Facebook (USA) domina e spicca sugli altri con un 62% mentre al secondo posto si posiziona Twitter (USA) con un 14%.

Anche nel settore dei motori di ricerca, Google (USA) sovrasta con un 92%, seguito da Bing (USA) con un 2% circa.

Se si passa a livello di server o di cloud services, i numeri sono sempre estremamente favorevoli agli Stati Uniti. Nel mondo Server, secondo i dati di Statista, nel primo semestre del 2019, il 55% del mercato è detenuto da aziende statunitensi (Dell, HPE, IBM, Lenovo, Oracle, Cisco). Huawei si attesta attorno al 5,4%.

Nel mondo Cloud, Amazon AWS (USA), Microsoft Azure (USA) e Google Cloud (USA) detengono il 56% del mercato mentre la cinese Alibaba Cloud appena il 5,4%.

Worldwide cloud infrastructure spending and annual growth
Canalys estimates: Q4 2018

Vendor	Q4 2018 (US$ billion)	Q4 2018 Market share	Q4 2017 (US$ billion)	Q4 2017 Market share	Annual growth
AWS	7.3	32.3%	5.0	32.2%	+46.3%
Microsoft Azure	3.7	16.5%	2.1	13.7%	+75.9%
Google Cloud	2.2	9.5%	1.2	7.6%	+81.7%
Alibaba Cloud	1.0	4.2%	0.6	3.5%	+73.8%
IBM Cloud	0.8	3.6%	0.6	4.2%	+27.6%
Others	7.7	33.8%	6.1	38.9%	+26.7%
Total	22.7	100.0%	15.6	100.0%	+45.6%

canalys

Source: Canalys Cloud Channels Analysis, February 2019

Queste analisi si potrebbero fare per tutte le tipologie di device o applicativi per vederne la fetta di mercato e la distribuzione geografica. Se si passa ad esempio al mercato del mobile, Samsung (Korea del Sud) ha una quota di mercato di circa il 32% seguita da Apple (USA).

Sul sito www.shodan.io, noto a tutti gli addetti alla cyber security, si possono inserire modelli specifici di dispositivi ITA per comprendere la distribuzione geografica e numerica delle stesse, per quelle che sono ovviamente raggiungibili via internet.

In questa panoramica non è stato considerato il mercato IoT e la diffusione del 5G che potrebbero cambiare in parte anche le percentuali nazionali, aumentando soprattutto la quota cinese.

Altra considerazione deve essere fatta anche sulle materie prime utili alla produzione dei chip, come il silicio.

Essendo risorse finite, è in atto una corsa all'approvvigionamento. In questo caso non virtuale ma fisica. Sarà molto importante anche il recupero delle stesse attraverso sistemi di gestione per riciclaggio. Questo è un tema su cui non è stata fatta molta sensibilizzazione ancora in UE.

Si deve considerare anche che la manifattura dei suddetti elementi avviene per la maggior parte in Asia e pertanto la possibilità che l'integrità del prodotto venga compromessa, è un'opzione da tenere a mente. Le analisi statiche e dinamiche sui singoli device sono costose e spesso mancano analisti capaci di farlo, oltre al fatto che non è fattibile per tutti gli apparati, soprattutto per quelli utilizzati dagli utenti finali. La proprietà di questi asset è per la maggioranza privata. Sono aziende e cittadini che utilizzano la maggior parte degli asset di cui sopra. Gus Coldebella, durante uno speech nel 2019, affermò che l'85% delle infrastrutture critiche americane sono in mano a privati.

Aziende di diverse nazioni stanno affidando i propri dati a servizi cloud esteri. Questo avviene anche per operatori di servizi essenziali, ponendo un serio problema in tutti gli Stati perché la prima linea di difesa contro potenziali attacchi sono appunto aziende private, spesso non supportate in modo adeguato dai Governi. I Governi spesso si concentrano a definire o recepire normative di settore invece di supportare operativamente le aziende.

Cerchiamo di fare il punto di quanto espresso finora:

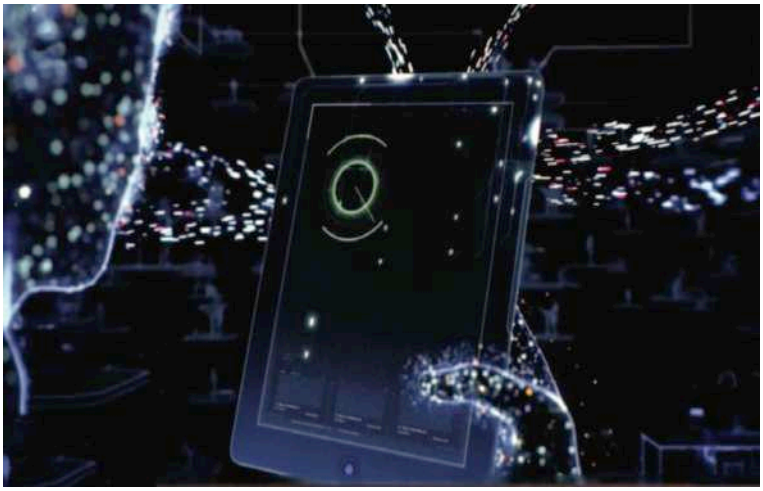
Alcune teorie geopolitiche propendevano per il controllo di determinati domini per controllare il mondo. La tecnologia e la disgregazione dei blocchi, occidentale e sovietico, hanno portato ad un cambiamento del panorama globale. L'avvento di Internet è stato *disruptive*.

Il cyberspace è uno spazio senza confini dove pubblico e privato erogano servizi di qualsiasi natura. I prodotti digitali statunitensi sono prevalenti rispetto ad altre Nazioni. La Cina potrebbe ridimensionare il divario sia con l'implementazione del 5G a livello mondiale, sia con la massiccia produzione di IoT, distribuiti in tutto il mondo e la cui sicurezza spesso è molto debole.

L'Europa non è una potenza al riguardo, è un'utilizzatrice di tecnologia ma per quanto riguarda la produzione di hardware e software non è comparabile con la produzione cinese e statunitense.

Attualmente il cyberspace è un campo perfetto per le attività di spionaggio. Ci sono stati attacchi volti alla compromissione o all'interruzione di servizi ad esempio in Iran e Ucraina. La vera battaglia però è quella della raccolta informazioni. Una volta tali informazioni erano collocate su documenti cartacei, ora viaggiano sotto forma di dati. Infatti, gli Advanced Persistent Threat mirano ai concentratori di dati e informazioni come possono essere i social network o i servizi cloud.

Spiare è meno rischioso, nascondendosi dietro una tastiera e sfruttando servizi di connessione anonima o server compromessi. Il gioco delle spie



non si è mai fermato ma sotto certi punti di vista è diventato più semplice ed economico.

Cosa succederebbe in caso di guerra mondiale?

Le super potenze potrebbero diventare più aggressive e quindi sfruttare gli asset privati per i loro scopi. I principi della FIDUCIA, della TRASPARENZA e della SICUREZZA verrebbero messi in secondo piano. L'obiettivo primario sarebbe dominare l'avversario, prendere il controllo delle sue infrastrutture, realizzare attacchi che mettano in ginocchio il Paese ostile. Attraverso Internet, questo potrebbe essere effettuato senza distruggere le infrastrutture critiche, ma rendendole temporaneamente inutilizzabili.

Per farlo, basterebbe che le aziende private inviassero dei pacchetti ufficiali di aggiornamento delle loro tecnologie in grado però di installare backdoor, scaricare ransomware, variare parametri di controllo e così via. I gestori dei servizi Cloud potrebbero negare l'accesso ai clienti dell'area interessata dal conflitto, bloccando servizi essenziali. I proprietari di motori di ricerca o social network potrebbero iniettare notizie false e manipolare l'opinione pubblica.

L'amministratore delegato che permettesse questo genere di azioni sarebbe un folle. Sarebbe un suicidio commerciale, a meno che questo comportamento non sia imposto per cause di forza maggiore o per cause belliche.

Alcune considerazioni da tenere a mente:

- Stati Uniti 1917, Giappone 1938, Regno Unito 1939, le *"National mobilization laws"* obbligarono industrie strategiche private dei rispettivi Paesi a passare sotto il controllo statale attraverso una legge di nazionalizzazione;
- Febbraio 2010, la Repubblica Popolare Cinese emana la *"National Defense Mobilization Law"*, in cui sostanzialmente il National People's Congress Standing Committee approvò speciali misure per supervisionare e controllare industrie e aree chiave cinesi.

In caso di guerra o necessità, le Nazioni possono approfittare delle proprie aziende private per scopi di interesse nazionale.

La guerra sotterranea che si sta combattendo è di collezionare informazioni e collezionare artefatti in grado di bucare eventuali piattaforme. Come ha affermato in un'intervista Andrea Zapparoli Manzoni, Executive Director di Crowdefense, l'87% delle *vulnerability 0 day* sfruttabili per attacchi è ancora considerata *0 day*. Significa che non sono state rese pubbliche. Ne viene pubblicata 1 su 20 in media.

Esistono analisti governativi e privati, persino aziende, che ricercano le *0 day* sfruttabili per attacchi. La maggior diffusione di alcune tecnologie rispetto ad altre rappresenta una medaglia a due facce. Da una parte sono potenziali armi sfruttabili in caso di guerra, dall'altra rappresentano superfici di attacco molto ampie che potrebbero contenere vulnerabilità critiche sfruttabili dagli avversari.

Ogni singola nazione ha il compito di identificare i propri servizi essenziali (n.b. non operatori ma servizi). Ogni servizio poggia su una catena di asset fisici e virtuali. Una volta identificati i servizi e le catene, le nazioni dovrebbero simulare stress sulle stesse, ipotizzando compromissioni, mancanza di erogazione, assenze etc. etc. Questo dovrebbe permettere di costruire scenari di impatto utili per procedere poi a piani di resilienza e continuità precisi. Questo lavoro dovrebbe essere fatto presupponendo la mancanza di un pilastro essenziale nei confronti dei vendor stranieri: il TRUST.

È necessario mettersi nella peggiore delle ipotesi per poi comprendere quali sono le migliorie da apportare al proprio sistema-paese per resistere a urti con impatti catastrofici. ■

- **Alfred T. Mahan: "The influence of Sea Power upon History"; "The Interest of America in Sea Power"**
- **Figura Heartland: https://birminghamwarstudies.wordpress.com/2012/06/04/215/**
- **Alexander P. de Seversky: "Victory Through Air Power"**
- **Bertrand Badie: "The End of Territories"**

La crisi del modello economico occidentale

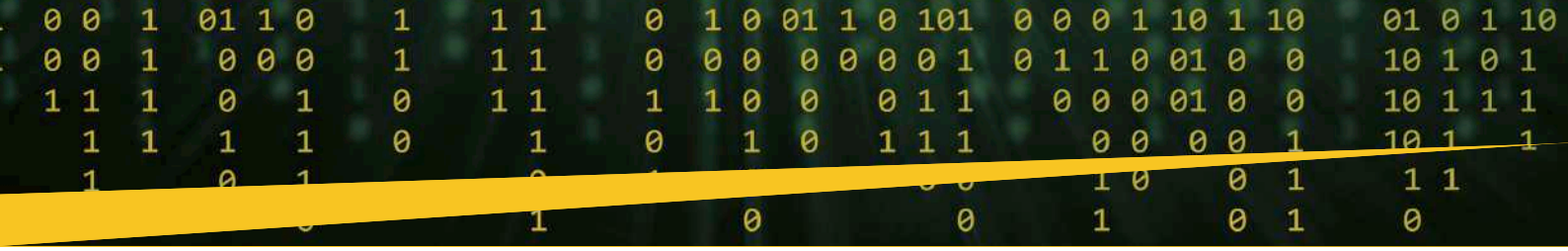
Autore: Francesco Corona

L'Europa è sotto attacco, su più fronti: crisi sanitaria da Covid-19 paragonabile ad una vera e propria guerra chimico-biologica, crisi connesse alle emergenze climatiche e alla geoingegneria, con relative catastrofi naturali sempre più intense, e poi crisi economiche strutturali legate al modello della **moneta di debito** (come l'Euro) e all'ingerenza di multinazionali private nel capitale delle Banche Centrali che depauperano gli Stati democratici occidentali come l'Italia delle loro risorse principali a favore della finanza apolide, che ricordiamo persegue logiche di profitto e non di tutela dei patrimoni nazionali ed europei. Poi ancora i problemi connessi ai nuovi assetti geopolitici e a zone di influenza sia in Europa, Africa, Sud America sia in Asia e Medio Oriente, determinati dalle politiche estere aggressive di nuove economie emergenti che sfruttano le debolezze degli Stati europei a loro vantaggio in particolar modo il disallineamento tra esigenze di sviluppo dei popoli e delle nazioni rispetto alle logiche di profitto di grandi gruppi economici occidentali che dominano sulle economie di interi Stati. Per inciso, questo è un elemento determinante dell'attuale crisi in atto e del successo delle politiche economiche di queste paesi emergenti come la Cina. In sostanza possiamo parlare di minacce ed attacchi concreti in tutti e cinque i domini della conflittualità: aria, mare, spazio, terra e cyberspace. Per quanto concerne le minacce provenienti dal cyberspace ci riferiamo, in particolar modo agli attacchi APT[B001] ora più che mai legati alle esigenze di Tutela e Sicurezza Nazionale/Europea. Cresce infatti la minaccia cyber e l'escalation di attacchi, sempre più sofisticati, volti a colpire le infrastrutture critiche civili e militari e/o esfiltrare segreti industriali e militari: servono quindi contromisure adeguate e su più livelli. Come già affermato su più tavoli ed in attesa di potenza di calcolo quantistica, una delle misure più interessanti è sicuramente la criptazione dei dati con un rapido svecchiamento delle stesse chiavi di codifica. Risulta tuttavia fondamentale che le strutture territoriali (NIS compliant) afferiscano al CSIRT NAZIONALE secondo schemi di maturità in grado di superarsi in una specifica agilità proattiva e predittiva nella gestione della minaccia stessa e nell'eventuale attivazione di sistemi offensivi o di autodifesa nazionali in linea con le attuali disposizioni sul Perimetro di Sicurezza dello Spazio Cibernetico, sulla Golden Power (5G) e sugli accordi NATO per il settore militare, con specifiche attenzione regole di ingaggio. Regole ancora non del tutto chiare. Infatti la NATO ha avuto

Fonte: http://enterprise-securityposhibure.blogspot.com/2017/10/enterprise-security-capability-model.html

BIO

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



decenni di esperienza operativa nella formulazione di regole di ingaggio (ROE) per armi cinetiche, ma diverse caratteristiche delle operazioni militari nel dominio cibernetico aumentano la loro complessità e risultano per ora informazioni classificate "Top Cosmic". Le questioni legate ai meccanismi di Comando e Controllo (CC) e all'escalation dell'uso di forza cibernetica anche in risposta ad attacchi cinetici (e viceversa) svolgono un ruolo importante nella definizione di ROE specifiche per l'Europa. In sintesi, la formulazione di ROE per le armi informatiche sono possibili con sforzi particolari per impartire tale esperienza ai leader politici e ai comandi militari in contesti di attivazione di unità di crisi come nell'esempio italiano.

Un problema, quello Cyber, che si inserisce nel quadro più ampio già evidenziato: l'Europa sta attraversando una crisi profonda che tocca tutti i settori della vita sociale ed economica ciò però non è vero per le grosse multinazionali finanziarie legate al mondo dei big data e di internet che continuano a macinare profitti da capogiro e nello stesso tempo concordare con gli Stati europei percentuali bassissime di oneri tributari (3%) anche in virtù della direttiva PSD2. Premesso che ogni Stato europeo presenta debolezze ed eccellenze strutturali proprie, resta il fatto che il trend globale parla molto chiaro, ora più che mai evidenziato dalla crisi da Covid-19, soprattutto se confrontato con le performance della Cina, che non nasconde di voler competere con Stati Uniti, Europa, e Giappone su settori strategici a forte impatto tecnologico. Secondo fonti del WTO, è dal 2013 che la Cina mantiene un disavanzo a suo favore di circa 200 miliardi di dollari tra import ed export verso l'Europa. Questo vale anche nei confronti degli Usa, che con Trump si sono mossi per primi attuando misure cautelative basate sui dazi doganali al 25%. Riteniamo che queste misure non siano sufficienti a frenare la corsa tecnologia e di affermazione geopolitica della Cina e neppure l'epidemia da Covid-19 che ha colpito la città cinese di Whuan. Non parliamo poi degli investimenti in Africa da parte di aziende cinesi che hanno superato i 36 miliardi di dollari per anno già dal 2016. Come dicevamo, è il modello economico delle democrazie occidentali ad essere in profonda crisi, modello basato su economie del debito che solo le Banche Centrali o i Ministeri del Tesoro sono in grado di risolvere estromettendo ingerenze di multinazionali finanziarie e variandolo di segno per esempio con emissione di Titoli di Stato al portatore (Mini BOT). Il nostro debito da italiani che al 31 dicembre 2019 ammontava a 2.409 miliardi di euro ci costa molto di più del suo valore nominale e la responsabilità di questo è da attribuire al Sistema della Banche Centrali che vede per l'Europa nella BCE con sede a Francoforte il suo fulcro principale. Attualmente sono solamente 9 i Paesi che hanno una Banca Centrale non riconducibile a partecipazioni dirette o indirette di alcuni gruppi finanziari ben precisi, essi sono: Cina, Russia, Iran, Venezuela, Ungheria, Siria, Cuba, Islanda e Corea del Nord. Tre di questi Paesi, nell'ordine Russia, Iran e Venezuela, sono anche le tre più grandi riserve energetiche del mondo. Direttamente o indirettamente tutte le restanti 193 banche centrali che gestiscono le politiche monetarie dei rispettivi paesi, appartengono o sono partecipate da alcuni gruppi economici privati attraverso loro società satelliti. Ci sono inoltre quattro banche centrali che sono quotate in borsa in particolare quelle di: Belgio, Grecia, Giappone e Svizzera. La Banca centrale di Grecia oltre che essere quotata alla Borsa di Atene è quotata anche alla Borsa di Germania. Come risulta dal sito ufficiale la Banca d'Italia (Istituto di Diritto Pubblico) alla voce partecipazioni mostra le quote di partecipazione al capitale che ad una prima analisi rivela come la percentuale di quote di rappresentanza pubblica si aggira intorno al 7% ed è detenuta da INPS e INAIL. Con queste quote i due enti pubblici giovano di benefici all'atto di ripartizione di introiti che garantiscono un supporto alle politiche sociali e pensionistiche del paese; anche se un regolamento interno stabilisce che i dividendi non debbano essere superiori al 3% per ogni partecipante al capitale e quindi il restante 94% dei dividenti, de iure e de facto, è proprietà privata e non pubblica. Ad esempio Intesa San Paolo e Unicredit detengono insieme il 52% delle quote di Banca d'Italia. Ovviamente nel capitale di queste grandi banche italiane, rientra quello di grossi gruppi finanziari transnazionali che attraverso JpMorgan, ad esempio, partecipano a Intesa San Paolo e controllano Monte dei Paschi di Siena, che attraverso Mediobanca partecipano Unicredit e che attraverso il Banco Santander Central Hispano controllano ABN AMRO, un altro azionista di Unicredit. Senza escludere poi l'americana Blackrock Inc. secondo grande azionista di Apple, primo azionista di Unicredit e secondo azionista di Intesa San Paolo che in Europa fu scelta dalla Troika per studiare i conti delle banche a rischio fallimento. Blackrock Inc. detiene ingenti quote di Atlantia (la nuova Autostrade), Telecom, Enel, Banco Popolare, Fiat, Eni e Generali, Finmeccanica, Banca Popolare di Milano, Fonsai, Mediobanca e Ubi; inoltre, è entrata anche nella gestione del risparmio di Poste italiane. Capiamo bene che così non può funzionare non su ciò che determina decisioni pubbliche, sociali e di sicurezza nazionale.

Questo antico retaggio delle quote in Banca d'Italia aveva senso quando la moneta era a corso forzoso, ovvero direttamente collegata alle riserve auree prima degli accordi di Bretton Woods del 1944. Ma con la successiva moneta a corso legale sostanzialmente legata al dollaro anche il sistema delle riserve di capitali di enti pubblici ed istituti di credito privati ed assicurativi non giustifica più l'attuale modello di emissione a prestito e quindi il relativo addebito di nuova moneta. Difatti, un altro aspetto fondamentale è che l'Euro è una moneta di debito, ovvero, viene acquistata dagli Stati membri dell'Unione e quindi anche dall'Italia, ed è pagata al valore nominale più oneri finanziari in Titoli di Stato pubblici che aumentano in modo impressionante il debito, secondo quanto stabilito dagli accordi di Maastricht. Tali accordi necessitano di una immediata revisione soprattutto in queste fasi cruciali di epidemia da Covid-19. Quindi entrambi gli scenari, ovvero, quello del capitale privato presente nelle Banca Centrale Europea e quello dell'emissione di moneta a debito, i quali sono più sostenibili e di fatto inaspriscono la crisi economica iniziata nel 2008 e che nessuna misura della BCE, con i suoi piani di intervento come il Quantitative Easing, [B002] è mai riuscita a risolvere. Inoltre, si pone una questione cruciale di Sicurezza Nazionale legata

Partecipanti al capitale della Banca d'Italia al 20 febbraio 2020		
	ENTE PARTECIPANTE	QUOTE
1	Intesa Sanpaolo S.p.A.	60.283
2	UniCredit S.p.A.	32.645
3	Generali Italia S.p.A.	11.010
4	Banca Carige S.p.A. - Cassa di Risparmio di Genova e Imperia	10.493
5	Istituto Nazionale della Previdenza Sociale	9.000
6	Istituto Nazionale per l'Assicurazione contro gli Infortuni sul Lavoro	9.000
7	Cassa Nazionale di Previdenza e Assistenza Forense	9.000
8	Cassa Nazionale di Previdenza ed Assistenza per gli Ingegneri ed Architetti Liberi Professionisti – INARCASSA	9.000
9	Ente Nazionale di Previdenza ed Assistenza dei Medici e degli Odontoiatri – Fondazione ENPAM	9.000
10	Cassa Naz. Previdenza Assistenza Dottori Commercialisti - CNPADC	9.000
11	Cassa di Sovvenzioni e Risparmio fra il personale della Banca d'Italia S.c.p.a.r.l.	9.000
12	Banca Nazionale del Lavoro S.p.A.	8.500
13	Ente Nazionale di Previdenza per gli Addetti e gli Impiegati in Agricoltura – Fondazione E.N.P.A.I.A.	8.280
14	Crédit Agricole Italia S.p.A.	8.080
15	Banca Monte dei Paschi di Siena S.p.A.	7.500

Stralcio primi 15 partecipanti al capitale di Banca d'Italia

alla gestione dei dati digitali e all'utilizzo di infrastrutture critiche finanziarie[B003] e di telecomunicazioni da parte di soggetti esteri che perseguono logiche di profitto e non logiche di tutale del Sistema Paese. Ricordiamo ai lettori che a marzo 2020 la BCE ha dichiarato una nuova emissione di monete di debito a sostegno dell'emergenza Covid-19 per un totale di 700miliardi di euro per tutta la zona euro, ma date le premesse poste in essere, questa massa ingente di denaro graverà sugli Stati che la riceveranno.

Come uscire dalla crisi

Il fabbisogno di moneta è determinato da un elemento fondante di uno Stato democratico sovrano come l'Italia, sancito dal primo articolo della Costituzione ovvero "L'Italia è una repubblica fondata sul lavoro" e non sul debito. Questo elemento fondante espresso dal lavoro di milioni di cittadini e cittadine è armonizzato dal PIL - il Prodotto Interno Lordo [B007] oramai sempre più svilito nel volerlo rapportare al debito pubblico (rapporto DEBITO/PIL) - che assume i connotati di un vero e proprio sudario di colpe da espiare. In realtà, questo debito non dovrebbe neanche esistere, perchè sono le **soprattutto le** stesse banche centrali ad averlo prodotto a loro vantaggio all'atto dell'emissione di nuova moneta. In parole semplici, il PIL rappresenta l'insieme di beni e servizi prodotti, ovvero la forza lavoro di una intera nazione in un dato arco temporale. Questa forza costituisce un elemento inequivocabilmente positivo del bilancio di uno Stato e non negativo. La quantità di moneta introdotta è quella necessaria a misurare lo scambio dei beni e servizi rapportato al PIL, ma stranamente questo fabbisogno positivo di moneta, all'atto dell'emissione cambia di segno e diviene negativo, cioè viene inserito nelle passività di bilancio. Questo modus operandi per molti illustri studiosi ed economisti è una vera e propria truffa ai danni dello Stato che si configura come un FALSO DI BILANCIO da parte delle Banche Centrali che emettono moneta appropriandosi del suo valore. Pagare l'emissione di moneta ad organismi privati in titoli di Stato con relativo indebitamento potrebbe essere risolto con emissione di titoli interni emessi dal ministero del Tesoro, come i mini bot oppure bond o minibond[B006] resi fruibili come moneta circolante e con diritto di cambio garantiti dallo Stato.

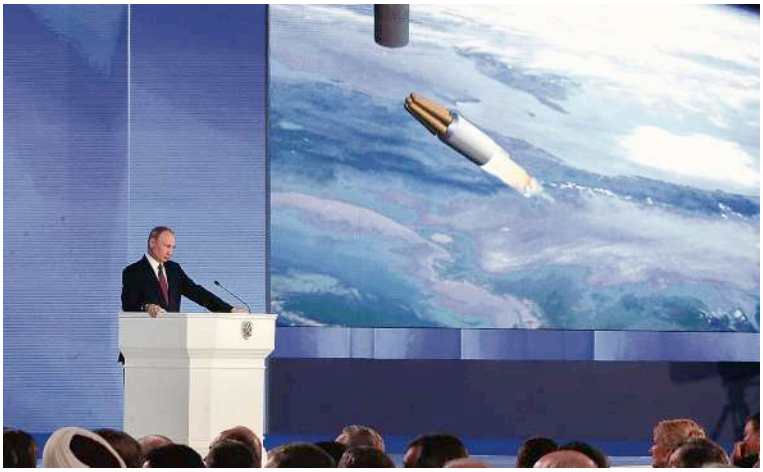
La ricetta di Putin

Concludiamo questo articolo ricordando ai lettori che Putin fu eletto presidente della Federazione Russa, nel 2000, quando la nazione era in bancarotta. La Russia doveva 16,6 miliardi di dollari al Fondo Monetario Internazionale (FMI) diretto dai Rothschild, mentre il debito estero alle controllate Rothschild di Londra e Parigi ed altri creditori, ammontava a 36 miliardi di dollari. Nel 2015 dopo aver ottemperato a tutti i debiti verso il FMI e verso gli altri creditori, Putin emise un decreto per escludere dal territorio della federazione russa tutti i membri della famiglia Rothschild, dopo i fatti legati alle loro ingerenze per tramite dell'oligarca Boris Berezovsky**. Inoltre,** estromise dalla Bank of Russian ogni elemento riconducibile a questa famiglia ripristinando **così** una situazione di indipendenza monetaria dall'Occidente finanziario.

Attraverso questa indipendenza Putin seppe rafforzare tutti i settori economici e negli anni dal 2015, ad oggi, è riuscito a potenziare l'apparato militare dimostrando le sue capacità strategiche, tattiche ed operative nella guerra in Siria. Inoltre, ricordo che l'esercito russo oscurò per sette giorni tutto il sistema di comunicazione NATO durante le operazioni di sbarco delle sue truppe nella baia di Tartus.

US - B2 Spirit

Nel dicembre 2019, pochi mesi or sono, dopo varie presentazioni spettacolari del suo arsenale, Putin ha annunciato la piena operatività del sistema missilistico ipersonico Avangard, vera spina nel fianco della NATO, con piena manovrabilità in volo e velocità nell'atmosfera di Mach 27, circa 33.000 chilometri l'ora. Ricordiamo, inoltre, che a marzo 2020 gli Stati Uniti, in piena crisi Covid-19 nell'ambito della già nota esercitazione militare Defender Europe 2020 hanno provveduto a rischierare nelle Azzorre e in Gran Bretagna un numero imprecisato di bombardieri strategici nucleari Northrop Gruman B2 Spirit, il più avanzato aereo strategico degli Stati Uniti.



Putin presenta il missile Avangard

Sala CC Avangard

Considerazioni finali

Quindi di fronte a questi scenari geopolitici e di possibile escalation militare, scenari di crisi economica e di forte emergenza sanitaria indotta dal Covid-19, non resta che allertare preventivamente i decisori politici e militari affiche ci sia un ripensamento serio ad un nuovo sistema economico occidentale legato alle emissioni di moneta non più basato sul modello del debito agli Stati. Questo modello ha concesso privilegi inimmaginabili al capitalismo finanziario, un sistema economico che ha depauperato totalmente gli assets strategici di tutti i paesi della zona euro inclusa la Germania, ed ha indotto necessariamente forme di repressione fiscale non più sostenibili. Paesi come l'Italia, ad esempio, sono stati costretti a ridurre le spese sanitarie che in alternativa sarebbero state fondamentali nella gestione di questa emergenza da Covid-19. L'Italia è stata, inoltre, costretta a svendere i propri patrimoni nazionali (porti, compagnie di bandiera, musei, intere filiere industriali strategiche) a favore di potenze come Cina, Russia, Stati Uniti, Francia ed Arabia Saudita e alle loro aziende collegate. I paesi come l'Italia già strangolati dal deficit e dai diktat imposti della Troica (BCE, FMI, CE) non possono più tollerare l'arresto del proprio motore economico pulsante, sarebbe un suicidio annunciato che si estenderà di concerto a tutto il mondo occidentale. Chi ha attinto risorse improprie trasformando i frutti del lavoro di milioni di cittadini europei in un sudario fatto di debito, ora deve fermarsi e rivedere le proprie strategie di profitto. Solo una volontà politica univoca, incorruttibile ed autorevole potrà gestire questo passaggio cruciale, magari imponendo come prima mossa la remissione dei debiti verso tutti i debitori proprio seguendo una logica che esalti l'essenza stessa del pensiero religioso occidentale.

Riferimenti bibliografici utili

[B001] https://gcsec.org/it/advanced-persistent-threats-study/

[B002] https://docplayer.it/1300295-Flussi-finanziari-verso-una-nuova-politica-della-bce-a-cura-di-francesco-corona.html

[B003] https://www.cybertrends.it/infrastrutture-critiche-finanziarie-nuovi-modelli-dinamici-di-protezione-e-simulazione/

[B004]http://www.opinione.it/economia/2019/07/19/ruggiero-capone_corsera-hillary-clinton-wall-street-steve-bannon-partiti-nazionalisti-populisti-anti-euro-blackrock-rockefeller-rothschild-soros/

[B005[https://www.lintellettualedissidente.it/controcultura/economia/blackrock-comprare-quando-scorre-il-sangue/

[B006] https://www.money.it/Minibond-cosa-sono-e-come-funzionano

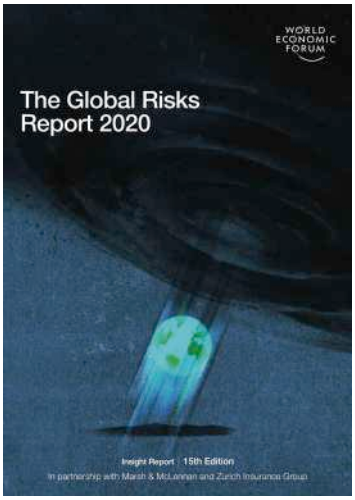
[B007] https://www.borsaitaliana.it/notizie/sotto-la-lente/pil.htm PIL (Prodotto Interno Lordo) è il valore dei prodotti e servizi realizzati all'interno di uno Stato sovrano in un determinato arco di tempo. Detto valore è quello che risulta da un processo di scambio ovvero, in parole povere, dalla vendita di prodotti e servizi: questo esclude dal computo i prodotti/servizi realizzati da un soggetto per autoconsumo e i servizi resi a titolo gratuito. Da sito ■

Equilibri geopolitici e sicurezza cibernetica

Autore: Gianluca Bocci

Nell'ambito giornalistico e in generale nelle trasmissioni televisive che trattano temi di politica, è ricorrente l'uso del termine *"Geopolitica"*, al punto che spesso se ne abusa; sorge spontanea la domanda, apparentemente banale, sul vero significato di questo termine.

Purtroppo, trovare una risposta non è semplice, infatti sembra non esistere una definizione univoca di questa parola; a partire dalla metà del XIX, periodo in cui fu coniata, diverse sono state le scuole di pensiero che continuamente nel tempo e fino ai giorni nostri ne hanno rivisto e fatto evolvere il significato. La rivista Limes[1], nell'articolo *"Cos'è la geopolitica e perché va di moda[2]"*, afferma che *"la geopolitica analizza conflitti di potere in spazi determinati"*; in tal senso l'analisi si pone l'obiettivo di comprendere come nel breve-medio periodo potrebbero mutare e ridefinirsi gli equilibri tra gruppi di potere, siano essi rappresentati da Stati più o meno grandi, entità sovranazionali, grandi imprese industriali e commerciali con elevata capacità di condizionamento, nonché gruppi *"forti"* anche non statali e dunque di qualsiasi natura, che agiscono e interagiscono su aree geografiche che potrebbero tra loro influenzarsi.



Si tratta di analisi complesse a causa degli effetti globalizzanti che, rispetto a qualche decennio fa, caratterizzato da un mondo sostanzialmente bipolare dove da una parte avevamo la zona atlantica e dall'altra quella sovietica, hanno iper-frammentato il contesto di riferimento. Tra i gruppi di potere più rilevanti oggi troviamo: gli Stati Uniti e la Cina che, in forte contrapposizione su diversi fronti[3], vogliono rispettivamente mantenere e conquistare la posizione di prima potenza mondiale, gli americani attraverso le pressioni delle grandi lobby dell'alta finanza, i cinesi attraverso quella della dirigenza del Partito Comunista; la Russia che sogna di tornare ai tempi della grande Unione Sovietica; la Germania che vuole affermarsi come la locomotiva d'Europa; molti altri attori che, un po' su tutto il pianeta, stanno cercando di trovare un loro spazio (ad es. l'Iran, la Corea del Nord).

Un panorama mondiale in continuo fermento, caratterizzato da molteplici rischi che sono stati ben illustrati e discussi nel rapporto "Global Risk Report 2020[4]", recentemente pubblicato dal World Economic Forum[5],

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.

prima a Londra, il 15 gennaio, ed ufficialmente a Davos dal 21 al 24 febbraio. Dal documento si evince che i principali rischi sono riconducibili al clima attraverso eventi meteorologici di grande portata che causano sempre più danni in termini di perdita di vite umane e danni alle infrastrutture, il fallimento delle misure di mitigazione poste o che si pensa di porre in essere per mitigare il rischio stesso, i crimini ambientali commessi dall'uomo nei confronti dell'ecosistema terrestre e marino.

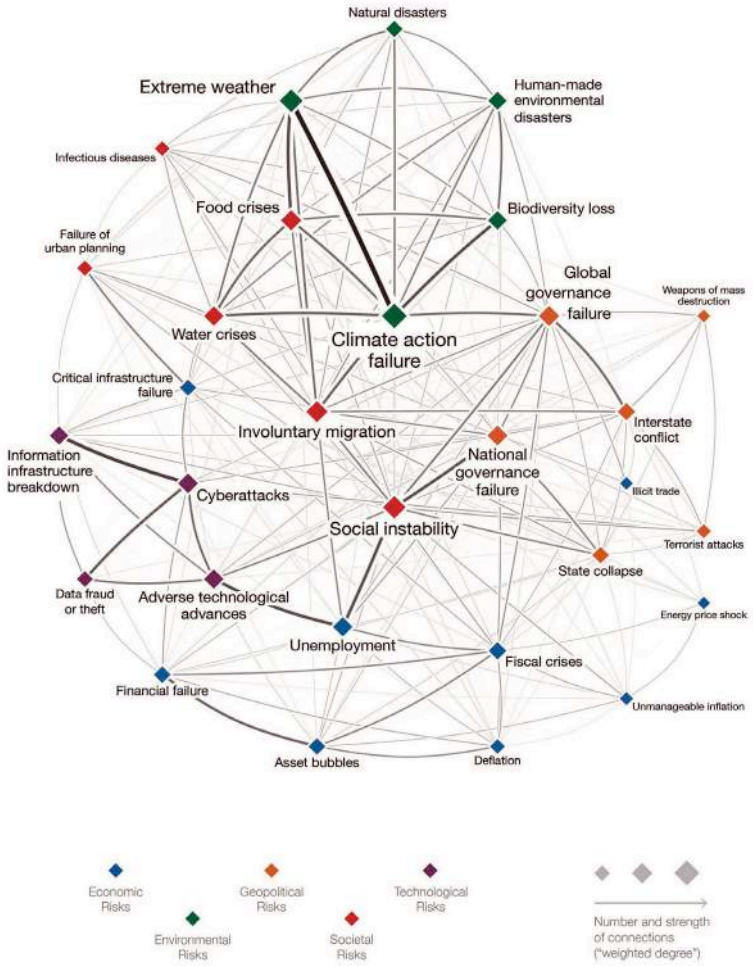


Figura 1 *The Global Risks Interconnections Map 2020 Source: World Economic Forum Global Risks, Perception Survey 2019–2020*

È interessante notare come nello stesso documento la frammentazione digitale è ritenuta un fattore di rischio tale da essere citato subito dopo quello climatico: *"Attualmente, oltre il 50% della popolazione mondiale ha accesso a Internet, circa un milione di persone vi accede per la prima volta ogni giorno e due terzi della popolazione globale possiedono un dispositivo mobile. Sebbene la tecnologia digitale offra enormi vantaggi economici e sociali alla maggior parte della popolazione mondiale, questioni quali la disparità dell'accesso a Internet, l'assenza di un modello globale di governance della tecnologia e la scarsa sicurezza informatica pongono rischi significativi. Anche l'instabilità geopolitica e geo-economica, tra cui la possibilità di uno spazio informatico frammentato, minacciano la piena realizzazione di tutto il potenziale delle tecnologie di prossima generazione. Gli intervistati ai fini del sondaggio hanno indicato l'«interruzione delle infrastrutture di informazione» come il sesto rischio per impatto nei prossimi anni fino al 2030* [6]*".*

Un'affermazione la precedente che mette anche in evidenza come la mancanza di un modello globale di *"governance"* delle tecnologie (soprattutto quelle emergenti) e aspetti di natura *"cyber"* preoccupino al punto da sentire sempre più forte l'esigenza di gestire in maniera adeguata la sicurezza nel *"cyberspazio"*. Del resto, molte delle tecnologie che si utilizzano, stanno ridefinendo in maniera radicale l'assetto di società ed economie; basti pensare alle reti di quinta generazione (5G), all'Internet of Things (IoT) in tutte le sue diverse declinazioni, al Cloud, all'informatica quantistica e all'intelligenza artificiale.

La stabilità, la prosperità e l'indipendenza che devono e dovranno garantire questi nuovi assetti, devono necessariamente passare per la risoluzione di tutti i problemi appena menzionati, *"in primis"* la sicurezza delle tecnologie e dei servizi digitali che sono nel frattempo diventati di estremo interesse per quei gruppi di potere citati all'inizio dell'articolo. Non a caso negli ultimi anni le cronache ci hanno abituato a sentir parlare di attacchi informatici condotti nei confronti di target pubblici e privati, spesso strategicamente rilevanti per un sistema paese, con l'obiettivo: di destabilizzarlo politicamente; di ottenere nel breve e medio periodo vantaggi competitivi, ad esempio ostacolandone la crescita economica o sottraendogli proprietà intellettuale ad alto valore aggiunto; più in generale, di rimetterne in discussione equilibri interni ed esterni (consolidati o precari che siano) così da esasperare in ultima analisi le rivalità geopolitiche.

Affianco a queste considerazioni, occorre altresì ricordare come l'elevata compenetrazione tra il mondo digitale e quello fisico ha accentuato i rischi a cui è esposta la nostra società, soprattutto se si pensa alle infrastrutture critiche del settore energetico, dei trasporti, della sanità, ma non solo, che, se interessate da attacchi informatici possono subire impatti devastanti concreti. Per le precedenti ragioni, geopolitica e cybersecurity presentano una forte relazione d'interdipendenza (in termini di rischio), anche illustrata nel già citato rapporto *"Global Risk Report 2020"*. In particolare nella fig.1 *"The Global Risks Interconnections Map 2020"* si evidenzia la relazione tra il rischio di un attacco informatico (Cyberattacks) e quello relativo alla perdita di capacità di governo da parte di uno Stato (National Governance Failure), piuttosto che quello di disputa tra Stati (Interstate Conflict). In tal senso, l'attacco informatico non deve essere più inteso come lo strumento utilizzato dai c.d. *"hacker tradizionali"*, il cui obiettivo è monetizzare le proprie gesta, piuttosto invece, come lo strumento utilizzato per rimettere in discussione equilibri geopolitici in essere.

La rilevanza della dimensione digitale

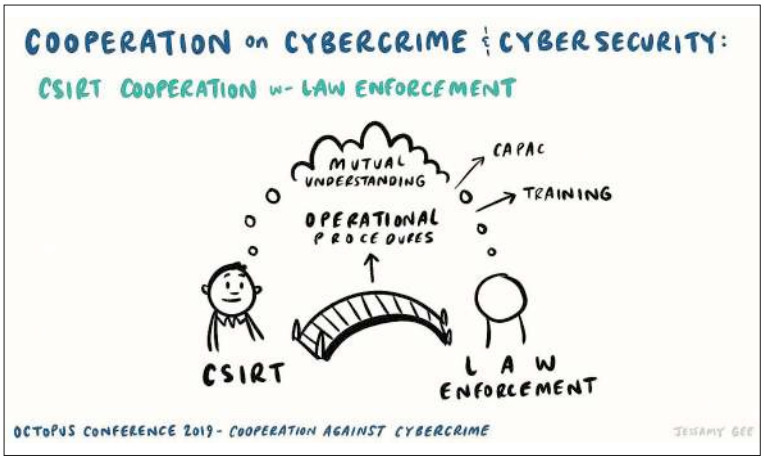
In questi ultimi anni la dimensione digitale, a differenza di quella terrestre, marittima, aerea e spaziale, ha dunque assunto un ruolo prevalente e strategico per tutti quei gruppi di potere che hanno interesse nel rimettere in discussione l'assetto geopolitico di un sistema paese; infatti per perseguire tale obiettivo, l'attacco informatico presenta molteplici vantaggi per l'attaccante: il suo carattere spesso asimmetrico, non permette di attribuire con certezza la paternità e la responsabilità dell'attacco stesso, da cui un limitato rischio di ritorsione, anche di tipo convenzionale (ad es. risposte militari), da parte di chi ha subito l'offesa; la disparità di risorse impiegate, anche a livello finanziario, che consente ad piccolo Stato o attore non statale di condurre un attacco e avere la meglio nei confronti di soggetti dotati anche di elevate capacità difensive e offensive, ciò anche grazie a strumenti, competenze e servizi *"ad hoc"* resi disponibili in modalità *"as-a-service"* nel Dark Web; l'intrinseca vulnerabilità che caratterizza le tecnologie digitali, sia in ragione della loro complessità, sia della velocità con le quali si tende a portarle sul mercato; il ritardo nell'adozione di sistemi di certificazioni che garantiscono l'affidabilità delle tecnologie utilizzate, ecc.

Questi motivi hanno indotto i Governi di molti Stati, quelli appartenenti alla Comunità Europea ne sono un esempio, a cambiare il modo di concepire la sicurezza cibernetica, ad esempio ponendo maggiore attenzione alla protezione delle proprie infrastrutture critiche, nel sostenere e garantire i valori della società e del mercato digitale e prevenire in generale l'escalation di conflitti tra Stati. In tal senso, in questi ultimi anni, proprio gli sforzi della Comunità Europea e di Stati come l'Italia, ma non solo, hanno fatto sì che si ponessero al centro del dibattito temi rilevanti e d'attualità come la necessità di una governance tecnologica, l'adozione di misure di sicurezza comuni, schemi di certificazione e modelli di approvvigionamento delle tecnologie orientati alla sicurezza, il contenimento dei rischi con l'offshoring dei dati e molto altro; per cui, i legislatori, sia a livello comunitario, sia nazionale, hanno emanato molteplici provvedimenti per innalzare il livello della sicurezza cibernetica delle infrastrutture critiche, dei sistemi e dei servizi digitali utilizzati nei rapporti con la pubblica amministrazione e nei mercati digitali, per la sicurezza nazionale, al fine di garantire quella voluta e necessaria capacità di governo da parte degli Stati che poi si riflette in senso positivo sulle imprese e il benessere dei cittadini. In maniera non esaustiva ricordiamo alcuni tra i principali provvedimenti che, in maniera diretta o indiretta sono stato emanati negli ultimi 5 anni in materia di sicurezza:

- la direttiva (UE) 2015/2366 sui servizi di pagamento digitali (la c.d. direttiva PSD2)
- il regolamento (UE) 2016/679 in materia di trattamento dei dati personali e privacy (il c.d. regolamento GDPR);
- la direttiva (UE) 2016/1148 sulla sicurezza delle reti e dei sistemi informativi (la c.d. direttiva NIS)
- il regolamento (UE) 2019/881 con il quale si completa la strategia europea per la sicurezza cibernetica (il c.d. Cybersecurity Act)
- il Dpcm del 24 gennaio 2013 prima e poi quello del 17 febbraio 2017 (rispettivamente il c.d. Decreto Monti e Gentiloni) per istituire, attraverso successivi decreti attuativi della Presidenza del Consiglio dei Ministri, un'architettura istituzionale deputata alla tutela della sicurezza nazionale relativamente alle infrastrutture critiche

- il D. lgs. del 18 maggio 2018, n. 65 in attuazione alla direttiva (UE) 2016/1148;
- il D.l. del 21 settembre 2019, n. 105, con il quale sono state introdotte misure urgenti in materia di perimetro di sicurezza nazionale cibernetica
- il Dpcm dell'8 agosto 2019, recante disposizioni sull'organizzazione e il funzionamento del Computer Security Incident Response Team (CSIRT) italiano, in attuazione della direttiva NIS
- la Legge del 18 novembre 2019, n. 133 che ha convertito il già citato D.L. n. 105 del 21 settembre 2019.

Proprio in questi giorni il nostro Governo per far fronte alle forti oscillazioni della Borsa di Milano a causa dell'emergenza Coronavirus, e dunque al pericolo di manovre speculative da parte di gruppi stranieri con possibili scalate nei confronti di aziende strategiche (non solo in termini di capacità produttiva, ma anche per la sicurezza nazionale) del nostro Sistema Paese, ha attivato la c.d. Golden Power approvata per estensione a settembre 2019 con il D.l. n.105. La Golden Power anche se al momento è stata utilizzata per motivi che non hanno attinenza con le tecnologie, si ricorda che è uno degli elementi caratterizzanti il perimetro di sicurezza nazionale, proprio in riferimento alla tecnologia 5G; al riguardo la disposizione richiede a tutti i soggetti inclusi nel perimetro di comunicare accordi e contratti che riguardano servizi di telecomunicazioni basati su questa tecnologia e che vedono il coinvolgimento di soggetti extra-UE, riservandosi lo Stato il diritto di veto per motivi di sicurezza nazionale.



Conclusioni

I molteplici sforzi normativi fatti finora, hanno tracciato una direzione di assoluto interesse affinché la sfida per ottenere un adeguato livello di sicurezza dello spazio cibernetico possa essere vinta. Si tratta di un obiettivo assolutamente perseguibile, che richiede insieme allo sforzo dei legislatori, che dovranno comunque adeguarsi alla velocità con cui le tecnologie evolvono, anche quello delle istituzioni coinvolte, delle imprese pubbliche e private, nonché dei cittadini. Sforzi commisurati alla complessità della materia, con investimenti adeguati a tutti i livelli, il coinvolgimento di personale affidabile e altamente qualificato (dotato di adeguate competenze organizzative, di processo e tecnologiche), lo sviluppo di programmi mirati a far crescere la consapevolezza in materia di sicurezza, nonché lo sfruttamento dell'enorme potenziale derivante dai programmi di ricerca e innovazione. Centrale in questa sfida sarà la capacità di prevenire gli attacchi informatici o quantomeno limitarne gli effetti, promuovendo in ottica preventiva: l'uso di sistemi di monitoraggio avanzati; in generale la cultura della condivisione delle informazioni sugli incidenti di sicurezza e le tecniche utilizzate dagli attaccanti; lo sviluppo di rigorosi programmi d' *"intelligence"* per la ricerca, il trattamento e la distribuzione di informazioni strategiche nel processo decisionale, anche in questo caso a qualsiasi livello. Del resto, la sicurezza di uno Stato dipende anche dal contributo che ogni singola impresa e gli stessi cittadini sono in grado di fornire. ■

1 https://www.limesonline.com/
2 https://www.limesonline.com/rubrica/cose-la-geopolitica-e-perche-va-di-moda
3 Relativamente ai rapporti tra Stati Uniti e Cina, l'Organizzazione per la cooperazione e lo sviluppo economico (OCSE) avverte "Escalatingtradeconflicts are taking an increasingtoll on confidence and investment, adding to policy uncertainty, aggravatingrisks in financialmarkets and endangeringalreadyweakgrowthprospectsworldwide."
4 http://www3.weforum.org/docs/WEF_Global_Risk_Report_2020.pdf
5 https://www.weforum.org/
6 http://www3.weforum.org/docs/WEF_GRR20_Executive_Summary_Italian.pdf

COVID#19, quando la sicurezza digitale avrebbe molto da insegnare ai governi in materia di gestione di crisi.

Autore: Laurent Chrzanovski

Sul terreno: la politica del caos e l'ideologia dell'"ognuno per sé"

La gestione europea del COVID#19 (Coronavirus) è catastrofica: piani di emergenza nazionali con misure sempre più restrittive che si susseguono come la chiusura delle frontiere e l'isolamento degli individui. Tali misure portano le popolazioni ad uno stato d'assedio e talvolta di panico.

Tutto ciò è amplificato da un cinismo politico dove l'emergenza si traduce in una triplice sfida: combattere efficacemente l'espansione del virus, fare funzionare al meglio l'economia e non perdere la propria quota di popolarità elettorale.

Nei "think tank" dei leader europei, dove tutti hanno esigenze chiare e precise, questi tre fronti sono completamente conflittuali. Il risultato è evidente, viviamo nel caos dove ogni paese applica leggi di emergenza, misure sanitarie e terapie differenti. La situazione attuale viene riassunta bene nella recente descrizione fatta da Giorgio Agamben: *"Mai come oggi si è assistito allo spettacolo, tipico delle religioni nei momenti di crisi, di pareri e prescrizioni diversi e contraddittori, che vanno dalla posizione eretica minoritaria (pure rappresentata da scienziati prestigiosi) di chi nega la gravità del fenomeno al discorso ortodosso dominante che l'afferma e, tuttavia, diverge spesso radicalmente quanto alle modalità di affrontarlo. E, come sempre in questi casi, alcuni esperti o sedicenti tali riescono ad assicurarsi il favore del monarca, che, come ai tempi delle dispute religiose che dividevano la cristianità, prende partito secondo i propri interessi per una corrente o per l'altra e impone le sue misure"* (1).

La politica del caos: Korczowa - Krakovets, punto di frontiera tra Polonia e Ucraina, 28 marzo 2020. In piena crisi del COVID#19, decine di migliaia di cittadini ucraini si ammassano per riuscire a tornare nel loro paese prima della chiusura delle frontiere. ©Novynarnia.

Le persone vengono lasciate in balia di un'esplosione di informazioni allarmistiche, peggio ancora di disinformazione attraverso fake news. Lo stato di confusione e abbandono generale si riassume nel motto di Noam Chomsky: *"The general population doesn't know what's happening and it doesn't even know that it doesn't know".*

La collaborazione europea ed internazionale, l'unica che potrebbe fronteggiare al meglio l'epidemia, è quasi inesistente. Ciò viene magistralmente sottolineato da Yuval Noah Harari: *"Penso che la cosa peggiore sia la disunione che vediamo nel mondo, la mancanza di cooperazione, di coordinamento tra i diversi Paesi. E la mancanza di fiducia, sia tra gli Stati sia tra le popolazioni e i governi. (…) Quindi, ciò che mi spaventa davvero è la mancanza di leadership e cooperazione. E ciò di cui la gente dovrebbe rendersi conto è che la diffusione dell'epidemia in ogni singolo Paese minaccia il mondo intero, a causa del fatto che, se non viene contenuto in tempo, il virus si evolverà. Questo è forse uno dei peggiori scenari con questo tipo di epidemia: una rapida evoluzione del virus."* (2).

Peggio ancora, nei paesi a frontiere chiuse dove tra le misure di sanità pubblica è prevista la quarantena totale, assistiamo ad un vero e proprio colpo di stato dettato dall'incapacità di identificare ed isolare i focolai del virus sul territorio per mancanza di test sufficienti. Questo genera una psicosi dove il parente, il vicino, l'amico diventano tutti casi sospetti verso i quali bisogna creare una frontiera. Il pericolo di questo isolamento è ben spiegato da Michel Onfray: *"Ma cos'è questo confinamento se non un invito a creare tantefrontiere quanti sono i francesi? Il confine nazionale non è un buon confine, ma il confine che separa una persona da un'altra viene presentato come la soluzione, l'unica soluzione, ci viene detto. (…) Maastricht tossisce, sputa e minaccia l'embolia."* (3)

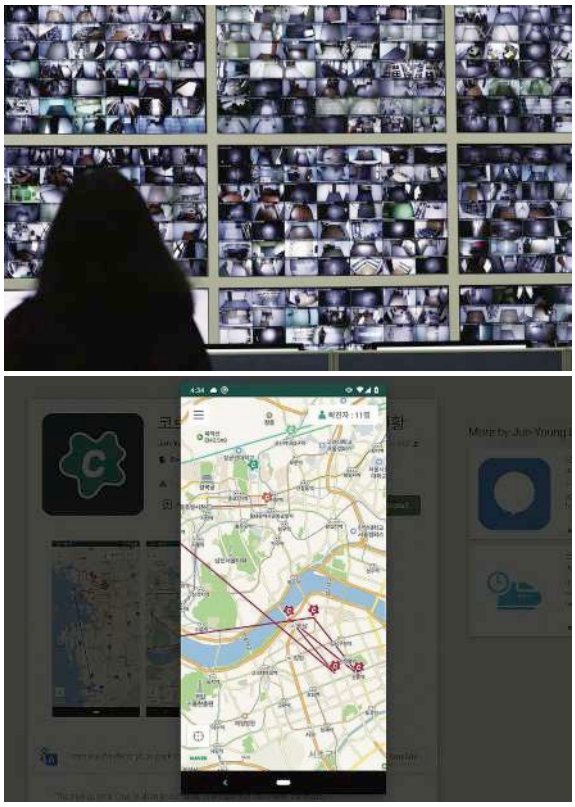
Le democrazie di fronte alla tentazione della sorveglianza di massa

Non poche di queste misure fanno riflettere sul nostro futuro in primis quello digitale. Infatti, aumenta il numero di governi che in questo periodo attivano un controllo della nostra localizzazione attraverso i nostri stessi "tool". Il rischio che tali misure di controllo potessero essere adottate anche dalle democrazie era stato previsto da Slavoj Žižek: *"L'epidemia causata dal coronavirus serve a giustificare e legittimare misure di controllo e regolazione delle popolazioni finora impensabili in una società democratica occidentale - il confinamento totale dell'Italia non è forse una fantasia totalitaria? Non sorprende che la Cina (che già faceva un uso massiccio delle nuove tecnologie a fini di controllo sociale) si stia dimostrando la più attrezzata per affrontare un'epidemia catastrofica - almeno a giudicare da quella che sembra essere la situazione attuale. Questo significa che la Cina incarna il nostro futuro, almeno per certi aspetti?"*(4).

BIO

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

Yuval Noah Harari, nel suo ultimo saggio, va ben oltre quando argomenta sulla possibilità che la sorveglianza legata al Coronavirus, adottata in alcune democrazie, divenga uno strumento d'uso comune. A tal riguardo afferma: *"Per fermare l'epidemia, intere popolazioni devono rispettare alcune linee guida. Ci sono due principali vie per raggiungere questo obiettivo. (…) Oggi, per la prima volta nella storia dell'umanità, la tecnologia consente di monitorare tutti continuamente. Cinquant'anni fa il KGB non poteva seguire 240 milioni di cittadini sovietici 24 ore al giorno, né poteva sperare di elaborare efficacemente tutte le informazioni raccolte. Il KGB si basava su agenti umani e analisti e non riusciva proprio a collocare un agente umano per seguire ogni cittadino. Ma ora i governi possono fare affidamento su sensori onnipresenti e potenti algoritmi invece che su spettri in carne e ossa. (…)*



Monitoraggio in tempo reale, Corea del Sud
© The Conversation
App del Governo della Corea del Sud segnalando itinerari e luoghi dove si trovano persone infettate © Businessinsider

Molte misure di emergenza a breve termine diventeranno un appuntamento fisso. Questa è la natura delle emergenze. Portano i processi storici ad avanzare rapidamente. Le decisioni che in tempi normali potrebbero richiedere anni di deliberazione vengono prese nel giro di poche ore. Le tecnologie immature e persino pericolose vengono messe in servizio, perché i rischi di non fare nulla sono maggiori. Esperimenti sociali su larga scala manifestano la loro utilità per interi paesi. Cosa succede quando tutti lavorano da casa e comunicano solo a distanza? Cosa succede quando intere scuole e università operano online? In tempi normali, governi, aziende e consigli scolastici non accetterebbero mai di condurre tali esperimenti. Ma questi non sono tempi normali. In questo momento di crisi, abbiamo due scelte particolarmente importanti davanti a noi. La prima è tra sorveglianza totalitaria e la responsabilizzazione dei cittadini. La seconda è tra l'isolamento nazionalista e la solidarietà globale." (5)

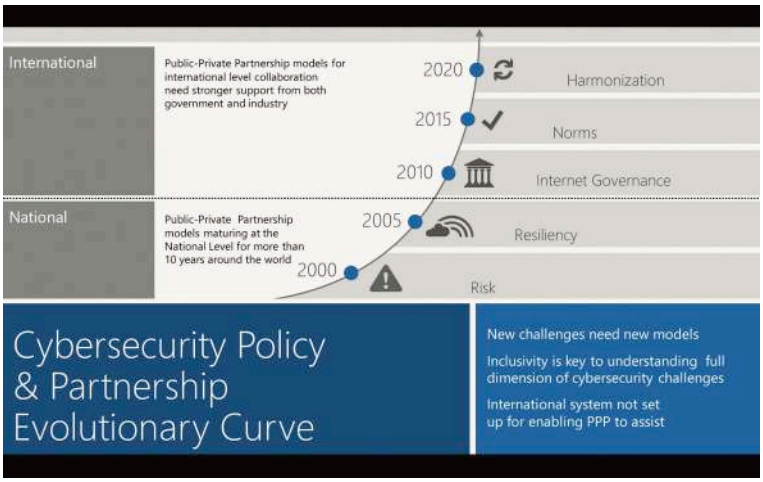
Cybersecurity: un campo globale con attori in dialogo permanente

Ed è proprio qui che **la cybersecurity ed il suo coordinamento sembrano quasi esemplari se paragonati** a molte scelte governative.

Il perché è semplice: oltre ai danni economici legati meramente al virus – che varie fonti sottolineano essere già i sintomi di una recessione peggiore della crisi del 2007 - bisogna capire i danni ulteriori provocati dal cybercrime.

Per dare una dimensione metaforica a quanto sta accadendo nel mondo digitale, se al momento della redazione di questo testo, il COVID#19 fosse un virus informatico, il numero delle sue vittime (asintomatiche, sintomatiche, guaribili o meno) avrebbe al meno quattro zero in più del numero delle persone che hanno contrattato la malattia. Non solo, la diffusione di virus informatici non interesserebbe un solo sistema (come quello respiratorio umano nel caso del virus reale), ma metterebbe a rischio ogni singola parte interna ed esterna del nostro corpo.

Una mobilizzazione mondiale di tutti i settori in un vero partenariato pubblico-privato, meta direi ottimista fissata per il 2020 dalla Microsoft in un rapporto del 2012, si sta concretizzando proprio sotto i nostri occhi.



L'evoluzione auspicata da Matt Thomlinson in Cybersecurity Norms and the Public Private Partnership: Promoting Trust and Security in Cyberspace
© Microsoft, 05.10.2012

La nascita di questa mobilitazione non è meramente economica: anche se il virus fosse rimasto contenuto nella sola megalopoli di Wuhan, qualsiasi altro evento peggiore che si fosse verificato in Cina o negli Stati Uniti, avrebbe avuto un impatto globale economico, politico e… cyber. La mobilitazione degli esperti di sicurezza digitale è partita già nei primi giorni di febbraio a inizio epidemia.

Infatti, oltre all'espansione della pandemia, si va delineando il peggiore degli scenari, ovvero lo sfruttamento da parte dei gruppi cyber-criminali dell'attuale situazione di emergenza. Il cybercrime si sta adattando tempestivamente: attacchi a tutto campo, strategie multiple, con tutti i mezzi e in tutte le lingue, per tentare di colpire tutte le tipologie di utenti e tutti gli strumenti (hard, soft, cloud) possibili. [Per i dati tecnici, si veda il rapporto molto dettagliato della Insikt Group, *"Capitalizing on Coronavirus Panic Threat Actors Target Victims Worldwide"* (6)].

Tali azioni erano già state eseguite, ma con minor successo proprio perché non c'erano state reazioni governative così incoerenti a livello globale, durante il primo picco dell'epidemia di Ebola (2002-2003), come **ben** spiegano François Mouton e Arno de Coning nell'introduzione del loro recentissimo studio su quanto sta accadendo nel mondo virtuale (7).

La differenza con la gestione epidemica: vere PPP internazionali o addirittura globali

Nel fronteggiare una serie di attacchi **verso** attività private e professionali, la grande differenza tra la gestione della *pandemia virale umana* e quella della *pandemia virale cyber* è che in quest'ultima il fattore politico è assente. Sono le agenzie specializzate dei vari stati ad assumersi la responsabilità di limitare i danni ai cittadini, alle imprese e, *last but not least*, agli strumenti digitali del proprio stato. La coerenza, il rigore, l'altissima qualificazione e la costante interazione interdisciplinare di chi si occupa in tutto il mondo dell'urgenza digitale attuale è, in paragone, agli antipodi di quanto vediamo sul fronte fisico-umano.

Come sempre, spiccano paesi che sono all'avanguardia nella pubblicazione tempestiva non solo di nuove vulnerabilità di hard-e software, (incluse le patch rilasciate dalle rispettive aziende produttrici), ma sono anche **di** informazioni *in primis* generali e successivamente più tecniche dei vari ransomware, virus e zero-days. **Singapore,** a nostro parere, ha il CERT più dinamico al mondo in materia di concentrazione, smistamento e diffusione delle informazioni (8).

Bisogna sottolineare che il SingCert non solo fa parte del servizio cyber dell'Intelligence dello Stato, ma ha un numero record di collaborazioni con stati terzi e aziende private, sia di grandi e medie dimensioni.

Peraltro, l'efficacia del piccolo Stato asiatico stupisce il pianeta anche sul fronte sanitario. Forte dell'esperienza della gestione della SARS, ricordiamo che Singapore è, prima di Taïwan e Hong Kong, il paese che ha gestito al meglio la crisi, riuscendo a contenere il virus umano senza nessun confinamento della popolazione e lasciando scuole e attività commerciali aperte (9).

La pagina "news" del Singcert e un asilo a Singapore, 24 marzo © Axios

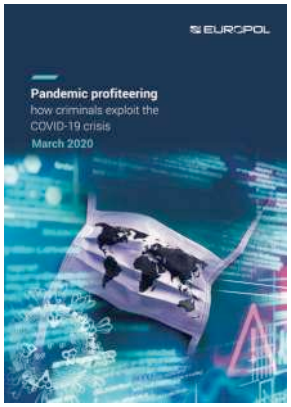
Dall'altra parte del globo, gli Stati Uniti d'America hanno moltiplicato gli sforzi e sono riusciti a fare un salto quantico che rari paesi europei hanno raggiunto: **creando un unico punto informativo** evitando innumerevoli ricerche e consultazioni di website pubblici e privati. L'ONG **Staysafeonline** propone da pochi giorni una "COVID-19 Security Resource Library" (10) utilissima e costantemente aggiornata, con tre rubriche: rapporti di stato, rapporti di aziende e articoli di specialisti. I comunicati brevi, invece, sono nelle apposite newsfeed dedicate ad ognuno dei quattro target principali: bambini, adulti, professionisti, aziende.

La spiegazione è semplice: Staysafeonline è un'emanazione della **National Cybersecurity Alliance**, potentissimo gruppo di lavoro che include il Department of Homeland Security e quasi tutte le più grandi **aziende, white** hats e università. La stessa è da considerarsi al momento come il più efficace ecosistema PPP al mondo eccezione fatta dei partenariati cyber dedicati a specifici settori (infrastrutture critiche, industrie o settori particolari come quelli bancari e sanitari).

La pagina COVID-19 Security Resource Library © Staysafeonline

Un solo esempio per illustrare il fronte costruito per contrastare gli attacchi

Per far fronte all'assedio totale di tutti gli oggetti connessi e dei loro utilizzatori, in tutto il mondo, è arrivata, mercoledì 25 marzo, la più impressionante delle risposte. Il fondatore del famoso congresso Def Con, ha creato la **COVID-19 Cyber Threat Intelligence**



vede già la partecipazione di 400 massimi esperti di sicurezza informatica da più di 40 paesi, su base volontaria.

La CTI League ha già firmato protocolli di mutua collaborazione con i vertici di numerosi stati, in primis il Canada, o direttamente con i loro enti di Cyber Intelligence. Lasciando da parte i malware e le vulnerabilità zero day sofisticate, che sono ora monitorate e isolati dal gruppo tempestivamente, Rogers ha motivato la fondazione di questo gruppo di élite costatando che *"I've never seen this volume of phishing. I am literally seeing phishing messages in every language known to man."* Grazie alla sua idea di reclutamento dei migliori, da white hats a senior cybersecurity officers di grandi multinazionali nonché specialisti di società di sicurezza, dopo solo qualche giorno si è assistito ad un'apertura delle agenzie di Stato come mai prima. Roger, soddisfatto della collaborazione raggiunta tra Enti ed aziende, conclude dicendo: *"I have never seen this level of cooperation, I hope it continues afterwards, because it's a beautiful thing to see."* (11). I risultati della League, che non vuole pubblicità, avranno senza dubbio effetti rapidi quanto efficaci, senza che l'utente se ne renda conto.

Il settore privato al lavoro 7 giorni su 7 giorni H24

Oltre agli sforzi collettivi menzionati, non è da meno il contributo delle aziende specializzate, che offrono ogni giorno nuovi rapporti dettagliatissimi, elaborati dai loro team, attivi in tutti i continenti. Non occorre qui farne una elenco, che non potrebbe essere esaustivo, il miglior modo di conoscerli, è quello di consultare il materiale informativo disponibile a tutti. Inoltre, per rimanere aggiornati si possono leggere gli articoli quotidiani e le riviste online specializzate, come gli eccellenti testi di Montalbano (12), Pilkey (13), Lakshmaman (14) o, in italiano, l'ottimo testo di Salvatore Lombardo (15) con tanto di utili consigli e link.

Un'Europa con enti sempre timidi e poco coordinati, nell'UE come nei singoli paesi membri

Nonostante l'emergenza totale di cyber-attacchi, l'Europa fornisce, certo, informazioni, ma pochissimi sono gli enti centrali che hanno creato una sezione speciale COVID sulla loro homepage. Il CERT-EU (www.cert-europa.eu), ad esempio, continua come se nulla fosse pur offrendo tutti i dettagli tecnici degli attacchi riscontrati ed esaminati, così come l'ENISA (www.enisa.europa.eu). L'agenzia più proattiva rimane quindi la cellula EC3 dell'EUROPOL, che non solo ha realizzato una vignetta educativa disponibile a tutti, ma ha anche redatto un rapporto ragguardevole *"Pandemic Profiteering: How Criminals Exploit The Covid-19 Crisis"* (16) con consigli ed esempi utilissimi. Inoltre, ha dedicato una sezione ad hoc sulla sua homepage (www.europol.europa.eu).

Se osserviamo poi i singoli paesi, c'è un contrasto colossale tra la Spagna e gli altri Stati. A Madrid, si è scelto di centralizzare tutte le informazioni sul sito dell'INCIBE (Instituto Nacionál de Ciberseguridad) (www.incibe.es), creando sulla homepage un banner enorme dedicato proprio agli attacchi COVID (17).

Alcune delle "pillole" spagnole © INCIBE

Oltre a rapporti periodici e ad una newsfeed tempestivamente aggiornata, i vari messaggi sono anche capillarmente diffusi da tutte le forze dell'ordine – da Polizia ad esercito a protezione civile ed enti fiscali - sui loro siti web, sotto forma di 30 "pillole" con una bella grafica.

L'Italia, come quasi tutti gli altri paesi del continente, offre al cittadino un vero e proprio labirinto di siti che, diminuiscono così la visibilità dei loro consigli e documenti, seppur utilissimi e redatti con grande cura. La **Polizia delle Comunicazioni** aggiorna quotidianamente sui fatti più gravi (www.commissariatodips.it). Importante, anche l'impegno dimostrato dal **Cert della Pubblica Amministrazione** (18), dall'**Agenzia per l'Italia Digitale** (19), dal **CertFIN** (20) e dall'**Associazione italiana ingegneri clinici** (21) dedicando pagine al COVID Cybercrime sui loro siti. Gli altri enti, ad immagine del CERT-EU, hanno preferito, sino ad oggi, trattare gli attacchi man mano che accadono, sia quelli legati al COVID# 19 e sia quelli legati alle specificità dello stile di vita e di lavoro ormai imposti a tutti gli Italiani. ■

COVID#19: un fronte cyber senza nessun limite. Attacchi mai visti finora, per diversità e quantità.

Ad uso dei nostri lettori, desideriamo proporre qui una un elenco dei principali mezzi usati dai cyber criminali per attaccare quasi ogni tipologia di persone e di enti, "urbi et orbi". Secondo l'azienda Bitdefender, gli attacchi globali del mese di marzo hanno visto una crescita del 500% rispetto a quelli del mese di febbraio… che erano già altissimi.

1. La disinformazione di massa in periodo di panico, con e-virus incluso

Molti paesi hanno **adottato** misure straordinarie per censurare le fake news. Imbattendosi quasi sempre sul problema che hanno tutti gli specialisti del campo: le reti sociali e l'estraterritorialità. Il non saper discernere tra un comunicato ufficiale ed una fake news, di molti cittadini, continua a riproporre *ad eternam* il tema dell'awareness.

Non mancano peraltro esempi di falsi documenti ufficiali, come è avvenuto in Italia. Infatti, è notizia di questi giorni la diffusione di false lettere ministeriali con l'immagine del Ministero dell'Istruzione mandata sui social e denunciata dallo stesso Ministro Lucia Azzolina (22).

▸ Imparate ad informarvi correttamente!

Con l'urgenza del COVID, la proattiva *News Litteracy Project* ha lanciato, per il pubblico anglofono, una delle migliori iniziative possibili: un'app di insegnamento diretto, quasi ironicamente intitolato *Are you informable?* ("Ma Lei è informabile?") (https://newslit.org/coronavirus/).

L'app per calmare il panico e tornare alle fonti attendibili
© News Litteracy Project

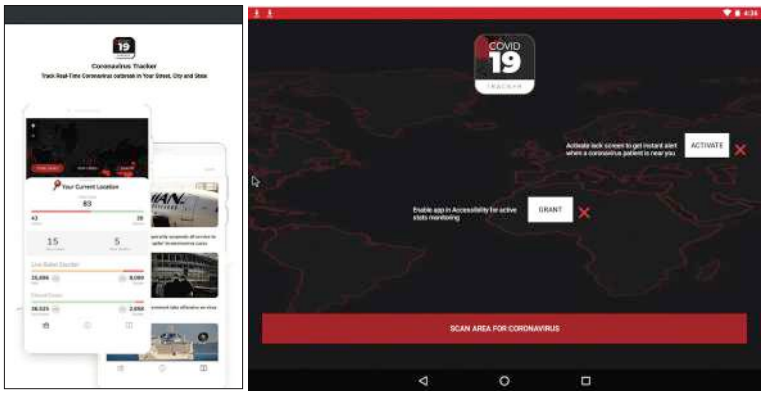
Un fenomeno in pieno boom è proprio l'uso delle stesse fake news per nascondere potenti malware, come è stato rivelato da un recente rapporto di Adam Pilkey per la azienda F-Secure (cf. biblio 13), magistralmente illustrato e qui riprodotto parzialmente. ***Nell'articolo sono indicati esempi di malware presenti*** in **ben 12 paesi, dall'Asia** all'Europa sino agli Stati Uniti. **Un'altra preoccupazione maggiore è quella del numero di domini che rimandano al nome ufficiale opopolare del virus, tutti potenzialmente in mano a criminali, come sottolinea** il rapporto di Lakshmanan *(biblio n. 14)*.

2. Cercasi info per mobile tools disperatamente: le app malevoli dedicate al Covid#19

Al numero di fake news inviate tramite mail, di tipo scam o la presenza di link malevoli sulle reti sociali, si aggiunge settimanalmente la diffusione di decine di false app destinate ad "informare" l'utente sulla situazione globale, nazionale e a fornire "indicazioni utili".

Quasi tutte destinate agli smartphone dotati di sistema Android, stanno dando filo da torcere **agli** specialisti di sicurezza. Benché rifiutate dai vari "store" nativi delle aziende produttrici di smartphone, vengono scaricate direttamente da internet dagli utenti. Se molte di queste app si limitano a copiare parti più o meno cospicue del contenuto dello smartphone della vittima, altre spiano gli utenti attivando microfono e camera video.

Al momento, la più malevola di queste App è senza dubbio **"Covid 19 Tracker"**, scoperta il 10 marzo, perché non solo è un potentissimo spyware ma è pure un ransomware. Qualche ora dopo la sua attivazione, blocca lo smartphone con un potente crypto-ransomware e richiede 100 dollari in bitcoin per sbloccarlo, come ben spiega Tarik Saleh (23).



"Covid 19 tracker": pubblicità, visuale e… ricatto
© Saleh, Domaintools

▸ SCARICATE le app indicate dagli Stati, ATTENZIONE all'utilizzo delle app delle GAFAM

A fronteggiare il numero gigantesco di app sul tema del virus, l'Organizzazione Mondiale della Sanità lancerà, al più tardi nei primi giorni di aprile, un' App ufficiale, gratuita e disponibile in tutte le lingue del mondo, chiamata "WHO MyHealth" (24).

L'interfaccia dell'app WHO MyHealth secondo il prototipo dato ai media ©New York Post

Nel frattempo, in Italia, vi sono due iniziative **in atto**. La prima è la progettazione di un'app, a scopo sanitario e di divulgazione scientifica. L'app ha la funzione di rassicurare, dare consigli, facilitare l'autodiagnosi dei primi sintomi del virus e a tracciare i contagi. È frutto del lavoro di un gruppo scientifico di eccellenza, ora si attende la validazione finale del Ministero della Sanità (25).

La seconda app, mira alla collaborazione dei cittadini, alla gestione della crisi e facilita il completamento delle modulistiche. E' stata sviluppata dall'Associazione Italian Digital Revolution con SOS Italia, nel quadro del progetto governativo «Innova per l'Italia» (26). L'app ha come primo scopo la semplificazione della gestione della pandemia, grazie a un sistema che integra: uno strumento di autodiagnosi, un resoconto delle ultime notizie e comunicazioni ufficiali, una mappa dei contagi e un sistema di gestione delle autocertificazioni basato sui QR Code che semplifica il lavoro di controllo da parte delle forze dell'ordine (27).

Il prototipo dell'interfaccia della app «Sos Italia» © La Stampa

Le app delle GAFAM, sempre la stessa gestione extraeuropea, sempre le stesse pratiche: i vostri dati diventano loro, *ad eternam*. È doveroso, in questo campo, invitare alla prudenza e alla riflessione ogni qualvolta si decid**a** di scaricare ed usare una delle app ufficiali delle GAFAM e delle aziende di loro proprietà

Questo vale anche per la maggior parte delle app a pagamento che sono nate sull'onda di questo nuovo mercato. Verificate quali parametri e informazioni del vostro smartphone vi vengono richiesti di autorizzare obbligatoriamente *"per un funzionamento ottimale"* prima di scaricarle!

Come per le reti sociali, dovremmo chiederci se saremmo disposti ad accettare con un click un contratto lunghissimo che spiega che tutti i vostri dati **potranno/saranno registrati (senza scadenza di tempo) "per migliorare i nostri prodotti"**, come si legge, per dare un esempio, nella privacy policy dell'app "COVID-19 Screening Tool" della Apple (https://www.apple.com/legal/privacy/en-ww/).

3. Cuore d'oro? Non lasciate che i criminali approfittino della vostra generosità!

Sulle pagine web e social di tutte le polizie d'Europa, non passa un giorno senza che sia postat**a** una segnalazione di false raccolte fondi, come quell**a** emess**a** dalla Polizia delle comunicazioni in Italia. (28).

Il più grave degli attacchi ha preso di mira l'Ente mondiale a carico della gestione globale della crisi, l'Organizzazione Mondiale della Sanità (WHO). Milioni di mail di phishing sono stati mandate, in quasi tutte le lingue del mondo, con la richiesta di donazioni. Le mail contengono il logo dell'OMS, parti delle descrizioni del "COVID-19 Solidarity Response Fund" (https://covid19responsefund.org), nonché falsi numeri di conti bancari. Inoltre, le mail spesso raccolgono dati personali, e talvolta contengono, ciliegia sulla torta, allegati con tanto di malware incluso. La reazione ufficiale dell'Ente dell'Onu spiega bene la gravità dell'accaduto (29):

World Health Organization

Beware of criminals pretending to be WHO

Criminals are disguising themselves as WHO to steal money or sensitive information. If you are contacted by a person or organization that appears to be from WHO, verify their authenticity before responding.

The World Health Organization will:

- never ask for your username or password to access safety information
- never email attachments you didn't ask for
- never ask you to visit a link outside of www.who.int
- never charge money to apply for a job, register for a conference, or reserve a hotel
- never conduct lotteries or offer prizes, grants, certificates or funding through email.

The only call for donations WHO has issued is the COVID-19 Solidarity Response Fund, which is linked to below. Any other appeal for funding or donations that appears to be from WHO is a scam.

- **Usate solo le indicazioni fornite dai siti ufficiali**

L'unico consiglio, in questo periodo più che mai, è di non dar mai retta a richieste di donazioni ricevute tramite email. Una volta scelto l'Ente o l'Onlus al quale si desidera fare una donazione, è d'obbligo verificare sul sito originale dell'organizzazione di vostra scelta quali si**a**no le modalità di pagamento, le coordinate esatte e i riferimenti bancari corretti.

4. Impauriti? Attenti ai medicinali, mascherine ed altri utensili sanitari in vendita online

Su tutti i siti con "ads" dominano ormai le pubblicità che invitano all'acquisto di "antivirali miracolosi" , mascherine di protezione, e una vasta gamma di mezzi destinati

a "prevenire **il** contagio". Una grande parte delle email scam - alcune contenenti potenti virus in allegato (30) – ha infatti fiutato nella paura umana e nel bisogno di cercare protezione, l'anello più debole di una razionalità che tendiamo tutti a perdere quando c'è in gioco la nostra vita o quella dei nostri cari.

È DOVEROSO RICORDARE CHE AL MOMENTO NON ESISTONO NÈ VACCINO NÈ CURA OMOLOGATI PER FRONTEGGIARE IL COVID#19.

Le cure - in ospedale e solo lì - che hanno permesso la guarigione di molti pazienti che non soffrivano di precedenti patologie gravi sono, infatti, diverse da paese a paese e spesso da ospedale a ospedale. È da sottolineare che alcuni prodotti farmaceutici osannati dalla stampa, come la **Clorochina** - sono solo componenti parziali dei "cocktail farmaceutici" creati dagli ospedali. Come tali, non devono mai essere usati in automedicazione - essendo illegale il loro acquisto, infatti il loro uso senza controllo medico ha già causato parecchi morti negli Stati Uniti.

L'acquisto online su siti che nascondono bene la loro reale localizzazione geografica è pericolosissimo. Un esempio sono i siti che offrono false polizze assicurative per la copertura da COVID-19 denunciate dalla Polizia delle Comunicazioni (31), il cui rischio è che non vi venga consegnato nessun premio assicurativo dopo il vostro pagamento, in questo caso direi il minor dei mali.

Invece, il peggior dei casi sarebbe è che vi arrivi a casa l'ordine che avete acquistato, con tanto di scatoline contenente medicinali contraffatti, che nella migliori delle ipotesi contengano miscugli di farina, e nella peggiore contengano sostanze dannose che potrebbero rappresentare un serio danno per la vostra salute, come è ben illustrato da una pagina del fumetto del *Gruppo di Prevenzione Svizzera contro la Criminalità (32).*

‣ Usate solo i siti web ufficiali di farmacie o di negozi online ben noti, del vostro paese

Per rispettare le leggi emesse dalle autorità del vostro paese, non acquistate medicinali in altri paesi, anche dell'Unione Europea. Infatti, gli obblighi di prescrizione per ogni singolo medicinale sono molto diversi da paese a paese, così come i dosaggi.

Lo stesso vale per l'acquisto di mascherine, disinfettanti ed altri prodotti a scopo sanitario. La miglior soluzione rimane quella di recarvi fisicamente nella propria farmacia di fiducia e ordinare tutto il necessario.

Attenzione massima ai messaggi di "cura antivirus" che rimandano al sito antivirus-covid. (vari registri): una volta aperta la pagina web, il vostro PC viene infettato da un potentissimo malware chiamato BlackNet (33). Se avete il proprio PC infettato, contattate immediatamente la Polizia delle Comunicazioni.

5. Confinati a casa? Attenti ai vostri bambini!

Un'attenzione particolare va **dedicata** ai minorenni. Con le scuole chiuse, i cybercriminali stanno moltiplicando la creazione di nuovi giochi contenente malware. Inoltre, è stata segnalata dalla Polizia delle Comunicazioni un'ondata di tentativi di adescamenti verso minori (34).

‣ Usate solo i giochi originali proposti dai vari app store delle aziende produttrici di Smartphone e dai negozi abilitati a vendere licenze di Online Games

L'insieme di misure da tenere in considerazione, in funzione dell'età dei minorenni, è stata magistralmente redatta dalla PPP Inglese GetsafeOnline, con tanto di tutorial sotto forma di cortometraggi e clip facili da capire e creati su misura per la situazione attuale *"Keeping children safe online during the Coronavirus outbreak"* (35).

6. Confinati a casa? Attenti ai vostri momenti di divertimento e di acquisti!

Assistiamo ad un assalto generalizzato alle piattaforme di video streaming – un potente zero-day ha anche interrotto *Google Play Store*, risolto in un'ora – e si moltiplicano add e scam che rimandano a i siti criminali con l'offerta gratis di pacchetti di film e giochi per interi mesi, con tanto di richiesta di carta di credito per iscriversi.

Da segnalare l'aumento in modo esponenziale di mail di phishing con false offerte commerciali di tutti i tipi, le stesse comunque facilmente riconoscibili perché generalmente contengono molti errori grammaticali– nelle lingue "minori" – o per l'utilizzo di frasi generiche. La sfiducia dell'utente è però, talvolta, messa alla prova. Come è accaduto in Romania, caso nazionale denunciato dal CERT-RO (vedi figura in basso). L'email è stata ben studiata conteneva, infatti il logo di una grande catena tedesca di supermercati e l'indirizzo della multinazionale (Kaufland.com) al quale però sono stato aggiunti "-bon" (voucher) e soprattutto il registro finale del sito (.club).

‣ Non comperate nulla di ciò che vi viene proposto via e-mail cliccando sul link integrato

Anche se conoscete perfettamente i siti dei negozi dei quali siete clienti e dove avete registrato un account, come misura di cautela, non cliccate sulle offerte, anche quelle legittime, degli stessi negozi che vi vengono inviate, ma visitate sempre il sito ufficiale per sapere se ci sono offerte a voi dedicate

7. Confinati a casa? Diffidate di qualsiasi offerta bancaria / finanziaria!

In Italia come in quasi tutti i paesi europei è massiccia la porzione di e-mail phishing legata al mondo finanziario. Le mail contengono offerte incredibili come crediti alti a tasso zero, moratoria sulle rate di ipoteche, restituzione di percentuali di denaro se usate tale "nuovo strumento" etc.,

come è stato ottimamente riassunto dalla Polizia delle Comunicazioni (37).

Il grafico dell'Articolo di Haig © Cointelegraph

Ancora, **occhio ai vostri conti bancari**. Verificate spesso tramite e-banking la situazione del vostro conto. Per chi possiede Bitcoin, eseguite solo le transazioni indispensabili: è in azione un potentissimo ransomware proprio mirato ai movimenti di Bitcoin (38).

8. Al lavoro a casa? Attenti a tutti gli oggetti connessi!

Molte aziende non erano pronte per fare lavorare tutti i loro impiegati da casa. I protocolli di videoconferenza, di accesso dati, di interazione tra lo smartphone e il laptop privato dell'impiegato e l'infrastruttura IT centrale dell'azienda (ed il cloud), sono sotto assedio. Basti pensare che degli hackers sono riusciti a trovare una falla nella solidissima VPN degli iPhone, ora risolta da Apple.

Peraltro, nella "vecchia Europa", le reti fisse – escluse le zone servite dalla fibra ottica – sono quasi al collasso in molte regioni, mentre la velocità realmente disponibile di quelle mobili variano da posizione a posizione anche in uno stesso quartiere.

Ovviamente, questo rappresenta il paradiso che da molto aspettavano i cybercriminali, non solo per saturare ancora di più le reti, ma per immettervi malware e zero days di ogni tipo e scams. Possono utilizzare, addirittura, chiamate telefoniche false presentando ordini dell'azienda di appartenenza o di altre ditte/clienti/fornitori.

‣ Assicuratevi che avete il meglio del meglio in materia di protezione

a) Istallate ed aggiornate tutti gli antivirus/protezioni ed aggiornate regolarmente i sistemi operativi di tutti i vostri device.

b) Coprite la camera video / le camere video ed i microfoni di laptop e cellulari una volta finita la teleconferenza professionale (molti sistemi e protocolli di teleconferenza sono stati hackerati: le aziende hanno risposto con patch - spesso non installate dalle PMI - che a loro volta sono stati di nuovo hackerati).

c) Consigli per smartphone, tablet e pc: al momento i migliori consigli per rendere sicuro il vostro "ufficio a domicilio" si possono trovare, nella lingua italiana, nel sito del CertFin (cf. 20). Per smartphone e tablet, sulla pagina dei Servizi di Intelligence tedeschi (39). Consiglio per la traduzione: scaricare il materiale ed immettere i testi su www.deepl.com, il miglior traduttore online al momento per le lingue più importanti.

Per un'igiene digitale completa, specialmente per i liberi professionisti, ma anche per i semplici impiegati, si rivelano utilissime le linee guida (pdf) del Canadian Centre for Cyber Security (40) e quelle della IVCAEW (Institute of Chartered Accountants in England and Wales) (41)

Alle aziende si consiglia, per testare l'efficacia del sistema VPN, di consultare l'eccellente rapporto dettagliato sia delle minacce che delle soluzioni della Homeland Security (42), nonché tutti i consigli di Staysafeonline, categoria «Business» (n.10).

9. Dottore, specialista in medicina, manager di ospedale? Siete il bersaglio più ambito!

Non occorre qui entrare nei dettagli degli innumerevoli attacchi che hanno preso di mira le strutture sanitarie e i medici, ed in particolare le apparecchiature sanitarie. Come già abbiamo spiegato numerose volte, i dati sanitari dei pazienti valgono cento volte di più sul mercato nero di quelli di una carta di credito.

Attenzione, non vi sono solo attacchi super sofisticati, medici, infermieri, impiegati e chiunque lavori nell'ecosistema di un ospedale, può essere vittima di scam, phishing ed altri tentativi di adescamento, in quantità esponenzialmente maggiore rispetto a quella dei professionisti di altri settori (43).

‣ Informatevi dai migliori

Considerando che in Canada e negli Stati Uniti d'America il sistema medico è per la maggior parte privato, le linee guida, gli alert e i consigli si possono reperire sia sui siti governativi che privati di questi due paesi.

Raccomandiamo quindi a tutti gli addetti ai lavori del campo digitale nel settore sanitario di visitare quotidianamente i seguenti siti (esempi scelti): https://cyber.gc.ca/en/alerts/cyber-threats-canadian-health-organizations; https://www.cisa.gov/identifying-critical-infrastructure-during-covid-19?utm_source=hp_slideshow&utm_medium=web&utm_campaign=dhsgov; www.healthcareitnews.com ; https://healthitsecurity.com/.

Dove andremo ?

Per concludere con una nota ottimista, speriamo che cittadini e governi sappiano trarre le dovute lezioni di quanto sta accadendo. Come scrisse Yuval Noah Harari (n.5), *"L'umanità ha bisogno di fare una scelta. Percorreremo la via della disunione o adotteremo la strada della solidarietà globale? Se scegliamo la disunione, ciò non solo prolungherà la crisi, ma probabilmente porterà a catastrofi ancora peggiori in futuro. Se scegliamo la solidarietà globale, sarà una vittoria non solo contro il coronavirus, ma contro tutte le future epidemie e crisi che potrebbero assalire l'umanità nel ventunesimo secolo."* Tocca ormai ad ognuno di noi fare le scelte giuste e dare l'esempio. ■

NOTE:

(1) Giorgio Agamben, Riflessioni sulla peste, in Quodlibet, 27.03.2020 (https://www.quodlibet.it/giorgio-agamben-riflessioni-sulla-peste)
(2) Yuval Noah Harari, In the Battle Against Coronavirus, Humanity Lacks Leadership, in Time, 15.03.2020 (https://time.com/5803225/yuval-noah-harari-coronavirus-humanity-leadership/ ; ndr: proponiamo qui un estratto in lingua italiana dall'intervista alla CNN durante la quale Harari ha ripreso gran parte degli argomenti del suo articolo https://it.gariwo.net/educazione/yuval-noah-harari-sull-emergenza-covid19-21870.html)
(3) Traduzione (autore) di due paragrafi finale di Michel Onfray, Berezina, in Les Observateurs, 17.03.2020 (https://lesobservateurs.ch/2020/03/17/michel-onfray-berezina/)
(4) Traduzione (autore) di un paragrafo di Slavoj Žižek, TRIBUNE. Surveiller et punir ? Oh oui, s'il vous plaît ! in Le Nouvel Observateur, 18.03.2020 (https://www.nouvelobs.com/coronavirus-de-wuhan/20200318.OBS26237/tribune-surveiller-et-punir-oh-oui-s-il-vous-plait.html)
(5) Yuval Noah Harari, Il mondo, dopo il Coronavirus, in Ottimisti e Razionali, 22.03.2020 (http://www.ottimistierazionali.it/il-mondo-dopo-il-coronavirus/)
(6) Insikt Group, Capitalizing on Coronavirus Panic Threat Actors Target Victims Worldwide, 13.03.2020 https://go.recordedfuture.com/hubfs/reports/cta-2020-0312-2.pdf
(7) François Mouton, Arno de Coning, COVID-19: Impact on the Cyber Security Threat Landscape (pre-print paper, March 2020) www.researchgate.net/publication/340066124_COVID-19_Impact_on_the_Cyber_Security_Threat_Landscape
(8) https://www.csa.gov.sg/singcert
(9) Benjamin J. Cowling and Wey Wen Lim, They've Contained the Coronavirus. Here's How. Singapore, Taiwan and Hong Kong have brought outbreaks under control — and without resorting to China's draconian measures, in The New York Times, 13.03.2020 https://www.nytimes.com/2020/03/13/opinion/coronavirus-best-response.html
(10) Stay Safe Online : COVID-19 Security Resource Library https://staysafeonline.org/covid-19-security-resource-library/
(11) Joseph Menn, Cybersecurity experts come together to fight coronavirus-related hacking, in Reuters, Technology News, 26.03.2020 https://www.reuters.com/article/us-coronavirus-cyber/cybersecurity-experts-come-together-to-fight-coronavirus-related-hacking-idUSKBN21D049
(12) Elizabeth Montalbano, Spread of Coronavirus-Themed Cyberattacks Persists with New Attacks, in Threatpost, 06.03.2020 https://threatpost.com/coronavirus-themed-cyberattacks-persists/153493/
(13) Adam Pilkey, Coronavirus email attacks evolving as outbreak spreads, F-Secure, 13.03.2020 https://blog.f-secure.com/coronavirus-email-attacks-evolving-as-outbreak-spreads/
(14) Ravie Lakshmanan: Hackers Created Thousands of Coronavirus (COVID-19) Related Sites As Bait, in The Hacker News 18.03.2020 https://thehackernews.com/2020/03/covid-19-coronavirus-hacker-malware.html
(15) Salvatore Lombardo: L'allarme: Coronavirus, in aumento attacchi cyber, phishing e malspam: consigli per difendersi, in Cybersecurity360, 26.03.2020 https://www.cybersecurity360.it/nuove-minacce/coronavirus-in-aumento-campagne-di-phishing-e-malspam-a-tema-covid-19-consigli-per-difendersi/
(16) Europol REPORT: PANDEMIC PROFITEERING: HOW CRIMINALS EXPLOIT THE COVID-19 CRISIS (pdf) https://www.europol.europa.eu/publications-documents/pandemic-profiteering-how-criminals-exploit-covid-19-crisis
(17) Subdomenio COVID dell'INCIBE (Instituto nacional de Ciberseguridad) https://www.incibe.es/cibercovid19
(18) Cert Pubblica Amministrazione, pagina COVID: https://www.cert-pa.it/notizie/coronavirus-attenzione-agli-sciacalli/
(19) Agenzia per l'Italia Digitale, pagina COVID: https://www.agid.gov.it/it/agenzia/stampa-e-comunicazione/notizie/2020/03/27/coronavirus-difendersi-malware-truffe-online
(20) CertFin, pagina COVID: https://www.certfin.it/newsroom/rendi-la-tua-casa-una-cyber-fortezza/
(21) Associazione italiana ingegneri clinici, pagina COVID: http://www.aiic.it/covid19/
(22) Polizia delle Comunicazioni: Coronavirus: Il Ministro Lucia Azzolina denuncia falso documento del Ministero Dell'Istruzione, 21.03.2020 https://www.commissariatodips.it/notizie/articolo/coronavirus-il-ministro-lucia-azzolina-denuncia-falso-documento-del-ministero-dellistruzione/index.html
(23) Tarik Saleh, CovidLock: Mobile Coronavirus Tracking App Coughs Up Ransomware, in Domaintools, 13.03.2020 – con ulteriore link contenente la descrizione tecnica completa del malware https://www.domaintools.com/resources/blog/covidlock-mobile-coronavirus-tracking-app-coughs-up-ransomware#
(24) Kyle Bradshaw, World Health Organization to launch COVID-19 tips app for Android, iOS, in 9to5Google, 26.03.2020 https://ww.9to5google.com/2020/03/26/world-health-organization-covid-19-app/#
(25) Elena Tebano, Coronavirus, pronta la app italiana per tracciare i contagi: «Così possiamo fermare l'epidemia», in Corriere della Sera, 20.03.2019 https://www.corriere.it/tecnologia/20_marzo_18/coronavirus-pronta-app-italiana-tracciare-contagi-cosi-possiamo-fermare-l-epidemia-c6c31218-6919-11ea-913c-55c2df06d574.shtml?refresh_ce-cp
(26) https://innovaperlitalia.agid.gov.it/home/
(27) Andrea Nepori, SOS Italia, ecco come potrebbe essere l'app per il monitoraggio dell'epidemia, in La Stampa, 26.03.2020 https://www.lastampa.it/tecnologia/news/2020/03/25/news/sos-italia-ecco-come-potrebbe-essere-l-app-per-il-monitoraggio-dell-epidemia-1.38636482
(28) Polizia delle Comunicazioni : Coronavirus: attenzione alle false campagne di raccolta fondi ! https://www.commissariatodips.it/notizie/articolo/coronavirus-attenzione-alle-false-campagne-di-raccolta-fondi/index.html
(29) https://www.who.int/about/communications/cyber-security
(30) Polizia delle Comunicazioni : Coronavirus: BlackNET: RAT distribuito tramite falso "Corona Antivirus" https://www.commissariatodips.it/notizie/articolo/coronavirus-blacknet-rat-distribuito-tramite-falso-corona-antivirus/index.html
(31) Polizia delle Comunicazioni : Coronavirus : false proposte assicurative per la copertura da COVID-19 https://www.commissariatodips.it/notizie/articolo/coronavirus-false-proposte-assicurative-per-la-copertura-da-covid-19/index.html
(32) Storie di Internet. Ufficio federale delle comunicazioni UFCOM Ufficio federale del consumo UFDC Incaricato federale della protezione dei dati e della trasparenza IFPDT Servizio di coordinazione per la lotta contro la criminalità su Internet SCOCI Centrale d'annuncio e d'analisi per la sicurezza dell'informazione MELANI Consultabile e scaricabile onlile su : https://www.websters.swiss/it/
(33) Polizia delle Comunicazioni : BlackNET: RAT distribuito tramite falso "Corona Antivirus" https://www.commissariatodips.it/notizie/articolo/coronavirus-blacknet-rat-distribuito-tramite-falso-corona-antivirus/index.html
(34) Polizia delle Comunicazioni : Coronavirus : rischio adescamento minori online https://www.commissariatodips.it/notizie/articolo/coronavirus-rischio-adescamento-minori-online/index.html
(35) Keeping children safe online during the Coronavirus outbreak https://www.getsafeonline.org/news/keeping-children-safe-online-during-the-coronavirus-outbreak/
(36) Continuă valul de campanii de tip scam. Atacatorii se folosesc acum de imaginea Mega Image https://cert.ro/citeste/alerta-scam-kaufland-ikea
(37) Polizia delle Comunicazioni : Coronavirus : smishing con falsi messaggi di istituti di credito https://www.commissariatodips.it/notizie/articolo/coronavirus-smishing-con-falsi-messaggi-di-istituti-di-credito/index.html
(38) Samuel Haig, 'CovidLock' Exploits Coronavirus Fears With Bitcoin Ransomware, in Cointelegraph, 14.03.2020 https://cointelegraph.com/news/covidlock-exploits-coronavirus-fears-with-bitcoin-ransomware
(39) BSI-BUND, Smartphone und Tablet effektiv schützen https://www.bsi-fuer-buerger.de/BSIFB/DE/Empfehlungen/BasisschutzGeraet/EinrichtungMobileGeraete/EinrichtungMobileGeraete_node.html
(40)Canadian Centre for Cyber Security, Cyber Hygiene for COVID-19 https://cyber.gc.ca/sites/default/files/publications/Publication-COVID-19-e.pdf
(41) IVCAEW (Institute of Chartered Accountants in England and Wales), Coronavirus guide: cyber hygiene and data https://www.icaew.com/-/media/corporate/files/technical/information-technology/tech-faculty/coronavirus-guide-cyber-hygiene-and-data.ashx
(42) CISA (U.S. Department of Homeland Security) : Alert (AA20-073A) Enterprise VPN Security https://www.us-cert.gov/ncas/alerts/aa20-073a
(43) Gareth Corfield, Health workers are top of phishers' target lists thanks to data value, in The Register, 16.03.2020 https://www.theregister.co.uk/2020/03/16/proofpoint_interview/

Cybersecurity e mondo finanziario

Autore: Giancarlo Butti

Il mondo finanziario è uno dei più esposti al rischio cyber e le varie normative e linee guida che sono state nel tempo pubblicate in tale ambito per contrastarlo possono costituire un valido punto di riferimento anche per altri settori.

A differenza degli standard internazionali o dei framework di sicurezza che richiedono un adattamento alla specifica realtà, le linee guida o le normative emesse per uno specifico settore possono costituire un valido punto di riferimento in quanto ne costituiscono già un'applicazione reale.

Spesso tali documenti fanno esplicito riferimento agli standard e ai framework dai quali sono stati ispirati e ne rappresentano una esemplificazione pratica della loro messa a terra che può essere da guida ad analoghi adattamenti.

Già nell'ottobre del 2016 la Commissione europea, riconoscendo che le minacce informatiche sono tra i principali rischi per la stabilità finanziaria, accoglieva il lavoro svolto dal gruppo di esperti informatici del G7 per affrontare l'aumento di complessità, frequenza e persistenza delle minacce informatiche nel settore finanziario, ritenendo un tale approccio essenziale per promuovere la coerenza agli approcci alla sicurezza informatica tra i partner G7.

Il documento **G7 FUNDAMENTAL ELEMENTS OF CYBERSECURITY FOR THE FINANCIAL SECTOR**, prendeva in considerazione 8 punti di alto livello e non vincolanti con i quali enti pubblici e privati possono contrastare il rischio cyber:

Element 1: Cybersecurity Strategy and Framework.

Establish and maintain a cybersecurity strategy and framework tailored to specific cyber risks and appropriately informed by international, national, and industry standards and guidelines.

Element 2: Governance.

Define and facilitate performance of roles and responsibilities for personnel implementing, managing, and overseeing the effectiveness of the cybersecurity strategy and framework to ensure accountability; and provide adequate resources, appropriate authority, and access to the governing authority (e.g., board of directors or senior officials at public authorities).

Element 3: Risk and Control Assessment.

Identify functions, activities, products, and services—including interconnections, dependencies, and third parties—prioritize their relative importance, and assess their respective cyber risks. Identify and implement controls—including systems, policies, procedures, and training—to protect against and manage those risks within the tolerance set by the governing authority.

Element 4: Monitoring.

Establish systematic monitoring processes to rapidly detect cyber incidents and periodically evaluate the effectiveness of identified controls, including through network monitoring, testing, audits, and exercises.

Timely (a) assess the nature, scope, and impact of a cyber incident; (b) contain the incident and mitigate its impact; (c) notify internal and external stakeholders (such as law enforcement, regulators, and other public authorities, as well as shareholders, third-party service providers, and

customers as appropriate); and (d) coordinate joint response activities as needed.

Element 5: Response.

Timely (a) assess the nature, scope, and impact of a cyber incident; (b) contain the incident and mitigate its impact; (c) notify internal and external stakeholders (such as law enforcement, regulators, and other public authorities, as well as shareholders, third-party service providers, and customers as appropriate); and (d) coordinate joint response activities as needed.

Element 6: Recovery.

Resume operations responsibly, while allowing for continued remediation, including by (a) eliminating harmful remnants of the incident; (b) restoring systems and data to normal and confirming normal state; (c) identifying and mitigating all vulnerabilities that were exploited; (d) remediating vulnerabilities to prevent similar incidents; and (e) communicating appropriately internally and externally.

Element 7: Information Sharing.

Engage in the timely sharing of reliable, actionable cybersecurity information with internal and external stakeholders (including entities and public authorities within and outside the financial sector) on threats, vulnerabilities, incidents, and responses to enhance defenses, limit damage, increase situational awareness, and broaden learning.

Element 8: Continuous Learning.

Review the cybersecurity strategy and framework regularly and when events warrant—including its governance, risk and control assessment, monitoring, response, recovery, and information sharing components—to address changes in cyber risks, allocate resources, identify and remediate gaps, and incorporate lessons learned.

Sullo stesso tema un rilevante numero di documenti è stato pubblicato da varie istituzioni.

Nel seguito un elenco non esaustivo:

World Economic Forum

- Advancing Cyber Resilience Principles and Tools for Boards

EBA (European Banking Autority):

- Orientamenti sulla valutazione dei rischi relativi alle tecnologie dell'informazione e della comunicazione (Information and Communication Technology - ICT) a norma del processo di revisione e valutazione prudenziale (SREP), nel settembre 2017
- Guidelines on the security measures for operational and security risks of payment services under Directive (EU) 2015/2366 (PSD2), nel dicembre 2017
- Guidelines on ICT and security risk management, nel novembre 2019

European Central Bank

- Cyber resilience oversight expectations for financial market infrastructures, nel dicembre 2018
- TIBER-EU Framework Bank for International Settlements, del quale abbiamo parlato in un precedente articolo

Bank for International Settlements

- Guidance on cyber resilience for financial market infrastructures, giugno 2016
- FSI Insights on policy implementation No 2 Regulatory approaches to enhance banks' cyber-security frameworks, nell'agosto del 2017

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.

- Cyber-resilience: Range of practices, nel dicembre 2018

Banca d'Italia

- Circolare 285

È impossibile in questa sede analizzare tutti i documenti che sono comunque facilmente reperibili on line sui siti dei vari enti, ma raccomando in particolare i seguenti documenti dal taglio molto pratico:

- **Advancing Cyber Resilience Principles and Tools for Boards**, nel quale sono presenti i 10 Board Principles for Cyber Resilience:

Principle 1: Responsibility for cyber resilience.

The board as a whole takes ultimate responsibility

for oversight of cyber risk and resilience. The board may delegate primary oversight activity to an existing committee (e.g. risk committee) or new committee (e.g. cyber resilience committee).

Principle 2: Command of the subject.

Board members receive cyber resilience orientation upon joining the board and are regularly updated on recent threats and trends – with advice and assistance from independent external experts being available as requested.

Principle 3: Accountable officer.

The board ensures that one corporate officer is accountable for reporting on the organization's capability to manage cyber resilience and progress in implementing cyber resilience goals. The board ensures that this officer has regular board access, sufficient authority, command of the subject matter, experience and resources to fulfil these duties.

Principle 4: Integration of cyber resilience.

The board ensures that management integrates cyber resilience and cyber risk assessment into overall business strategy and into enterprisewide risk management, as well as budgeting and resource allocation.

Principle 5: Risk appetite.

The board annually defines and quantifies business risk tolerance relative to cyber resilience and ensures that this is consistent with corporate strategy and risk appetite. The board is advised on both current and future risk exposure as well as regulatory requirements and industry/societal benchmarks for risk appetite.

Principle 6: Risk assessment and reporting.

The board holds management accountable for reporting a quantified and understandable assessment of cyber risks, threats and events as a standing agenda item during board meetings. It validates these assessments with its own strategic risk assessment using the Board Cyber Risk Framework.

Principle 7: Resilience plans.

The board ensures that management supports the officer accountable for cyber resilience by the creation, implementation, testing and ongoing improvement of cyber resilience plans, which are appropriately harmonized across the business. It requires the officer in charge to monitor performance and to regularly report to the board.

Principle 8: Community.

The board encourages management to collaborate with other stakeholders, as relevant and appropriate, in order to ensure systemic cyber resilience.

Principle 9: Review.

The board ensures that a formal, independent cyber resilience review of the organization is carried out annually.

Principle 10: Effectiveness.

The board periodically reviews its own performance in the implementation of these principles or seeks independent advice for continuous improvement.

- le **Guidelines on ICT and security risk management**, nel quale si entra nel dettaglio delle misure di sicurezza organizzate secondo questo schema:
  - Governance and strategy
  - ICT and security risk management framework
  - Information security
  - ICT operations management
  - ICT project and change management
  - Business continuity management
- la **Cyber-resilience: Range of practices**, nella quale vengono affrontati i seguenti temi
  - Cyber-resilience standards and guidelines
  - Cyber-governance
  - Approaches to risk management, testing and incident response and recovery
  - Communication and sharing of information

E propone inoltre metriche per misurare la cyber resilienza:

Annex C: Cyber-resilience metrics		
	Event	Practices
Before compromise	• External scanning blockedconnections (count) • New vulnerabilities (by OWASP type: count) • Malware stopped (count) • Phishing sites known (count) • Phishing site takedown (count, hours open) • Uniquemalware targeting bank (count) • Vulnerabilities per line of code (count) • Applications going into production with codevulnerabilities (count) • Securityevents detected (count)	• Penetration testing (by type: count and finding rating) • Systems protected by IAM (count) • Internally developed systems whichcannotbeupdated (by type: count) • Systems with out-of-vendor support components (by type: count) • Systems without anti-malware solutions (count) • Non-authorised (compliant) devices (by type:count) • Information security configuration compliance (coverage %) • Awarenessexercises (coverage %, count) • Staff responding to phishing tests (% of total staff) • User access review (coverage %) • Security assessments of providers over12 months (%coverage of relevant thirdparties) • Patch ageing (by criticality:days) • Assurance reporton information security (findings by rating, ageingto remediation)

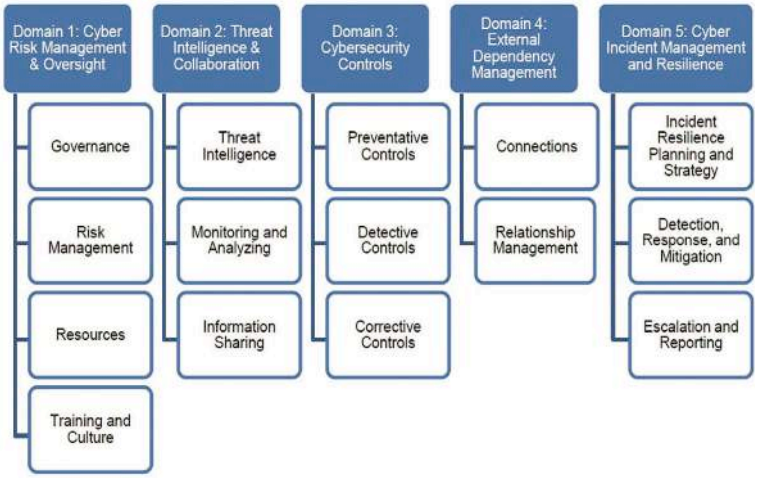
Annex C: Cyber-resilience metrics		
	Event	Practices
Compromise	• Detectedmalicious software endpoints (count) • Detectedmalicious software on servers (count) • Online directoriescontaining staff/customer info (count) • Incident type overperiod (count per: denial of service,maliciouscode,misuse, reconnaissance, socialengineering, unauthorisedaccess, other)	• Resolutionand recovery plans developed (bytype: count) • Incident rehearsals (by type: count)
After compromise	• Detected APT(count) • Blockedconnections to malicious websites (count) • Data breaches detected (count) • Bank losses (value) • Customer loss (value)	• Post-incident reports (count)

▸ e la **Guidance on cyber resilience for financial market infrastructures**, nella quale sono analiticamente trattati i seguenti argomenti:

- Governance
- Identification
- Protection
- Detection
- Response and recovery
- Testing
- Situational awareness
- Learning and evolving

Di tutt'altro genere è la documentazione prodotta dalla **Federal Financial Institutions Examination Council's (FFIEC)**, che rende disponibili dei veri e propri manuali e delle check list ed in particolare il **Cybersecurity Assessment Tool.**

Quest'ultimo propone un sofisticato framework per aiutare le istituzioni a identificare i loro rischi a determinare la loro preparazione nell'ambito della sicurezza informatica. La valutazione fornisce un processo ripetibile per misurare la loro preparazione alla cybersecurity.



Viene inoltre fornita una tavola di corrispondenza fra il framework proposto dalla **FFIEC e il NIST** Cybersecurity Framework.

La metodologia proposta è decisamente insolita e si basa sulla combinazione di profili di rischio negli ambiti:

- ▸ Tecnologie e tipi di connessione
- ▸ Canali
- ▸ Prodotti online / mobile e servizi tecnologici
- ▸ Caratteristiche organizzative
- ▸ Minacce esterne

Category: Technologies and Connection Types	Risk Levels				
	Least	Minimal	Moderate	Significant	Most
Total number of internet service provider (ISP) connections (including branch connections)	No connections	Minimal complexity (1–20 connections)	Moderate complexity (21–100 connections)	Significant complexity (101–200 connections)	Substantial complexity (>200 connections)
Unsecured external connections, number of connections not users (e.g., file transfer protocol (FTP), Telnet, rlogin)	None	Few instances of unsecured connections (1–5)	Several instances of unsecured connections (6–10)	Significant instances of unsecured connections (11–25)	Substantial instances of unsecured connections (>25)
Wireless network access	No wireless access	Separate access points for guest wireless and corporate wireless	Guest and corporate wireless network access are logically separated; limited number of users and access points (1–250 users; 1–25 access points)	Wireless corporate network access; significant number of users and access points (251–1,000 users; 26–100 access points)	Wireless corporate network access; all employees have access; substantial number of access points (>1,000 users; >100 access points)

e i livelli di maturità dei seguenti domini:

- ▸ Gestione e supervisione del rischio informatico
- ▸ Intelligence e collaborazione sulle minacce
- ▸ Controlli di sicurezza informatica
- ▸ Gestione delle relazioni con terze parti
- ▸ Gestione e resilienza degli incidenti informatici

Assessment Factor: Risk Management		
RISK MANAGEMENT PROGRAM	Baseline	An information security and business continuity risk management function(s) exists within the institution. *(FFIEC Information Security Booklet, page 68)*
	Evolving	The risk management program incorporates cyber risk identification, measurement, mitigation, monitoring, and reporting. Management reviews and uses the results of audits to improve existing cybersecurity policies, procedures, and controls. Management monitors moderate and high residual risk issues from the cybersecurity risk assessment until items are addressed.
	Intermediate	The cybersecurity function has a clear reporting line that does not present a conflict of interest. The risk management program specifically addresses cyber risks beyond the boundaries of the technological impacts (e.g., financial, strategic, regulatory, compliance).

Conclusioni

Il mondo finanziario e le sue istituzioni rendono disponibili documenti di vario livello e profondità utili a tutte le organizzazioni per la prevenzione e la gestione del rischio cyber. ■

Report di Analisi delle Minacce Globali - 2020

Autore: Stefano Lamonato, Sales Engineering Manager, Southern Europe, CrowdStrike

Informazioni su Crowdstrike

CrowdStrike® Inc. (Nasdaq: CRWD), leader della sicurezza informatica a livello globale, sta ridefinendo la sicurezza nell'era del cloud grazie alla sua piattaforma di protezione degli endpoint creata appositamente per bloccare le compromissioni. L'architettura basata su un unico agent a basso impatto della piattaforma CrowdStrike Falcon®, applica l'intelligenza artificiale a livello del cloud per offrire protezione e visibilità istantanee sull'intera azienda e per prevenire gli attacchi sugli endpoint all'interno e all'esterno della rete. Sfruttando la tecnologia proprietaria di CrowdStrike Threat Graph®, ogni settimana CrowdStrike Falcon crea correlazioni in tempo reale tra piú di 3 migliaia di miliardi di eventi legati agli endpoint provenienti da tutto il mondo, alimentando una delle piattaforme di sicurezza più avanzate mai esistite.

Anche l'anno appena trascorso è stato impegnativo per la sicurezza **informatica sia per le attività dell'eCrime sia per quelle degli avversari** di tipo "Nation-State", che hanno preso di mira le organizzazioni praticamente di tutti i settori. CrowdStrike ha rilevato incidenti mirati ad entità del settore accademico, governativo, sanitario, alberghiero, tecnologico, energetico, manifatturiero e finanziario di tutto il mondo in organizzazioni di diverse dimensioni, dalle piccole imprese ai grossi gruppi "Global 1000".

Nel Global Threat Report 2020 il team CrowdStrike® Intelligence, il team di Threat Hunting Falcon OverWatch e il team dei servizi di Incident Response di CrowdStrike presentano gli eventi e i trend più significativi in materia di sicurezza informatica emersi nello scorso anno.

La fetta principale dei profitti derivanti dagli attacchi ransomware sembra destinata a finire nelle mani di chi padroneggia metodi diversi per monetizzare le proprie risorse e competenze.

Criminalità informatica

- **È stata osservata un'escalation della cosiddetta "caccia grossa"**, vale a dire attacchi ransomware a sfondo criminale diretti a imprese di grandi dimensioni. La caccia grossa si è rivelata l'attività più lucrativa per i criminali informatici perché le richieste di riscatto hanno raggiunto alcuni milioni di dollari causando ripercussioni finora inimmaginabili. Per il momento, niente fa supporre che questi aggressori intendano allentare la presa.
- **I criminali informatici utilizzano i dati sensibili come arma di ricatto per fare pressione sulle vittime del ransomware.** Sono stati riscontrati casi in cui gli aggressori hanno minacciato di divulgare dati sensibili - e altri

BIO

Stefano entra in CrowdStrike nel Febbraio 2017 con l'obiettivo di stabilirne la presenza tecnica nelle nazioni del Sud Europa e, grazie al successo dell'azienda e alla sua espansione, oggi guida il gruppo di prevendita per questa regione.
Il suo viaggio nella Cyber Security Stefano lo inizia nei primi anni '90 con lo studio di diversi linguaggi di programmazione, di architetture di rete complesse e di diversi sistemi operativi per poi spostarsi velocemente verso l'Ethical Hacking, gli Assessment di sicurezza, la Forensic e l'Incident Response. Nel corso degli ultimi 15 anni ha lavorato ogni giorno aiutando le aziende nel fortificare la loro postura di sicurezza e migliorare le loro capacità di rispondere alle minacce.
Grazie all'innovativa piattaforma ed ai servizi di CrowdStrike, Stefano è in grado di abilitare i propri clienti nell'ottenere il più importante risultato nell'odierno panorama delle minacce: lo "STOP THE BREACHES".

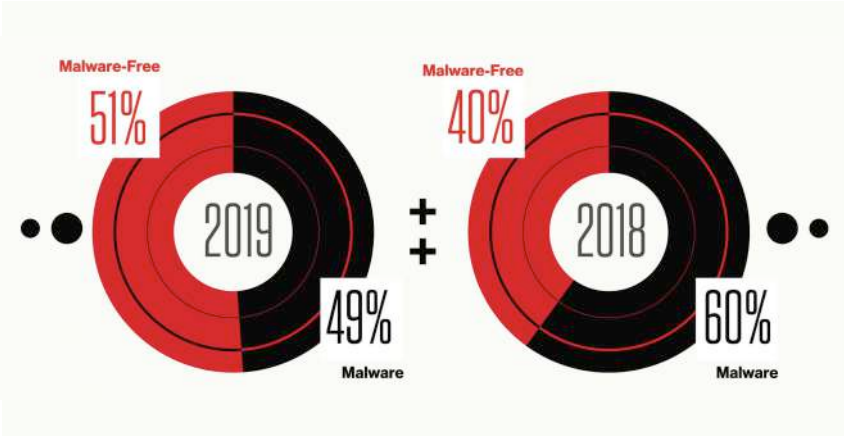
in cui l'hanno realmente fatto - al fine di ottenere il pagamento di un riscatto dalle vittime che avevano scelto di ripristinare l'integrità dei loro ambienti ricorrendo a copie di backup.

- **L'ecosistema eCrime continua ad evolversi, maturare, potenziarsi e specializzarsi**. Organizzazioni criminali consolidate hanno continuato ad espandersi, allontanandosi dagli attacchi basati sui trojan bancari e muovendosi verso:
  - Sviluppatori Ransomware-as-a-service **(RaaS)** che sferrano gli attacchi di "caccia grossa"
  - Sviluppatori Malware-as-a-service **(MaaS)** che aggiungono moduli ai ransomware
  - Operazioni a supporto del Download-as-a-service **(DaaS)** per la distribuzione di malware di terzi

Questi sforzi messi in atto a favore delle campagne di "caccia grossa" sottolineano l'impatto che il ransomware mirato ha avuto all'interno dell'ecosistema criminale.

- **Oltre alle operazioni di "caccia grossa", è stato osservato un aumento delle campagne eCrime mirate agli istituti finanziari per illeciti trasferimenti di denaro o prelievi dai bancomat**, con attività che si espandono al di fuori degli Stati Uniti, Canada ed Europa per colpire l'America Centrale, il Sud America e l'Africa.

- **La tendenza di attacchi con tattiche che non utilizzano malware è accelerata, sorpassando il volume degli attacchi basati su malware**. Il fatto che nel 2019 il 51% degli attacchi abbia utilizzato tattiche che non coinvolgevano malware rispetto al 40% registrato nel 2018, sottolinea la necessità di dotarsi di soluzioni di protezione più sofisticate rispetto ai semplici antivirus.



- **Gli avversari continuano ad evolvere e a perfezionare le proprie tattiche, tecniche e procedure (TTP)** arricchendole di risvolti più sofisticati, come il blocco dei prodotti di sicurezza, il tunneling DNS, l'utilizzo di siti compromessi ospitanti il sistema di gestione dei contenuti WordPress, l'intromissione fraudolenta in thread e-mail, le compromissioni dell'autenticazione a due fattori e i programmi di creazione dei documenti che fungono da dropper per i servizi di distribuzione.

La pubblicazione delle TTP associate alle operazioni osservate nel 2019 degli avversari di tipo "Nation-State" potrebbe comportare la loro adozione di metodologie meno ovvie per l'anno in corso, ma lo scopo dei loro attacchi rimane invariato: raccogliere informazioni e promuovere il disaccordo all'interno delle comunità.

NAMING CONVENTIONS

This report follows the naming conventions instituted by CrowdStrike to categorize adversaries according to their nation-state affiliations or motivations (e.g., eCrime or hacktivist). The following is a guide to these adversary naming conventions.

Adversary	Nation-State or Category
BEAR	RUSSIA
BUFFALO	VIETNAM
CHOLLIMA	DPRK (NORTH KOREA)
CRANE	ROK (REPUBLIC OF KOREA)
JACKAL	HACKTIVIST
KITTEN	IRAN
LEOPARD	PAKISTAN
LYNX	GEORGIA
PANDA	PEOPLE'S REPUBLIC OF CHINA
SPIDER	eCRIME
TIGER	INDIA

Attacchi mirati sponsorizzati dagli stati

CrowdStrike segue una serie di avversari responsabili di intrusioni sponsorizzate dagli stati in varie parti del mondo, tra cui gruppi di attaccanti riconducibili alla Corea del Nord (o Repubblica Democratica Popolare di Corea), alla Cina, alla Russia e all'Iran. Come negli scorsi anni, la maggior parte delle intrusioni mirate condotte da questi avversari sembra esser stata motivata dai tradizionali obiettivi di raccolta di informazioni. Il team di Intelligence di CrowdStrike sta, inoltre, investigando su possibili collaborazioni tra sofisticati criminali informatici ed i gruppi di intrusioni mirate sponsorizzate dagli stati, dove gli indizi iniziali suggeriscono una condivisione degli strumenti criminali e/o un livello di cooperazione con i servizi di intelligence di Corea del Nord e Russia.

Corea del Nord (DPRK): Chollima

Le intrusioni mirate orchestrate dalla Corea del Nord rappresentano le operazioni più attive del 2019. Le organizzazioni della Corea del Sud continuano a rappresentare un interesse strategico per gli attaccanti affiliati alla Corea del Nord. In aggiunta diversi incidenti hanno coinvolto l'India, e un attaccante ha orchestrato operazioni mirate negli USA e in Giappone con l'obiettivo di raccogliere informazioni strategiche sul nucleare e sulle attinenti sanzioni.

Cina: Panda

Gli attacchi provenienti dagli attaccanti cinesi non hanno subito flessioni nel corso del 2019 e si sono concentrati prevalentemente sul settore delle telecomunicazioni. La scelta delle telecomunicazioni come bersaglio, specialmente nell'Asia Centrale e nel Sud-Est Asiatico, si iscrive nel piano cinese di creare una "via della seta digitale", a cui contribuisce anche lo sviluppo delle reti mobili 5G. Prendendone atto, i governi di vari paesi hanno rifiutato di lavorare con il gigante cinese delle telecomunicazioni Huawei esprimendo preoccupazione circa i rapporti che l'azienda ha intrattenuto con le forze armate e i servizi segreti cinesi, russi e nordcoreani. Il targeting delle società statunitensi attive in settori chiave e di interesse strategico vitale per la Cina – incluso l'energia pulita, la sanità, le biotecnologie ed i prodotti farmaceutici – ci sia aspetta che continuerà con molta probabilità.

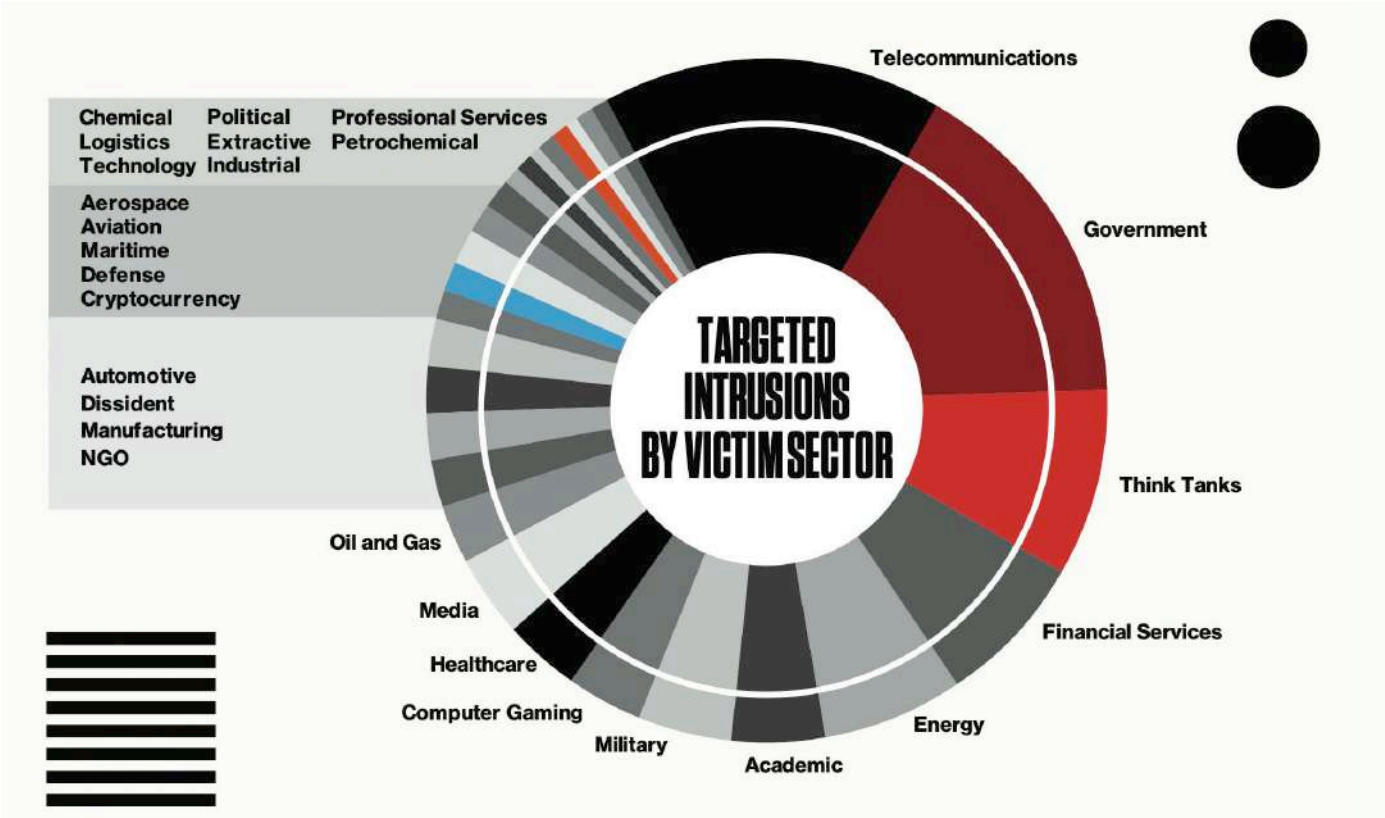
Russia: Bear

Durante tutto il 2019, il team di Intelligence di CrowdStrike ha osservato attività di intrusione mirate della Russia contro l'Ucraina. I bersagli della gran parte di questi attacchi sembrano esser stati diplomatici e responsabili della sicurezza nazionale ucraini, verosimilmente con lo scopo di raccogliere informazioni strategiche dal punto di vista politico e militare sul conflitto tra i due paesi. Apparentemente gli attaccanti russi hanno tentato di influenzare l'esito delle elezioni presidenziali ucraine nel marzo del 2019 con diversi riscontri di campagne di disinformazione, attacchi DDoS (Distributed Denial-of-Service) e compromissioni dei social media. Poiché il conflitto tra Ucraina e Russia rimane irrisolto, è verosimile che in futuro le attività di raccolta di informazioni appoggiate dalla Russia continuino o, addirittura, si intensifichino.

Iran: Kitten

In risposta al clima politico sempre più teso tra Iran e Stati Uniti, le attività di avversari riconducibili all'Iran indicano un crescente interesse verso bersagli governativi e della difesa. Nella prima metà del 2019, le attività degli attaccanti iraniani erano dirette verso paesi del Medio Oriente e del Nord Africa (MENA), mentre nella seconda parte dell'anno c'è stata un'evidente escalation degli attacchi verso entità statunitensi, verosimilmente in risposta alle tensioni esplose tra Stati Uniti e Iran a partire dal maggio 2019. Il team di Intelligence di CrowdStrike può affermare con molta sicurezza che gli attaccanti riconducibili all'Iran continueranno ad impiegare il cyber spionaggio assieme alle tradizionali operazioni di raccolta di informazioni con particolare enfasi sulla regione MENA e il Nord America.

In base alle attività osservate nel 2019, le organizzazioni che operano nei settori della difesa, dei commerci marittimi, delle telecomunicazioni e dell'informatica nella regione MENA saranno probabilmente di particolare interesse per gli attaccanti iraniani nel 2020.



Il cambio dei paradigmi di sicurezza nel 2020

In un clima già molto impegnativo sul fronte della sicurezza digitale dove, come abbiamo già detto, diverse minacce che hanno caratterizzato il 2019 continueranno anche nel 2020, l'anno appena iniziato ci porta a dover fare i conti con l'emergenza COVID-19 che sta obbligando molte aziende, se non tutte, ad adottare immediatamente un modello di lavoro in remoto.

Oltre alla ovvia pressione che questo repentino cambiamento esercita sul personale IT, sulle architetture di rete e sui fornitori dei servizi, le aziende devono prendere in considerazione che nuovi rischi informatici si stanno affacciando alla loro usuale operatività.

Sicuramente, la sicurezza dei lavoratori remoti parte con la rivisitazione delle politiche di sicurezza informatica per includere lo smart working e dalla predisposizione sicura di dispositivi personali dei dipendenti (BYOD) per la connessione ai sistemi aziendali.

Ma le organizzazioni devono anche considerare fattori di rischio finora esterni alle loro organizzazioni: l'utilizzo dei dipendenti remoti di reti Wi-Fi non protette o la scarsa pulizia informatica dei dispositivi personali, unita alla mancanza di visibilità su questi dispositivi, potrebbero porre le basi per la perdita di dati sensibili.

Infine, è inoltre fondamentale mantenere alta la vigilanza degli utenti in merito alle truffe legate al coronavirus con informazioni costanti in merito alle diverse attività di phishing rilevate nonché abilitare i piani di Incident Response per renderli attuabili sui lavoratori remoti.

Consigli di Crowdstrike

Ecco i consigli di CrowdStrike per proteggere la propria organizzazione e rafforzare la rete difensiva contro gli avversari sempre più agguerriti di oggi e domani:

Sfruttare appieno la rete di protezione già esistente. La proliferazione delle attività di "caccia grossa" ha aumentato drammaticamente le ricadute sulle organizzazioni che non si proteggono adeguatamente. Le aziende più accorte si adopereranno per ottimizzare i controlli di sicurezza già in essere.

Proteggere le identità. Nel corso dell'anno scorso, l'impiego delle tecniche di attacco prive di malware si è intensificato. Come punto di partenza, è necessario predisporre l'autenticazione a due fattori (2FA) per tutti gli utenti perché i criminali informatici del giorno d'oggi sono esperti nell'utilizzare credenziali valide per accedere ai sistemi e comprometterli velocemente. Affiancando questa misura a un efficace processo di gestione dei privilegi di accesso, è possibile limitare i danni causati dagli attaccanti a seguito di un'intrusione.

Mobilitare gli utenti. Nonostante la tecnologia rivesta chiaramente un ruolo critico nella lotta agli attaccanti, l'utente finale rimane un anello vitale della catena. È importante avviare programmi di sensibilizzazione per combattere i continui rischi collegati alle campagne di phishing ed alle tecniche di social engineering.

Abbracciare la "regola 1-10-60". Per combattere in modo efficace minacce sempre più complesse, CrowdStrike sollecita le aziende a fare riferimento alla "regola 1-10-60": rilevare le intrusioni entro 1 minuto, analizzarle e classificarle nel giro di 10 minuti, contenere e neutralizzare un attacco entro 60 minuti.

Cercare partner con le competenze giuste. Serve qualcosa di più della semplice tecnologia per riuscire ad agire alla velocità imposta dalla «regola 1-10-60». Per difendersi da minacce altamente sofisticate sono necessari processi strutturati e professionisti della sicurezza efficaci e competenti, attivi 24 ore su 24. Per ovviare alla mancanza di competenze specifiche nel modo più economicamente conveniente, le aziende di maggior successo spesso si affidano a partner che offrono le migliori soluzioni del settore.

Favorire soluzioni a servizio per garantire la massima sicurezza a tempo zero. In un momento in cui tutto sta cambiando, rompere gli schemi con il passato non significa solo scegliere nuove soluzioni, ma anche nuove modalità di fruizione, come le soluzioni a servizio come CrowdStrike Falcon Complete. I clienti possono infatti affidare l'implementazione, la gestione e la risposta agli incidenti relativi alla sicurezza dei loro endpoint al team di esperti della sicurezza di CrowdStrike per ottimizzare istantaneamente la sicurezza dei loro endpoint senza dover impiegare risorse interne, probabilmente impegnate dalla gestione di queste transizioni forzate allo smart working.

Scarica la tua copia GRATUITA del **Global Threat Report 2020 di CrowdStrike®** per approfondire le tue conoscenze in materia di sicurezza informatica basandoti sugli incidenti osservati in tutto il mondo nel corso del 2019 e per scoprire come neutralizzare gli aggressori informatici sempre più agguerriti nel 2020: http://crowdstrike.com/gtr

Inoltre, se si è interessati a maggior informazioni in merito alla sicurezza informatica ai tempi del COVID-19, i nostri suggerimenti per rendere lo smart working efficace e sicuro sono disponibili in questo webcast: https://go.crowdstrike.com/CC-Embracing-Remote-Workforce-Blog.html

Le organizzazioni che adottano la "regola 1-10-60" hanno molte più probabilità di espellere gli avversari prima che l'attacco si diffonda oltre la fase di ingresso iniziale, minimizzando l'impatto e la portata dell'intrusione. ■

Next Generation IPS: una scelta di qualità

Autore: Matteo Arrigoni,
Principal Sales Engineer, Trend Micro Italia

Oggi le aziende sono consapevoli che è impensabile limitarsi a guardare e rilevare le minacce che attraversano le proprie reti. È fondamentale agire e fermarle quanto prima, per tutelare le proprie infrastrutture e i propri dati salvando così il business da dispendiose interruzioni.

BIO

Matteo Arrigoni ha alle spalle 20 anni nel settore della cybersecurity. Nel corso della sua carriera ha accumulato esperienze sia tecniche che manageriali, che gli hanno consentito di rivestire ruoli di responsabilità sempre maggiore, soprattutto lato clienti finali, con particolare focus su Large Enterprise e Telco. L'esperienza gli ha consentito di seguire progetti di sicurezza legati ai Software Defined Datacenter e alla Cloud Adoption in ambito Large Enterprise. In ambito Telco, invece, ha avuto la possibilità di collaborare con i principali operatori italiani, sviluppando soluzioni di sicurezza gestita pensate per una clientela mid e large enterprise. Negli ultimi anni ha approfondito anche i temi legati alla security in ambito industriale, partecipando come relatore a diversi eventi e seguendo progetti in ambito Network cybersecurity. Esperienze che gli hanno permesso di divenatare professore all'interno del "Master Universitario di II livello in Cybersecurity and Critical Infrastructure Protection", che si svolge presso l'Università di Genova.
Matteo approda in Trend Micro con il ruolo di Principal Sales Engineer, dopo aver trascorso gli ultimi anni in Fortinet. Il suo compito sarà quello di supportare il mercato delle very large enteprise con un particolare focus nei progetti di Network Security e di Cloud Security.

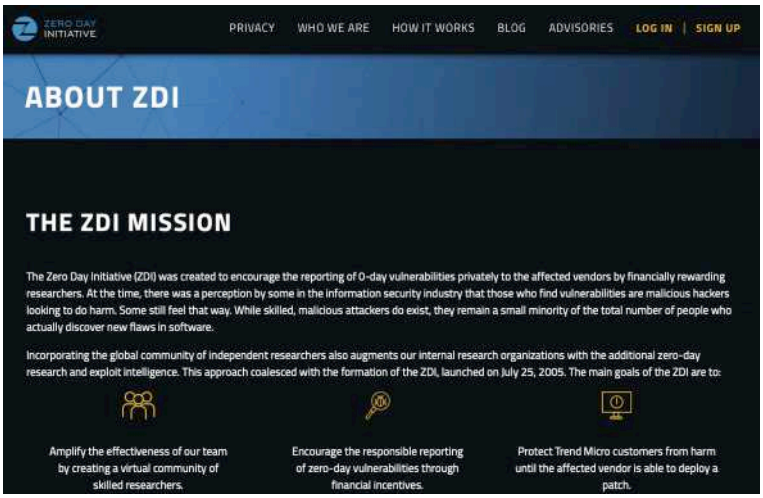
Tra molteplici ambienti, dal cloud all'IoT passando per l'Industry 4.0 sono tante le soluzioni, che presentano livelli di efficacia diversi. È difficile per un'azienda orientarsi sulla migliore strategia da seguire, specialmente quando si parla di reti e della necessità di scegliere una soluzione di *intrusion prevention* rispetto ad altre, oppure anche in considerazione di un approccio diverso, come quello di un Next Generation Firewall ad esempio.

Un asset strategico per la sicurezza
Il sistema di *intrusion prevention*

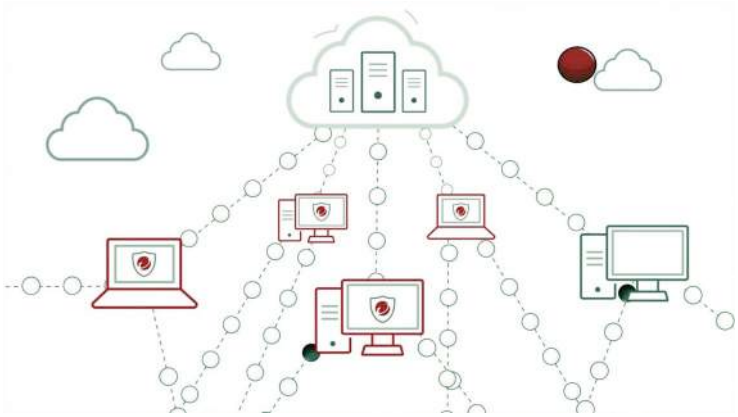
In ambito networking possiamo distinguere due diverse direttrici. La prima è quella Nord/Sud, che rappresenta il traffico che dalla rete internet si muove verso quella aziendale. In questo caso bisogna proteggersi da ciò che è esterno e quindi dalle minacce che provengono da fuori. L'azienda mette quindi al sicuro i servizi esposti, come i siti vetrina e gli e-Commerce. Si deve tenere conto, però, che oggi grazie al cloud questa direttrice non viaggia esclusivamente verso la rete locale dell'organizzazione, ma anche verso il data center dell'azienda distribuito tra i diversi Cloud Service Provider. È importante quindi prestare molta attenzione alla protezione di questo ambito, perché il cloud aumenta la superficie di attacco e anche perché la sicurezza nel Cloud è completamente a carico del cliente, così come indicato dallo *shared resposability* model.

La direttrice Est/Ovest, invece, riguarda i movimenti all'interno della rete aziendale. Una volta il concetto di perimetro aziendale era il dogma sul quale si strutturavano le strategie di difesa, ma a partire dal 2009 il fenomeno del BYOD introduce il concetto che le minacce possono già trovarsi al di là di quel fortino costruito intorno alla rete aziendale. Con l'aumentare del nomadismo digitale dei dipendenti e grazie allo smart working e ai servizi cloud il concetto di perimetro aziendale viene poi completamente ribaltato. È fondamentale quindi mettere delle protezioni anche all'interno del fortino aziendale, per tutelarsi da quelle minacce che sono già all'interno. Tra queste

anche le eventuali vulnerabilità, che sono in sensibile aumento (i numeri ci dicono che raddoppiano ogni anno) come testimoniano i dati della Trend Micro Zero Day Initiative (ZDI). In questo caso un endpoint potrebbe compromettere l'intera rete aziendale, ecco perchè è importante avere una protezione interna. Queste considerazioni sono valide per le aziende ma anche per le fabbriche. Pensiamo al fenomeno dell'Industry 4.0, dove è ancora più importante segmentare la rete IT per proteggere quei sistemi OT che magari presentano vulnerabilità vecchie e non coperte al loro interno.



In tale scenario la tecnologia da implementare che offre maggiori garanzie è individuabile nel sistema di Next Generation IPS, (nel ventaglio delle soluzioni praticabili quella messa in campo da Trend Micro TippingPoint, presenta degli importanti profili di eccellenza) in quanto permette una puntuale prevenzione delle intrusioni, rispetto alle diverse tipologie di minacce che, com'è noto, oggi viaggiano in rete, spazio virtuale che non ha "zone franche".



Le vulnerabilità passate al "setaccio"

Il Next Generation IPS è un sistema che passa al setaccio quello che viene portato all'interno della rete. Funziona, ad esempio, come lo scanner dei controlli aeroportuali, concentrandosi sulla protezione delle minacce identificandole all'interno del traffico mentre lo analizza ai raggi X. Il Next Generation Firewall, invece, è un sistema che osserva ciò che viene portato all'interno della rete, cercando di identificare il vettore utilizzato (ad esempio Google Play, YouTube etc…). Rimane una semplice porta, che in questo caso si potrebbe paragonare all'addetto ai controlli. Questo sistema ha quindi lo scopo principale di identificare le eventuali minacce, partendo dalle violazioni alle politiche di accesso impostate tipicamente sulle applicazioni (vettore utilizzato), a cui è possibile eventualmente associare anche un controllo IPS.

Prendendo in esame tre parametri essenziali si può facilmente dimostrare la qualità superiore dei Next Generation IPS.

a. Efficacia

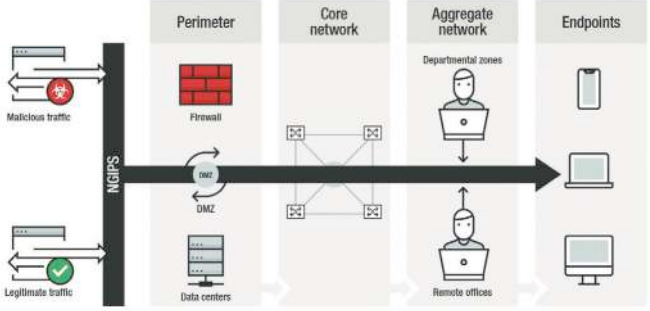
La soluzione *Next Generation IPS* protegge da vulnerabilità non ancora individuate e già comunicate al vendor del software garantendo la sicurezza nel lasso di tempo che intercorre tra la notifica al vendor e la risoluzione. Mediamente un nostro cliente è protetto 60 giorni prima che la vulnerabilità venga risolta. Questo grazie agli sforzi compiuti dell'azienda, che hanno portato alla individuazione di uno spettro di vulnerabilità, che in termini di ampiezza, è pari al doppio rispetto a quanto i competitor sono in grado di mettere sul mercato.

b. Funzionalità

Rispetto ad altre soluzioni conosciute dal mondo aziendale Tipping Point si caratterizza per una particolare funzionalità di Enterprise Vulnerability Remediation che ne marca immediatamente la differenza in positivo. Adottando TP è possibile implementare una protezione che blocca solo le vulnerabilità attive, secondo una logica *taylor made* rispetto all'infrastruttura dell'azienda cliente. Questa soluzione garantisce un'ulteriore funzionalità IPS in modalità trasparente, in altri termini si può inserire all'interno della rete cliente senza apportare eventuali modifiche. Questa funzionalità facilita l'inserimento di questa tecnologia rispetto a quanto è possibile effettuare con *Next Generation Firewall*, che raramente viene implementato in questa modalità. Il complesso di tali requisiti si rileva particolarmente importante per le infrastrutture cloud, ambito in cui i Firewall mettono a nudo tutte le proprie carenze in termini di flessibilità.

c. Performance

Altra valida ragione che svela la superiore qualità di un Next Generation IPS è individuabile nella ricchezza di un prodotto che permette di soddisfare le esigenze sia delle PMI che delle aziende di maggiori dimensioni. Questo prodotto risulta, infatti, perfettamente in grado di adattarsi alle diverse realtà presenti sul mercato. ■



Pasquale Preziosa e Dario Velo, *La difesa dell'Europa, Ed. Cacucci*

LA "NUOVA" CENTRALITÀ DELL'EUROPA

Siamo alla ricerca di un nuovo ordine mondiale, mentre sperimentiamo un profondo cambiamento d'epoca. Il post guerra si è definitivamente concluso nel 2008 sulla spinta di due eventi: il fallimento della *Lehman Brothers* che ha fatto piombare il pianeta nel buco nero di una crisi economico-finanziaria per effetti e durata senza precedenti e l'esplosione della questione georgiana, con cui la Russia ha alzato il capo rivendicando per la prima volta un ruolo da protagonista nell'orizzonte geopolitico della contemporaneità. La gran parte dei problemi con cui gli stati nazionali sono costretti oggi a misurarsi hanno preso le mosse in quell'anno che si può definire di "svolta" sul piano dell'evoluzione storico-politica.

Nuovi attori hanno cominciato a farsi strada sullo scenario globale, per comodità racchiusi in una sigla BRIC, pronti a far sentire la loro influenza sul governo del pianeta. In questo teatro in movimento l'offerta politica dell'Europa non è stata capace di dare le risposte che sarebbe stato lecito aspettarsi, come dimostrano l'eclissi della Grecia, culla della civiltà universale, inghiottita dal debito ed emarginata da Bruxelles e l'esito della *Brexit*, un grave *vulnus* che indebolisce il vecchio Continente fiaccato dai virus diffusi del sovranismo e del populismo che lo attraversano da Nord a Sud. Per invertire la rotta occorre che L'Europa recuperi in fretta un'iniziativa politica forte e un'identità perduta, questo il messaggio che arriva dall'interessante saggio *La difesa dell'Europa* (ed. Cacucci, €12.00) di **Pasquale Preziosa e Dario Velo**, massimi esperti di geopolitica e sicurezza internazionale. Preziosa insegna presso l'Università Niccolò Cusano di Roma, dopo essere stato Capo di Stato Maggiore dell'Aereonatica, e aver guidato importanti missioni strategiche in molti teatri di guerra; Velo ha svolto un importante ruolo nel processo di integrazione europea, collaborando con **Jean Monnet, Robert Triffin, Altiero Spinelli,** svolge un'importante attività pubblicistica e di docenza in diversi prestigiosi atenei.

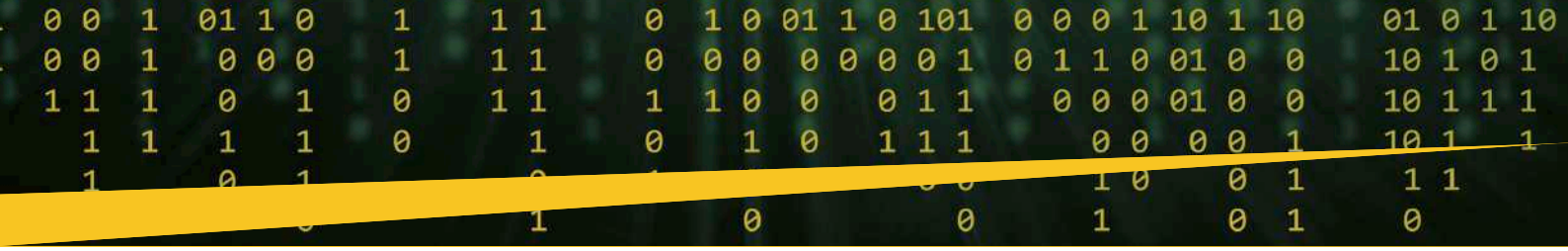
"Il nostro studio – ci tiene a precisare Dario Velo – ha inaspettatamente anticipato gli esiti del recente Consiglio Europeo dello scorso 12 dicembre, che su proposta della **Merkel** e **Macron** ha messo in agenda una Conferenza intergovernativa proprio sul futuro dell'Europa. Oltre ai temi legati all'immigrazione, al clima, alla crescita economica che va riavviata, la difesa sarà una delle grandi questioni da affrontare e risolvere, a partire dal ruolo che l'eurozona dovrà svolgere nelle aree calde del mondo, dal Medio Oriente al Nord Africa".

Il punto nodale, che fa anche da *fil rouge* della trattazione, va individuato nella necessità di riprendere e attualizzare il grande "sogno europeo" dei padri fondatori. "Non scordiamoci – commenta Preziosa - che L'Europa era nata quasi per un "obbligo" imposto dagli USA dopo il grande incendio del secondo conflitto mondiale, che aveva causato milioni di morti. Era emersa chiaramente già allora l'esigenza che le diverse nazioni ritrovassero uno spazio di dialogo, per evitare che si potesse ripetere una pagina così terribile della storia. Senza un continuo confronto con il passato e un adeguato esercizio della memoria non sarà possibile ridare slancio al vecchio Continente, evitando di commettere gli stessi errori del passato".

Una storia che parte da lontano

Il saggio ripercorre alcuni passaggi storici importanti che hanno portato alla nascita della CECA, al fallimento della Comunità Europa di Difesa, gli autori analizzano con lucidità il lungo lavorio che ha portato alla creazione dell'UE. "L'Europa ha alimentato nel suo organismo, il cancro del nazifascismo. Questo vuol dire che le democrazie non sono immuni da errori, soprattutto quando non sono vive e quando tendono a mortificare il principio di partecipazione e di ascolto delle minoranze, finendo con lo smarrire il perseguimento del bene comune. Per non ritrovarsi ancora sull'orlo del baratro bisogna elaborare una strategia di difesa europea adeguata. Non si tratta di armare gli stati – prosegue l'analisi dello studioso – piuttosto di costruire un equilibrio e un bilanciamento sostenibile tra le nuove potenze che operano nello scenario internazionale, impegnandosi concretamente nel mantenimento e nel rafforzamento della pace".

Esiste una "domanda di Europa" espressa da molte nazioni di che hanno bisogno di un interlocutore affidabile per reggere le spinte egemoniche esercitate dei nuovi "padroni" del mondo. La Cina è cresciuta a dismisura, la Russia guarda con sempre maggiore attenzione a quello che avviene oltre confine, il risultato è che gli USA non hanno più la capacità di essere arbitri esclusivi dei destini del mondo. La dichiarazione di Putin nel corso di un recente vertice, sull'importanza strategica dell'ipersonico, è la dimostrazione che ormai vecchi schemi e sistemi di deterrenza non tengono alla prova dell'innovazione. Si è innescata una corsa verso il nuovo che nessuno conosce. Con la nuova tecnologia dell'ipersonico disponibile, lo spazio è divenuto un dominio militare, che modificherà strategie, interventi e investimenti. In questa prospettiva la vecchia Europa non può rinunciare a ridefinire un suo ruolo, che possa garantire sicurezza in un contesto così "liquido" e in continuo divenire.



Sovranità e fine dei territori

La "fine dei territori", per usare una celebre definizione del politologo francese **Betrand Badie**, con il conseguente declino del "Leviatano" e delle logiche hobbesiane, impone un diverso paradigma della sovranità e della sicurezza, tutto da ripensare con realismo critico, al di là del *velo di maya* delle ideologie e degli *"ismi"* che hanno armato gli stati nel Novecento. Attenzione però: nel progetto di una nuova presenza attiva dell"Europa in un quadro geopolitico mutato sostenuto nel saggio, si tiene conto che l'UE è troppo giovane per possedere il *konw - how* e gli strumenti militari della NATO. Gli autori sono consapevoli di questa debolezza: "Nessun tentativo – precisano – di creare una seconda NATO, si tratta di costruire un pilastro all'interno della struttura già esistente che risponda alla complessità delle esigenze di cui sono portatori i diversi governi europei. In questo tentativo il rischio da scongiurare è quello delle fughe in avanti: la costruzione di un esercito europeo è ancora di là da venire, serviranno passaggi ulteriori e una capacità di *governance* coerente rispetto alle trasformazioni in atto, soprattutto da parte di classi dirigenti continentali, non ancora preparate ad affrontare le esigenze del nuovo scenario mondiale". Fare il passo più lungo della gamba vorrebbe dire suscitare pericolose spinte reazionare, già verificatesi in passato, spinte che in un momento di crisi come quello che stiamo attraversando, si tradurrebbero in una voglia di chiusura delle frontiere e in un rigurgito di autoritarismo, la cui deriva sarebbe difficile da prevedere.

Altro aspetto da non trascurare, che pesa come un macigno sulle scelte politiche, è rappresentato dalle difficoltà di bilancio. L'esplosione dei debiti sovrani hanno indebolito gli stati, le risorse drenabili per un progetto di difesa sono perciò da recuperare sol in sede europea. Su questo bisognerebbe seguire l'esempio degli USA, che pur avendo in pochi anni raddoppiato il loro debito, continuano a dedicare somme ingenti agli investimenti nella difesa. L'impegno nella difesa vuol dire impegno nella ricerca e nell'innovazione. La tecnologia è infatti per definizione neutra, la possibilità di applicarla e di spalmarla su una vasta gamma di prodotti, fa poi la differenza. La Cina ha saputo imitare e applicare il modello americano, L'Europa per recuperare capacità di innovazione e competitività nei mercati globali dovrà riprendere un'iniziativa concertata se non vuole rassegnarsi a un declino facilmente prevedibile. "Siamo indietro non solo nella ricerca sull'ipersonico – commenta Preziosa - ma anche sul fronte della *cyber security,* settori considerati ormai strategici, mentre si sta affermando la quarta rivoluzione industriale, che ha un'anima digitale e che sta cambiando i modi di concepire e organizzare il lavoro di miliardi di persone in tutto il pianeta.

L'importanza dello *scouting* tecnologico

Non disperiamoci, la possibilità per riprendere i "sentieri interrotti" tracciati dai fondatori si intravede, a dispetto delle tante criticità del tempo presente. I paesi dell'Est iniziano, infatti, a considerare l'UE un valido partner per la costruzione di nuovi equilibri, in un momento storico in cui stiamo finalmente comprendendo come la sicurezza sia un concetto olistico, che oggi ingloba aspetti economici - finanziari, oltre a implicare questioni filosofiche, psicologiche ed esistenziali di più vasta portata.

I pericoli sulla strada del futuro non mancano di certo, a iniziare dallo *scouting* tecnologico attuato da molti paesi per sottrarre cervelli e competenze alla vecchia Europa, che ne subisce inevitabili ripercussioni. L'Italia detiene un triste primato in questo campo, l'emorragia di una fuga di intelligenze, difficile da tamponare. "I padri fondatori hanno fatto molto per noi - conclude Velo - è il momento di dimostrare che abbiamo capito la lezione, riaffermando i valori dell'Europa, che storicamente si sono tradotti nell'attuazione di un'economia sociale di mercato. La stessa si sta diffondendo anche negli USA e in America Latina il contraltare del neocapitalismo, nel rispetto delle libertà e della diversità plurale, nella pratica della sussidiarietà, quale principio ispiratore dell'organizzazione dello stato".

Sarà decisivo un salto di visione, che deve portarci a considerare la difesa europea non tanto e non solo come protezione fisica di confini, per altro sempre più permeabili nell'epoca della globalizzazione crescente, quanto come riaffermazione di una centralità del Vecchio Continente poggiata nella prospettiva del recupero di un "nuovo umanesimo" che servirà a coagulare risorse prima di tutto intellettuali e poi economiche. Inoltre, servirà a dare vita a un progetto di difesa strategica che possa condurre a uno sviluppo effettivo delle competenze, aperto all'articolazione dei sistemi biologici, culturali e sociali, attorno a cui la vicenda umana organizza da sempre i fattori che possono segnare un oggettivo e misurabile progresso. ■

Il fattore umano nella cyber security. Valori e strategie da costruire insieme. A cura di Nicola Sotira, Ed. Franci Angeli

IL CYBER SPAZIO BENE COMUNE E "FRONTIERA" DA PRESIDIARE

Frutto di un lavoro corale sviluppato da un team di esperte di cyber security, guidate da **Nicola Sotira**, direttore generale della Fondazione no-profit GCSEC *(Global Cyber Security Center)* e responsabile del *CERT* di Poste Italiane, *Il fattore umano nella cyber security* è un interessante manuale che offre un punto di vista originale sulle metodologie e gli strumenti più efficaci che le aziende sono chiamate ad adottare per diffondere una maggiore consapevolezza nell'uso del web e dei nuovi sofisticati strumenti di comunicazione, di cui tutti disponiamo. Nel contesto mutante della "quarta rivoluzione", attraversato da

Bibliografia - Cybersecurity Trends

luci e ombre, il *cyber spazio* è la prima frontiera da presidiare, che ci fa vedere quanto sia difficile trovare un equilibrio sostenibile tra la libertà che innerva e nutre la democrazia e la sicurezza, da cui dipende la sua stessa tenuta. Non vi sono target "protetti", i sistemi di difesa che aziende e istituzioni devono mettere in atto, devono focalizzarsi su due aspetti: il prepotente progresso scientifico e tecnologico che sta modificando i modi di concepire e praticare il lavoro, e l'aggiornamento costante dei saperi e delle professionalità che operano nell'ambito della *cybersecurity*, cui viene ormai riconosciuto un valore strategico, tanto da figurare ai primi posti nell'agenda di molti stati nazionali, in uno scenario geopolitico in costante divenire.

Vivere on life

"L'accelerazione imposta dal digitale ha messo in evidenza come il problema della sicurezza cyber sia oggi uno dei problemi da affrontare per garantire un'efficace transizione dall'analogico al digitale – scrive Nicola Sotira nell'introduzione del volume –. Sono proprio le istituzioni e le organizzazioni produttive le realtà che oggi hanno una maggiore probabilità di ricevere attacchi di *phishing* o *ransomware*, mentre molti dipendenti / clienti non sanno nemmeno che cosa significhino queste due sigle". E' l'individuo l'anello debole di una catena di comunicazione e connessione che investe tutti gli aspetti salienti della nostra quotidianità. *"OnLife"*, il responsabile del CERT di Poste Italiane utilizza più volte questo neologismo coniato nel 2013 da Luciano Floridi per fotografare nella maniera più fedele possibile la nuova condizione socio esistenziale in cui tutti ci troviamo, proiettati in un orizzonte che richiede conoscenza degli strumenti, consapevolezza, padronanza dei linguaggi e misura. La terribile emergenza sanitaria di questi giorni, la crisi più grave dal secondo dopoguerra ad oggi, rende ancora più forte il messaggio di questa ricerca, che insiste in ogni sua parte sulla centralità della competenza e sul valore professionale che manager e imprenditori devono esprimere, in ogni momento della loro delicata attività. Dagli aspetti psicologici e cognitivi, sezione del volume curata da **Alessandra Rose** alle tecniche di costruzione per una campagna vincente di *awareness*, alla definizione delle aree di intervento e di presidio di strumenti *hi tech* sempre più sofisticati, come scrive puntualmente **Elena Mena Agresti**, il *fil rouge* della trattazione rimane il fattore umano, che va protetto, ma anche fortificato nel suo corredo culturale e professionale, che lo vede agire in una "giostra" multimediale certamente affascinante, ma anche densa di insidie. Conoscere la sintassi dell'innovazione per padroneggiare i nuovi canali della comunicazione, come spiegano **Chiara Abbadessa** e **Sonia Ciampoli**, risulterà certamente decisivo, così come sarà fondamentale alzare le antenne per osservare l'universo dei giovani, come ricorda **Marianna Cicchiello**, quella generazione del pollice che sta "crescendo" dentro la rete, e che la vive in una dimensione omeopatica, diventando purtroppo sempre più oggetto "privilegiato" dei reati più turpi messi in atto dal *cyber crimine*.

La necessità di un modello avanzato di awareness

Il lavoro di ricerca fa intravedere molto bene uno scenario molto articolato che vede le imprese al centro di molteplici fenomenologie del cambiamento, investite da un compito sfidante: affinare osservazione critica, motivazione, lucidità, attitudine all'innovazione, rapidità di intervento. Anticipare le situazioni di crisi può, infatti, generare un vantaggio competitivo in situazioni ambientali caotiche, per struttura lontane dall'equilibrio, in cui risulta particolarmente difficile la previsione di quelle componenti che sono in grado di minare l'integrità di reti e sistemi. Sarebbe perciò illusorio, di fronte alla complessità crescente, ipotizzare uno *status* di "sicurezza definitiva", circoscritta in un perimetro limitato e rigido; diventa, proprio per questa ragione, di cruciale importanza l'investimento sulla qualità del fattore "umano", quale elemento determinante per mettere in campo interventi efficaci di prevenzione, di *governance* del rischio e più in generale di awareness, finalizzati a far crescere la cultura della sicurezza ad ogni livello delle organizzazioni produttive .

Quello che in particolare si avverte, scorrendo le pagine del volume, è la necessità di costruire *un"intelligenza collettiva"*, fatta di expertise, sensibilità, competenze. La società del rischio, per usare la celebre definizione del sociologo tedesco di *Ulrich Beck*, ha infatti bisogno di regole, di comportamenti, ma anche di strumenti e codici che consentono di far parlare mondi e saperi diversi. Per raggiungere questo obiettivo, spiegano molto bene gli autori, non basterà in futuro lavorare all'interno delle organizzazioni produttive, ma risulterà, inoltre, utile un confronto costante con tutto ciò che avviene fuori dal circuito lavorativo. Affermare un modello avanzato di *security by design* è sicuramente una delle mission principali che GCSEC sta cercando di promuovere e portare avanti. In quest'ottica diventa importante la progettazione di momenti di incontro, seminari di approfondimento, giornate di studio, mostre tematiche, iniziative di coinvolgimento delle scuole e del mondo della ricerca, tutti aspetti su cui Elena Agresti si sofferma con dovizia di particolari facendo riferimento alle diverse tipologie di attività praticate in Poste Italiane. Sono, infatti, molte le aree da presidiare: dalla posta elettronica, alle *password*, ai *social network*, strumenti straordinariamente delicati e importanti, che danno l'idea della fragilità intrinseca all'universo digitale, una fragilità che fa da complemento alla potenza tecnologica

che è il tratto caratterizzante di quella *"Società del rischio"*, di cui *Ulrich Beck* ha offerto un insuperabile ritratto.

Verso la cittadinanza digitale

Mettere in campo delle metodologie adeguate di misurazione, come ricorda **Michela Cristiani** nel capitolo conclusivo del volume, è un ulteriore imprescindibile banco di prova, se si vogliono migliorare i livelli di performance insieme alla qualità generale di protezione degli asset tangibili e intangibili dell'impresa e, cosa non secondaria, modificare le tante cattive abitudini in cui tutti continuiamo a indulgere, addetti ai lavori e non. Le illustrazioni di **Fabiana Totti** iconizzano, con dosata ironia e leggerezza di tratto, le regole da osservare, i comportamenti a rischio, l'importanza delle password, facendo comprendere al lettore come la sicurezza, oltre ad essere una delle grandi questioni del nostro tempo, è un valore universale, di cui abbiamo bisogno come l'aria per svolgere tutte le nostre attività.

L'originale concezione della **Security Awareness** che si fa strada, seguendo il percorso narrativo proposto dagli autori, proietta, in conclusione, una diversa luce sul compito del *security manager* del futuro, che si muoverà sul terreno della interdipendenza e della complessità, toccando con mano la progressiva trasformazione del suo ruolo, destinato a evolvere da sentinella posta a presidio della tecnologia a responsabile di più ambiti interdisciplinari, impegnati nella delicata missione di catalizzatori della crescita della cittadinanza digitale, categoria inedita dell'esistenza, destinata a innestarsi in un orizzonte sociale e giuridico ancora tutto da esplorare. ■

Giovanni Mari, La Libertà nel lavoro, Edizioni Il Mulino

IL LAVORO DI FRONTE ALLA SFIDA DEL DIGITALE

Giovanni Mari già professore ordinario di Storia della Filosofia dell'Università di Firenze, Presidente della Firenze *University Press* e della rivista "Iride", ha dato alle stampe un interessante scritto (*La libertà nel lavoro*, ed. Il Mulino) in cui volge lo sguardo verso la nuova dimensione della *Smart Factory*. Con la capacità speculativa del filosofo e la lente interpretativa del semiologo l'autore entra nell'"anima" tecnologica di questa nuova realtà organizzativa che va inserita nella cornice della quarta rivoluzione digitale, quale "luogo ideale utile per capire lo svolgimento e la natura del nuovo lavoro", che viene descritto come "atto linguistico performativo". Nel nuovo modello di impresa, secondo l'analisi dello studioso che ci pone di fronte a un salto logico e culturale profondo rispetto alla concezione del lavoro e della fabbrica che la modernità aveva elaborato, si producono "beni comunicando,

come quando il dipendente comunica alla stampante 3D il modello dell'oggetto fisico, che poi la macchina fabbrica in base alla sola comunicazione del modello digitale".

Manager e imprenditori devono prepararsi ad affrontare dunque scenari inediti e a maneggiare linguaggi che ancora non conoscono e che ci porterà verso orizzonti per molti aspetti inediti. "Se il lavoro nella nuova dimensione della *smart factory* è essenzialmente linguaggio – spiega l'autore - occorre operare in un ambiente produttivo in cui la libertà sia ampiamente riconosciuta: senza libertà non si comunica e interloquisce, non si è creativamente autonomi, non si realizza un lavoro soddisfacente che richiede un ozio altrettanto creativo e attivo, nel tempo di non lavoro, soprattutto non si può trasformare il conflitto in una dialettica partecipativa in grado di confrontarsi sulla base delle conoscenze. Tutto questo richiede un *management* che abbia superato il modello *top-down* fordista e che si dimostri, invece, capace di rapporti collaborativi e autonomi tra direzione e dipendenti a tutti i livelli". La necessità di affrontare un percorso di Formazione appare evidente in un universo sociale ed economico che sta sperimentando un delicato e complesso passaggio di paradigma dall'analogico al digitale.

La città del lavoro

Sono molteplici le questioni affrontate nello scritto, il cui titolo presenta una forte connotazione evocativa richiamando la lezione di Vittoria Foa, storico del sindacato, protagonista della resistenza, che ha dedicato una vita ad affermare quella che definiva *"La libertà dentro il lavoro"*. Mari fa un richiamo puntuale della figura di Bruno Trentin autore del libro *"La città del lavoro", uno scritto del 1997,"* in cui appare molto netta la denuncia del "lavoro fordista, in auge in Italia fino agli anni Ottanta, attività eterodiretta in cui la libertà della persona era coercitivamente piegata a direttive definite senza alcuna partecipazione del lavoratore, che è tenuto a realizzarle passivamente secondo la regola che l'operaio deve eseguire e non pensare". Una concezione che lasciava "la democrazia sulla soglia della fabbrica" come ha insegnato un grande filosofo della politica Norberto Bobbio. Per provare finalmente a capovolgere questa prospettiva e riguadagnare degli spazi di autonomia possibili per l'individuo bisogna fare leva sul fatto che l'innovazione richiede un "coinvolgimento" intellettuale ed emotivo del lavoratore, raggiungibile solo con il riconoscimento di un sufficiente grado di libertà e con l'affermazione della centralità della persona, che dovrà diventare un must per l'odierna scienza manageriale.

Le organizzazioni reticolari e il lavoro 4.0

In quest'ottica bisogna chiedersi se le organizzazioni reticolari siano effettivamente in grado di facilitare l'espressione autonoma dei lavoratori, facendo emergere nuove leadership. Il saggio dà una risposta moderatamente ottimista: "L'organizzazione a filiera e reticolare, che sempre di più configura la produzione, richiede sempre di più un lavoro di squadra *(team)*, individuale e responsabile, creativo e capace di risolvere autonomamente i problemi che sarebbe impossibile organizzare con un *management* fordista".

Se è condivisibile questa lettura, come giustificare il dispotismo dell'algoritmo che decide assunzioni, strategie, orientamenti? Quale spazio può avere l'etica in un ecosistema letteralmente dominato dalla tecnologia?

"Non esiste un "ecosistema dominato dalla tecnologia" – la risposta di Mari - ma solo dall'organizzazione e dal *Design* che l'uomo gli ha dato ed in cui è prevista la collaborazione e l'impiego delle macchine digitali. Non è l'algoritmo che assume personale, ricordiamocelo, ma l'uomo che impiega questo strumento. La digitalizzazione dell'economia esige livelli maggiori e non minori di partecipazione e informazione delle persone che operano nelle organizzazioni produttive. Nel lavoro 4.0 l'efficienza dell'impresa richiede autonomia, creatività e responsabilità che presuppongono un grado inedito di libertà. Questo accade nella *Smart Factory* che deve "coinvolgere" tutti i dipendenti. Nella "fabbrica 4.0" e nelle forme di partecipazione e di collaborazione che in essa si possono realizzare, i diritti della cittadinanza democratica sono in gran parte riconosciuti, per cui si può affermare che questa particolare tipologia di "fabbrica" è a pieno titolo una *"città del lavoro"*, per usare la definizione di Bruno Trentin.

La svolta culturale e professionale legata a questo cambiamento d'epoca, ben descritto da Giovanni Mari, è dunque avviata. Ora sta all'impegno di tutti tradurre principi, visioni e regole in prassi vissuta e realmente condivisa. ■

Recensioni bibliografiche: Massimiliano Cannata

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

Una pubblicazione

web for business
swiss webacademy

A cura del

GLOBAL CYBER SECURITY CENTER

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

ISSN 2559 - 1797
ISSN-L 2559 - 1797

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

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

ITALIANO ENGLISH

CyberSecQuiz
BROWSE SAFELY?

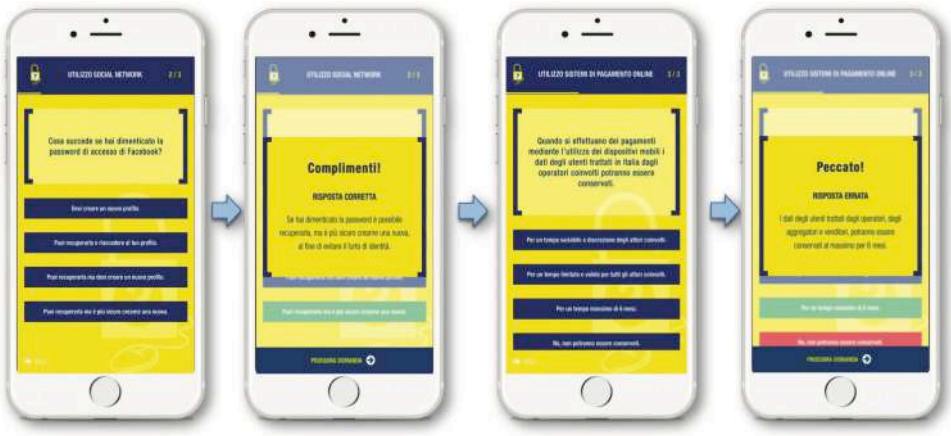
VALUTA SUBITO IL TUO LIVELLO DI CONOSCENZA SULLA SICUREZZA INFORMATICA SU INTERNET

INIZIA IL TEST

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/

TREND MICRO | THE ART OF CYBERSECURITY

SMART WORKING E SECURITY

COME CAMBIA LA SICUREZZA NELL'EPOCA DELLO SMART WORKING E COME FARE PER RIMANERE PROTETTI

A cura di Gastone Nencini, Country Manager Trend Micro Italia

In questi tempi si parla sempre più spesso di **Smart Working**. Lo Smart Working esiste già da molto tempo, ma le ultime vicissitudini hanno spinto molte aziende italiane a suggerire ai propri dipendenti di lavorare dal proprio spazio domestico.

Da un punto di vista tecnologico però, non tutte le infrastrutture possono essere preparate per gestire un aumento di utenti in Smart Working. La maggior parte delle organizzazioni si basa su strutture on premise che possono andare in affanno a causa della mancanza di banda che serve per gestire una quantità di traffico aumentato. Un altro punto da considerare è legato invece alla sicurezza delle reti e dei router delle utenze casalinghe che vengono utilizzate per collegarsi alle reti aziendali, oltre alle policy di sicurezza relative alla navigazione web.

Come affrontare la sfida dello smart working?

Le infrastrutture Cloud possono aiutarci a risolvere e a gestire in modo più snello i livelli di sicurezza, semplificando di molto l'impatto infrastrutturale. Pensiamo ad un utente che fino a poco tempo fa si presentava in ufficio e aveva la sua postazione Notebook o Desktop collegata alla rete aziendale dove erano presenti strumenti e software di sicurezza che proteggevano il suo lavoro, come firewall, proxy, protezione della navigazione web, posta e relativa sicurezza, controlli network tramite IPS/IDS e tutto quanto necessario per proteggere le informazioni trattate.

Lo Smart Working cambia questo approccio, perché le informazioni passano da un router non controllato ed entrano in una rete aziendale che era stata predisposta per avere quel PC all'interno dell'infrastruttura, con un impatto probabilmente non previsto in precedenza in termini di bandwidth.

I vantaggi del cloud e delle soluzioni Saas

Come mantenere quindi gli stessi livelli di sicurezza e policy che l'azienda può garantire quando il PC è all'interno della rete aziendale? Questo è possibile grazie al cloud e, lato security, attraverso soluzioni SaaS. Trend Micro ha prodotti specifici che offrono l'opportunità alle aziende di avere la maggior parte delle soluzioni in questa modalità.

Le soluzioni Worry Free e Apex One proteggono gli Endpoint senza la necessità di avere i server di gestione all'interno dell'infrastruttura. Questi sono disponibili all'interno del Cloud Trend Micro, per cui in qualsiasi punto il dipendente lavori sarà sempre protetto con le policy e le regole definite dall'azienda, evitando maggiori consumi di banda anche nel momento in cui si trova al di fuori della struttura. Trend Micro Web Security protegge la navigazione web e attraverso una configurazione ibrida permette di poter impostare le regole per la navigazione indipendentemente da dove il lavoratore si trova, proteggendo allo stesso modo anche i dispositivi mobili. Soluzioni ad hoc come Cloud App, inoltre, proteggono la posta nel caso si utilizzino sistemi di posta cloud (Office365 – Google Mail etc.) e anche tramite sistemi di protezioni gestiti direttamente da Trend Micro nei propri Data Center.

Oggi la tecnologia Cloud ci permette anche di offrire soluzioni di IPS/IDS come Tipping Point in modalità SaaS, in modo da poter controllare il traffico network da e verso il cloud, riducendo quindi il rischio che eventuali vulnerabilità possano colpire i nostri sistemi.

In conclusione le soluzioni SaaS possono aiutare molto grazie alla loro flessibilità e potenza e Trend Micro si conferma anche come il giusto partner per affrontare la gestione dello smart working.

CERTrating
Maturity Evaluation Tool

Il primo Tool per valutare il livello di maturità del tuo CERT e dei suoi Servizi

Available Now

www.certrating.it

GLOBAL CYBER SECURITY CENTER

Per maggiori dettagli
Info@gcsec.org

Il fattore umano nella cyber security

Valori e strategie da costruire insieme

A cura di Nicola Sotira

MANAGEMENT

TOOLS

GLOBAL CYBER SECURITY CENTER

FrancoAngeli