Il ruolo dell'Italia nella sicurezza cibernetica

Minacce, sfide e opportunità

a cura di
Valerio De Luca
Giulio Terzi di Sant'Agata
Francesca Voce

FrancoAngeli

Il ruolo dell'Italia nella sicurezza cibernetica

Minacce, sfide e opportunità

a cura di
Valerio De Luca
Giulio Terzi di Sant'Agata
Francesca Voce

FrancoAngeli

Ristampa

0 1 2 3 4 5 6 7 8 9

Anno

2018 2019 2020 2021 2022 2023 2024 2025 2026

Stampa: Digital Print Service srl - sede legale: via dell'Annunciata 27, 20121 Milano;
sedi operative: via Torricelli 9, 20090 Segrate (MI) e via Merano 18, 20127 Milano.

INDICE

PREFAZIONE

di *Marco Castaldo*[*]

Si calcola che un quindicenne in un villaggio africano in possesso di uno *smartphone*, è potenzialmente in grado di accedere ad un volume di informazioni superiore in quantità e qualità a quelle che erano disponibili al Presidente Roosevelt durante la seconda guerra mondiale.

Credo che questa immagine sia particolarmente efficace per rappresentare la portata dell'incredibile progresso tecnologico che abbiamo vissuto negli ultimi anni grazie al digitale, che garantisce, ad ognuno di noi individualmente ed alle comunità di cui facciamo parte, un enorme potenziale di sviluppo economico, politico, intellettuale. Il problema è che questa rivoluzione tecnologica non sfugge all'universale e sempiterna legge della natura umana: tutto ciò che di buono la digitalizzazione sta portando nella nostra vita professionale e personale, può essere fortemente compromesso, ed in casi estremi distrutto, da un uso criminale della tecnologia, nel senso più ampio del termine.

Scienziati, studiosi del diritto, top manager delle multinazionali digitali, imprenditori visionari, capi politici, capi religiosi, governi, organismi sovranazionali, tutti sono chiamati dunque ad uno sforzo di comprensione e di innovazione per affrontare qualcosa che sta cambiando nel profondo le regole di funzionamento delle relazioni umane e di qualsiasi organizzazione.

La cyber security è dunque "lo scudo" con il quale tentiamo di difendere dai "criminali digitali" il nostro potenziale sviluppo, la nostra libertà politica, la nostra privacy, i nostri affari, la nostra vita di relazioni professionali ed individuali ed oramai sempre di più anche la nostra sicurezza fisica.

[*] Amministratore Delegato di CSE Cybsec Enterprise S.p.A.

Ho ritenuto necessario fare un incipit che può suonare quasi filosofico per porre l'attenzione su quanto sia complesso il problema che questo libro tratta, da quanti indispensabili punti di vista vada affrontato e quali e quante energie debbano essere messe in campo per ottenere risultati significativi per il "sistema" nella sua interezza. Ritengo pertanto altamente meritoria e di enorme utilità l'iniziativa della Fondazione Einaudi di avere prima organizzato il convegno e poi di avere deciso la pubblicazione degli interventi, su un tema di così straordinaria rilevanza e sono onorato di averne preso parte.

C'è un detto nel mondo della finanza dal quale provengo: "*There's no such thing as a free lunch*"; il suo significato sostanziale è che non si può avere qualcosa in cambio di nulla.

Il digitale ci ha concesso – e sempre più ci concederà – vantaggi incredibili ed impensabili fino a soltanto pochi anni fa, ma ci ha abituati a pensare che viviamo in un mondo "gratuito", come spiega magnificamente Jeremy Rifkin nel suo "*The zero marginal cost society*" che consiglio vivamente di leggere; connessi con chiunque a costo – quasi – zero, con informazioni disponibili in abbondanza, con mercati "perfetti" come gli studiosi di economia classica potevano soltanto sognare, dove la trasparenza dei prezzi è assoluta e la competizione porta soltanto vantaggi, con dinamiche politiche che consentono ad "innovatori" con limitate risorse di imporsi all'attenzione generale ed intercettare sacche potenziali di consenso rivoluzionando in tempi brevissimi sistemi politici che erano cristallizzati da decenni, e potremmo continuare a lungo con gli esempi.

Tutto questo stiamo scoprendo invece giornalmente non è affatto gratuito, ma ha un "costo"; e questo costo è la necessità di un cambio significativo di mentalità, un vero e proprio shock culturale; e lo sono anche gli investimenti necessari conseguenti.

Le libertà e i vantaggi che il digitale ci assicura vanno infatti difesi; con investimenti in tecnologia certo, ma anche con assunzioni di responsabilità individuale; nella verifica delle informazioni, ad esempio, tema caldissimo di cui illustri autori hanno scritto nei loro interventi in questo libro, nella comprensione dei meccanismi di profilazione dell'influenza che possono esercitare sui comportamenti di acquisto e nell'orientamento politico, o anche solo nella semplice adozione di pratiche di "sicurezza" e di buon senso, nell'utilizzo dei nostri dispositivi digitali.

Scendendo da un piano generale a quello più ristretto dell'attività della società di cui sono uno dei fondatori – CSE Cybsec SpA – ossia fornire

soluzioni e strategie di cyber security ad aziende e ad organismi privati e pubblici, quella che ho appena definito "assunzione di responsabilità" è la sostanza su cui abbiamo costruito il nostro innovativo approccio al mercato ed il nostro carattere distintivo e che a nostro avviso dovrebbe diventare la strada maestra per affrontare i rischi di cui stiamo parlando e cioè:

- responsabilità da parte dei vertici aziendali di farsi carico del problema della sicurezza digitale delle loro organizzazioni, prendendo consapevolezza che sono in gioco gli *assets* strategici e quindi gli interessi diretti e concreti di tutti gli *stakeholders* e la sopravvivenza stessa dell'azienda o dell'organizzazione; un tema che non può essere delegato soltanto ai responsabili tecnologici;
- responsabilità da parte dei fornitori di soluzioni di cyber security di dover affrontare la ricerca di soluzioni e di strategie di contenimento dei rischi per i propri clienti da un punto di vista integrato , facendo dell'eccellenza tecnologica soltanto la base su cui costruire un efficace sistema di difesa che si fondi sulla comprensione profonda dei reali *assets* strategici da difendere e sulla capacità di conciliare i due opposti: necessità di sicurezza declinata al più alto livello concepibile e necessità di lasciare per quanto possibile intatto il potenziale di sviluppo e di innovazione garantito dall'adozione sempre più intensa della digitalizzazione.

Questo significa mettere in campo team che abbiano molteplici competenze – tecnologiche, strategiche, gestionali, finanziarie etc. – pronti ad una sfida che vede "i cattivi" partire da quello che chiunque abbia anche solo letto un libro di strategia militare sa essere un grandissimo vantaggio: scegliere quando e dove attaccare ed avere a disposizione "armi di attacco" a costi a volte irrisori.

Occorre dunque prendere atto della indispensabilità di predisporre difese efficaci, nell'interesse individuale delle singole organizzazioni e di quello generale del sistema; e che tali difese avranno bisogno di investimenti significativi, di professionalità sempre più elevate e necessiteranno di continua implementazione.

Ma occorre anche la piena consapevolezza che quegli sforzi, quell'attenzione e quelle risorse sono il piccolo costo che siamo tenuti a pagare per i vantaggi, i progressi, i mezzi illimitati di sviluppo e di aumento del benessere generale che la digitalizzazione del mondo ha la potenzialità di portare.

INTRODUZIONE

di *Valerio De Luca*[*]

La rivoluzione digitale sta velocemente cambiando le nostre vite, ed insieme il nostro modo di pensare e di relazionarci, favorendo la connettività, lo scambio di idee e la condivisione delle informazioni, attraverso nuove forme interattive sul piano politico, economico e sociale.

Negli ultimi decenni, la diffusione delle nuove tecnologie dell'informazione ha progressivamente focalizzato il centro delle attività umane all'interno di una nuova dimensione: lo spazio cibernetico.

All'interno di questo nuovo ambiente artificiale viene ridefinita continuamente la nostra identità informatica attraverso forme ibride e strumenti ad alto potenziale che schiudono un'ampia gamma di opportunità, e allo stesso tempo moltiplicano rischi e minacce in grado di colpire singoli individui e rendere più vulnerabili Stati e aziende di fronte agli attacchi di quanti (criminali, hacker, terroristi) intendono ottenere, in modo fraudolento, dati sensibili e informazioni personali e/o commerciali.

In particolare, sotto attacco sono le infrastrutture considerate critiche per la nazione, in quanto fornitrici di servizi essenziali, quali luce, gas, acqua, ecc., che devono garantire non solo il normale svolgimento della vita quotidiana dei cittadini, la disponibilità e l'integrità, ma anche il diritto alla riservatezza.

Di qui, l'interesse nazionale degli Stati nel tutelare le proprie infrastrutture critiche, il cui danneggiamento rappresenta sia una perdita economica sia una minaccia al benessere e alla sicurezza dei cittadini.

[*] Direttore del Dipartimento Relazioni Internazionali della Fondazione Luigi Einaudi e Direttore del programma "Global Security and Foreign Affairs", AISES-Centro Studi Americani.

La protezione dello spazio cibernetico assume, dunque, una valenza strategica al fine di assicurare la crescita economica e favorire lo sviluppo democratico attraverso l'uso consapevole e responsabile dei mezzi informatici da parte degli utenti.

Attualmente, le priorità nel settore della cyber security – a livello nazionale, europeo ed internazionale – sono il contenimento del crimine informatico, la protezione delle infrastrutture critiche informatizzate e la tutela delle informazioni personali in formato digitale, che richiedono il coinvolgimento non solo dei governi nazionali, attraverso il potenziamento della cooperazione a livello europeo ed internazionale nello scambio di informazioni, ma soprattutto la necessaria "istituzionalizzazione" di una partnership pubblico-privato.

Da non sottovalutare il ruolo di ponte tra le istituzioni e le imprese, che le università e degli istituti di ricerca giocano sia nell'attivazione di programmi di formazione e nel trasferimento del know-how, sia nella diffusione di una cultura della sicurezza informatica che si rivela essenziale per il progresso civile e lo sviluppo economico e sociale di ogni sistema paese.

A partire da queste considerazioni generali, la Fondazione Luigi Einaudi in collaborazione con il programma "*Global Security and Foreign Affairs*", avviato dall'Accademica Internazionale per lo Sviluppo Economico e Sociale (AISES) e dal Centro Studi Americani, ha coinvolto esperti ed accademici in una pubblicazione che intende indagare le questioni sollevate dalla cyber security e le sfide che l'Italia e l'Europa dovranno affrontare nei prossimi anni per aumentare, a tutti i livelli, la consapevolezza della minaccia cyber. Riteniamo fondamentale che questa consapevolezza accresca in futuro, in ragione dell'affermarsi di un nuovo modello di sicurezza nazionale, capace di combinare la necessaria protezione della vita quotidiana dei cittadini e la tutela dei diritti umani con la crescita economica e lo sviluppo dei sistemi democratici.

1. LA CYBER SECURITY IN EUROPA NELL'ATTUALE SCENARIO GEOPOLITICO

di *Giulio Maria Terzi Di Sant'Agata*[*]

1.1. La dimensione cyber: un ambiente complesso e instabile

La geopolitica è diventata un terreno di fondamentale rilevanza per le iniziative poste in essere nel dominio cyber dagli attori statuali e non, in modo legittimo o del tutto illegale, con finalità che si spingono alla destabilizzazione regionale o globale, al sovvertimento dello Stato di Diritto e della democrazia liberale sul piano interno, alla negazione del diritto attraverso un sistematico uso della forza e alla politica del fatto compiuto nelle relazioni internazionali. Gli esempi dell'impressionante crescita di potenza della dimensione cyber nelle relazioni tra stati sono molti e riguardano fatti non solo recenti.

Nell'agosto 2012 ci fu una diatriba tra India e Pakistan scatenata dalle accuse di Nuova Delhi a Islamabad di sostenere un gruppo di hackers che, tramite la diffusione di una serie di notizie false, avevano fomentando la violenza interetnica tra hindu e musulmani, generando scontri gravissimi[1]. In altri scacchieri, Hanoi è stata sospettata di non essere estranea alla diffusione di verbali riportanti una conversazione tra il Presidente filippino Rodrigo Duterte e il Presidente americano Donald Trump che risultavano "imbarazzanti" per le Filippine.[2] In aggiunta, a maggio 2017 le rivelazioni diffuse da alcuni

[*] Chairman of the Board of Directors di CSE Cybsec Enterprise SPA; Ambasciatore, già Ministro degli Affari Esteri della Repubblica Italiana.

[1] Siddiqui T., *In wake of mass panic, India blames Pakistan- backed cyber attack*, The Christian Science Monitor, 24 agosto 2012, disponibile online: https://www.csmonitor.com/World/Asia-South-Central/2012/0824/In-wake-of-mass-panic-India-blames-Pakistan-backed-cyber-attack.

[2] *Trump full of praise for Duterte's brutal drugs crackdown, leaked call reveals*, The Guardian, 24 maggio 2017, disponibile online: https://www.theguardian.com/us-news/2017/may/24/trump-duterte-us-philippines-drugs-crackdown.

hackers attraverso la stampa ed i social media qatariani, poi dimostratesi false, sono state l'innesco della crisi tra Doha e gli altri Paesi del Golfo[3].

Sinora c'è stato poco da fare per impedire questo tipo di operazioni: costano poco e sono facilmente confutabili. In aggiunta, nessuna delle "vittime", incluse quelle americane ed europee, ha ancora trovato il modo di far pagare il giusto prezzo ai perpetuanti dell'attacco. L'Amministrazione Obama, ad esempio, ha reagito all'interferenza russa nella competizione elettorale dell'autunno 2016 e all'hackeraggio del Convegno Nazionale Democratico espellendo diplomatici di Mosca, requisendo proprietà russe e imponendo sanzioni. Ciononostante gli hackers russi hanno continuato ad agire.

L'esponenziale accelerazione degli attacchi informatici con finalità di intelligence, con scopi militari oppure mirati alla sistematica sottrazione di dati sensibili per governi, imprese ed enti di ricerca, si traduce in una casistica pressoché infinita di fattispecie dove realtà e fantasia si confondono. A esemplificarlo bastano alcune recenti notizie.

La prima riguarda il caso Equifax, la società americana specializzata nella valutazione dei crediti, diventata sempre più abile nell'acquisire – senza esplicito consenso degli interessati – masse enormi di dati personali da rivendere ad imprese di credito. Le gravi inadempienze accertate nella protezione dei dati personali di cui Equifax aveva la totale responsabilità, hanno fatto sì che 143 milioni di americani – praticamente la metà dell'intera popolazione statunitense – abbiano subito un danno irreparabile senza che nessuno sembri doverne rispondere, a parte il CEO, Richard Smith, che è stato licenziato[4]. A questo proposito, Thomas Friedman, uno dei più importanti saggisti ed editorialisti americani, ha affermato che viviamo in un mondo dove miliardi di persone sono interconnesse, ma lo sono senza sufficienti architetture giuridiche di supporto. Non c'è, infatti, un adeguato livello di protezione e sicurezza, e di onestà – "muscoli morali" – tra imprese ed utenti, che permetta di gestire le interconnessioni senza abusi. Questa realtà è ben diversa dal mondo dei sogni che ci aspettiamo come risultato delle nuove tecnologie e può facilmente diventare un mondo di incubi.

[3] Hunt K., *Middle East freezes out Qatar: what you need to know*, CNN, 27 luglio 2017, disponibile online: http://edition.cnn.com/2017/06/06/middleeast/qatar-middle-east-diplomatic-freeze/index.html.
[4] *Equifax data breach: credit rating firm replaces key staff,* BBC News, 16 settembre 2017, disponibile online: http://www.bbc.com/news/technology-41291643.

Lo scenario al momento più preoccupante riguarda il ruolo dei social media nella destabilizzazione delle democrazie liberali, con le gravi ombre emerse dal *Russiagate* nelle elezioni americane e le punte di altri simili iceberg nel referendum in Catalogna, nelle elezioni francesi e tedesche. Secondo gli inquirenti americani, in particolare il Presidente della Commissione Senatoriale di Intelligence, Mark Warner, la sensazione è che sinora *Facebook, Twitter* e *Google* "non abbiano preso in modo sufficientemente serio le minacce che Russia ed altri agenti stranieri pongono, né abbiano investito abbastanza per rivelare quanto accaduto nel 2016 e sta ancora accadendo"[5]. Lo scorso novembre Mark Zuckerberg aveva liquidato come "piuttosto folle" l'idea che ci fossero persone che utilizzassero Facebook per generare notizie false che andassero a condizionare le elezioni presidenziali americane. In seguito all'evidente esistenza di centinaia di accounts russi mirati a campagne infiammatorie su temi particolarmente divisivi, Zuckerberg ha dichiarato che "chiamarla folle è stato irresponsabile e me ne dispiaccio"[6]. Qualcosa di simile è accaduto per *Twitter*, che a fine settembre 2017 ammetteva l'esistenza di solo qualche centinaio di account russi organizzati per una campagna sistematica nelle elezioni americane, mentre ricercatori indipendenti davano valori assai più alti. A questo proposito, il Senatore Warner ha affermato che "c'è un'enorme mancanza di comprensione da parte di *Twitter* di quanto seria sia la questione, e della minaccia che essa pone alle istituzioni democratiche"[7]. Successivamente è stata la volta di Google che ha rivelato di avere le prove incriminanti alcuni agenti russi di aver speso decine di migliaia di dollari per acquistare annunci ad ampia diffusione, per interferire nelle elezioni presidenziali d'oltreoceano.

Thomas Friedman fa una considerazione che mi sembra necessaria e condivisibile. Questi tre giganti, ovvero *Facebook. Twitter* e *Google*, rappresentando una sorta di "sovrastruttura globale e onnipotente nell'informazione, nella ricerca, nella finanza", realizzano miliardi di profitti vendendo i nostri dati personali. I tre giganti hanno persino ottenuto deroghe alle normative europee e nazionali in materia e restano tutt'oggi estremamente riluttanti ad

[5] Borger J., *Top Senate intelligence duo: Russia did interfere i 2016 election*, The Guardian,4 ottobre 2017, disponibile online: https://www.theguardian.com/world/2017/oct/04/senate-intelligence-committee-russia-election-interference.
[6] Levin S., *Mark Zuckerberg: I regret ridiculing fears over Facebook's effect on election*, 28 settembre 2017, disponibilie online: https://www.theguardian.com/technology/2017/sep/27/mark-zuckerberg-facebook-2016-election-fake-news.
[7] Jacobs P., *Top Democrat blasts Twitter: Presentation to congressional Russia investigators 'inadequate on almost every level'*, Business Insider, 28 settembre 2017, disponibile online: http://www.businessinsider.com/mark-warner-blasts-twitter-russia-testimony-2017-9?IR=T.

assumersi qualsiasi responsabilità per quanto concerne usi e abusi che si verificano sulle loro piattaforme. Pur sostenendo di non essere responsabili della diffusione di notizie false o di propagande incendiarie, questi social media esigono di essere regolati alla stregua dei servizi di pubblica utilità e di godere, quindi, di tutte le libertà d'informazione garantite agli altri media. Da qui nasce l'urgenza di regole chiare ed effettive, come d'altra parte è sempre avvenuto nella storia delle economie liberali ogni volta che sono sorte situazioni di monopolio. L'Unione Europea, tramite le sue iniziative, si muove appunto in questa direzione.

La seconda recente notizia riguarda la crisi coreana. Fonti parlamentari a Seoul hanno denunciato la sottrazione di alcuni documenti militari ad alta classifica, contenenti i piani da attuare in caso di guerra con la Corea del Nord, tra i quali figura l'eliminazione del regime di Kim Jong-Un[8]. Non è certo la prima volta che attacchi hacker su ampia scala si verificano tra Pyongyang, Seoul e Washington, al limite di quella che potremmo considerare una cyber war. Ricordiamo l'attacco contro la Sony dell'ottobre 2014, presumibilmente attribuibile alla Corea del Nord, e la pronta risposta, ritenuta opera dell'apparato della difesa cyber statunitense, seguita dalla temporanea neutralizzazione delle reti informatiche impiegate[9]. Non possiamo ignorare che, nell'ultimo triennio, ci sono state evidenti conferme di un avanzamento di capacità in questo settore, non inferiori a quelle sviluppate nel settore missilistico e nucleare.

La terza notizia riguarda l'utilizzo spregiudicato di strategie cyber a fini di concorrenza sleale in ambito commerciale. Non si tratta più solo di sottrarre dati per rivenderli nel mercato nero della criminalità organizzata o per furti di proprietà intellettuale; attualmente l'hackeraggio viene "commissionato" da alcuni soggetti per colpire i concorrenti e compromettere il normale funzionamento dei mercati. In passato ciò era avvenuto nel quadro di conflitti regionali e di operazioni di intelligence; ad esempio, nell'agosto 2012, un attacco cyber su ampia scala e di grande efficacia aveva bloccato tutta l'attività del gigante petrolifero saudita Aramco, la più grande compagnia

[8] Sang- Hun C., *North Korean Hackers Stole U.S.- South Korean Military Plans, Lawmaker Says*, The New York Times, 10 ottobre 2017, disponible online: https://www.nytimes.com/2017/10/10/world/asia/north-korea-hack-war-plans.html.
[9] Peterson A., *The Sony Pictures hack, explained*, The Washington Post, 18 dicembre 2014, disponibile online: https://www.washingtonpost.com/news/the-switch/wp/2014/12/18/the-sony-pictures-hack-explained/?utm_term=.6f8636d971b6.

petrolifera mondiale. Il temporaneo blocco di 35.000 computer aveva colpito la principale industria strategica saudita in una fase particolarmente critica dei rapporti tra Teheran e Riyad[10].

Gli attacchi di hacker contro imprese e operatori economici sembrano ora commissionati da alcune grandi aziende inserite nel *gotha* delle cinquecento censite da Fortune. Secondo il Financial Times, sarebbe di questa natura la vicenda di una società multinazionale di giochi online colpita recentemente da un *Distributed Denial of Service* (DDoS) esattamente nel momento in cui si stava svolgendo un popolarissimo, e assai redditizio, campionato mondiale di poker.[11] Un sondaggio condotto tra 4000 aziende di 25 Paesi ha rivelato che le vittime di attacchi DDoS ritengono che i responsabili siano da cercare più tra i concorrenti che non tra la criminalità operante nel cyberspace. Infatti, secondo il sondaggio, solo il 38% riconduce questi attacchi alla criminalità, mentre il 43% li addebita ai concorrenti nel settore[12]. Raj Samani, capo ricerca di McAfee, ha dichiarato a Wired Magazine: "Uscire e distruggere il tuo competitor può costare meno di una tazza di caffè"[13]. La vulnerabilità è maggiore per attività concentrate in ristretti periodi temporali. A questo supporto, un'altra rilevazione statistica effettuata su 6 milioni di clienti di una società di cyber security indica che ognuno di loro subisce un attacco DDoS ogni tre minuti[14].

Gli attori non statuali – si tratti di organizzazioni terroristiche come lo Stato Islamico dell'Iraq e della Siria (ISIS), di sindacati del crimine o di gruppi autonomi – hanno acquisito capacità operative simili a quelle degli Stati. Essi infatti acquisiscono dati protetti, orientano i social media con obiettivi geopolitici, diffondono radicalizzazione e violenza.

Vediamo dunque una definizione di regole per la dimensione cyber ancora molto arretrata rispetto alla proliferazione degli attacchi.

Da oltre un decennio, infatti, diverse proposte sono state presentate all'Assemblea Generale delle Nazioni Unite da Russia, Stati Uniti e altri paesi membri. Ma considerazioni geopolitiche, diversità di interessi

[10] Pagliery J., *The inside story of the biggest hack in history*, CNN Tech, 5 agosto 2015, disponibile online: http://money.cnn.com/2015/08/05/technology/aramco-hack/index.html.
[11] Clark P., *Your biggest cyber threat? It's not who you think it is*, Financial Times, 9 ottobre 2017, disponibile online: https://www.ft.com/content/b69fc21e-a9d6-11e7-93c5-648314d2c72c.
[12] *Ibidem.*
[13] *Ibidem.*
[14] *Ibidem.*

nazionali e soprattutto asimmetrie nel progresso tecnologico sono tra i principali protagonisti che hanno ostacolato qualsiasi negoziato per una Convenzione "tipo Ginevra" sull'utilizzo delle tecniche cyber a scopi militari e sulle stesse armi cibernetiche. Queste ultime costituiscono ovviamente la preoccupazione più grande per la Comunità internazionale. Le più recenti sessioni negoziali non sono riuscite ad esprimere un'intesa su quello che dovrebbe apparire principio fondamentale e ineludibile: il diritto internazionale deve essere applicabile anche e soprattutto alla dimensione cibernetica.

1.2. La situazione europea e "l'effetto trasformativo" delle misure adottate con il General Data Protection Regulation (GDPR) e la Direttiva Security of Network and Information Systems (NIS)

Attraverso il Regolamento sulla Protezione dei Dati e la Direttiva sulla Sicurezza della Rete, l'Unione Europea sta creando le premesse per un'evoluzione molto significativa della sicurezza informatica, della collaborazione tra pubblico e privato e dell'interazione tra Paesi alleati per prevenire, resistere e contrastare gli attacchi informatici.

L'adozione nel luglio 2016 – dopo due anni di lavori del Parlamento Europeo, del Consiglio e della Commissione – di una normativa ampia e vincolante, sanzionata da precisi obblighi e responsabilità, sulla protezione dei dati è stata accompagnata dalla creazione di un "sistema strutturato" per la protezione di sei comparti strategici – energia, trasporti, credito, finanza, salute e risorse idriche – attraverso misure di rafforzamento della "prontezza operativa", dello scambio di informazioni e della cooperazione sistematica tra Stati membri. Completano il quadro la definizione di coerenti strategie nazionali di cyber security, l'individuazione dei "business operators" di servizi essenziali e dei "service providers", la precisazione di standard obbligatori per i sistemi di sicurezza ai diversi livelli e un nuovo mandato per l'Agenzia Europea per la Sicurezza della Rete (ENISA).

Si tratta di sviluppi molto importanti per l'Italia. Recenti sondaggi rilevano infatti che solo il 46% delle imprese italiane si dichiarano pronte ad applicare tutte le misure previste dalle normative GDPR e NIS, sin dalla data della loro entrata in vigore, mentre l'88% precisa che sussistono ancora problemi tecnici, legali e organizzativi da risolvere urgentemente.

In ogni caso, per la prima volta sarà realizzato in Europa un sistema normativo unitario sulla sicurezza dell'informazione, posto sotto la responsabilità delle Autorità nazionali, con la supervisione di quelle europee e comunque regolato da comuni standard di sicurezza.

Il Regolamento per la protezione dei Dati (GDPR) sostituisce la Direttiva sulla Protezione dei Dati 95/46/EC ed è stato concepito per armonizzare in tutta Europa le leggi sulla privacy, per proteggere e rafforzare i diritti dei cittadini, per riformare interamente una materia che influisce su prevenzione, deterrenza, resilienza, risposta alla criminalità e terrorismo in ambito cibernetico. In sintesi, le principali innovazioni del GDPR sono:

1) l'obbligatorietà di norme specificamente sanzionate, in misura economicamente significativa, nei confronti di chiunque sia responsabile di violazioni;
2) il GDPR riguarda tanto la sfera dei controlli che quella dei processi;
3) la notifica degli incidenti – attacchi con sottrazione di dati che possano comportare rischi per i diritti e le libertà delle persone – deve aver luogo entro il termine massimo e vincolante delle 72 ore; 4) il GDPR si applica anche all'esterno dell'Unione Europea.

La Direttiva NIS costituisce "l'elemento strutturale" dell'architettura normativa messa in atto dall'Unione Europea. Essa precisa anzitutto i sei settori di interesse strategico – energia, trasporti, credito, finanza, salute e risorse idriche – ai quali sono destinate le norme sulla protezione dei dati, con l'obiettivo di potenziare la sicurezza complessiva attraverso:

a) il rafforzamento delle capacità di ogni singolo Stato membro, l'istituzione dei *Computer Security Incident Response Team* (CSIRT) e delle Autorità Nazionali competenti per l'attuazione della Direttiva, le *Data Protection Authorithy* (DPA), in Italia il Garante della Privacy;
b) la cooperazione e lo scambio di informazioni su incidenti e rischi tra tutti gli Stati membri, e creazione di un "Network CSIRT";
c) l'identificazione a livello nazionale degli operatori dei servizi essenziali e dei providers dei servizi digitali;
d) la cooperazione rafforzata tra Paesi membri dell'Unione nel caso di incidenti di particolare gravità;
e) un nuovo e più incisivo mandato per l'*European Agency for Network Information Security* (ENISA);

f) la definizione di una strategia nazionale, la creazione di un'Autorità competente e di un Computer Emergency Response Team (CERT) per gestire incidenti e rischi;
g) la determinazione degli standard obbligatori per gli operatori pubblici e privati;
h) attribuzione alle Autorità competenti del potere di indagine sui casi di inadempienza.

Questo insieme di regole e di misure rappresenta una riforma di assai ampia portata per l'Unione Europea. Esso crea per la prima volta un sistema integrato, governato da autorità nazionali ed europee, sulla base di standard di sicurezza comuni, e di norme opportunamente sanzionate. Per tali motivi, si può a buon titolo parlare di "effetto trasformativo".

Appare evidente il considerevole salto di qualità che si verrà a determinare nell' "ambiente" europeo della sicurezza informatica, non soltanto nei sei comparti strategici individuati dalla Direttiva NIS, ma anche in un settore come quello della salute.

L'effetto trasformativo agirà in profondità sull'*environment* della sicurezza informatica in Europa e non solo; avrà infatti una portata globale, dato che GDPR e NIS impegnano anche entità esterne all'Unione che sono coinvolte nel trasferimento dei dati protetti. Appare evidente che il significativo progresso di cui stiamo parlando influirà positivamente sul rafforzamento della sicurezza militare e della difesa comune, sia questa destinata a rimanere ancorata essenzialmente all'Alleanza Atlantica o sia destinata ad evolvere rapidamente in una vera e propria Difesa Europea. L'insieme delle misure di protezione dei dati nelle comunicazioni, nella logistica e nella tutela delle risorse essenziali rafforza la resilienza dei paesi interessati. Sarebbe impensabile, inoltre, attuare il Regolamento GDPR e la Direttiva NIS senza un deciso salto di qualità anche nello scambio di informazioni e di dati utili a livello di intelligence. Il terreno applicativo è quindi tipicamente "dual use". Su di esso vi è inoltre ampio spazio per sviluppare strategie di difesa, anche di natura militare, di deterrenza e di risposta.

Il processo di integrazione europea deve quindi concentrarsi sulla dimensione cibernetica per recuperare il tempo perduto dai paesi europei, dall'Italia più di altri. Senza volersi confrontare con le esperienze maturate dalle principali potenze mondiali, guardiamo ad esempio a quanto avvenuto in Israele, un Paese eminentemente agricolo nei primi vent'anni dalla sua indipendenza e successivamente, per deliberate scelte di una politica economica

fortemente focalizzata su scienza e innovazione, è diventato leader riconosciuto nelle tecnologie più avanzate, cruciali tanto per la crescita economica che per la difesa del Paese. Ricordo che la decisione di dare alla dimensione cyber la massima priorità nella difesa e sicurezza del Paese fu presa da Benjamin Netanyahu nel 1999, incaricando i maggiori specialisti del Paese di creare le necessarie infrastrutture, di intraprendere massicci programmi formativi e di collegare organicamente tutta la ricerca e lo sviluppo cibernetico con gli apparati di intelligence e militari, le Università e il mondo imprenditoriale. A quasi vent'anni da tale svolta, Israele costituisce oggi una realtà avanzatissima alla quale è utile guardare soprattutto per la sua capacità di innovazione assicurata da una strettissima interrelazione tra il settore pubblico (Università, Enti di Ricerca e Difesa) e settore privato, con oltre 400 start up che operano nel campo della cyber security.

2. LO STATO DELL'ARTE DELLA CYBER SECURITY ITALIANA

di *Francesca Voce*[*]

Negli ultimi anni la rivoluzione informatica ha costretto individui, aziende, istituzioni finanche apparati governativi ad affacciarsi su un nuovo spazio nel quale riprodurre relazioni, connessioni, scambi e rapporti: il cosiddetto cyberspazio. Con cyberspace ci riferiamo ormai convenzionalmente all'intero ambito delle tecnologie delle informazioni e delle comunicazioni che includono strumenti digitali e virtuali, tra cui anche Internet.

Ci troviamo dunque in una nuova fase estremamente dinamica non solo per la società, ma anche per la politica, caratterizzata appunto da questa nuova dimensione cyber e dalle sue potenzialità, che si manifestano in particolar modo nei settori dell'economia, dell'informazione, dell'educazione, della ricerca e dell'innovazione. Al giorno d'oggi, tutti noi ci riferiamo alle tecnologie informatiche sia in maniera diretta – attraverso le varie attività su dispositivi mobili come lo *smartphone* o il computer – sia in modo indiretto ed inconsapevole, poiché, ad esempio, l'erogazione e la gestione di servizi da parte dello Stato è portata avanti grazie alle reti informatizzate. Allo stesso modo servizi fondamentali, quali quelli finanziari, economici ed anche sanitari, si basano su strumenti digitali.

Allo stesso tempo, il cyberspazio è diventato il quinto dominio dell'arena internazionale e rappresenta una nuova sfida per gli Stati, laddove questi si confrontano in un ambiente senza confini reali, avvolto dalle ombre, dove viene meno persino la distinzione amico-nemico, a causa soprattutto dell'anonimato. Ciò rischia di far crollare le dinamiche classiche della

[*] Studentessa del Maser in International Security Studies della Scuola Superiore Sant'Anna di Pisa e l'Università degli Studi di Trento.

politica internazionale, come l'identità degli attori in gioco e le frontiere spazio temporali.

I dati concorrono a definire le nostre identità sia come singoli individui, sia come nazione. A livello personale, le tecnologie informatiche vengono utilizzate nella gestione di database che contengono tutte le nostre informazioni personali, sia quelle che decidiamo di condividere che quelle che rilasciamo inconsciamente. Con il tempo si è andata a creare un'identità digitale parallela a quella reale, che riguarda anche la nazione in senso stretto. Ad esempio, il patrimonio culturale nazionale ha subito un forte processo di digitalizzazione che se da un lato rappresenta un valore positivo per la diffusione della conoscenza, dall'altro lato non è esente da rischi e minacce. Per salvaguardare la nostra identità, anche sotto questa sfaccettatura, è indispensabile affrontare con attenzione questa questione ed adottare una strategia che garantisca un elevato livello di protezione e sicurezza, che permetta in ultima analisi di diventare attori forti e competitivi nello scenario internazionale.

Lo spazio cibernetico è l'unico dominio realizzato dall'uomo e come tale presenta un'importante caratteristica: è uno spazio privo di confini tangibili, dove il tradizionale concetto di protezione fisica del *limes* viene meno. La mancanza di frontiere concrete rende l'arena un campo di gioco complesso in cui sono molti gli anelli deboli e la superficie di attacco è indeterminata. A causa di questa peculiarità, gli attacchi possono assumere svariate forme, dalle interferenze nei processi elettorali, agli attacchi alle infrastrutture critiche, i quali hanno dimostrato avere un potenziale realmente distruttivo. Per lo Stato, i rischi che si incorrono nella dimensione cibernetica sono molteplici. In un'ottica interna, ci sono le minacce al sistema economico- con i fenomeni di criminalità e spionaggio cibernetico-, alla democrazia- attraverso il diffondersi delle fake news e l'interferenza nei processi democratici- e alla tutela dei singoli cittadini – violazioni dei dati, dei diritti umani e della privacy. In un'ottica esterna, la politica e le relazioni tra Stati sono altresì condizionate dal dominio cyber, dove sempre più assistiamo all'avanzare del terrorismo, fino agli attacchi cibernetici contro obiettivi politici e militari che rischiano di degenerare in una vera e propria guerra cyber. Dal Rapporto Clusit 2017 risulta che l'Italia è stata, nel 2016, fra i paesi più colpiti al mondo dagli attacchi informatici[1]. È necessario dunque avviare un'azione

[1] *Rapporto CLUSIT 2017 sulla sicurezza ICT in Italia*. Disponibile online: https://clusit.it/wp-content/uploads/download/Rapporto_Clusit%202016.pdf.

concreta per limitare e contenere tali rischi, ed al contempo essere in grado di sfruttare al meglio le opportunità.

A questo proposito, dal punto di vista della normativa interna, il DPCM Gentiloni dello scorso febbraio recante indirizzi per la protezione cibernetica e la sicurezza informatica nazionale, è normativa vigente, ma ancora non soddisfacentemente attuata, praticamente "a costo zero". Al contempo, ad oggi, manca ancora un'efficace guida politica, poiché le nomine che il predetto DPCM richiedeva, non sono ancora state decise, ma rimandate alla prossima legislatura. Se l'Unione Europea, che grazie alla normativa Network and Information System (NIS) ed il Regolamento sulla Protezione Generale dei Dati (GDPR) (che l'Italia è chiamata a implementare entro maggio 2018) ha creato le premesse per un'evoluzione "trasformativa" della sicurezza cibernetica, in Italia stenta ad affermarsi una cultura della cyber security, che viene percepita non come un investimento, ma come un costo superfluo. L'Italia deve, quindi, dotarsi di un sistema normativo e operativo solido, che vada di pari passo con lo sviluppo della materia e che si conformi al panorama giuridico europeo; allo stesso tempo deve adottare strumenti diplomatici che la rendano in grado di giocare un ruolo da protagonista nello scenario cibernetico internazionale. In quanto membro dell'Ise Shima Group, ovvero il tavolo di lavoro cyber del G7, l'Italia deve sviluppare una proiezione internazionale all'altezza di un foro così esclusivo. Inoltre, la questione cyber security dovrebbe rappresentare una priorità nell' agenda della prossima presidenza italiana dell'OSCE.

Considerata la vastità della tematica e la molteplicità degli ambiti che racchiude, l'Italia necessita di una politica per la società digitale con una visione di ampio spettro e che affronti la questione in maniera strutturata ed omnicomprensiva. Il cyberspace non dev'essere visto solo come una minaccia, ma come una grande, nuova opportunità. Il dominio cibernetico può rappresentare un importante indotto economico che deve contribuire allo sviluppo di un'economia digitale. Il nostro paese è ancora lontano dalla media mondiale e tra gli ultimi, in questo settore, tra i paesi OSCE, nonostante l'Agenda digitale europea abbia inserito tale obiettivo, assieme alla riduzione del divario digitale, tra quelli da conseguire entro il 2020.

Il divario digitale deve essere inteso come una sfida ed un'opportunità: attraverso investimenti in quest'ambito si possono ottenere effetti economici positivi per i fornitori dei servizi digitali ed al contempo si può garantire una

maggiore "digitalizzazione" degli individui, che può portare ad una maggiore informatizzazione dei servizi della Pubblica Amministrazione.

Dal punto di vista occupazionale, il mercato è fortemente alla ricerca di esperti e professionisti del settore. Vista la trasversalità della materia, i profili ricercati sono molteplici: dai tecnici-informatici, agli analisti che si occupino di policymaking, ai giuristi esperti delle tematiche in questione. Le università e gli istituti di ricerca si stanno attrezzando, ma c'è bisogno di una visione strategica basata su un'adeguata agenda politica.

Manca, allo stato attuale, un vero partenariato pubblico-privato basato su tre pilastri fondamentali: istituzioni, accademia ed impresa. Tra questi tre attori si deve andare a creare un circolo virtuoso che rechi benefici alla sicurezza nazionale e vada a creare un indotto economico e scientifico di alto livello.

In questo senso, la politica per la società digitale deve fare un salto di qualità rispetto al passato considerando la tematica cyber non più un elemento secondario ma una vera e propria priorità per le azioni politiche italiane.

3. CYBER DIPLOMACY E RELAZIONI INTERNAZIONALI: LE INIZIATIVE DIPLOMATICHE PER MITIGARE IL RISCHIO DI ESCALATION MILITARE NEL CYBERSPAZIO

di *Luigi Martino*[*]

Abstract

Il presente contributo analizza le iniziative "diplomatiche" del cyberspazio che si stanno delineando a livello regionale e internazionale, con il fine ultimo di ricostruire l'attuale impostazione della cyber diplomacy. La ricerca, partendo dal presupposto che il dominio cyber, pur essendo stato riconosciuto come la "quinta dimensione della conflittualità", sottolinea come ancora oggi questo "ambiente" sia paragonabile a un *ungoverned space*, uno "spazio" dove non esistono "regole del gioco" condivise sulla condotta degli Stati e sulla limitazione degli effetti deleteri dell'uso malevolo degli strumenti informatici.

3.1. Il ruolo "politico" degli Stati e la necessità di regolare il dominio cyber

La creazione di "cornici giuridiche" ha permesso agli Stati nazione, sin dall'epoca Moderna, non tanto di eliminare la guerra, quanto piuttosto di limitarne e regolamentarne gli effetti catastrofici[1]. Verrebbe da chiedersi se tutto ciò sia ancora possibile nel dominio cyber il quale, dopo terra, mare, aria e spazio extra atmosferico, rappresenta la "quinta dimensione della

[*] Dottorando presso la Scuola Superiore Sant'Anna di Pisa.

[1] A. Colombo, *La guerra ineguale. Pace e violenza nel tramonto della società internazionale*, il Mulino, Bologna, 2006.

conflittualità"[2]. In altre parole, volendo analizzare l'impatto dello spazio cibernetico sull'attuale sistema internazionale, il primo quesito di analisi dovrebbe basarsi sulla valutazione della capacità politica degli Stati (ancora oggi i principali – ma non i soli – attori delle relazioni internazionali) di porre (o meno) delle "regole del gioco" in una dimensione che, pur avendo raggiunto un consolidato livello di militarizzazione, è ancora paragonabile ad un *ungoverned space*. È indubbio che il cyberspazio e le *Information and Communication Technologies* (ICT) abbiano garantito potenziali enormi per lo sviluppo economico, sociale e individuale delle società contemporanee, ma tuttavia, il crescente utilizzo malevolo degli strumenti informatici per scopi politici e militari pone rischi significativi per la pace, la stabilità e la sicurezza internazionale.

Infatti, la "bassa" barriera di accesso alle capacità di sviluppo di tecnologie ICT, la velocità dei progressi tecnologici e la complessità dell'ambiente cyber rispetto, ad esempio, alla definizione giuridica tradizionale dei confini, tutte queste caratteristiche concorrono ad aumentare e rendere più complesse le nuove sfide affrontate dagli Stati. Sia questa complessità, che l'attuale incapacità di attribuzione certa dei *cyber attacks* rappresentano le patologie intrinseche del dominio cyber e contribuiscono a frenare i tentativi di dialogo e fiducia all'interno della Comunità internazionale. Inoltre, gli elevati investimenti da parte degli Stati al fine di sviluppare *cyber weapons* con capacità offensive, nonché un crescente numero di scenari– quali ad esempio, l'Estonia (2007), la Georgia (2008), l'Iran (2010) e, più recentemente, L'Ucraina (2015-2017) – hanno aumentato notevolmente la consapevolezza che l'uso

[2] Cfr. L. Martino, *La quinta dimensione della conflittualità. La rilevanza strategica del cyberspace e i rischi di Guerra cibernetica*, reperibile su www.cssii.unifi.it Si veda inoltre, Stockholm International Peace Research Institute, *Information and communication technology, cybersecurity and human development*, SIPRI Year Book 2016, Stoccolma, ottobre 2016; M.D. Cavelty, *The Militarisation of Cyberspace: Why Less May Be Better*, in «Proceedings 2012 4th International Conference on Cyber Conflict», NATO CCD COE Publications, Tallinn, 2012, pp. 141-153; R. Deibert, R. Rohozinski, *The new cyber military-industrial complex*, «The Globe and Mail», 28 marzo 2011, url: http://www.theglobeandmail.com/news/opinions/opinion/the-new-cyber-military-industrial-complex/article1957159/ > 05/2017; J. Valentino-DeVries, L. Thuy Vo, D. Yadron, *Cataloging the World's Cyberforces*, «The Wall Street Journal», 28 dicembre 2015, url: http://graphics.wsj.com/world-catalogue-cyberwar-tools/ > 05/2017.

delle *cyber weapons* possa portare ad una *escalation* o persino a un conflitto tra Stati[3].

3.2. Le iniziative dell'ONU e dell'OSCE volte ad accrescere la sicurezza e la cooperazione nello spazio cibernetico

Riconoscendo l'urgenza di dover affrontare le potenziali tensioni politiche o addirittura militari scaturite dall'uso malevolo delle ICT[4], i decisori politici hanno posto al centro dell'agenda politica globale la c.d. *cyber stability* e hanno avviato diversi processi (internazionali e regionali) al fine di rafforzare la stabilità, migliorare la cooperazione e accrescere la fiducia tra gli Stati nel dominio cyber. Tali sforzi comprendono soprattutto: l'individuazione di norme di comportamento responsabile degli Stati e misure di rafforzamento della trasparenza per ridurre i rischi di incomprensione e di conflitti nello spazio cibernetico. La prima iniziativa è stata avviata in seno alle Nazioni Unite, dove nel 1998, a seguito della proposta avanzata dalla Federazione russa, l'Assemblea Generale ha approvato la risoluzione 53/70[5].

[3] A proposito delle attività di carattere conflittuale nel dominio *cyber* si vedano: R.A. Clarke, R.K. Knake, *Cyber War*, New York, HaperCollins, 2011; J.A. Green (a cura di), *Cyber Warfare: A multidisciplinary Analysis*, Londra, New York, Routledge, 2015; mentre sugli eventi specifici qui citati: Estonia (2007), C.M. Jackson, *Estonian Cyber Policy after the 2007 Attacks: Drivers of Change and Factors for Success*, «New Voices in Public Policy», vol. VII, primavera 2013, George Mason University; Georgia (2008), D. Hollis, *Cyberwar Case Study: Georgia 2008*, «Small Wars Journal», 6 gennaio 2011, url: http://smallwarsjournal.com/jrnl/art/cyberwar-case-study-georgia-2008 > 05/2017; Iran (2010), K. Zetter, *An unprecedented look at Stuxnet, the world's first digital weapon*, «Wired», 3 novembre 2014, URL: https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/ > 05/2017 ; Ucraina (2015), K. Zetter, *Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid*, «Wired», 3 marzo 2016, URL: https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/ > 05/2017; Wannacry (2017), E. Groll, *Security Firms Tie WannaCry Ransomware to North Korea. But in the murky world of cyberspace, that doesn't mean Pyongyang ordered the attack*, «Foreign Policy», 23 maggio 2017, http://foreignpolicy.com/2017/05/23/security-firms-tie-wannacry-ransomware-to-north-korea/ > 05/2017.

[4] Secondo il *Cyber Index*, report pubblicato nel 2013 dall'United Nations (UN) Institute for Disarmament Research (UNIDIR), 47 Stati membri hanno sviluppato programmi ICT con fini military, di cui quindici con capacità offensive, UNIDIR *The Cyber Index International Security Trends and Realities*, New York, Ginevra, 2013; si veda, poi, anche S. Meulenbelt, *The 'Worm' as a Weapon of Mass Destruction*, «The RUSI Journal», vol. 157, n. 2, aprile-maggio 2012, pp. 62-67.

[5] Si vedano United Nations Office for Disarmament Affairs - UNODA, *Developments in the field of information and telecommunications in the context of international security – Fact*

L'obiettivo primario di questa risoluzione è stato quello di ricercare meccanismi utili per la mitigazione dei rischi causati dall'uso malevolo delle ICT e migliorare la cooperazione internazionale nel cyberspazio.

In seguito all'adozione di questa risoluzione, l'Assemblea Generale ha istituito il Gruppo di Esperti Governativi (UNGGE) interamente focalizzato sugli sviluppi nel campo delle ICT nel contesto della sicurezza globale. Il primo gruppo di lavoro dell'UNGGE si è riunito nel 2004 ed il suo obiettivo principale è stato quello di studiare le minacce e le sfide alla sicurezza internazionale derivanti dal dominio cyber, per arrivare a proporre azioni utili per il miglioramento della stabilità e della cooperazione internazionale.

Il *report* del secondo gruppo di lavoro dell'UNGGE, pubblicato nel 2010, ha rilevato come "l'incertezza circa l'attribuzione e l'assenza di una comprensione comune sul comportamento statale possono aumentare il rischio di instabilità e di una percezione errata" e, al fine di prevenire il rischio di escalation politica e militare, il Gruppo di Esperti ha raccomandato "un migliore dialogo tra gli Stati per discutere le norme relative all'uso responsabile statale delle ICT per ridurre il rischio collettivo".[6] Infine nella relazione del 2013 si giunge a raccomandare l'applicazione di "regole o principi di comportamento responsabile degli Stati e misure di costruzione della fiducia nello spazio informatico"[7].

Sheet, New York, gennaio 2017; e, in generale, la pagina di riferimento sul sito dell'UNODA con i dettagli della *roadmap* della tematica in seno alle Nazioni Unite, url: https://www.un.org/disarmament/topics/informationsecurity/ > 05/2017.

[6] Nel report si legge inoltre come «The global network of ICTs has become an arena for disruptive activity. The motives for disruption vary widely, from simply demonstrating technical prowess, to the theft of money or information, or as an extension of State conflict. The source of these threats includes non-State actors such as criminals and, potentially, terrorists, as well as States themselves. ICTs can be used to damage information resources and infrastructures. Because they are inherently dual-use in nature, the same ICTs that support robust e-commerce can also be used to threaten international peace and national security. […]. Capacity-building is of vital importance to achieve success in ensuring global ICT security, to assist developing countries in their efforts to enhance the security of their critical national information infrastructure, and to bridge the current divide in ICT security. Close international cooperation will be needed to build capacity in States that may require assistance in addressing the security of their ICTs». Si veda UN General Assembly, *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security Note by the Secretary General*, A/65/2001, 30 luglio 2010.

[7] Si veda Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, UN Report (A/65/201), 30 luglio 2010; UN General Assembly, *Resolution Adopted by Assembly: Developments in the*

Successivamente, nelle relazioni del 2013 e del 2015, l'UNGGE ha indicato, tra le altre priorità, la necessità di approfondire l'analisi sull'approccio da seguire per rendere il diritto internazionale esistente applicabile all'ambiente cyber. Altra raccomandazione fondamentale emersa dai lavori dell'UNGGE del 2015 è stata individuata nella necessità di prevedere delle misure atte a costruire la fiducia, la trasparenza e la cooperazione tra gli Stati. A tal proposito gli esperti spiegano come:

"Le *confidence building measures* volontarie possono promuovere la fiducia e la sicurezza tra gli Stati e contribuire a ridurre il rischio di conflitti aumentando la prevedibilità e riducendo la percezione errata. Possono dare un contributo importante per affrontare le preoccupazioni degli Stati sull'uso delle ICT da parte degli altri Stati e potrebbero costituire un passo importante verso una maggiore sicurezza internazionale. Gli Stati dovrebbero considerare lo sviluppo di misure pratiche di rafforzamento della fiducia per aumentare la trasparenza, la prevedibilità e la cooperazione"[8].

In questo quadro di iniziative promosse dalle Nazioni Unite, si inserisce anche l'azione portata avanti dall'Organizzazione per la Sicurezza e la Cooperazione in Europa (OSCE), basata sulla sua consolidata capacità di sviluppare strumenti utili per favorire la stabilità, trasparenza, fiducia e dialogo regionale[9].

A tal fine, l'OSCE, riprendendo quanto raccomandato dall'UNGGE, si è posta l'obiettivo di avviare azioni di *cyber diplomacy* sviluppando specifiche *confidence building measures* (CBMs) al fine di ridurre il rischio di conflitti derivanti dall'uso malevolo delle *cyber technologies* e con l'obiettivo principale di migliorare la trasparenza, la cooperazione e la stabilità tra gli Stati membri dell'Organizzazione[10].

Field of Information and Telecommunications in the Context of International Security, A/RES/66/24, 13 dicembre 2011.

[8] Si veda *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, UN Report (A/70/174), New York, luglio 2015, in particolare pp. 11-13.

[9] Questi "mezzi" sono risultati vincenti durante il confronto bipolare, soprattutto con ottimi risultati raggiunti nel settore del controllo degli armamenti nucleari.

[10] Nel 2008, l'OSCE ha iniziato a porre la questione sulla sicurezza relative al cyberspazio con una serie di incontri governativi, e nel maggio del 2011 ha fatto seguito dall'*OSCE Conference on a Comprehensive Approach to Cyber Security: Exploring the Future OSCE Role*. Il 26 aprile 2012, il Consiglio Permanente dell'OSCE ha approvato, poi, durante la 909esima sessione plenaria la decisione sullo sviluppo di CBM per ridurre il rischio derivante da un uso malevolo della tecnologia ICT, stabilendo dunque un gruppo di lavoro aperto (IWG) al fine

Il 26 aprile 2012, l'OSCE, attraverso la decisione del Consiglio permanente n. 1039 (PC.DEC /1039), ha istituito l'*informal working group* (IWG) finalizzato allo sviluppo di CBMs per ridurre i rischi di conflitti nel dominio cyber. Il lavoro dell'IWG ha portato a risultati concreti nel 2013, quando tutti i 57 Stati partecipanti dell'OSCE, attraverso la PC.DEC / 1106, hanno approvato un *set* iniziale di 11 CBMs incentrati principalmente sullo sviluppo di misure di trasparenza e canali di comunicazione e di fiducia.

Nel marzo 2016, l'OSCE ha adottato ulteriori CBMs contenute nella decisione del Consiglio permanente n. 1202 (PC.DEC/1202). Questo secondo *set* si concentra su misure improntate alla cooperazione tra gli Stati partecipanti nel cyberspazio, ponendo particolare attenzione ad esempio alla mitigazione di attacchi informatici contro le infrastrutture critiche ed evidenziando il rischio di come tali attacchi si possano ripercuotere, come un effetto domino, contro tutta l'Organizzazione.

Infine, il 9 dicembre 2016 il Consiglio ministeriale dell'OSCE, riunito ad Amburgo, ha approvato una decisione specifica sulle attività svolte dall'OSCE nello spazio cibernetico, segnando il primo documento di questo genere adottato dal livello politico più alto dell'Organizzazione in materia di *cyber security*[11].

di «to elaborate a set of draft [CBMs] to enhance interstate co-operation, transparency, predictability, and stability, and to reduce the risks of misperception, escalation, and conflict that may stem from the use of ICTs; To help build consensus for the adoption of such a set of CBMs in 2012; [and] To provide progress reports ... and preliminary proposals on possible CBMs». Il vantaggio dell'organizzazione regionale risisde nel carattere ampio e a più dimensioni dell'impegno e della tradizione storica come luogo di cooperazione. Durante il Consiglio dei Ministri dell'OSCE del dicembre 2012 a Dublino si è ampliato il dibattito sulla sicurezza nell'ICT e sulle CBM relative: in particolare, una nuova misura prevede che i governi prenotifichino le attività nel dominio ICT che possano essere, in maniera non volontaria, causa di tensioni o conflitti. Si vedano: OSCE Secretariat's Conflict Prevention Centre, Operations Service, *OSCE Guide on Non-military Confidence-Building Measures (CBMs)*, Vienna, 2012; in generale, per un aggiornamento continuo delle attività dell'organizzazione sul tema si consiglia di fare riferimento alla pagina web dell'OSCE Secretariat Cyber/ICT Security Section, http://www.osce.org/secretariat/cyber-ict-security. Infine, si veda anche: United Nations Institute for Disarmament Research – UNIDIR, *The Cyber Index International Security Trends and Realities*, New York, Ginevra, 2013, url: http://www.unidir.org/files/publications/pdfs/cyber-index-2013-en-463.pdf > 05/2017.

[11] Secondo P. Meyer, diplomatico canadese, già ambasciatore presso le Nazioni Unite, rappresentante presso la Conferenza sul Disarmo a Ginevra (2003-2007) e Director-General of the Security and Intelligence Bureau of DFAIT (2007-2010): «One advantage the OSCE has over some other regional organizations is its extensive experience with CBMs in the conventional arms control field, as there is much in that experience which could be applied to

3.3. La "Dichiarazione di Lucca" come primo step verso la cyber diplomacy

Anche il gruppo delle "sette grandi potenze" (il G7) si è mosso lungo il sentiero tracciato dalle iniziative internazionali intraprese dall'ONU. Nel 2016 infatti, i leader del G7, durante la Presidenza giapponese, hanno dato vita all'*Ise-Shima Cyber Group* (ISCG), tavolo permanente istituito in seno al gruppo dei Ministri degli Esteri, interamente dedicato alle problematiche *cyber*[12].

Il "gruppo di lavoro cyber" si è riunito per la prima volta nel 2017, durante il G7 presieduto dall'Italia. La presidenza italiana dell'ISCG, sin da subito, ha avviato iniziative puramente diplomatiche, al fine di stabilire delle *norms of responsible State behavior in cyberspace* allineando la sua attività con quanto previsto anche dall'UNGGE.

Infatti, il report del 2015 redatto dal gruppo di esperti ONU, al fine di stabilire dei mezzi utili per ridurre i rischi e le minacce per la pace, la sicurezza e la stabilità internazionale, tra le altre indicazioni ha anche avanzato la raccomandazione di identificare una serie di norme politiche non vincolanti di comportamento statale responsabile nel cyberspazio. A tal proposito, nel *report* del 2015 è possibile leggere come:

"Le norme volontarie e non vincolanti relative a un comportamento responsabile statale possono ridurre i rischi per la pace, la sicurezza e la stabilità internazionale. Di conseguenza, le norme non mirano a limitare o proibire azioni altrimenti coerenti con il diritto internazionale. Le norme

cyberspace», in Id. *Diplomatic Alternatives to Cyber-Warfare*, «The RUSI Journal», vol. 157, n. 1, febbraio 2012, p. 14.

[12] Cfr. http://www.mofa.go.jp/fp/nsp/press3e_000073.html Lo scrivente è membro del G7 Ise-Shima Cyber Group e insieme al collega Pierluigi Paganini, al Ministro Gianfranco Incarnato e al Consigliere Marco Lapadura, ha contribuito al drafting della Dichiarazione di Lucca, nonché alla presentazione di un progetto per l'attribution strategica e la mitigazione dei rischi di escalation politico militare nel dominio cyber attraverso la classificazione degli incidenti e degli attacchi tramite il metodo "triage".
Attualmente, tale dibattito coinvolge anche l'OSCE, in particolare i lavori dell'Informal Working Group "on the development of confidence-building measures (CBMs) to reduce the risks of conflict stemming from the use of information and communication technologies". Sempre presso lo stesso IWG, dal 2016 l'Università di Firenze ha avviato un progetto congiunto con l'OSCE (del quale l'Autore è Project Manager) sulla valutazione del livello di implementazione delle 16 CBMs approvate nel 2013 e nel 2016, i relativi ostacoli e l'individuazione di raccomandazioni da inviare agli Stati partecipanti per migliorare l'implementazione delle CBMs e della trasparenza e la fiducia nel dominio cyber".

riflettono le aspettative della comunità internazionale, fissano norme per comportamenti responsabili dello stato e consentono alla comunità internazionale di valutare le attività e le intenzioni degli Stati. Norme possono contribuire a prevenire conflitti nell'ambiente cyber e contribuire al suo uso pacifico per consentire la piena realizzazione delle tecnologie ICT per aumentare lo sviluppo sociale ed economico globale".

Il processo di negoziato avviato dalla presidenza italiana, pur partendo da una proposta basata inizialmente su un vero e proprio codice di condotta nel cyberspazio, con relative appendici sulla verifica e le azioni da intraprendere in caso di attacco e incidente informatico, in fase di stesura si è orientato verso una dichiarazione politica. Quest'ultima è stata approvata durante il *meeting* di Lucca dei Ministri degli Esteri con il nome di *Declaration on Responsible States Behaviour in Cyberspace*[13], nota anche come "Dichiarazione di Lucca". ed è stata inoltre avallata anche nel *Leaders' Communiqué* redatto alla Ministeriale di Taormina.

In sostanza, la "Dichiarazione di Lucca" riconosce *in primis* il ruolo predominante degli Stati nel processo di costruzione di un ambiente informatico più sicuro e stabile; inoltre basa la sua legittimità sulle attività svolte dall'UNGGE e dall'OSCE e infine, riconosce la possibilità di applicare il diritto internazionale esistente anche al dominio cyber.

In aggiunta, la dichiarazione introduce una novità interessante: pur trattandosi di Stati *like-minded*, viene riconosciuta a livello internazionale una necessità politica (quindi non tecnica) nel gestire le sfide e i rischi provenienti dal dominio cyber[14]. In altre parole, il lavoro svolto dall'ISCG, sotto

[13] Cfr. http://www.esteri.it/mae/resource/doc/2017/04/declaration_on_cyberspace.pdf.

[14] Come sottolinea P. Pawlak: «The discussion about confidence-building measures in cyberspace is closely linked to the parallel debates about acceptable norms of state behaviour. While the focus on norms, both in the existing international law and non-binding political agreements, help to establish international level of expectations about states' behaviour in cyberspace, development of CBMs provides practical tools to manage these expectations […] Consequently, the process of development of norms and CBMs are closely linked and interdependent. If norms serve as a certain ideal behaviour that stetes spire to, an adequate mix of CBMs – ranging from those improving situational awareness to building resilience and facilitating cooperation – is supposed to help states achieve them. In addition, whereas CBMs can prevent unintentional conflicts by stopping or slowing down the spiral of escalation, their usefulness is limited in case of intentional conflict and escalation. Consequently, achieving the full potential of confidence-building measures to minimise misperceptions may be limited by a number of factors that undermine credibility of the parties involved: a limited political will and commitment to preventing a conflict, such as a threat to resort to offensive capabilities as opposed to law enforcement and other alternative approaches; distribution of resources

presidenza italiana, ha cercato di porre intrinsecamente l'accento sulla necessità di passare da un approccio prevalentemente tecnico (come avviene attualmente in sede ONU dove l'UNGGE ha facoltà solo di avanzare raccomandazioni e i limiti di "efficacia" di questo esercizio sono evidenti nel mancato *consensus* che ha fatto naufragare l'approvazione del report 2017) a un processo puramente politico-diplomatico che, in definitiva, giunga a prevedere delle regole di condotta condivise -con la speranza in futuro anche vincolanti-valide per il caso specifico del *cyberspace*.

3.4. Conclusioni

L'avvenuta militarizzazione del cyberspazio, ufficialmente decretata dal Summit della NATO tenutosi a Varsavia nel 2016, ma *de facto* sancita nell'ultima decade da varie dottrine militari e *cyber security strategies* nazionali, ha tolto qualsiasi "ipocrisia" rispetto alla volontà da parte degli Stati di piegare alle pratiche della politica e della conflittualità uno spazio inizialmente nato con caratteristiche puramente tecnologiche.

Il campo di battaglia è diventato dunque (anche) virtuale, così come la capacità delle *cyber weapons* (strumenti virtuali) di arrecare danni reali è oggi un dato incontrovertibile. Gli stessi attori in campo, pur essendo ben definiti, non sono i classici protagonisti delle relazioni internazionali. L'arena cyber è affollata da una serie di *stakeholders* che non sono più solo gli Stati, ma anche attori non statali, multinazionali, terroristi, individui, che si confrontano senza un quadro normativo di riferimento.

In altre parole, assistiamo oggi al consolidamento del campo di battaglia, delle armi, degli attori, senza tuttavia, avere delle "regole del gioco" ben definite, elemento essenziale per governare la violenza ed evitare che questa si trasformi in bieca anarchia caotica.

Le iniziative internazionali in essere hanno tracciato la strada da seguire, quella politica-diplomatica; pur essendo queste iniziative "volontarie", lasciano intravedere un minimo di cooperazione internazionale (basti pensare che in sede ONU siedono *top players* come Cina, Russia e Stati Uniti e in

by investment in defence rather than resilience and skills; a weak legal system, such as ineffective rule of law and administration of justice; or recurring hostilities such as cyber attacks», in Id., *Confidence-Building Measures in Cyberspace: Current Debates and Trends*, in A. Osula, H. Rõigas (a cura di), *International Cyber Norms: Legal Policy and Industry Perspectives*, NATO CCD COE Pubblications, Tallin, 2016, pp. 133-135.

sede OSCE l'accordo sulle CBMs interessa anche Russia e Stati Uniti). Tuttavia, come hanno sottolineato i lavori della "Dichiarazione di Lucca", gli Stati devono riprendersi la loro prerogativa originale: la responsabilità di proteggere se stessi ed i propri cittadini, riconoscendo che un ambiente cibernetico caotico può minare la stabilità e la sicurezza internazionale. In questo senso si può dire che, anche grazie ai lavori svolti dall'ultimo G7, superando l'*impasse* creata dall'iniziale dibattito ruotante attorno al fumoso concetto di *multistakeholderism*, si è cercato di mettere in moto un esercizio del tutto diverso, che abbia come obiettivo più alto quello di avviare un processo politico, in altre parole di *cyber diplomacy*, al fine di definire una cornice giuridica e diplomatica di riferimento per rendere più sicuro lo spazio cibernetico.

4. HACKING, UN CONCETTO FONDAMENTALE NEI CONFLITTI MODERNI

di *Pierluigi Paganini*[*]

Prima di addentraci nell'analisi del ruolo dell'*hacking* nell'attuale contesto dell'Information Warfare partiamo da una semplice frase pronunciata da John Chambers, Executive Chairman Cisco Systems al World Economic Forum 2015.

Chambers disse che esistono sostanzialmente due tipologie di aziende, quelle che sono state hackerate e quelle che non sanno ancora di esser state vittime di un attacco. Questa frase riassume perfettamente l'attuale contesto cibernetico in cui ogni azienda e organizzazione è un potenziale obiettivo, ma soprattutto spesso ci si accorge dell'attacco quando è troppo tardi, ovvero nel momento in cui è impossibile porre rimedio a quanto accaduto a causa della complessità dell'offensiva.

Altro concetto apparentemente scontato, ma di cruciale importanza quando si analizzano le minacce cibernetiche, è il fatto che ci si muove in uno spazio virtuale in cui viene meno il concetto di frontiera. Questo aspetto ha notevoli ripercussioni sotto il profilo tecnologico, politico e legislativo.

Nell'attuale scenario stiamo assistendo ad un aumento esponenziale degli attacchi informatici, ma ciò che maggiormente preoccupa è il crescente livello di sofisticazione che rende difficile le attività di individuazione ed attribuzione.

Nuovi paradigmi come l'Internet delle code, *mobile computing*, e *cloud computing* stanno allargando la nostra superficie di attacco in maniera significativa.

[*] Chief Technology Officer presso CSE Cybsec Enterprise S.p.A.; Membro del Gruppo di Lavoro Cyber G7 2017 presso Ministero degli Affari Esteri e della Cooperazione Internazionale; Membro Gruppo Threat Landscape Stakeholder Group ENISA e Collaboratore SIPAF, Ministero Dell'Economia e delle Finanze. Professore presso la Link Campus University.

Le tipologie di attaccanti più pericolosi sono i sindacati criminali e gli hacker che operano per conto di governi. Purtroppo nel cyberspazio esistono molteplici categorie di attaccanti che minacciano i nostri sistemi, compresi gruppi di cyber criminali, agenzie di intelligence, hacktivisti, cyber terroristi e *sript-kiddie* (ovvero individui che utilizzano codici e programmi ideati da altri per attività di hacking e che il più delle volte non hanno particolari capacità tecniche).

Gli eventi osservati negli ultimi mesi nel cyberspazio sono strettamente correlati a quanto accade nella realtà che viviamo, in molti casi si influenzano in maniera reciproca e dall'osservazione dei fenomeni nel mondo virtuale è possibile fare previsioni su quanto sta per accadere nel mondo reale.

Le presidenziali Americane dello scorso anno hanno portato all'attenzione delle masse i possibili effetti di campagna di disinformazione sulla politica di un governo.

Oggi tutto ciò sembra scontato, ma pensate che circa 6 anni fa proposi a Wikipedia il termine *Social Network Poisoning* (https://it.wikipedia.org/wiki/Social_Network_Poisoning) anticipando quando poi stiamo oggi assistendo. La mia lungimiranza mi costò l'esclusione dalla piattaforma Wikipedia. Mentre la voce italiana "Social Media Poisoning" da me scritta è ancora presente, quella inglese fu rimossa ed io fui accusato di proporre contenuti privi di fondamento.

La moderna società si trova quindi impreparata a dover affrontare una nuova tipologia di rischio, quello cibernetico.

Negli ultimi due anni tale rischio è stato incluso nell'annuale rapporto sui rischi presentato nel corso del *World Economic Forum.* Un attacco cibernetico è oggi un evento ad elevata probabilità di occorrenza ed elevato impatto, non solo, il rischio cibernetico è direttamente correlato a rischi di altra natura, come quello geopolitico, economico, tecnologico, sociale ed ambientale.

Figure 1 – World Economic Forum (World Economic Forum)

E se a condurre attacchi cibernetici fossero governi stranieri?

Nel luglio del 2016, nel corso del Summit di Varsavia, la NATO riconosce il cyberspazio come il quinto dominio di guerra, dopo cielo, terra, mare e spazio.

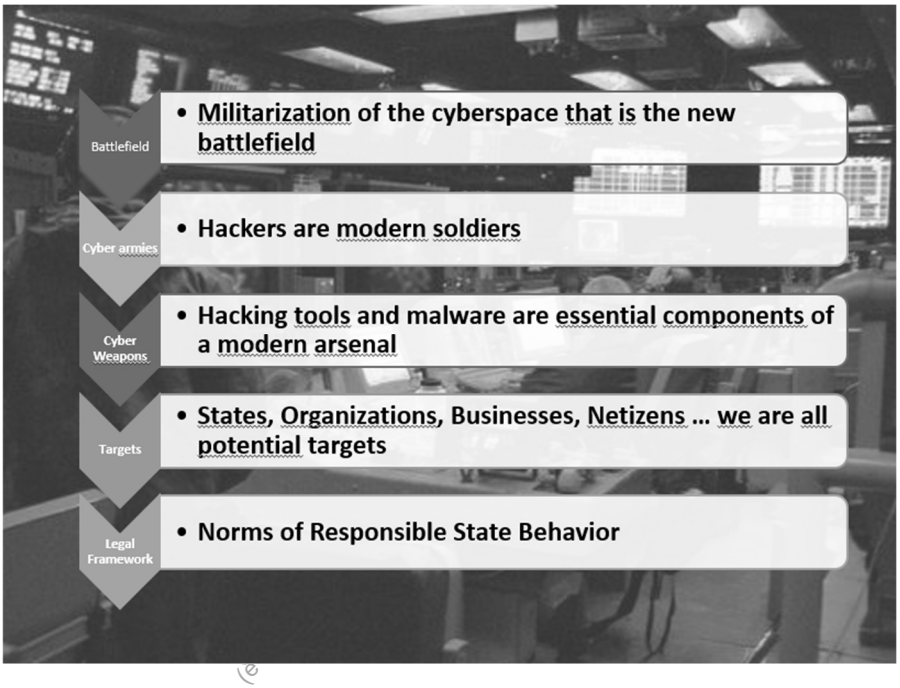
Tutto ciò ovviamente ci induce ad una serie di riflessioni sul moderno concetto di guerra e porta quindi alla genesi del termine Information Warfare, o guerra cibernetica come molti preferiscono chiamarla.

Cambiano radicalmente quindi i concetti di campo di battaglia, eserciti, armi, obiettivi e regole di ingaggio.

Il campo di battaglia diviene quindi il cyberspazio, e gli hacker sono i moderni soldati che utilizzano codici malevoli ed *hacking tool* come armi cibernetiche.

Siamo tutti potenziali obiettivi, stati, aziende private, organizzazioni, e cittadini, per questo motivo sono necessarie regole di comportamento tra stati nel cyberspazio.

Figure 2 – Slide da presentazione apertura lavori G7 Summit Ministero degli Esteri



Stiamo osservando un progressivo e pericoloso fenomeno di militarizzazione del cyberspazio, un attacco cibernetico può avere i medesimi effetti di un attacco cinetico convenzionale.

Un cyber attacco è asimmetrico per natura, istantaneo e può essere condotto in qualunque momento (anche in "tempo di pace") e da ogni dove, tutti fattori che rendono estremamente complessa la risoluzione del problema dell'attribuzione.

Altro elemento di interesse è l'investimento ridotto per l'organizzazione di un attacco informatico che quindi si candida come un'opzione privilegiata

nell'ambito di una strategia militare, talvolta anche solo come elemento di supporto ad azioni cinetiche convenzionali.

I costi ridotti di un cyber attacco stanno attirando nuovi attori nella cyber arena, molti stati come Iran e Nord Corea riconoscendo il cyberspazio come un dominio strategico investono in maniera significativa per incrementare le proprie capacità cyber rappresentando una minaccia persino per le super potenze.

Le armi cibernetiche sono efficaci quanto furtive, l'incapacità di attribuire il loro uso ad uno specifico attore consente all'attaccante di evitare eventuali sanzioni della comunità internazionale.

Un'arma cibernetica ha costi ridotti rispetto alle armi convenzionali e la fase di preparazione è molto più semplice da coprire rispetto ad un'arma convenzionale.

Un'arma cibernetica potrebbe consentire agli stati con minori risorse militari ed economiche di competere con le maggiori potenze internazionali.

L'impegno dei governi nello sviluppo di nuove capacità ed armi di questo genere ha ovvie ripercussioni su qualunque sistema esposto in rete.

Volete un esempio? La falla utilizzata dal virus Stuxnet (CVE-2010-2568), riconosciuto come la prima arma cibernetica della storia ed utilizzato per interferire con il programma nucleare iraniano, nel periodo intercorso tra novembre 2013 and giugno 2014 è stata sfruttata più di 50 milioni di volte in attacchi contro 19 milioni di macchine in tutto il mondo.

Vale a dire, un codice utilizzato da uno stato per attaccare un suo avversario è divenuto poi di dominio pubblico ed è stato utilizzato da una moltitudine di attori in attacchi in rete.

Altro esempio eclatante dei potenziali effetti della militarizzazione del cyberspazio è rappresentato dal *ransomware* WannaCry che ha distrutto sistemi di tutto il mondo all'inizio dell'estate 2017 causando miliardi di dollari di danni ad organizzazioni ed imprese. Il *malware* sfruttava due codici malevoli (DOUBLEPULSAR and ETERNALBLUE exploit) rubati dal gruppo Shadow dall'arsenale dell'agenzia americana NSA.

Come sottolineato in precedenza, in questo nuovo scenario di guerra, gli hacker sono i moderni soldati, le loro capacità cyber sono indispensabili per l'offesa quanto per la difesa. Esistono molteplici profili di hacker, da quelli formatisi nell'underground criminale a quelli esperti addestrati da governi per condurre operazioni di spionaggio e sabotaggio contro i sistemi di stati nemici.

Negli scorsi mesi ho condotto una articolata analisi dei principali profili di hacker molto attivi nell'underground, la maggior parte dei quali giovani con nessuna percezione del crimine informatico.

Questi hacker sono principalmente motivati dal proprio ego, dalla volontà di emergere o di sentirsi parte di un collettivo che ritengono possa combattere un sistema corrotto.

Solo una piccola parte di loro sta pensando di trarre profitto hackerando sistemi in rete, operando per lo più in piccoli gruppi (non più di 5 membri) e molti di loro non hanno un livello di istruzione universitario.

Sorprende il fatto che nella maggior parte dei casi questi giovani hacker non abbiano alcuna idea dei bersagli da colpire.

Per trovarli è sufficiente visitare i principali forum di hacking in rete.

Circa il 25% degli hacker che ho incontrato sembra avere buone capacità tecniche (è in grado di sviluppare un *malware* o sviluppare uno script per condurre un attacco contro uno specifico obiettivo), in un caso mi son trovato dinanzi un esperto in grado di sviluppare un *exploit zero-day*, ovvero di individuare e sfruttare una falla non nota in un sistema da attaccare.

La conclusione alla quale sono arrivato è che le principali comunità di hacker in rete sono facili da infiltrare da parte di attori governativi che potrebbero reclutarli per attacchi diversivi oppure per attività di Psycological Operation, ad esempio attraverso la manipolazione dei social network.

In un contesto come quello descritto urgono norme di comportamento tra stati ed in questa direzione ci siamo mossi in sede G7.

La Dichiarazione adottata dal G7 Esteri a Lucca, di cui sono co-autore, rappresenta un cruciale passo in avanti nella definizione di regole di comportamento tra Stati nel cyberspazio.

Sebbene non si tratti di norme vincolanti, il fatto stesso che i Paesi del G7 siano giunti ad una Dichiarazione condivisa di intenti dimostra l'importanza del tema trattato. La Dichiarazione è stata concepita per promuovere la collaborazione tra Paesi nel fronteggiare le minacce provenienti dal cyberspazio e la stabilità in quello che è riconosciuto essere il quinto dominio del *warfare*. A questo proposito, il documento promuove la cooperazione tra Stati, la condivisione delle informazioni, ed attribuisce a ciascun membro precise responsabilità per l'adozione di misure atte a contenere le minacce cibernetiche.

Gli eventi recenti dimostrano l'urgenza di regole condivise e la necessità di stabilire un tavolo di lavoro permanente sulle tematiche cyber. Nel corso dei mesi in cui siamo stati impegnati nella stesura della dichiarazione si è

spesso discusso di temi come armi cibernetiche e relativa proliferazione. Sebbene nella dichiarazione finale non si trovi esplicito riferimento a questa nuova generazione di armamenti, le regole proposte e condivise hanno come scopo quello di promuovere una discussione tra Stati anche su questo fronte.

5. UNA CONVENZIONE DIGITALE DI GINEVRA PER IL CYBERSPACE

di *Pier Luigi Dal Pino*[*]

Come ricordato dal Presidente di Microsoft Corporation Brad Smith durante i lavori delle Nazioni Unite a Ginevra il 10 novembre, la cyber security è diventata chiaramente una delle questioni più importanti del nostro tempo. Stiamo assistendo ad una corsa agli armamenti informatici da parte di nazioni che investono nello sviluppo di una nuova generazione di armi destinate ai governi per scopi militari e civili (*Dual use*). Questi investimenti stanno generando elevate capacità offensive nello spazio cibernetico; assistiamo inoltre ad attacchi da parte degli stati contro i civili.

Mentre la tecnologia continua a rimodellare il mondo, è chiaro che i conflitti tra le nazioni non sono più limitati alla terra, al mare, all'aria e allo spazio extra atmosferico. Il mondo ha bisogno di nuove regole internazionali per proteggere il pubblico da minacce che sorgono nella nuova dimensione: lo spazio cibernetico. In breve, il mondo ha bisogno di una Convenzione Digitale di Ginevra (*Digital Geneva Convention*), un insieme di norme ed accordi internazionali volti a proteggere e difendere i civili dagli attacchi.

Nel maggio 2016, l'attacco di *ransomware* WannaCry, presumibilmente sponsorizzato da attori statali, ha colpito più di 200.000 computer in più di 150 paesi e ha mostrato al mondo l'ampio danno che le armi cyber "invisibili" possono infliggere. Questo non ha causato soltanto danni ai macchinari informatici ma ha avuto anche pesanti ripercussioni sui servizi da essi forniti Ad esempio, l'Ufficio di Revisione Nazionale del Regno Unito, infatti, ha recentemente concluso un'analisi sull'impatto di WannaCry, che ha costretto il Servizio Sanitario Nazionale a deviare le ambulanze ed annullare oltre 19.000 appuntamenti per persone bisognose di vedere un medico o di

[*] Direttore Centrale relazioni istituzionali ed industriali di Microsoft Italia ed Austria.

sottoporsi ad un intervento chirurgico. WannaCry ha rappresentato un importante campanello di allarme nel mondo ed ha messo in luce debolezze rilevanti per la sicurezza nazionale. Mentre le aziende tecnologiche come Microsoft hanno una responsabilità primaria e si trovano, a tutti gli effetti, in prima linea nell'affrontare queste problematiche, sarebbe un errore pensare che il settore privato sia in grado da solo di impedire o arrestare il rischio di attacchi cyber. Si richiede dunque uno sforzo comune ed una collaborazione forte fra pubblico e privato. WannaCry ha messo inoltre in luce la necessità di dotarsi di norme ed accordi internazionali per proteggere i civili come già posto in evidenza. Emerge quindi l'esigenza di costruire regole condivise e diffondere la consapevolezza sulla tematica.

5.1. Un accordo giuridicamente vincolante

Sebbene nessun accordo internazionale sia mai perfetto, il mondo ha già tratto benefici e visto importanti miglioramenti grazie alla stipula di convenzioni globali, come dimostrato dal Trattato sulla Non Proliferazione delle Armi Nucleari e dalla Convenzione sulle Armi Chimiche. Una Convenzione Digitale di Ginevra creerebbe un quadro giuridicamente vincolante per governare il comportamento degli stati nel cyberspace. Sebbene ci sia urgenza nel rispondere ad aspettative emergenti, è possibile procedere su misure condivise passo dopo passo, e in misura sempre crescente, al fine di prediligere degli accordi realmente condivisi e in maniera sempre più estesa a tutti gli aspetti che la gestione del cyberspace richiede. Ci sono infatti già importanti opportunità per progredire verso un accordo giuridicamente vincolante attraverso iniziative volontarie o politicamente vincolanti. Già in passato i governi hanno stabilito e messo in pratica regole internazionali in vari settori come, appunto, la non proliferazione. Allo stesso modo si dovrebbe procedere nello spazio cibernetico. Le clausole principali che costituiscono l'essenza della Convenzione Digitale di Ginevra dovrebbero impegnare gli Stati parte ad evitare attacchi verso sistemi la cui distruzione non solo avrebbe effetti negativi sulla sicurezza dei cittadini, ma comprometterebbe altresì i benefici di una società globalmente connessa. Per questo è necessario che le regole possano definire l'accettabilità o l'inaccettabilità di alcuni comportamenti, ponendosi l'obiettivo di ridurre i rischi, aumentare la prevenzione e la prevedibilità di alcune pratiche, e limitare gli impatti pericolosi, soprattutto

per quanto riguarda le attività governative che potrebbero portare ad una vera e propria guerra. Tali norme possono assumere due forme differenti, a seconda che siano volte ad aumentare le capacità di difesa, per ridurre il rischio di attacchi, o norme che possano limitare le operazioni di conflitto o offensive, destinate a ridurre i confitti, evitando escalation e limitando impatti potenzialmente catastrofici nello spazio cibernetico.

Tra le più importanti è possibile menzionare le seguenti:

- astenersi dall'inserimento di "*backdoor*" nei prodotti della tecnologia commerciale di massa;
- accettare una politica chiara per acquisire, conservare, proteggere, utilizzare e segnalare le vulnerabilità;
- esercitare una limitazione nello sviluppo di armi informatiche, garantendo di mantere il controllo delle loro armi in ambiente sicuro;
- acconsentire a limitare la proliferazione delle armi informatiche;
- limitare l'impegno in operazioni offensive per evitare danni di massa ai civili ed impegnarsi in sole attività difensive;
- assistere gli sforzi del settore privato per individuare, contenere e rispondere ad attacchi cyber.

Passare da norme politicamente vincolanti a norme giuridicamente vincolanti richiederà tempo e impegno; alcuni responsabili politici potrebbero dunque vedere tali proposte troppo idealiste, a discapito di un approccio realista. Anche se fare progressi significativi sarà una sfida, specialmente se i cambiamenti demografici, politici ed economici metteranno alla prova i modelli tradizionali di collaborazione, siamo tuttavia ottimisti che, attraverso il dialogo e lo sviluppo di pratiche condivise, alcune norme di cyber security possono evolvere nel diritto internazionale consuetudinario nel tempo. Al contrario, le conseguenze dell'inazione sono inaccettabili. I mondi politico, diplomatico, accademico e industriale devono impegnarsi a proteggere le funzioni vitali dello spazio cibernetico in modo che la società possa continuare a realizzare i considerevoli vantaggi economici e sociali che le tecnologie consentono.

5.2. Tech Accord

È importante che anche l'industria del digitale faccia la sua parte, ponendo le basi per un accordo tecnico (*Tech Accord*) volto a proteggere le persone nello spazio cibernetico. L'industria digitale, infatti, non solo riveste

un ruolo preponderante in termini di capacità e di competenze nella gestione della cyber security, ma è solitamente in prima linea nella reazione e gestione di attacchi informatici. Alla luce di queste competenze e di questa posizione, assume la forma di un processo naturale quello di convogliare l'industria digitale nelle connotazioni e nelle regole da conferire allo spazio cibernetico. L'inclusione, e quindi il raggiungimento, del *tech accord* dovrebbe poggiare su due pilastri: un rapporto di fiducia dell'industria digitale con gli utenti e la promozione di un approccio difensivo. Per quanto attiene al primo punto, la gente deve potere riporre fiducia nella tecnologia, nei creatori della tecnologia, e quindi dell'industria digitale, e nel cyberspazio stesso, idealmente basato su regole condivise. Questa fiducia è essenziale per i consumatori e le imprese per continuare a lavorare, acquistare, imparare e interagire grazie ad Internet: tale rapporto di fiducia che gli utenti si impegnano a costruire con le aziende tecnologiche condurrebbe a notevoli vantaggi, sia per sé stessi, sia per le loro comunità e le loro economie. Viceversa è quindi importante che i fornitori di tecnologia agiscano per creare un ambiente affidabile per gli utenti di Internet, accettando e sostenendo una serie di principi e comportamenti comuni per proteggere i civili nel cyberspazio a partire dallo sviluppo di software di natura difensiva e non offensiva. La fiducia, la tutela della privacy e la trasparenza costituiscono i principi su cui incardinare i due pilastri sopracitati e saldare la collaborazione tra Stati e industria digitale nel cyberspazio per il fine ultimo della protezione dei civili. L'industria svolge dunque un ruolo fondamentale nel mantenere stabile, aperto e sicuro il cyberspazio, ed è in quest'ottica che il settore privato deve avviare dei partenariati e delle collaborazioni con il settore pubblico, in particolare le istituzioni governative.

Un accordo tecnologico funzionale dovrebbe basarsi su una varietà di input provenienti da una vasta gamma di partner industriali; questi attori dovrebbero essere in grado di adattarsi rapidamente all'evoluzione tecnologica per riuscire a far fronte ad una realtà in costante evoluzione che richiede sempre più la condivisione di idee e una presa di impegni condivisa. Come punto di partenza, un accordo tecnico potrebbe essere fondato su sei obiettivi comuni.

1. **Nessuna assistenza per le operazioni offensive in rete**: le aziende tecnologiche globali dovrebbero astenersi dall'aiutare i governi ad attaccare l'infrastruttura di informazioni di qualsiasi cliente in qualsiasi parte del mondo. Dovrebbero altresì convenire che non aiuteranno alcun governo a sfruttare o compromettere i prodotti e servizi tecnologici commerciali e di massa.

2. **Assistenza per proteggere gli utenti in tutto il mondo**: le aziende tecnologiche globali dovrebbero impegnarsi a proteggere i clienti, emettendo patch per i loro prodotti e servizi destinati a tutti gli utenti, di fatto salvaguardandoli da rischi.
3. **Collaborazione per rafforzare gli sforzi di risposta**: le aziende tecnologiche globali dovrebbero impegnarsi a collaborare per proteggere gli utenti in modo proattivo contro i attacchi cyber e per ridurre al minimo la durata e l'impatto di questi. Una maggiore collaborazione in tutto il settore aumenterebbe l'efficacia della risposta collettiva e renderebbe l'ecosistema tecnologico più sicuro per gli utenti.
4. **Sostenere gli sforzi di risposta dei governi**: le aziende tecnologiche globali dovrebbero sostenere gli sforzi del settore pubblico nell'identificazione, prevenzione, rilevazione, risposta e recupero in caso di incidenti verificatesi nello spazio cibernetico.
5. **Coordinamento per affrontare le vulnerabilità**: le aziende tecnologiche globali dovrebbero impegnarsi a collaborare per affrontare i problemi di sicurezza, le cosiddette vulnerabilità. La segnalazione e la gestione di quest'ultime, condotte in modo coordinato, consentirebbero di proteggere meglio gli utenti, riducendo al minimo il rischio di sfruttare queste falle. A tal fine, emerge chiaramente la necessità di dotarsi di procedure quanto più coordinate e condivise tra gli attori parte della convenzione per aver un sistema di gestione delle vulnerabilità armonico.
6. **Combattere la proliferazione delle vulnerabilità**: le aziende tecnologiche globali dovrebbero impegnarsi a non trafficare in vulnerabilità informatiche per scopi offensivi, né dovrebbero abbracciare modelli di business che implichino la proliferazione di vulnerabilità informatiche per scopi offensivi. Per contrastare la minaccia causata da vulnerabilità *zero-day* disponibili sul mercato nero, l'industria tecnologica dovrebbe sfruttare programmi pubblici di cyber security per disinnescare eventuali *bugs* in grado di fornire il riconoscimento ed una compensazione destinata agli individui che segnalano bug, in particolare quelli che si riferiscono a vulnerabilità di sicurezza.

5.3. Un'organizzazione internazionale di attribuzione

L'altro aspetto promosso nella Convenzione è la necessità di creare un'organizzazione internazionale di attribuzione (*Attribution Organization*) dei cyber attacchi su scala globale, volta a rafforzare la fiducia degli utenti nei confronti del digitale. Infatti, se nel mondo "reale" quando qualcuno ruba o danneggia la proprietà fisica, gli investigatori possono raccogliere prove e coinvolgere i tribunali, nel mondo "digitale" le prove di cyber attacchi sono spesso difficili da recuperare, considerato anche il numero limitato di esperti, in settori pubblici o privati, capaci di reperirle. Inoltre, se un attacco cibernetico è sponsorizzato da uno stato, dimostrare la responsabilità diventa una sfida ancora più complessa. L'incremento sia quantitativo che qualitativo degli attacchi informatici ha dimostrato l'impellente necessità di creare un organismo di attribuzione. Ad oggi non esiste un'organizzazione indipendente che possa presentare un'analisi politicamente neutrale e basata sui fatti verificatisi. La responsabilità deve seguire l'attribuzione dell'attacco e sulla base di queste informazioni, gli Stati devono potere analizzare come agire.

Il mondo ha quindi bisogno di un'organizzazione o una struttura che possa ricevere e analizzare prove relative a un sospetto attacco cibernetico, e che possa essere in grado di individuarne i responsabili grazie ad esempio ad una collaborazione pubblico privata. L'esperienza delle imprese di tecnologia nel settore privato potrebbe infatti fungere da base per questa organizzazione di attribuzione non politica. La capacità di questi attori di raccogliere ed analizzare i dati provenienti da attacchi cibernetici è migliorata notevolmente negli ultimi anni. I fornitori di servizi online egli analisti esperti in sicurezza sono ora in grado di identificare alcuni attacchi di cyber crime lanciati da stati o da proxy sponsorizzati da stati. Abilitando queste aziende a collaborare, combinare e confrontare i dati con un'organizzazione di attribuzione, si rafforzerebbe la fiducia della società civile nell'organizzazione stessa. L'organizzazione di attribuzione dovrebbe essere costituita principalmente da esperti del settore privato in *cyber-forensics* e discipline correlate, in grado di analizzare le tecnologie e le tecniche di un attacco. Il lavoro di ricerca ed analisi potrebbe essere altresì supportato dagli strumenti resi disponibili dalla tecnologia cloud, assicurando così che le prove relative a particolari attacchi siano raccolte e presentate in modo da essere utilizzate da esperti governativi e da essere comprese dal pubblico. Gli accordi tra l'organizzazione di attribuzione e le imprese del settore privato sarebbero

fondamentali e, se oculatamente costruiti, non potranno che condurre a benefici collettivi.

Dal momento che un'iniziativa come la Convenzione Digitale di Ginevra potrebbe richiedere un decennio per svilupparsi, potrebbe essere necessaria un'azione più veloce, basata ad esempio su strumenti già esistenti come la Carta delle Nazioni Unite e la Quarta Convenzione di Ginevra. Tutto ciò comporterebbe la collaborazione con organizzazioni internazionali, come il gruppo di esperti governativi per gli sviluppi delle Nazioni Unite (UNGGE), il G7 e l'Organizzazione per la sicurezza e la cooperazione in Europa (OSCE). È quindi necessario un approccio multi-stakeholder per potere gestire una realtà complessa come quella del cyberspazio, funzionale a convogliare gli sforzi dei diversi attori coinvolti. Ad esempio, costituito nel luglio 2017 da *Facebook, Microsoft, Twitter* e *YouTube*, il Global Internet Forum per la lotta al terrorismo (GIFCT) formalizza e struttura le modalità di collaborazione di queste aziende per ridurre la diffusione del terrorismo e dell'estremismo violento nei servizi per gli utenti. Basandosi sui lavori avviati all'interno dell'European Internet Forum dell'Unione Europea, il GIFCT sta promuovendo una collaborazione con aziende tecnologiche più piccole, gruppi della società civile, accademici e governi. Per raggiungere questo obiettivo, stiamo unendo le forze attorno a tre strategie: impiegare e sfruttare la tecnologia, condividere conoscenze, informazioni e buone pratiche, e condurre lavori di ricerca ed analisi. Ad esempio, il G7 dei Ministri dell'Interno sul terrorismo online tenutosi sotto la Presidenza italiana ha previsto un tavolo di lavoro a cui hanno partecipato sia i ministeri interessati, sia le aziende tecnologiche, costituendo un ulteriore passo verso la costruzione di un dialogo virtuoso tra le istituzioni e l'industria digitale volto a creare collaborazioni efficienti.

In conclusione, un accordo tecnologico fra tutte le imprese informatiche che offrono servizi e soluzioni digitali dimostrerebbe l'impegno del settore privato ad elaborare un insieme comune di principi e comportamenti per proteggere i civili nello spazio cibernetico. Ciò non significa solamente accordarsi su azioni che l'industria dovrebbe prendere o non prendere, ma anche condividere obiettivi e sforzi collaborativi per migliorare la difesa informatica.

Chiunque dipenda dal cyberspazio deve essere in grado di aver fiducia nella tecnologia che utilizza. Mentre i governi dovrebbero agire, adottando una Convenzione Digitale di Ginevra per proteggere i civili nel cyberspazio in tempi di pace, il settore tecnologico dovrebbe intraprendere i propri passi per aumentare tale fiducia. È responsabilità condivisa promuovere, anche in

modo proattivo, un Internet più tranquillo e sicuro ed in questo un accordo tecnologico sarebbe di grande aiuto a progredire.

Queste sfide sono fasi naturali e comprensibili di quello che inevitabilmente si presenta come un processo lungo e complesso. Man mano che i dibattiti emergono su norme esistenti e nuove minacce, sarà importante che esperti del settore governativo, della società civile, del settore privato e del mondo accademico aiutino a identificare le lacune esistenti ed a implementare nuove tecnologie e approcci per prevenire i continui danni ai civili da parte dei criminali informatici. La tecnologia ha fatto molta strada dai tempi dei fucili e dei cannoni, tuttavia un bisogno resta costante: mentre la tecnologia evolve, il quadro normativo e le regole comuni devono evolvere con essa. Come nell' Ottocento, il settore privato è nuovamente il motore propulsore di un cambiamento e si fa portavoce dell'esigenza che i governi creino una nuova cornice normativa. Questo va di concerto con la richiesta di un incremento della partnership pubblico-privato, che possa lavorare su accordo tecnologico più formale per agire in modo efficace e in modo responsabile a livello globale. Abbiamo bisogno che i governi agiscano insieme, sia per aderire alle attuali norme internazionali sia per creare nuove leggi in grado di colmare le lacune esistenti. Il mondo ha bisogno di una Convenzione Digitale di Ginevra, così come altre iniziative, per garantire un mondo più sicuro.

6. LA CYBER SECURITY NELL'ERA COGNITIVA: I RISCHI PER LE IMPRESE E PER IL SISTEMA PAESE

di *Domenico Raguseo*[*]

Il *cybercrime* e, più in generale, furto e compromissione di dati sono oggi tra le priorità dei vertici manageriali di imprese di ogni settore e dimensione. Particolarmente attente a questi temi, e ai rischi che ne derivano, sono le organizzazioni governative, l'industria della produzione e distribuzione energetica che, come emerso dal recente G7, a livello mondiale vi stanno dedicando sempre maggiori attenzione e risorse. Le ragioni sono evidenti, in quanto attacchi a infrastrutture critiche, come ad esempio quelli realizzati utilizzando *malware* come Stuxnet o Shamoon ad impianti per la fornitura di carburanti, di elettricità o di acqua potabile, sono in grado di causare danni che vanno al di là di quelli strettamente economici, arrivando a toccare valori come la salute ed il benessere di intere comunità.

Quindi la resilienza delle infrastrutture critiche rispetto ad attacchi cyber deve essere obiettivo prioritario delle organizzazioni e dei settori d'industria di appartenenza. E anche del Sistema Paese.

IBM ha un punto di osservazione importante sulla Cyber security: IBM X-Force Research, uno dei gruppi di ricerca sulla sicurezza aziendale più rinomati al mondo. Questi professionisti di sicurezza monitorano e analizzano problemi che provengono da numerose fonti, alimentando con il proprio contenuto di *threat intelligence* il portafoglio di soluzioni e prodotti di IBM Security. I risultati della Ricerca di IBM X-Force vengono anche condivisi attraverso report periodici.

Il report IBM X-Force Threat Intelligence Index del 2017 è basato sulle osservazioni di oltre 8.000 clienti in ambito security monitorati nel 2016 in 100 paesi e su dati ricavati, sempre nel 2016, da dati esterni raccolti e

[*] Manager of Europe Technical Sales IBM Italia.

analizzati dal team X-Force, monitorando oltre otto milioni di attacchi di spam e di *phishing* ogni giorno e analizzando al contempo più di 37 miliardi di pagine ed immagini web.

Il dato che emerge nel 2017 è che il numero dei record compromessi ha raggiunto un valore storico, passando da 600 milioni a oltre 4 miliardi. I criminali informatici hanno introdotto nuove tecniche, ma soprattutto emerge un cambiamento nelle strategie dei criminali informatici: oltre a prendere di mira, informazioni strutturate come numeri di carte di credito, password e dati sanitari personali, abbiamo osservato violazioni di dati non strutturati, quali archivi di e-mail, documenti aziendali, proprietà intellettuale e codici sorgente.

I *malware* sono sempre più dei *framework* di codice malevolo che possono essere costruiti utilizzando diverse componenti reperibili spesso sul dark web. Exploit di vulnerabilità specifiche, componenti per criptare i dati sottratti, componenti e servizi per chiedere il riscatto hanno fatto diventare i *ransomware* una vera e propria attività di business criminale, con organizzazioni strutturate con personale dedicato alla Ricerca e Sviluppo, al supporto e ai servizi, dove la decisione di *make or buy* delle componenti fa parte di un disegno strategico. Quindi una strategia chiara e l'industrializzazione del servizio stanno alla base dei *ransomware*, come Wannacry e Petya, che quest'anno hanno catturato l'attenzione dell'opinione pubblica per i danni causati a servizi critici di diversi settori, da quello sanitario a quello industriale.

Tuttavia i rischi di cyber security non dipendono solo dai *ransomware*. L'Internet delle cose e i processi di digitalizzazione delle fabbriche, delle industrie e, sempre più, delle imprese in generale comporta l'inteconnessione tra prodotti e sistemi che sono oggi un bersaglio appetibile per i cybercriminali. Si pensi, ad esempio, alla integrazione fra *Information Technology* (IT) e *Operation Technology* (OT) che molte industrie hanno realizzato o stanno realizzando, ai sistemi SCADA (*Supervisory Control And Data Acquisition*) e ai sistemi di domotica: sono questi nuovi ulteriori contesti di potenziale attacco.

L'industria energetica e il settore delle Utility, per tornare al tema della cyber security nelle infrastrutture critiche, racchiudono diverse tipologie di organizzazioni, dalle centrali elettriche fino alle società di gestione della fornitura di acqua potabile, ognuna delle quali ha delle proprie specificità. Sebbene secondo il report IBM X-Force del 2016 il settore delle *Utility* non rappresentava l'industria con maggiori attacchi, nel 2017 è stato riscontrato un notevole incremento in questo ambito. Infatti, in aggiunta agli attacchi volti alle infrastrutture critiche, si sono verificati episodi che, compromettendo la

parte tradizionale di IT, hanno riguardato in qualche aspetto le operazioni a livello di OT. Questa non è di per sé una novità, in quanto anche lo stesso Stuxnet è stato costruito su vulnerabilità di sistemi IT tradizionali. Dagli attacchi DdoS dell'industria energetica Ucraina ai sistemi di ventilazione e raffreddamento in Finlandia, passando per il *ransomware* che ha costretto un'industria nel Michigan a pagare $25,000 per avere accesso a utenze critiche e a email server, si può comprendere come attacchi a sistemi IT tradizionali possano oggi arrecare danni anche ai sistemi OT più critici, in quanto non sono più separati e distinti dall'IT come in passato, ma anzi sempre più integrati. Integrazione che, se da un lato fornisce un indubbio miglioramento nella fornitura del servizio, dall'altro rende il servizio più esposto al cyber crime. Gli incidenti in questi settori critici spesso non sono resi pubblici. Tuttavia nel 2017 abbiamo notato attraverso X-Force un numero di casi leggermente superiore rispetto a quelli registrati nel 2016. Da questi emerge che sorgenti esterne hanno preso di mira sistemi SCADA di una centrale di energia in Ucraina per provocare una mancanza di energia a Kiev, forzando gli operatori a ripristinare il servizio manualmente. Una rete ucraina è stata danneggiata utilizzando il *malware* Black Energy, compromettendo le credenziali per accedere ai sistemi SCADA dall'esterno. Più recentemente sembra che con NotPetya[1] si sia voluto colpire anche agenzie governative, compagnie di trasporti, sistemi di controllo distribuito (DCS) e PLC (*Programmable logic controller*) a servizio dell'Industria energetica e di utility.

I sistemi SCADA rappresentano in genere un sottoinsieme dei sistemi di controllo industriale (ICS). La gran parte delle configurazioni ICS, che includono i sistemi SCADA, i sistemi di controllo distribuito e PLC, sono presenti nel mercato della produzione di energia e distribuzione in genere.

Il *malware* che si focalizza sui sistemi di controllo industriale ICS rappresenta un vettore che gli hacker usano per compromettere l'industria energetica. CrashOveride, conosciuto anche come Industroyer, è uno dei più recenti di questa famiglia. Questo *malware* è capace di controllare direttamente gli *switches*, modificando i dati e causando *Denial of services* (DoS) dei dispositivi compromessi. Questo e altri tipi di *malware* hanno fatto sì che i ricercatori di IBM X-Force riscontrassero un aumento degli attacchi del

[1] Leb L., NotPetya Operators Installed Three Backdoors on M.E.Doc Software Server Before Activating Malware, Security Intelligence, 10th July 2017. Available at: https://security intelligence.com/news/notpetya-operators-installed-three-backdoors-on-m-e-doc-software-server-before-activating-malware/.

110% nel 2016 rispetto al 2015. A metà del 2017 avevamo già raggiunto i livelli riportati nel 2016 per attacchi di questo tipo.

Considerata la vastità e la diversità degli attacchi, è importante che l'attenzione di responsabili e ricercatori in cyber security sia volta a determinarne l'origine al fine di ottimizzare gli investimenti sugli interventi di prevenzione, quando possibile, e di difesa. La prima cosa da verificare è se gli IP sorgenti e destinatari di attacchi sono interni o esterni all'organizzazione. I dati di IBM Managed Services evidenziano che nel settore Energy e Utility il 60% degli attacchi è compiuto da 'esterni' mentre il restante 40% è causato da 'insider'; di questi, il 24% fa riferimento a utenti che hanno causato problemi inavvertitamente. Gli insider che volontariamente compiono reati di questo tipi sono spesso collegati a stati nemici o a concorrenti. Attacchi commissionati da nemici, inclusi gli *Advanced Persistent Threat* (APT)[2], potrebbero per esempio essere diretti a ottenere i dati dei sistemi SCADA per determinare il flusso dell'energia e identificare eventuali vulnerabilità, arrivando fino a sostituire delle parti del Grid.

Non è difficile immaginare i danni che possono conseguirne. Con quasi la metà degli attacchi interni causati da persone che inavvertitamente creano questi problemi, l'industria dell'energia deve preoccuparsi non solo di potenziali attacchi esterni, ma anche del personale interno che per disattenzione espone i servizi al cyber crime.

Le vittime spesso aprono attachment malevoli ricevuti tramite email, rendendo possibile l'exploit di questi target. In un incidente avvenuto nel dipartimento di ricerca nucleare di un'università giapponese, migliaia di file sono stati rubati in otto mesi. Il tutto a causa di un dipendente che ha aperto una email malevola, infettando il proprio PC. Recentemente alcune centrali nucleari in USA sono state vittime di attacchi di tipo Watering Hole mediante una campagna di *spear-fishing* dove un documento word era infetto[3].

Le metodologie di attacco più comuni in questo settore sono:

- *Inject unexpected items* sembra essere quella più comune e include l'injection di dati errati per danneggiare un sistema;

[2] Si fa riferimento ad APT ogni qual volta un hacker prova diverse metodologie e processi per attaccare il suo target.

[3] *At risk: the energy and utilities sector infrastructure*, IBM X-Force Research. Available at: https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=SEL03135USEN&.

- *Command Injection* comprende: OS CMDi e SQLi. OS CMDi comprende anche l'exploit della vulnerabilità che prende il nome di Shellshock;
- altra categoria è quella legata a raccolta e analisi fraudolenta di informazioni: l'attaccante è in grado di acquisire l'identità digitale (sistemi operativi, vulnerabilità, architettura) che viene poi utilizzata per facilitare attacchi successivi. Attacchi di questo tipo sono comuni anche ad altri tipi di industria. Elemento fondamentale che serve agli hacker per disegnare una campagna di attacco è la conoscenza delle caratteristiche di ciò che si vuole attaccare. Stuxnet ha compromesso i PLC di una centrale nucleare acquisendo informazioni sulla identità digitale del suo target;
- altre metodologie di attacco consistono nell'abusare di una funzionalità, fino a renderla inservibile, modificare la struttura dei dati o comprometterne i processi di autenticazione e gestione delle identità;
- un'altra tecnica è quella nota come *man-in-the-middle*, nella quale gli attaccanti intercettano e modificano i messaggi tra due persone o sistemi;
- infine, le tecniche di compromissione delle risorse che i sistemi devono accedere, come *click jacking* e *brute force*.

Nel mondo del cyber crime ci sono degli eventi che passeranno alla storia. Se Stuxnet ha dimostrato che i sistemi industriali possono essere attaccati anche quando chiusi, Mirai[4] ha spiegato al mondo quanto insicuro possa diventare l'IoT quando i dispositivi introdotti e connessi non sono oggetto di un'accurata analisi del rischio. Infatti con Mirai, un *malware* che per la sua peculiarità e per l'impatto sul mercato ha una raggiunto una grandissima notorietà, sono state compromesse delle telecamere con l'obiettivo di disporre di migliaia di *botnet* per un attacco di tipo DDoS. La particolarità di questo attacco è relativa non solo al fatto che dispositivi IoT siano stati compromessi, ma soprattutto al fatto che hanno funto da tramite per attaccare terze parti. Un attacco di questo tipo, non sofisticato dal punto di vista tecnologico, ha messo a nudo un aspetto fondamentale: i controlli di sicurezza vanno identificati a prescindere dal valore dell'*assets* o del servizio. Infatti una telecamera può avere un costo

[4] Bonderud D., *Leaked Mirai Malware Boosts IoT Insecurity Threat Level*, Security Intelligence, 4th October 2016. Available at: https://securityintelligence.com/news/leaked-mirai-malware-boosts-iot-insecurity-threat-level/.

contenuto o fornire un servizio limitato, ma può essere utilizzata per un attacco importante e causare danni di grande valore.

Com'è possibile quindi ridurre il rischio in generale? Maggiore attenzione va prestata nella definizione e implementazione dei controlli di sicurezza. E non solo dal punto di vista tecnologico, ma anche dal punto di vista dei processi. Con riferimento al famoso *malware* Wannacry, le aziende colpite non sono state quelle che non avevano identificato gli opportuni controlli di sicurezza, bensì quelle che non avevano implementato un SOC o i processi CSIRT. Infatti se a essere violati sono stati diversi controlli di sicurezza, incluso la mancanza di backup dei dati, sicuramente l'integrazione dei controlli per identificare quanto prima l'eventuale violazione del controllo, è importante tanto quanto l'implementazione del controllo stesso. IBM ha deciso di rappresentare tutti i controlli di sicurezza come un sistema immunitario, dove ogni controllo è rappresentato da un atomo del sistema ed è collegato a tutti gli altri controlli. L'utilizzo di tecnologie cognitive è un elemento fondamentale nell'individuazione di controlli di sicurezza e di processi sempre più efficienti. Infatti esiste una differenza sostanziale tra il crimine informatico e quello reale: nel mondo virtuale, spesso una traccia viene lasciata, piccola ma viene lasciata. Come trovare le giuste informazioni in una moltitudine di dati e gestirle? Sicuramente da anni si è compreso che la sicurezza perimetrale può essere efficace nella *detection*, ma meno nell'analisi dell'incidente. Per fare un'analisi è necessario osservare cosa accade all'esterno, dove troviamo enormi quantità di dati, spesso non strutturati. Pertanto trovare la traccia vuol dire avere capacità di comprendere il linguaggio naturale, analizzare tutti questi dati e utilizzare algoritmi di *machine learning*. Le tecnologie cognitive rendono oggi tutto questo possibile.

È infine molto importante diffondere una maggiore consapevolezza sui temi della cyber security. A tal fine è necessario investire nello sviluppo di una maggiore cultura della tematica, che deve partire dalle scuole e proseguire poi all'interno delle aziende in un'ottica di formazione continua. Con la cultura di base si ovvia a rischi elementari, come lasciare utenze e password scritte su foglietti volanti. Oltre a questo è tuttavia fondamentale che i CISO (*Chief Information Security Officer*) in atto politiche e soluzioni per la governance delle identità e degli accessi.

La condivisione di informazioni è sempre importante a tutti i livelli, fra istituzioni, aziende clienti fino ai vendor fornitori di sicurezza. IBM con X-

Force Exchange mette a disposizione della comunità, dal 2015, tutto il contenuto informativo sul cyber crime che ha a disposizione.

La nuova era della sicurezza informatica è quella della cognitive security, caratterizzata da una generazione di sistemi in grado di comprendere, ragionare e apprendere le sfide in continua evoluzione. Con tali sistemi gli analisti hanno la possibilità di aumentare, e persino automatizzare, la loro comprensione di una minaccia rendendo più rapida l'individuazione di connessioni tra dati e strategie correttive. IBM ha iniziato a integrare comportamenti istintivi e competenze di sicurezza in nuovi strumenti difensivi, capaci di analizzare report di ricerca, testi web, dati sulle minacce, e altri dati non strutturati, che non vengono intercettati dai sistemi tradizionali. Nella lotta contro il moderno cyber crime, gli analisti di sicurezza devono agire sempre più rapidamente e diventa quindi imprescindibile avvalersi di tali tecnologie e competenze d'avanguardia.

7. IL RUOLO DELL'ITALIA NELLA SICUREZZA CIBERNETICA: MINACCE, CONSAPEVOLEZZE, RISPOSTE, SPERANZE

di *Giulio Massucci*[*]

Oggi siamo consapevoli di vivere in una società ove l'informatica è ovunque, ed è parte integrante delle nostre vite. Ora, sappiamo che i computer controllano ogni cosa: automobili e telecomunicazioni, le infrastrutture delle Nazioni, la difesa fisica e le apparecchiature militari. Hardware e software governano missili, satelliti, rete di difesa nucleare, e sono il mezzo che ci garantisce alcuni beni e servizi essenziali, come elettricità, acqua, cibo.

Partecipiamo ad una evoluzione digitale in ogni settore di business e nelle nostre vite, che ci offre opportunità e facilitazioni, ma che al contempo ci espone a rischi prima sconosciuti ed a minacce sempre più diffuse, e sempre meno prevedibili.

Il futuro è quindi già qui, ma non è sempre accogliente come avremmo sperato.

Virus, malware, cyber-attack, ransomware scopriamo fenomeni in ascesa che dipingono uno scenario preoccupante, e sempre più presente nelle nostre esistenze. Ci ritroviamo sempre più interdipendenti con le tecnologie informatiche, e così vulnerabili a tutti i livelli, Nazioni, Imprese, Individui.

A livello geopolitico, abbiamo imparato che i conflitti non hanno più confini fisici e geografici. E se di confini si può parlare, questi sono confini digitali, e il cyberspazio è un nuovo campo di battaglia.

Il potenziale delle armi informatiche è estremamente vasto, ed in continua e rapidissima evoluzione, e gli attacchi cyber possono bloccare aziende, produzioni, servizi essenziali, oppure trafugare dati riservati e segreti industriali, con impatti diretti su intere economie e Stati sovrani, ed è quindi di estrema importanza difendere tutto il nostro ecosistema cibernetico.

[*] Chief Executive Officer AVENURE.

Purtroppo le armi informatiche non sostituiscono in toto le armi fisiche e nucleari, bensì si aggiungono alle molteplici soluzioni di offesa, e sono quindi anche armi in più nell'arsenale terrorista (e non) già presente. Ne consegue un aumento del rischio di scatenare conflitti, perché la mancanza di separazione tra mondo digitale e mondo fisico, comporta che un conflitto digitale può trasformarsi in un conflitto armato e distruggere il mondo fisico.

Nel corso dei secoli le tecnologie militari sono riuscite a conservare o distruggere la pace nel mondo. Le innovazioni militari, fin dalla notte dei tempi, hanno garantito periodi di stabilità. Basti pensare alle tecniche ed alle attrezzature militari che si sono susseguite nella storia delle civiltà, alle fortificazioni dei secoli passati, agli "equilibri nucleari" tra le due superpotenze nel secolo scorso.

La guerra fredda fu un confronto duro, ma tra due giocatori, che quindi poterono applicare un approccio di stabilità ed un certo coordinamento. Oggi siamo in un mondo multipolare, in cui il coordinamento è assai più complesso. Ed è ancora più complicato dall'incertezza sulla unità di difesa o di attacco informatico, e sulla sicura identità dell'attaccante.

A differenza di quanto avveniva in passato, la nostra epoca ha perso la chiarezza dei conflitti, la certezza del nemico, le motivazioni degli attacchi, la certezza degli strumenti e delle tecniche usate. e su quanto velocemente queste tecniche evolvono. Nell'era digitale, e nei conflitti cibernetici, ogni nuova tecnologia, piattaforma, sistema, può essere adattata, implementata, acquisita e militarizzata da individui e organizzazioni, e quindi trasformata in arma digitale, spesso ancor prima che I governi possano reagire. *Technologies* e *capabilities* costano poco, e a volte sono addirittura gratuite. L'abilità tecnica è diffusa, e cresce esponenzialmente ovunque nel mondo.

Abbiamo quindi un nuovo fronte, In cui dobbiamo difenderci, e quindi oggi assistiamo ad una nuova cyber-corsa agli armamenti, con vere e proprie unità da cyber-combattimento.

Ma il cyber-attack è immateriale, senza confini, e talvolta anche non facilmente rintracciabile. Anzi, proprio per la natura stessa delle cyber-weapons, non è sempre certa l'identità dell'avversario, e non si può correre il rischio di vendicarsi contro il soggetto sbagliato[1].

[1] Diversi attacchi cibernetici non hanno portato a una definizione certa dell'attaccante. Tra i più rilevanti è il sabotaggio cibernetico che danneggiò il sistema di telecomunicazioni e il sistema bancario dell'Estonia nel maggio del 2007: nonostante diversi indizi abbiano

Siamo esposti ad un nuovo rischio persistente di attacco, di cui non possiamo tracciare limiti certi e stabili, ma abbiamo anche un nuovo modo per contrastare i nemici, per impedire azioni terroristiche o criminali. Del resto, una difesa adeguata comporta anche la capacità di offesa, e se nelle strategie militari il vantaggio dell'offensiva è assoluto, questo vale anche per le armi informatiche.

Nessuna nazione può escludere con certezza che qualcun altro non la stia per attaccare, e tale situazione di costante incertezza, tale minaccia persistente, viene definita come "*la paura reciproca di un attacco a sorpresa*: [...] *dato che non so se sto per essere attaccato oppure no, allora forse potrei prendere il sopravvento ed attaccare per primo*"[2].

Sono tanti gli Stati che dichiarano che la miglior difesa è l'attacco, e non possono sfuggire alla nostra attenzione alcune azioni di cyber-sabotaggio preventivo, mirate verso specifici target, allo scopo di indebolire il nemico e neutralizzare il rischio di possibili attacchi futuri.

Risulta poi oggettivamente difficile distinguere le Cyber Unit difensive da quelle di attacco, e: "*in un contesto in cui non sappiamo se il nemico potenziale stia preparando la difesa o l'attacco, e se le armi offrono un vantaggio per attaccare, allora questo ambiente è il più ideale per innescare un conflitto*"[3].

Come la storia ci ha insegnato, questo è l'ambiente dell'Europa alla vigilia della Prima Guerra Mondiale. Ma questo è anche l'ambiente che viene creato dalle armi informatiche di oggi, e determina un aumento dell'instabilità già presente.

Si richiede quindi tanta competenza e capacità di gestione, unita ad adeguata saggezza politica per non aumentare ulteriormente il rischio di scatenare conflitti.

I segnali che qualcosa stava cambiando risalgono a diversi anni fa.

Già nel 1982, la potenza devastante di un attacco cyber diviene chiara, manifestata da una potente esplosione[4] in un oleodotto nella Siberia

focalizzato le responsabilità dell'attacco sulla Russia, nessuna rappresaglia è stata ufficialmente intrapresa propria per l'impossibilità di provare con certezza l'identità dell'attaccante.

[2] Prof. Thomas Schelling – premio Nobel per l'Economia.

[3] Prof. Robert Jervis, Columbia University New York, nel 1978 descrive un modello per capire come possono emergere i conflitti.

[4] L'esplosione dell'oleodotto sprigionò una potenza di 3 chilotoni, circa 1⁄4 della potenza spigionata dalla bomba atomica sganciata su Hiroshima.

Sovietica, causata da azioni di sabotaggio della CIA che era riuscita ad infiltrarsi nei sistemi informatici di gestione dell'oleodotto[5].

Nel dicembre del 2008, il sistema informatico di CENTCOM, il comando centrale di gestione delle guerre in Iraq ed Afghanistan, viene infiltrato da hackers attraverso l'inserimento di USBkey.

Quasi un anno prima, nel novembre 2007, il Generale James E. Cartwright[6] riferisce al Congresso che "*gli attacchi informatici potrebbero essere potenti quanto le armi di distruzione di massa*".

Attendiamo però fino al 2011, per vedere la prima menzione ufficiale della Cyber Security nel rapporto annuale del Direttore della NSA[7], in fondo all'elenco delle minacce (dopo il traffico di droga nell'Africa occidentale).

L'anno successivo, nel 2012, lo stesso rapporto annuale del NSA Director vede la Cyber Security guadagnare posizione nella classifica delle minacce da fronteggiare (dopo terrorismo e proliferazione armi), ma è solo nel 2013 che il rapporto annuale del NSA Director posiziona il Cyber al top delle minacce, ove rimane negli anni successivi, e di sicuro in quelli che ci attendono.

Nella nostra cyber-era, il perimetro da difendere è più esteso e profondo, perché oggi tutto è in rete e il panorama dell'hacking e del cyber-crimine vede sia la presenza di soggetti motivati da obbiettivi politici, sia di chi ha motivazioni esclusivamente economiche.

Oltre alla protezione degli obiettivi più sensibili, quali sono le infrastrutture critiche, le capacità di cyber-defense di una Nazione devono essere estese anche agli obiettivi più deboli e vulnerabili, su cui si intrecciano i tessuti economici e sociali interni.

Bisogna favorire l'adeguamento rapido delle aziende, con un occhio di riguardo alle piccole e medie imprese che restano esposte per limitazioni di budget e mancanza di competenze tecniche.

Già nel settembre 2008 tre milioni di abitanti nello stato di Espirito Santo in Brasile erano finiti senza elettricità per un ricatto da parte di pirati informatici, ma poi è stato un crescendo continuo, fino all'ultimo anno, ove l'incremento di attacchi ha raggiunto livelli inimmaginabili.

[5] fonte: Thomas Reed – ex segretario Air Force nella gestione Ronald Reagan.
[6] Generale James E. Cartwright – Former Commander U.S. Strategic Command, Vice Chairman of the Joint Chief of Staff.
[7] NSA Director's Threath Assesment – National Security Agency.

La maggioranza delle aziende ha già sperimentato almeno un incidente di cyber security, e considerato ché può passare del tempo prima che ci si accorga di essere stati hackerati, il numero è senz'altro maggiore.

Nella realtà siamo tutti vittime di attacchi, con la differenza principale tra chi se ne è accorto, e chi non ancora.

Il numero complessivo degli incidenti cresce notevolmente se consideriamo anche gli attacchi non denunciati per evitare lesioni all'immagine, oppure per non diffondere insicurezza.

I danni economici sono ingenti, e spesso di difficile stima. Oltre ai costi necessari al completo rispristino dei servizi compromessi, vanno considerati i contraccolpi che si propagano sulle filiere produttive e sugli indotti, e gli impatti sociali conseguenti alla mancanza di servizi essenziali o di diffusa utilità.

Diversi sono gli esempi della virulenza di tali attacchi, ma tra gli impatti e le conseguenze "sociali" ci basti ricordare ii recente blocco del servizio ambulanze conseguente al contagio dei sistemi nel Regno Unito da parte del ransomware Wannacry.

Il ROI (*Return On Investment*) di un cyberattack è molto elevato e quindi in grado di attrarre organizzazioni criminali e talenti cibernetici. Tra le diverse tipologie di attacchi, i *ramsonware* sono facili da preparare e molto remunerativi, ed abbiamo visto *ramsonware* progettati per propagarsi sulla rete internet scansionando gli indirizzi pubblici alla ricerca di target vulnerabili, e *ramsonware* lanciati contro target ben definiti e programmati per diffondersi solo nei network aziendali.

L'analisi delle caratteristiche di progettazione e delle strategie di diffusione dei *ransomware*, mostra alcune differenze tra i vettori di attacco, i target e i presunti autori, ed appare chiaro che dietro la realizzazione e la diffusione degli ultimi attacchi ci sono gruppi di cyber-criminali esperti.

Con buona probabilità, possiamo anche dire di aver identificato le organizzazioni responsabili di alcuni specifici attacchi, ma il riscatto in *bitcoin* o altre *cryptocurrencies* non aiuta il "*follow-the-money*" per risalire con certezza assoluta a ricattatori e/o mandanti.

Nel prossimo futuro non si può che prevedere che le minacce continueranno a diffondersi e impatteranno più utenti e più dispositivi, compresi gli omni-connessi e molto vulnerabili *smartphone*.

Alcune stime considerano che più del 33% dei cellulari in circolazione sia insicuro, ma i migliori esperti considerano tali stime troppo ottimistiche

e portano tale percentuale ben oltre il 60%. Migliaia di *app* registrano e comunicano tutte le azioni fatte dall'utente sul proprio telefono cellulare, e il numero di attacchi per furto di dati e di identità cresce con incrementi esponenziali di anno in anno.

Nella realtà, il furto dei dati personali è già oggi a livelli superiori rispetto ai dati ufficializzati, e molto probabilmente i nostri dati personali sono già stati rubati almeno una volta dai nostri dispositivi, oppure dalle banche dati delle aziende con cui li abbiamo condivisi, anche se noi non ne siamo ancora consapevoli.

Purtroppo i numeri non sono incoraggianti neanche in ottica prospettica, perché è facile prevedere che il furto di dati sarà sempre più intenso, sia verso i singoli utenti, sia verso sistemi e dati aziendali: numerose indagini affidabili stimano che oltre il 90% delle organizzazioni non utilizza ancora protezioni sui dispositivi mobile, né firewall di prevenzione avanzata, né sistemi di sicurezza sul *cloud*.

L'*Artificial Intelligence*, interessantissima alleata nelle attività di prevenzione e contrasto, sarà sempre più applicata anche dagli attaccanti, e vedremo quindi tecniche di *spear phishing* sempre più targettizzate e pertinenti alla vita della vittima, e quindi più "subdole" e con maggior numero di vittime.

Anche l'inarrestabile diffusione di dispositivi ed oggetti interconnessi che facilitano le nostre vite, l'*Internet of Things*, rischia di incrementare i possibili "*point of weakness*" di qualsiasi strategia di difesa.

Internet e *digital technologies* hanno cambiato le nostre vite, e creato un nuovo fronte di combattimento e di contrasto alla criminalità, ma hanno anche modificato in modo esponenziale le modalità di propaganda, arruolamento e radicalizzazione.

Dal 2009 ad oggi, decine di migliaia di individui, soprattutto giovani con forte presenza sui social, hanno lasciato i loro Paesi occidentali per unirsi a gruppi radicali "combattenti", o cosa ancor più pericolosa, si sono radicalizzati rimanendo sul proprio territorio, come mine vaganti pronte a detonare.

Con la formazione, reclutamento e addestramento di singoli individui da impiegare in attacchi terroristici ovunque, l'interconnessione online-offline modifica ancora una volta le prime linee nei conflitti.

In questo contesto, le Nazioni soffrono di esposizioni di rischio mai viste prima, anche perché ci sono tante azioni nel cyberspazio che pur non avendo obiettivo diretto infrastrutture critiche o servizi essenziali, possono creare

danni economici rilevanti, oppure minare la fiducia dei cittadini con gravi conseguenze sociali.

Diviene quindi strategico combattere anche gli attacchi che hanno come target massivo gli individui, e contrastare tutte le azioni che, pur meno acute in malevolenza cibernetica, minano la percezione di sicurezza, oppure agiscono secondo sottili strategie di diffusione sociale per influenzare l'opinione pubblica.

Alcune strategie terroristiche combinano azioni offline ed azioni online, altri cyber-attack approfittano solo del momento "favorevole" che consegue eventi a forte impatto emozionale sul pubblico dei social, ma non per questo possono risultare meno dannose. Nel caso dell'attacco a Charlie Hebdo a Parigi, alla cruenta azione sul campo, fa seguito un attacco informatico sui social media, in cui alcune immagini postate nelle conversazioni di sostegno (*#JeSuisCharlie*) contenevano *malware* che violava il sistema degli utenti. Centinaia di migliaia di computer infettati, e molte settimane per circoscrivere e rimuovere la minaccia.

In progressiva ascesa è anche l'uso di tecniche di condizionamento, cioè quell'insieme di contenuti diffusi abilmente sui social media in modo da influenzare l'opinione pubblica. Rientrano in questo la creazione e diffusione di specifiche *fake-news* e contenuti distorsivi della verità, diffusi appositamente in modi, tempi e canali atti a indirizzare le opinioni del pubblico elettorale, come pure messaggi e commenti creati ad hoc per innescare mutamenti di opinione, od infiammare proteste.

L'argomento è spinoso, e di difficile contrasto, e rimanda alla nostra capacità personale di informarsi correttamente e distinguere il vero dal falso. Ciò nonostante, va considerato per la sua moderna accezione di condizionamento architettato e gestito da nemici della Nazione, o comunque da soggetti che operano contro l'interesse nazionale. In tale accezione, appunto, tali "influenze socio-mediatiche" rientrano nelle sottili tecniche di combattimento digitale, e dovrebbero anch'esse rientrare nei perimetri più allargati di Cyber Defense nazionale.

A riprova, è sufficiente ricordare che in USA alcuni post sui social hanno visto decine di migliaia di condivisioni, raggiungendo quindi un numero impressionante di cittadini americani, salvo poi scoprire che dietro l'account che aveva inserito tali post si celava una "regia" russa. Nell'ambito del c.d.

"Russiagate", la Facebook Inc. ha dichiarato[8] che i contenuti postati dai *troll* russi potrebbero essere stati visti da oltre 126 milioni di cittadini statunitensi. Poco meno della metà della popolazione, circa un elettore su due, potrebbe essere stato condizionato nella sua scelta elettorale da azioni di propaganda esogena.

Social media platforms, big player della rete, dell'e-commerce e delle telecomunicazioni, conoscono le nostre scelte, sanno chi siamo, sanno cosa abbiamo cercato online, e quali contenuti abbiamo apprezzato. Il continuo e capillare tracciamento di tutte le ns attività digitali, quindi dei nostri gusti, pensieri, azioni, offre in mano ad una manciata di player un crescente ed incontrollato potere di scansionare le ns vite, e di orientare le nostre idee.

Molto ci si deve interrogare sulle responsabilità, compresa quella delle piattaforme social, ma assai inquietante è la facilità con cui tali media sono utilizzabili a fini di condizionamento pubblico. L'hacking e l'inserimento di *troll* in questi sistemi, l'accesso a profili, cronologie, preferenze degli utenti, permette una profilazione dettagliata e precisa, e quindi la possibilità di indirizzare contenuti specifici, mirando accuratamente il target di chi deve ricevere il messaggio.

Si pone quindi un problema estremamente complesso, politico e tecnologico, che coinvolge tanto i governi quanto le grandi aziende tecnologiche, sempre più omniscienti della vita, dei gusti e dei pensieri di tutti noi utenti.

Non è difficile prevedere che attacchi e contagi telematici continueranno ad aumentare, e saranno sempre più aggressivi e dannosi, e probabilmente paghiamo anche le conseguenze di un certo vuoto di potere, una mancanza di presidio, sia a livello normativo, sia a livello di competenza e reattività, che ora dobbiamo assolutamente colmare.

Le difficoltà tipiche degli organismi istituzionali ad adattarsi e comprendere sfide e conflitti digitali, rischiano di renderci ancor più vulnerabili ed insicuri.

La consapevolezza che anche terrorismo e fondamentalismo utilizzano a vari livelli le tecnologie di comunicazione, ha portato ad accettare e giustificare la sorveglianza di massa, l'hacking diffuso da parte di agenzie governative, il divieto che alcune Nazioni hanno cercato di imporre sulla cifratura delle comunicazioni, l'introduzione di *backdoors*.

[8] Nella dichiarazione scritta depositata da Facebook Inc. presso la Commissione Giustizia del Senato americano.

Conviene però ricordare che governi ed agenzie governative non sono gli unici a poterlo fare. Non esistono grandi barriere che possono impedire a singoli cyber-criminali, come a piccole o grandi organizzazioni, di attuare le stesse tecniche di spionaggio e sorveglianza.

Inoltre, sussiste sempre il problema del controllo dei controllori: nessuno può garantire che la sorveglianza massiva non sia usata in modo improprio, a fini politici oppure economici.

Il controllo diffuso di telefonate, email, messaggi, navigazione internet e tracciature GPS, ci pone di fronte ad un problema di grave lesione della privacy, e la sorveglianza di massa presenta più rischi ed effetti collaterali dei benefici che offre.

Possiamo dire che ognuno di noi vive, più o meno coerentemente, un'esistenza "pubblica", una "privata", e una per definizione "segreta", lasciando alla scelta di ognuno di noi quanto condividere e con chi delle ultime due.

Etica e legalità sono valori assoluti e indiscutibili, ma qui non c'entrano. Tutti necessitiamo di mantenere riservate almeno alcune scelte ed alcune comunicazioni, sia di ambito personale, sia di business. È un diritto inviolabile.

Noi tutti, nel nostro quotidiano vivere di singoli individui, dobbiamo considerare che in pochissimi anni le nostre vite, i nostri business, le nostre attività personali e professionali sono state completamente digitalizzate. Tecnologie, prodotti e servizi "smart", facilitano le nostre attività, ma con il *trade-off* che ogni nostra attività "semina" nostre informazioni personali nella rete, con una persistenza senza limiti di tempo, ed un rischio di diffusione incontrollabile.

Nel passaggio da un mondo analogico ad un *habitat* digitale è mancata una transizione culturale che potesse far comprendere i rischi e l'uso più corretto, prudente, e sicuro di tali tecnologie. Siamo tutti impreparati, e ce lo dobbiamo ricordare.

La quasi totalità degli attacchi, sfruttano errori umani come l'apertura di mail con virus o la perdita di password, e quindi la mancanza di adeguata cultura all'"igiene digitale".

Dobbiamo aumentare la nostra consapevolezza sul valore patrimoniale ed economico dei nostri dati, ed è urgente pianificare ed attuare veri e propri programmi di educazione all'uso "appropriato" dei mezzi digitali.

Inoltre, se consideriamo anche enti, organizzazioni e imprese, conviene ricordare che ogni cyber-attack sfrutta la mancanza di competenze in termini di cyber security.

Purtroppo il know-how è ancora mediamente basso, e sono carenti le professionalità adatte per favorire una rapida ed estesa evoluzione comportamentale. Ma causa primaria è ancora una scarsa percezione del rischio, e i ritardi nell'aggiornare i sistemi informatici all'interno delle imprese.

Sic stantibus rebus, concetti e capacità di cyber-defense devono essere estesi anche agli obiettivi più deboli e vulnerabili, su cui si intrecciano i tessuti economici e sociali interni alle nazioni. Diviene strategico agire più intensamente per favorire la preparazione delle aziende, e per l'educazione dei cittadini al mutato contesto di esposizione verso il rischio conseguente all'epocale trasformazione digitale in atto.

Cosa possiamo fare?

Non credo esistano risposte univoche, perché ognuno deve svolgere il proprio ruolo.

In un'ottica generale, concentrarsi sulla difesa digitale significa, in primis, attuare un'efficace gestione del rischio e un'attenta prevenzione, in modo da garantire continuità operativa secondo un approccio di resilienza.

Quindi è importante cooperare, a tutti i livelli, anche attraverso la condivisione immediata di attacchi e minacce, perché la tempestività è fondamentale, e perché prima o poi tutti verremo attaccati, dunque è meglio essere preparati.

Vanno poi utilizzate al meglio le tecnologie disponibili, perché l'integrazione di *big data* e *artificial intelligence* permette un'analisi multi-dimensionale degli indizi, dei pattern e dei comportamenti e favorisce la previsione delle azioni e quindi del prossimo attacco, favorendo il passaggio da un modello di analisi dei dati a fini di conoscenza ("*data-to-knowledge*"), ad una Cybersecurity proattiva che sappia realmente prevenire ("*data-to-wisdom*").

L'aiuto previsivo che ci offre l'intelligenza artificiale sarà sempre più utile, ma non supererà la necessità del presidio umano, in termini di intuito ed intelligenza emotiva, perché sempre umani sono gli attori dietro ad ogni attacco.

Se poi guardiamo verso l'*Internet of Things*, o meglio, *of Everything*, gli smartphone, e suoi utilizzi BYOD in azienda, la diffusione inarrestabile del *cloud*, anche come estensione delle infrastrutture aziendali, è intuibile che dispositivi e sistemi sono, e saranno sempre più in rete, e che anche una vulnerabilità periferica, l'hacking di un solo dispositivo interconnesso, può scatenare l'aggressione a tutto il sistema.

Sarà opportuno sviluppare un approccio architetturale capace di integrare varie tecnologie di cybersecurity in un unico sistema di sicurezza perimetrale, in grado di offrire una protezione efficace contro attacchi diretti verso i diversi target. Certo i perimetri da difendere sono purtroppo tanti e a più livelli – cloud, mobile, data center, sistemi – ed è uno scenario impegnativo da realizzare in breve termine. Ma è in questa direzione che bisogna guardare definendo piani di lungo periodo, ed attuando immediatamente i primi concreti passi.

Sotto l'aspetto culturale, la nostra società evoluta e democratica, deve agire per favorire la diffusione delle tecnologie di comunicazione digitale nei territori dove nascono e si nutrono sentimenti radicali e pensieri anti-democratici e fondamentalisti, perché informazione e conoscenza sono i migliori antidoti a tali fenomeni.

Internet, social media *platforms*, e *digital technologies* in generale, aiutano tutti quegli attivisti e manifestanti che si oppongono a regimi totalitari e lottano per la democrazia, e in alcuni casi sono l'unico mezzo che oppositori di regimi hanno per comunicare tra loro, e per far conoscere al mondo quello che accade nei loro Paesi.

Le istituzioni democratiche dovrebbero comprendere che alcune tecnologie ritenute ancor oggi "pericolose" – come Tor, *cryptocurrencies*, etc. – sono spesso l'unico modo in cui attivisti contro regimi totalitari possono combattere, finanziarsi, raccontare la situazione del loro Paese, e comunicare le loro idee. Le istituzioni dovrebbero pertanto avvicinarsi a tali tecnologie e conoscerle a fondo, comprendendo che non potranno dominarle né imbrigliarle, ma almeno usarle al meglio. Questi "eco-sistemi" dovrebbero essere di ispirazione per le istituzioni, avere il loro supporto, e la loro partecipazione, in modo da alimentare i diritti civili, la libertà di opinione, e la democrazia.

La sorveglianza di massa presenta più rischi ed effetti collaterali dei benefici che offre, ed andrebbe meglio garantita la privacy di tutti. Si dovrebbe abbandonare il controllo di massa, superare le *backdoors*, ed investire nell'educazione digitale e nella libera informazione, al fine di aiutarci ad essere più sicuri. Ma chiaramente anche noi individui dobbiamo conoscere i rischi e imparare a comportarci conseguentemente.

I paradigmi culturali di difesa cibernetica dovrebbero indirizzarsi progressivamente verso "perimetri" tecnologici e modelli di presidio "collettivo". Ispirarsi ad un approccio di sicurezza collettiva, che comprende tutti noi, significa in primis proteggere sé stessi e poi, mediante relazioni *Peer-*

to-Peer, agire per la protezione collettiva, così da rafforzare la sicurezza individuale, nazionale ed internazionale.

Una interessante opportunità nella direzione di una *Peer-to-Peer-Security*, con perimetri, "nodi", sistemi e utenti certificati gli uni dagli altri, potrebbe darla l'applicazione della tecnologia *Blockchain* nelle relazioni e negli "scambi" digitali, ma gli ostacoli maggiori non sono di natura tecnologica, ma in una dimensione di pensiero che attribuisca fulcro alle relazioni di fiducia, al "*trust*" tra gli attori, i sistemi, le persone.

In ogni caso, approcci e modelli di cyber security universali e diffusi sono da ricercare come obbiettivi assoluti, perché oltre a preservarsi in una cyber security perimetrale che protegge con "alte mura e fossati", è importante diffondere una sorta di "vaccinazione" di massa, primo ostacolo e contrato alla diffusione delle epidemie cibernetiche.

Possiamo educare la prossima generazione, di cittadini, e di hackers, e tale approccio non riguarda solo gli individui, ma anche aziende ed organizzazioni, che hanno il vantaggio di poter agire più efficacemente, rapidamente e senza confini[9].

E non ragioniamo solo su ideali. Vantaggi e incentivi reali ci sono e possono essere declinati a livello sociale ed economico. Aziende e professionisti comprenderanno sempre più la valenza per il proprio business degli investimenti dedicati alla cyber security e alla privacy.

Aumenterà sempre più la leva competitiva, anche a seguito dell'incremento di sensibilità di clienti, utenti e partner. Anche le metriche valutative permetteranno di misurare meglio il *Return On Security Investment*, e il *Rurturn On Privacy Investment*.

La reputazione di fiducia è preziosa e redditizia nell'era digitale, e lo diventerà sempre più nelle future generazioni.

Abbiamo di fronte una grande sfida, ma come sempre, con un problema riceviamo anche un dono. Per la prima volta nella storia dell'umanità, oggi,

[9] Individui, piccoli gruppi, aziende ed organizzazioni hanno il vantaggio di essere più reattivi e svincolati, e agiscono più rapidamente di strutture militari e agenzie di intelligence, che in qualche caso sono ancora lente ed obsolete. Nel settembre del 2011, in risposta alle cruente azioni che il potente cartello della droga messicano Los Zetas aveva fatto contro due blogger che avevano pubblicato articoli sulle attività illecite del cartello, Anonymous agisce "minacciando" libera informazione sulle connivenze politico-militari del feroce cartello. Individui anonimi, non polizia, non militari, non politici, hanno instillato timore in una delle più potenti e violente organizzazioni criminali del mondo, aprendo la strada ad una nuova sfida, una nuova battaglia, in cui non sempre I governi hanno ruolo.

per mezzo della tecnologia, abbiamo l'opportunità di rendere più sicure miliardi di persone nel mondo.

È chiaramente fondamentale il ruolo dei Governi, perché a loro ci rivolgiamo per azioni di protezione e sicurezza collettiva.

In un contesto dinamico come la cyber-challange, con le innovazioni tecnologiche che ci saranno nel futuro, primo requisito fondamentale dei governi è individuare con sufficiente anticipo i rischi, i prossimi trend evolutivi, e quindi le necessarie azioni, sia quelle più immediate, sia le strategie e le pianificazioni di lungo periodo.

Per essere sempre più vigili ed efficaci, bisogna rammentare che in passato ci è mancata la consapevolezza della minaccia, ed in taluni casi il chiaro tracciamento delle responsabilità. Oggi sono ancora ottimizzabili alcune catene di comando, in modo da renderle in grado di reagire alla velocità necessaria per affrontare i momenti di crisi.

È inoltre indiscutibile la necessità di effettuare ingenti investimenti per adeguare e mantenere le capacità di fronteggiare le minacce informatiche e la cyber *warfare*, e le migliori risposte includono tutte un approccio di "alleanze".

La prima risposta è senz'altro la necessità strategica di costituire una unità di Cyber Defense Europea, quindi una profonda, solida e trasparente alleanza tra pari.

A tale alleanza, l'urgente compito di coordinare le esigenze degli Stati membri ed implementare velocemente una strategia cibernetica efficace, impostando una catena di comando chiara, snella, efficiente, e da tutti rispettata.

Gli investimenti da affrontare per adeguare e mantenere le capacità di fronteggiare le minacce informatiche e la cyber *warfare* devono essere ingenti, ed indirizzati sia per stimolare ed incentivare al massimo gli investimenti nell'ammodernamento e nella sicurezza delle infrastrutture tecnologiche delle aziende di tutti i settori, sia soprattutto per favorire la generazione e la crescita delle imprese che operano nel campo della sicurezza informatica, in modo da stimolare la creazione di una economia sulla sicurezza cibernetica. Una diffusa economia di imprese europee specializzate in cyber security, è fondamentale per proteggere adeguatamente le aziende di ogni altro settore e di ogni dimensione, che oggi vedono aumentare le loro esposizioni di rischio a seguito del processo di digitalizzazione.

Certo è necessario capire come trasformare tali problemi ed emergenze in opportunità di sviluppo economico, e se si parla della necessità di investire

nella sicurezza in generale e nella cyber Security, non si può non guardare a Israele come esempio, e soprattutto come modello di una valente economia della cyber security[10].

Israele ha capito in anticipo la sfida cyber, certamente grazie allo "stimolo" che consegue dalla storia del suo popolo e dalla sua situazione geopolitica, e già con i primi furti di informazioni negli anni '80, ha compreso che doveva imparare a difendersi anche sul fronte online. Poi, è stata capace di comprendere l'evoluzione e la diffusione delle tecnologie informatiche, mettendo in piedi già negli anni Novanta un'agenzia per proteggere le infrastrutture civili strategiche per la sicurezza del suo territorio, fino ad "inventare" un ecosistema locale che oggi è giustamente considerato la capitale mondiale della cyber security.

Il distretto della cyber security di Be'er Sheva è il miglior modello per ogni ragionamento che guardi ad una economia della cyber security che non si voglia limitare a spostare la stessa ricchezza da un'azienda all'altra, bensì voglia aprire un mercato più vasto, e generare ritorni e prosperità economica per l'intera comunità.

Israele nel campo delle politiche di difesa e nelle capacità di investimento non è certo un esempio facilmente replicabile, ma non possiamo pensare di avere una economia della sicurezza cibernetica europea, senza avere un vero e proprio presidio europeo nella ricerca e nell'innovazione.

Quando si parla di Ricerca di frontiera, come la cyber security che guarda alle minacce del futuro, la vera differenza è riuscire a progettare e realizzare un ecosistema ove far confluire capitali e cervelli. e che si traduce in ricerca avanzata, sicurezza evoluta, business e profitto.

La capacità di concentrare università e imprese, ricerca e talento, investitori e idee in un unico *environment*, in una location ben definita, in un *hub* in grado di accelerare confronti, soluzioni, delivery e ritorni, rappresenta una vera leva competitiva verso l'innovazione necessaria a presidiare in modo efficace la cyber security, e permette di considerare l'intera cyber challenge non solo come un problema globale ma come una opportunità di crescita e sviluppo.

E cosa può fare in più l'Italia?

[10] Start-up Nation, The Story of Israel's Economic Miracle - Dan Senor e Saul Singer - Grand Central Publishing.

Favorire in ogni modo un fronte di alleanza europeo, e favorire anche la nascita di un fronte globale, comunque il più vasto ed allargato fronte di alleanze possibile.

Se però si considera che un cyber-attack può bloccare aziende e produzioni, o portarle a perdite importanti attraverso la violazione delle proprietà intellettuale e dei dati riservati, forse non basta più l'Europa attuale, ancora non pienamente integrata e piena di rivalità economiche. Il riflesso diretto che un cyber attack può avere sull'economia di un Paese, suggerisce che anche l'Italia debba avere il suo presidio di eccellenza nel settore cyber.

Ben venga quindi la necessaria ed utile costituzione di un ecosistema europeo sulla sicurezza cibernetica, ma credo che l'Italia non possa esimersi dalla creazione di un ecosistema anche proprio. Lo stesso ruolo dell'Italia nello scacchiere di difesa europea sarà molto influenzato dall'essere riuscita a creare, oppure no, un proprio ecosistema di eccellenza.

Certo un ecosistema italiano dovrà agire in rete con gli altri ecosistemi europei, siano essi condivisi oppure di singoli stati membri, ma più eccellente sarà l'ecosistema italiano, meglio sarà anche per l'Europa intera.

Ma se la cyber security non è un'opzione, bensì un imperativo assoluto, cosa ci può impedire di valorizzare la sfida cyber realizzando anche qui in Italia un ecosistema di eccellenza?

In qualsiasi campo ad elevato tasso di innovazione, quali intelligenza artificiale, robotica, biotech – tanto per citare alcuni esempi – e in modo particolare nella cyber security, è assolutamente importante "sperimentare".

Agevolare chi fa Ricerca e Sviluppo, e quindi sperimentazione, vede tanti possibili esempi.

Me ne viene in mente uno, prossimo per distanza e recente, la c.d. Crypto-Valley di Zugo in Svizzera, ed un altro più piccolo ed in divenire che è proprio al nostro confine, ed è l'iniziativa sempre sulle cryptovalute che sta nascendo a Chiasso, a pochi chilometri da Milano, entrambi motivati dalla visione sul ruolo che avranno le cryptovalute e la tecnologia *Blockchain*, e dall'ambizione di diventare poli di riferimento per il commercio e la finanza del futuro.

In questi, come in altri casi, si nota come lo stimolo verso la ricerca e l'innovazione, e la "gemmazione" di aziende non dipenda tanto dai capitali messi a disposizione, ma dal contesto atto ad agevolare insediamenti, ricerca e sperimentazione.

Perché non valorizzare in tal senso tutta l'area dell'Expo a Milano, oppure altre aree del nostro Paese?

Probabilmente si andrà anche in tale direzione, ma per agire al meglio è utile capire cosa c'è dietro questi ecosistemi produttivi, per ricordare le condizioni minime che li rendono possibili, e tracciare una solida "via italiana" alla cyber security, ed all'innovazione in generale.

Imprese e Ricerca interagiscono e sono interagenti con l'ambiente in cui operano, e molto dipende dall'*humus* rappresentato dal sistema Paese, cioè da un *commitment* di ordine superiore, strategico, e quindi politico, tradotto in scenari normativi e azioni concrete a sostegno.

Fondamenta sono la certezza del diritto, inteso nel suo significato più ampio, quindi un quadro di riferimento per la R&D, la fiscalità per il settore, metodi meritocratici e trasparenti per l'assegnazione dei contributi, la tutela dei diritti di invenzione e proprietà, i tempi di risoluzione dei contenziosi.

È necessaria, pertanto, la concreta determinazione delle Istituzioni, a livello centrale e territoriale, ad affrontare l'impegno e a contribuire alla creazione dell'*environment* e alla sua promozione.

Le condizioni sistemiche sono fondamentali affinché un settore si sviluppi e attraversi una crescita reale e sostenuta. Generare Ricerca e Innovazione e far sì che questa si autoalimenti e sia generatrice di business e crescita economica non è una sfida che si affronta e si vince guardando ad orizzonti di breve periodo. La propulsione innestata dagli investimenti, consegue alla capacità di attrazione degli stessi, che a sua volta è un attributo del contesto ambientale che le istituzioni hanno saputo creare.

Gli ecosistemi svizzeri conseguono ad insieme di azioni atte a favorire gli innovatori in un contesto di "frontiera" come quello delle cryptovalute, grazie ad un pragmatismo "snello" che si riflette anche nella reattività delle loro istituzioni.

La FINMA, autorità di vigilanza su mercato finanziario svizzero, in pratica l'equivalente della nostrana CONSOB, ha fornito un contesto "protetto" per la ricerca e la sperimentazione sulle cryptovalute, creando una "sandbox" che permette agli "innovatori" di sperimentare emissioni e transazioni di cryptovalute fino a un milione di CHF.

Questi, come tanti altri possibili esempi, vedono il combinarsi di più azioni e l'impegno di donne e uomini determinati, con una "vision" per guardare lontano, per individuare prima di altri problemi, opportunità e soluzioni. Realizzare un giardino rigoglioso ove prima c'erano pietre, richiede di sicuro risorse adeguate da investire, ma queste non sono sufficienti se non sono accompagnate da un contesto e da un approccio in grado di attrarre i migliori talenti.

In uno scenario in cui l'innovazione tecnologica sta spostando sempre più l'origine del vantaggio competitivo sul talento e sul *know how*, diminuisce l'importanza dell'accesso alle risorse finanziarie, a vantaggio dell'accesso a risorse quali l'istruzione, le competenze, i talenti individuali, da plasmare e valorizzare[11]. L'autosviluppo e la crescita individuale sono oggi leve di ingaggio e motivazionali più importanti del semplice rapporto economico tra persone ed azienda, e in mercati globalizzati ove produzioni, prestazioni, e fruizioni si muovono senza confini, fanno altrettanto i talenti, e la capacità di attrarli, e soprattutto allevarli, diviene una vera e propria leva strategica.

Questa è una delle migliori caratteristiche del modello israeliano, ove i giovani vengono stimolati, responsabilizzati, e soprattutto seguono percorsi meritocratici. Il modello formativo israeliano favorisce la selezione e l'indirizzamento dei migliori talenti, dal liceo all'università, e valorizza gli anni di leva obbligatoria in unità dedicate che stimolano la crescita di competenze, metodi ed approcci che sono alla base del successo delle aziende di cyber security israeliane.

Non a caso la strategia di Israele è stata, ed è quella di formare intere generazioni di talenti informatici, interagendo con il mondo accademico, con quello dell'industria high-tech e con quello militare, garantendosi il presidio di un business in espansione e ad elevato ritorno. E non a caso nell'ecosistema israeliano ci sono università, grandi aziende tecnologiche, molte startup di successo, e moltissime che continuano a nascere.

Nella stessa direzione di attrazione ed allevamento di talenti, motivato dall'opportunità di presidiare un nuovo business globale, in espansione e redditizio, sembra muoversi anche la strategia della Svizzera con le cryptovalute, "allevando" di riflesso anche le competenze sulla rivoluzionaria *Blockchain* sottostante.

Nella dimensione che viviamo, la "coltivazione" dei talenti diventa un requisito fondamentale se si vuole giocare un ruolo nella cyber security, perché rivolto a fondare e a trasmettere i valori e le competenze distintive che differenziano una Nazione dalle altre.

Personalmente mi auspico con tutto il cuore che l'Italia possa presto riallineare i propri modelli e percorsi formativi alla nuova era che viviamo, riconsiderandoli come strumenti di formazione ed "educazione" del talento, ma anche come nuova strategia di crescita.

[11] From Capitalism to Talentism (World Economic Forum, Davos 2013).

8. LA SICUREZZA INFORMATICA È UN DIRITTO UMANO

di *Arturo Di Corinto*[*]

Richard Stennion, autore Del Libro *There Will Be Cyberwar,* ha detto che "il 2016 sarà ricordato come l'anno più importante per l'evoluzione dei *nation state attacks* e che lo spionaggio cibernetico è da tempo uno degli strumenti più importanti per hacker e servizi segreti, invitando tutti a migliorare il proprio livello di sicurezza informatica per il nuovo anno.

Difficile dargli torto visto che il 2016 è cominciato con il furto dei dati di 20 mila impiegati dell'FBI e finito con gli strascichi delle interferenze russe nelle elezioni presidenziali americane. Tuttavia bisogna ricordare che durante tutto l'anno massicci *data breach* aziendali hanno colpito le maggiori compagnie mondiali, mettendo a rischio la privacy di moltissimi utenti: dal miliardo di account rubati a Yahoo ai furti di dati personali e numeri di carte di credito ai danni di Ashley Madison, Adul Friend Finder, LinkedIn, Dropbox, Twitter eccetera.

A commettere questi furti sono stati non precisati "hacker", un termine passe-partout per indicare, negli esperti di reti e computer, gli autori delle intrusioni. In realtà sarebbe più corretto chiamarli *black hacker*, malevolent hacker o criminali informatici perché la parola hacker nel nostro lessico si riferisce a coloro che si dedicano a migliorare le difese informatiche di stati, aziende, individui. Questi ultimi sono chiamati comunemente *white hat hacker, blu hat hackers* o *ethical hackers*.

Ma vediamo perché.

[*] Attivista, giornalista e saggista italiano.

8.1. I data breach più dannosi del 2016

Il 9 febbraio 2016, per protestare contro l'appoggio statunitense alle politiche israeliane contro i palestinesi, hacker non identificati si sono introdotti nel database del Dipartimento di Giustizia Usa. Secondo quanto riportato dalla CNN questi hacker hanno, in seguito, diffuso online dati relativi a 10,000 impiegati del Dipartimento per la sicurezza nazionale e successivamente quelli di 20 mila impiegati dell'FBI. Le informazioni rubate riguardavano nomi, ruoli, numeri telefonici e indirizzi email.[1]

Il 3 marzo del 2016 con un attacco di *phishing* sono state sottratte le informazioni personali di 700 impiegati di Snapchat ai quali era stato fatto credere che il direttore dell'azienda di messaggistica istantanea, Evan Spiegel, richiedesse dati privati come nomi, numeri della sicurezza sociale e buste paga[2].

Il 25 marzo 2016 i dati di un milione e mezzo di clienti di Verizon sono stati sottratti da hacker ancora oggi anonimi e sono stati messi in vendita in alcuni forum underground[3]. Grazie al giornalista di cyber security, Brian Krebs, sono infine stati rintracciati Verizon ha confermato l'entità del *data breach* e l'intenzione di avvertire ogni cliente interessato.

Il 5 maggio 2016Una società di cyber security di Milwaukee, la Hold Security, rivelò l'avvenuta diffusione di 270 milioni di account email rubati, completi di username e password, nell'underground criminale russo. La società aveva, rilevato la presenza di 57 milioni di account Mail.ru, provider russo, 40 milioni di Yahoo, 33 di Hotmail e 24 Gmail che sarebbero stati diffusi a titolo gratuito e senza una controparte economica di riscatto. Secondo gli esperti, centinaia di migliaia di account erano relativi a provider cinesi e tedeschi, e le combinazioni username/password trovate erano appartenenti ad impiegati di banca e del commercio al dettaglio.

Il 17 maggio del 2016 è stato scoperto un furto massiccio di dati personali risalente al 2012 ai danni della piattaforma per servizi professionali LinkedIn. Anche stavolta la segnalazione è avvenuta grazie al blog Krebs on

[1] Mallonee, M.K., *Hackers publish contact info of 20,000 FBI employees,* CNN Politics, 9th February 2016. Available at: http://edition.cnn.com/2016/02/08/politics/hackers-fbi-employee-info/index.html.
[2] Rabinovits D., *Phishing Scams: How to Protect Yourself*, Identity Force, 5th November 2014. Available at: https://www.identityforce.com/blog/phishing-scams-how-to-protect-yourself.
[3] Leary J., *Verizon's Enterprise Unit Suffers Major Data Breach*, Identity Force, 25th March 2016, Available at: https://www.identityforce.com/blog/verizon-enterprise-data-breach.

security. Si tratterebbe di 117 milioni di dati relativi ad email e password degli utenti contenuti nello stesso database.

A giugno 2016 lo scalpore suscitato dal ripetuto furto delle email di alcune figure prominenti del Comitato Nazionale Democratico americano ha creato una nuova voce nei dizionari di cyber security: DNCLeaks. Insieme ad altri furti di dati, la diffusione di tali email avrebbe compromesso la vittoria di Hillary Clinton nelle presidenziali americane. I guai per Hillary ed i democratici cominciarono a metà giugno quando l'azienda di cyber security Crowdstrike rese nota la violazione del database del Comitato nazionale democratico ed il conseguente gigantesco furto di dati, attribuito a due gruppi hacker russi. Nello specifico, oggetto del furto furono 19.250 email con 8mila allegati successivamente pubblicate da WikiLeaks che hanno portato alle dimissioni della direttrice del comitato[4].

Il 19 luglio 2016 TheHackerNews riporta la notizia che il noto sito di incontri erotici – destinato a persone sposate o fidanzate – Ashley Madison è stato oggetto di un attacco che ha esposto al pubblico i dati personali, tra cui le carte di credito ed i numeri telefonici di 37 milioni di utenti. La società proprietaria del brand è stata multata di $1.6 di dollari per mancata adeguata protezione della privacy dei propri clienti.

In agosto 2016 Si venne a sapere che gli Shadow Brokers erano venuti in possesso di strumenti per lo spionaggio cibernetico usati dalla National Security Agency americana, in particolare cyber weapons e trojan virus che erano poi stati messi in vendita sul web.

A settembre 2016 Yahoo! ha rivelato di essere stata vittima di un vasto data breach, riguardante 500 milioni di account rubati nel 2014. La notizia compromise la vendita della società a Verizon che, ritenendosi danneggiata, chiese uno sconto sul suo acquisto.

Sempre a settembre, precisamente il 2, Dropbox, servizio per l'immagazzinamento di file, rivelò un data breach imponente ai danni dei suoi clienti risalente al 2012. Gli account furono usati fino al 2016 mettendo a rischio 68 milioni di utenti.

La botnet Mirai il 21 ottobre con un attacco di tipo *Distributed Denial of Service*(DDoS) mise offline buona parte della East Coast statunitense,

[4] *Elezioni USA, è il giorno della convention democratica: Bloomberg si schiera con Hillary*, Repubblica.it, 24 luglio 2016. Disponibile online: http://www.repubblica.it/esteri/elezioni-usa/primarie2016/2016/07/24/news/elezioni_usa_e_il_giorno_della_convention_democratica_per_hillary_arriva_l_endorcement_di_bloomberg-144753795/?ref=search.

rendendo impossibile usare i servizi di Twitter, Amazon, Netflix e accedere al sito del New York Times, per diverse ore. L'attacco ai DNS server della società DYN ha avuto ripercussioni anche in Europa. Lo ha fatto reclutando una rete botnet di circa 100.000 telecamere connesse a Internet basate su schede della cinese XiongMai Technologies, tutte con le stesse username e password.

Il 13 novembre 2016 LeakedSource rivelò che AdultFriendFinder, sito per incontri sessuali tra adulti, venne preso di mira dagli hacker per la seconda volta in due anni. In quest'occasione vennero rubate le credenziali di 412 milioni di utenti, pubblicate e messe in vendita in anonimi *marketplace* del *dark web* compresi di status utente, email e cronologia di navigazione. AdultFriendFinder non ha mai voluto confermare la rivelazione di LeakedSource.

Il 25 novembre 2016 un attacco al sistema informatico dell'autorità per il trasporto pubblico di San Francisco, Muni, bloccò per due giorni i sistemi di pagamento della metropolitana facendo viaggiare gratis i pendolari. Gli hackers rivendicarono di essere entrati in possesso di 30GB di dati degli impiegati e degli abbonati e chiesero un riscatto di 100 Bitcoins, circa $73,000 dollari.

Il 14 dicembre 2016, sempre la multinazionale Yahoo! annunciò che imprecisati hacker al soldo di uno stato non identificato hanno rubato nomi, indirizzi email, numeri di telefono, date di nascita e domande e risposte di sicurezza criptati o in chiaro da più di 1 miliardo di account. L'attacco risalirebbe al 2013 ma non avrebbe compromesso dati finanziari.

L'elenco non è non può essere esaustivo, sia per la naturale ritrosia delle aziende coinvolte ad ammettere *data loss* e *data breach*, sia perché, pur riguardando imprese transnazionali, non contempla gli attacchi avvenuti in quadranti del globo diversi da quello Occidentale. Che cosa c'è di grave in queste violazioni? la vita personale, le convinzioni, le pratiche, i rituali ed i bisogni delle persone via via coinvolte nei data breach sono state rilevate, esponendo questi individui a delle gravi minacce. Infatti, maggiori sono le informazioni che ci permettono di conoscere qualcuno, maggiori sono le capacità di manipolarlo. Per questo motivo la cyber security non riguarda solo gli stati, ma soprattutto le persone.

8.2. La Cyber security non riguarda gli stati ma le persone

Sotto il cappello della cyber security si tendono a raggruppare molti fenomeni diversi: le minacce cibernetiche, la guerra cibernetica, i crimini digitali (cyber threats, cyber warfare, cyber crimes). Queste denominazioni finiscono per indentificare, molto spesso, la cyber security esclusivamente con la sicurezza nazionale. Tuttavia non si deve dimenticare che i fenomeni citati riguardano le persone ed i loro comportamenti, definiscono i livelli di benessere e sicurezza degli individui, ma anche i diritti e le opportunità dei cittadini.

La cyber security riguarda sia gli individui che gli stati: sono gli individui, singoli ed associati, a soffrire gli effetti di attacchi informatici in un mondo dove le agenzie di sicurezza degli stati ed i giganti globali raccolgono e collezionano i dati personali e quelli relativi ai comportamenti di tutti noi. Il modo in cui queste informazioni sono gestiti limita sempre di più il diritto alla privacy e alla libertà d'espressione. Confondere la cyber security con la sicurezza nazionale, dunque, è sbagliato perché consente di eludere una riflessione globale su cosa significhi la sicurezza digitale in un contesto in cui, grazie alle nuove tecnologie, i poteri di sorveglianza statuali vengono ampliati, l'anonimato e la privacy vengono conseguentemente limitati e talvolta messi fuorilegge. Gli utenti sono molto spesso sorvegliati, i sistemi di garanzia indeboliti e le backdoor installate nei software più popolari, con la compiacenza di aziende spregiudicate o ricattate nel loro business principale: la gestione dei dati e delle identità degli utenti.

La cyber security è ormai l'altra faccia della privacy e riguarda diritti umani fondamentali, come il diritto di associazione, di cooperazione, di spostamento e di comunicazione. Questi sono i diritti di cui la privacy e la libera manifestazione del pensiero sono fondamento.

È un concetto difficile da apprendere? Se ci fermiamo a riflettere vediamo che non è così.

8.3. L'importanza della privacy

Privacy è un termine inglese che evoca significati talvolta mutevoli, accostabile ai concetti di "riservatezza", "privatezza". La sua prima concettualizzazione la dobbiamo a due avvocati, Samuel Warren e Louis Brandeis –

più tardi giudice della Corte Suprema americana – già alla fine del XIX secolo. Di fronte alla rivoluzione tecnologica dell'epoca, provocata dallo sviluppo della la fotografia, si sentirono obbligati a ripensare il diritto a essere lasciati in pace, schermati all'occhio inquisitore degli estranei. Oggi poiché viviamo in simbiosi con tecnologie in grado di monitorare ogni nostro comportamento, privacy non significa soltanto diritto di essere lasciati in pace o di proteggere la propria sfera privata, ma anche diritto di controllare l'uso e la circolazione dei propri dati personali che costituiscono il bene primario dell'attuale società dell'informazione.

Il diritto alla privacy è complementare al diritto alla sicurezza informatica per svariati motivi.

In primo luogo la privacy può essere interpretata come un limite al potere di governi e aziende. Come precedentemente accennato infatti, chi conosce i gusti, le inclinazioni ed i modelli di comportamento degli altri è potenzialmente in grado di manipolarne le scelte e le decisioni.

In aggiunta, attraverso il possesso dei dati personali, si può esercitare una sorta di controllo sulla vita degli individui. Attraverso questi ultimi infatti dipendono molte decisioni che influiscono tangibilmente sulla nostra vita, ad esempio la concessione di un mutuo, l'ottenimento di un''assicurazione o l'assunzione per un determinato lavoro. I dati personali sono usati per condurre indagini di polizia o per accordare la possibilità di viaggiare all'estero. Queste informazioni strettamente personali richiedono particolare attenzione soprattutto per quanto riguarda la loro diffusione mediante l'attività sul web. Se non sappiamo come vengono usati i nostri dati non siamo neppure capaci di correggerli e modificarli. Se non siamo autonomi non possiamo fare scelte libere.

In aggiunta, la privacy legata ai dati consente di gestire la propria reputazione ed è un aspetto molto importante perché quello che gli altri sanno di noi influenza opportunità, amicizie e benessere. Dal momento che conoscere i dettagli della vita di una persona non significa averne un'idea più accurata, la privacy ci aiuta ad evitare giudizi inaccurati che rischiano di diventare fonte di problemi.

Inoltre, ogni individuo stabilisce i confini fisici e informazionali della sua vita. A volte abbiamo bisogno di ritirarci e stare in solitudine, lontano dall'occhio indagatore degli altri. Spesso ci troviamo a regolare "i confini" delle informazioni che ci riguardano in base al tipo di persone con cui ci relazioniamo: la privacy ci aiuta a definire questi limiti.

La maggior parte delle relazioni interpersonali – dal rapporto psicanalista-paziente a quello tra il consulente bancario e un cliente – si basano sulla fiducia e il rispetto per la privacy è un elemento fondamentale per coltivarla e non rischiare di generare un clima di sfiducia socialmente pericoloso. Il diritto alla privacy va contemperato con altri diritti: l'intenzione di tenere privati determinati aspetti della propria vita, ovvero il diritto di cronaca, è spesso presentato come l'altro polo del diritto alla privacy. In aggiunta, elemento centrale dell'attività politica e sindacale è la riservatezza di cui gode il perseguimento di scelte personali prese in questi ambiti, un esempio è dato dalla segretezza del voto strumentale con lo scopo di evitare condizionamenti e rappresaglie.

Infine, la privacy permette di ricominciare, di cambiare vita, fallire ed imparare.

8.4. Le strategie nazionali

Secondo l'Unione Internazionale delle Telecomunicazioni (ITU), all'inizio del 2015, dei 193 paesi membri, 67 disponevano di una strategia nazionale per la Cyber security e 102 di un team di risposta agli incidenti informatici, i famosi CIRTs[5].

Ma è di poche settimane fa la decisione della Commissione Europa di stabilire delle norme certe di analisi e contrasto alle minacce informatiche e il Parlamento Europeo è orientato alla definizione di accordi e strategie di collaborazione tra gli stati membri che dovranno individuare i settori e le aziende (trasporti, sanità, imprese) da proteggere attraverso strumenti ad hoc.

Intanto organizzazioni internazionali come l'Unione Africana e quella degli stati americani lavorano da tempo a una serie di norme ed accordi di cooperazione validi a livello internazionale per elaborare strategie congiunte di confronto alle sfide odierne della Cyber security.

Tuttavia molto spesso queste negoziazioni sono strumentalizzate in chiave economica e diplomatica.

Il primo ministero cinese Xi Jinping nella sua ultima visita a Londra ha dedicato la parte centrale dei suoi incontri proprio alla definizione di una

[5] CIRT Programme: http://www.itu.int/en/ITU-D/Cybersecurity/Pages/Organizational-Structures.aspx.

strategia comune sulla cyber security[6] e lo stesso ha fatto poco dopo con gli Stati Uniti.

In antitesi, le più recenti leggi americane sulla cyber security riguardano la gestione della sorveglianza dei propri cittadini, in patria e all'estero, e, come lamentano la EFF e Access Now, anche dei cittadini stranieri di altri paesi.

In un'ottica di rispetto dei diritti umani, non è possibile pensare che la sottrazione dei dati personali di 22 milioni di dipendenti americani contenenti informazioni sulla salute, il reddito e l'abitazione possa essere inquadrata nella presunta guerra tra gli stati. In questo caso la colpa è ricaduta sulla Cina, anche se non sono state fornite prove[7]. Si è dunque preferito parlare di intromissione di una potenza avversaria e delle future rappresaglie invece di considerare l'organizzazione dei dati e la relativa normativa sulla loro detenzione.

Nonostante le ben note minacce dei nostri giorni, come lo stato di guerra permanente contro il terrorismo di matrice islamista, gli attentati nelle metropoli europee e gli allarmi per la sicurezza delle infrastrutture critiche, ci troviamo in una fase in cui la sicurezza informatica è diventata una priorità nella vita di tutti i giorni. Dal momento che i criminali informatici sono in grado di interferire con attività quotidiane, come controllare il GPS dell'automobile, svolgere attività di sorveglianza mediante un drone, spiare ed ascoltare attraverso una smart tv ed entrare con un click nella nostra casa domotica. Abbiamo quindi bisogno di una cyber security orientata alla protezione dei dati personali che anticipano e definiscono i nostri comportamenti. in un mondo in cui le nostre vite sono definite da un sé digitale che ogni giorno interagisce con realtà il cui core business è proprio l'estrazione e la raccolta dei dati personali per rivenderli al miglior offerente e che le stesse agenzie di welfare gestiscono in digitale tutto quello che ci rende cittadini con dei diritti (la salute, la pensione, la disoccupazione), mentre l'Internet of Things è lasciata priva di qualsivoglia controllo a causa di una legislazione insufficiente e arretrata.

[6] Mason R., *Xi Jinping state visit: UK and China sign cybersecurity pact*, The Guardian, 21st October 2015, Available at: https://www.theguardian.com/politics/2015/oct/21/uk-china-cybersecurity-pact-xi-jinping-david-cameron.

[7] Lever R., *Huge hack of US government data affected 21.5 mn*, Yahoo, 9th July 2015. Available at: https://www.yahoo.com/news/21-5-million-affected-us-government-data-breach-194354188.html.

Per questo occorre una nuova definizione di cyber security incentrata sui diritti delle persone e sugli utenti finali della tecnologia, e non sui sistemi nazionali e infrastrutturali.

Cosa possiamo fare? Secondo due ricercatori di *Open Democracy*, Andrew Puddephatt e Lea Kaspar occorre:

- definire un quadro legale e normativo, certo e dettagliato sulla proprietà dei dati personali in grado di rimettere in mano alle persone il controllo delle proprie informazioni e non lasciarlo ai fornitori di servizi internet;
- garantire la possibilità di usare la crittografia end to end nelle comunicazioni;
- avviare dei progetti per aumentare la consapevolezza dell'importanza dell'educazione alla privacy e alla protezione dei dati personali;
- costruire delle agenzie di monitoraggio che garantiscano la tutela dei diritti fondamentali nella raccolta dei dati in modo da limitarne e controllarne l'operato;
- chiedere ai governi di mettere in campo risorse umane e strumentali con personale competente in grado di intervenire a livello giudiziario sulle violazioni della privacy aziendale e individuale;
- coinvolgere i cittadini nella definizione delle *policies* pubbliche che li riguardano, a ogni livello, con un approccio *multistakeholder*;
- sviluppare un ampio dibattito pubblico su cosa significhi essere sicuri in un mondo digitale e interconnesso, dove l'apertura e la resilienza di Internet siano una risorsa anziché un limite alla gestione delle vite delle persone.

Alcune di queste proposte sono finite nel piano d'azione dell'Unione Europea preannunciato da Andrus Ansip e confermato da Carl Juncker nel suo discorso sullo stato dell'Unione del settembre 2017.

Da tutto questo discende un corollario: la sicurezza informatica è un diritto di tutti e per questo bisogna limitare l'hacking di stato.

Se la sicurezza informatica è un diritto umano ed è la precondizione per esercitare altri diritti come il diritto alla privacy, alla libera manifestazione del pensiero e alla libertà d'informazione, senza protezione dallo "sguardo" altrui non è possibile sviluppare la propria identità, proteggersi dai pregiudizi e esercitare le proprie libertà costituzionali. Per questo è ora di mettere un freno all'hacking di stato.

Possiamo essere grati a Snowden, Assange, e a tutti gli altri che hanno svelato come alcuni governi abbiano utilizzato larghe porzioni degli apparati statali, pagati dai contribuenti, per influenzare il comportamento e le decisioni dei propri cittadini e di quelli di altri paesi. Ma loro stanno pagando un prezzo altissimo per averlo fatto. Quante volte dovrà accadere ancora?

8.5. Che cos'è l'hacking di stato?

L'hacking di stato può essere definito in base ad alcuni dei suoi obiettivi: controllare i messaggi, causare un danno, sorvegliare, ed è per questo che è una pratica che riguarda tutti. Riguarda gli indagati per un reato penale e i loro interlocutori. L'hacking di stato non riguarda solo presunti criminali ma può riguardare semplici e ignari cittadini, estranei alle condotte che si vuole indagare o impedire. Può riguardare i cooperanti nelle zone di guerra, organizzazioni antimafia, servitori dello stato, *whistleblower* che denunciano truffe, sprechi e malversazioni nelle aziende e nei governi per cui lavorano.

Se non vogliamo considerare come l'uso di armi cibernetiche, della censura o il blocco di Internet (*Internet shutdowns*) da parte di governi e forze militari danneggi attività lecite e costituzionalmente protette, che dire dell'uso non regolato dei captatori informatici, dei trojan di stato, delle campagne di phishing e delle intercettazioni a strascico?

L'hacking di stato fornisce accesso a informazioni di fonti protette, come le fonti giornalistiche, le associazioni anti-pizzo, le organizzazioni non governative che combattono la tratta dei migranti o quelle dedite alle cause dell'inquinamento delle acque. Questo accade quando le informazioni sono create, transitano e vengono poi raccolte. Vi ricordate il blogger saudita Raif Badawi sorvegliato con gli strumenti di Hacking team? E la fine che hanno fatto gli oppositori di Assad e di Ahmadinejad in Iran, degli egiziani del movimento del 6 aprile? Tutti incarcerati. E i loro amici? Finiti in un girone dantesco.

Di concerto, l'hacking di stato può danneggiare software e hardware, producendo ingenti danni economici. In aggiunta, sempre secondo una prospettiva di tutela dei diritti umani, dispositivi di persone che non sono direttamente coinvolte con le operazioni di intelligence possono essere infettati e conseguentemente il lavoro di chi opera in quest'ultima, la loro identità e i loro scopi possono esserne compromessi.

L'hacking di stato, usato sia per la sorveglianza sia per la raccolta di informazioni, andrebbe quindi regolamentato.

1. L'hacking di stato dovrebbe essere regolamentato per legge e le sue modalità dovrebbero essere pubbliche e trasparenti senza produrre discriminazioni di sorta.
2. Gli attori dell'hacking di stato dovrebbero motivarne le ragioni e spiegare sempre perché è considerato il mezzo meno invasivo per ogni tipo di informazione cercata. La sorveglianza di massa andrebbe proibita.
3. L'autorizzazione governativa all'hacking di stato dovrebbe prevedere una conclusione temporale e non influenzare soggetti estranei alle operazioni.
4. L' hacking di stato dovrebbe essere approvato dall'autorità giudiziaria competente, che deve essere indipendente rispetto agli organi inquirenti.
5. L'hacking di stato dovrebbe prevedere delle comunicazioni di garanzia verso il bersaglio delle operazioni.
6. Le agenzie responsabili dell'hacking di stato dovrebbero pubblicare almeno annualmente dei rapporti che indichino l'estensione delle operazioni e la loro durata, ma anche i risultati o le conseguenze inattese.
7. L'hacking di stato non dovrebbe mai obbligare entità private a intervenire su prodotti e servizi con l'intento di comprometterne la sicurezza.
8. Se L'hacking di stato eccedesse scopi e autorizzazioni, i responsabili dovrebbero fare rapporto all'autorità giudiziaria e spiegarne i motivi.
9. L'hacking di stato extraterritoriale dovrebbe seguire norme giuridiche internazionali.
10. Le agenzie che fanno hacking di stato non dovrebbero poter collezionare bug, exploit e *zero-days*, anzi dovrebbero rendere pubbliche le vulnerabilità scoperte o acquisite e rilasciarne l'informazione almeno una volta l'anno.

9. CYBER SECURITY, CRIPTOVALUTE E CRIMINALITÀ

di *Irene Piccolo*[*]

Uno dei profili in cui gli Stati devono tutelare la propria sicurezza è, tradizionalmente, quello della lotta alla criminalità, non solo in termini di prevenzione dei reati, ma anche con riguardo ai proventi derivanti dalle attività criminali, al loro utilizzo e al loro riciclaggio. Tale compito da parte dell'autorità statale diventa più arduo e si complica nel momento in cui, da classici domini come terra, mare e spazio, si passa a quello cibernetico. Difatti, la lentezza dell'approccio con cui gli Stati si sono dedicati alla comprensione di questa nuova dimensione e del suo funzionamento, con relativi pregi e lati oscuri, ha fatto sì che il vuoto lasciato, *rectius* non ancora occupato, dallo Stato divenisse terreno in cui individui e organizzazioni criminali possono operare in maniera incontrastata.

Ciò è particolarmente vero per il *darknet*, che – sebbene venuto agli onori delle cronache in funzione del ruolo svolto nelle attività di proselitismo via web delle organizzazioni terroristiche nonché nelle attività propedeutiche alla realizzazione di attentati – è altresì il luogo in cui il mercato nero di armi, droga e altre "merci" (si pensi al contrabbando di fauna protetta riscontrato recentemente da Interpol[1]) vive e si nutre, e lo fa attraverso le criptovalute[2].

[*] PhD in Diritto pubblico, comparato e internazionale, attualmente ricopre la carica di Presidente dell'Associazione per la promozione della cultura internazionale "AMIStaDeS – Fai Amicizia con il Sapere".

[1] Vedi la *press release*: https://www.interpol.int/News-and-media/News/2017/N2017-080.

[2] La Banca Centrale Europea e la Banca d'Italia ne hanno evidenziato molteplici schemi: 1) valute virtuali non convertibili, spendibili solo all'interno della comunità virtuale che le accetta; 2) valute virtuali a convertibilità limitata, acquistabili con moneta tradizionale (es. utilizzando carte di credito o di debito), ma che non è possibile riconvertire in moneta tradizionale; 3) valute virtuali pienamente convertibili, scambiabili con moneta tradizionale, con valore derivante da domanda e offerta.

Il bitcoin è indubbiamente la moneta digitale più nota, ma non è certamente la sola; anzi, nel giro di pochi anni si è passati da un centinaio di criptovalute a oltre 550 di queste monete[3], che nel loro complesso – secondo le stime fatte da *Coinmarketcap* – hanno raggiunto una capitalizzazione complessiva di 376 miliardi di dollari, superando in questo modo ExxonMobil e JP Morgan.

Limitando la trattazione al bitcoin[4], esso è una valuta "coniata" da persone (c.d. *miners*[5]) che mettono a disposizione i propri computer e relativi sistemi di calcolo, organizzati in nodi in collegamento *peer to peer*[6] che validano i trasferimenti – concepiti come veri e propri cambi di proprietà di valuta – verificando l'autenticità e la disponibilità dei fondi. L'Italia si trova al 23° posto con ben 53 nodi attivi, concentrati soprattutto nel nord del Paese.

Il controllo e la ratifica delle operazioni di pagamento vengono quindi effettuati attraverso sei blocchi informatici (c.d. *blockchain*), che analizzano i codici identificativi dei proprietari del singolo bitcoin o frazione di bitcoin – divisibile fino a 16 volte – e si assicurano che, per lo stesso codice, la singola criptovaluta non venga spesa più di due volte. I codici alfanumerici (di circa 33 caratteri) costituiscono di fatto la chiave pubblica di decifrazione (c.d. indirizzi bitcoin) e sostituiscono nome e cognome del proprietario del conto, il quale può disporre del proprio "portafoglio" virtuale solo utilizzando la sua password di decriptazione (chiave privata con cui appone la propria firma digitale, verificata dalla rete attraverso la chiave pubblica e che, se smarrita, comporta la perdita irreparabile della somma di denaro/bitcoin contenuta nel portafoglio virtuale)[7]. Questa attività di criptazione (motivo

[3] Tra queste vi sono Litecoin, Peercoin (non decentralizzato), Ethereum, Primecoin Si segnala, per un approfondimento sul tema, *The Crypto-Currency. Bitcoin and its mysterious inventor*, in "The New Yorker", 10 ottobre 2011, www.newyorker.com/magazine/2011/10/10/the-crypto-currency.

[4] I principi del sistema sono descritti nel "libro bianco" pubblicato da Satoshi Nakamoto (pseudonimo utilizzato dal/i creatore/i della criptovaluta) nel 2008, da cui è stato realizzato il client ufficiale – il software libero *Bitcoin Core* – che implementa il protocollo di comunicazione utilizzando l'algoritmo *Elliptic Curve Digital Signature Algorithm* (ECDSA).

[5] Difatti, il processo di creazione della moneta è chiamata *mining* con riferimento piuttosto esplicito al *gold mining*.

[6] Tanto più le persone mettono a disposizione i propri sistemi tanto più le transazioni sono sicure: proprio questo aspetto, tuttavia, costringe a prendere in seria considerazione la variabile connessa all'energia elettrica consumata per la produzione dei bitcoin che, essendo in continuo incremento, prima o poi comporterà l'interruzione dell'attività di *mining*.

[7] Andreas M. Antonopoulos, *Mastering Bitcoin. Unlocking Digital Crypto-Currencies*, O'Reilly Media, aprile 2014.

per il quale siamo in presenza di una criptovaluta) implica che nel mondo dei bitcoin vige l'anonimato, *rectius* lo pseudonimato.

Non vi è quindi nella vita del bitcoin né un passaggio "creativo" né uno di controllo/vigilanza da parte di una banca centrale statale, per cui si parla di valuta decentralizzata[8] che non è né soggetta né assoggettabile a politiche monetarie di sorta. Se da un lato l'assenza di una banca centrale evita *ab initio* la possibilità di inflazione di bitcoin, dall'altro lato ciò implica minori garanzie per i possessori per quanto riguarda sia l'esistenza effettiva di tali criptovalute sia la prevenzione di eventuali bolle speculative create *ad hoc*.

9.1. Le criptovalute e la finanza

La regola fondamentale dell'economia secondo cui l'ottimismo e la predisposizione positiva degli individui sta alla base del successo di una politica economica si applica anche al bitcoin, che deve il suo exploit proprio alla fiducia riscontrata tra gli utenti. Le valute virtuali, infatti, hanno valore solamente se accettate dal mercato, quindi solo se ritenute utili da una comunità, per cui l'eventuale perdita di "consenso" costituirebbe un rischio per i possessori. Tuttavia, alcuni – tra cui il premio Nobel per l'economia Joseph Stiglitz, che suggerisce la messa al bando del bitcoin[9] – ritengono che tale fiducia sia legata essenzialmente al fatto che i bitcoin sono sottratti a una qualunque vigilanza e ciò fa sentire gli utenti liberi di tenere qualsiasi condotta, lecita o meno che sia.

Il valore, il cambio e la gestione del bitcoin dipendono quindi dall'incrocio delle linee di domanda e offerta, che si verifica su piattaforme specificamente predisposte, quali *Bitfinex* e *Coinbase*, che recentemente stanno però subendo massicci attacchi hacker. L'ultimo è avvenuto a danno di NiceHash

[8] Oltre alla distinzione tra valute virtuali centralizzate e decentralizzate, vi è quella tra valute virtuali decentralizzate e valute complementari locali, ossia quelle utilizzate in ambiti molto ristretti (es. una città o una regione) e tra un numero limitato di utenti, da non considerarsi quindi valute virtuali ai fini dell'applicazione delle normative in materia.

[9] *Bitcoin 'Ought to Be Outlawed,' Nobel Prize Winner Stiglitz Says*, Bloomberg, 29 novembre 2017, https://www.bloomberg.com/news/articles/2017-11-29/bitcoin-ought-to-be-outlawed-nobel-prize-winner-stiglitz-says-jal10hxd.

(marketplace di *mining*), che ha subito un "furto" di bitcoin per un valore di circa 70 milioni di dollari[10].

Alcuni temono che l'eccessiva volatilità del bitcoin (che alcuni giorni fa ha registrato il valore record di 19.000 $[11] con oscillazioni nell'arco della stessa giornata di 2 – 2.500 $) nasconda in realtà la creazione di un'enorme bolla speculativa destinata a scoppiare nel medio periodo. A fronte, ad esempio, dell'autorizzazione rilasciata dalla *Commodity Futures Trading Commission* (Cftc) alle Borse di Chicago, CME Group e CBOE Global Markets per lanciare *futures* sulle criptovalute (i.e. derivati su bitcoin), la *Futures Industry Association*, che raggruppa i principali broker – tra cui Goldman Sachs, JP Morgan Chase e Citigroup – ha inviato alla Cftc un documento in cui esprimeva forti dubbi su tali operazioni. Ciononostante, dal 10 dicembre 2017 (ore 24.00 italiane) il bitcoin può essere scambiato, con il codice XBT, al mercato delle opzioni di Chicago mentre lunedì 11 dicembre è il primo giorno di contrattazioni e, come si legge nel comunicato del *Cboe futures exchange*[12], sono previste tre diverse scadenze per le opzioni sulla criptovaluta: 17 gennaio, 14 febbraio e 14 marzo 2018. Il timore di bolla speculativa, tuttavia, induce molti utenti a cercare un'alternativa più stabile, quale ad esempio *tether*, una criptovaluta in circolazione dal 2015 che dovrebbe attualmente avere un valore di 814 milioni di dollari. In questo caso il condizionale è d'obbligo giacché la stabilità di questa valuta dipende dal suo essere ancorata al dollaro (i.e. si custodisce una riserva di un dollaro per ogni *tether* emesso, a garanzia della criptovaluta messa in circolazione, funzione pressoché assimilabile a quella svolta dalle riserve d'oro presso le banche centrali); tuttavia, i nomi delle banche in cui queste riserve sarebbero state depositate non sono noti[13].

[10] Vedi l'articolo al link: http://ilpiccolo.gelocal.it/trieste/cronaca/2017/12/09/news/gli-hacker-rubano-70-milioni-in-bitcoin-1.16217024.

[11] *Bitcoin a briglia sciolta, quotazioni impazzite fino a 19mila dollari*, in "Il Sole 24 Ore", 7 dicembre 2017. Questi rialzi hanno portato alla capitalizzazione del bitcoin per oltre 200 miliardi di dollari, sfidando la Johnson & Johnson per il settimo posto nella top ten di Wall Street delle società a maggior capitalizzazione dell'economia reale e superando colossi come la Coca Cola. Vedi: http://www.wallstreetitalia.com/bitcoin-senza-freni-sopra-15-mila-vale-piu-di-coca-cola-e-quanto-jj/.

[12] Reperibile al link: http://cfe.cboe.com/cfe-products/xbt-cboe-bitcoin-futures.

[13] *There's an $814 Million Mystery Near the Heart of the Biggest Bitcoin Exchange*, Bloomberg, 5 dicembre 2017, https://www.bloomberg.com/news/articles/2017-12-05/mystery-shrouds-tether-and-its-links-to-biggest-bitcoin-exchange.

Altri, invece, ritengono che questo drastico incremento nel valore del bitcoin sia spiegabile con motivazioni geopolitiche: se Cina (dove avviene la maggior parte degli scambi di bitcoin) e Russia iniziassero, ad esempio, ad accettare i bitcoin come alternativa al dollaro statunitense, il valore di questa moneta virtuale schizzerebbe in alto; altro esempio è l'ipotesi prospettata da Russell Newton, ex responsabile di JP Morgan, secondo cui dopo la Brexit il progetto dell'Euro è destinato a declinare venendo compensato dal ricorso al bitcoin.

La diffusione del bitcoin e delle criptovalute in generale è un fenomeno che deve essere considerato anche dalle autorità italiane, giacché molti erogatori di beni e servizi hanno da tempo iniziato ad accettare pagamenti in bitcoin e le operazioni in bitcoin sono attività sempre più diffuse tra gli italiani[14]. Ciò spiega l'installazione, già da alcuni anni, di primi ATM[15] da cui si possono prelevare e/o versare (a seconda della tipologia) contanti nel proprio conto bitcoin convertiti al tasso di cambio vigente al momento dell'operazione. La criptovaluta, inoltre, si sta diffondendo nel mondo del *gaming*[16] e anche l'Agenzia delle Entrate ha dovuto considerare il fenomeno valutando la possibilità di tassare i bitcoin[17]. Al contempo, l'Unità di Informazione Finanziaria (UIF) istituita presso la Banca d'Italia ha documentato casi di riciclaggio, ad esempio, tramite investimenti in valute virtuali di fondi pubblici destinati alla formazione professionale[18].

[14] Situazioni simili si riscontrano anche in altri Paesi, ad esempio per il pagamento in bitcoin di tasse universitarie o di servizi sanitari e trasporti pubblici. Cfr. *Le tasse universitarie a Cipro si pagano in Bitcoin*, in "Il Sole 24 Ore", 21 novembre 2013; *Zugo, la capitale del Bitcoin: sarà possibile pagare sanità e trasporti*, in "La Repubblica", 11 maggio 2016.

[15] Vedi ad esempio: http://www.repubblica.it/tecnologia/2014/10/20/news/bitcoin_italia-98573671/ e http://www.repubblica.it/tecnologia/2014/06/11/news/il_primo_bitcoin_bancomat_in_italia-88645518/.

[16] Nel 2014 è nato BetVip, primo boomaker con regolare licenza ad accettare esclusivamente puntate in Bitcoin; successivamente sono stati aperti anche casinò e poker on line.

[17] Agenzia delle Entrate, Risoluzione 72/E, 2 settembre 2016, consultabile al link: http://www.agenziaentrate.gov.it/wps/wcm/connect/52bf008f-fab5-46f6-9d64-f334f1f3119a/RISOLUZIONE+N.+72+DEL+02+SETTEMBRE+2016E.pdf?MOD=AJPERES&CACHEID=52bf008f-fab5-46f6-9d64-f334f1f3119a.

[18] Banca d'Italia, Unità di Informazione Finanziaria, *Quaderni dell'antiriciclaggio: Analisi e studi, Casistiche di riciclaggio e di finanziamento del terrorismo*, dicembre 2016, https://uif.bancaditalia.it/pubblicazioni/quaderni/2016/quaderni-7-2016/quaderni_7_2016.pdf.

9.2. Le criptovalute e la criminalità

Nonostante le notevoli implicazioni economiche messe in evidenza, l'altro ambito su cui questo paper vuole richiamare l'attenzione è quello della criminalità. Difatti, l'economia criminale è la maggior utilizzatrice di bitcoin, soprattutto nel *darknet* che usa protocolli di criptatura. Basti pensare, ad esempio, al caso del sito *Silk Road*, lanciato nel febbraio 2011[19] e chiuso definitivamente dall'FBI nel novembre 2014, in cui utilizzando come moneta proprio il bitcoin si vendevano principalmente droga, armi e documenti falsi.

Nel tempo il bitcoin, così come altre criptovalute, si è rivelato quotatissimo anche per il riciclaggio[20] di denaro che, sparendo in un punto preciso del mondo, viene fatto riapparire in un altro punto senza che sia possibile tracciarne i trasferimenti, giacché l'unico dato pubblico e visibile dei "correntisti" è il codice alfanumerico. Nell'ottobre 2015, con un nuovo report sui rischi del finanziamento al terrorismo[21], la *Financial Action Task Force* (FATF) è tornata a occuparsi dei bitcoin e ha alzato il livello di attenzione riportando il caso, verificatosi nello Stato americano della Virginia, di Ali Shukri Amin che, il 28 agosto 2015, è stato condannato a 11 anni di prigione per aver cospirato per fornire materiale, supporto e risorse allo Stato Islamico (IS) attraverso il ricorso a Internet. Nello specifico Amin usava Twitter per fornire, tra l'altro, istruzioni su come usare bitcoin per mascherare la fornitura di fondi per IS.

Progressivamente tutti gli organismi internazionali hanno dovuto attivarsi in questo campo, soprattutto con l'accrescersi delle possibilità che le criptovalute fossero strumento per foraggiare il terrorismo: se il Consiglio

[19] Vedi anche *Sesso, droga e armi: la faccia cattiva del web*, in "La Repubblica", 11 aprile 2012. disponibile al link: www.repubblica.it/tecnologia/2012/04/11/news/sesso_droga_e_armi_la_faccia_cattiva_del_web-33089682/.

[20] Definizione ex art. 648-bis C. p. italiano: "*Fuori dei casi di concorso nel reato, chiunque sostituisce o trasferisce denaro, beni o altre utilità provenienti da delitto non colposo, ovvero compie in relazione ad essi altre operazioni, in modo da ostacolare l'identificazione della loro provenienza delittuosa, è punito con la reclusione da quattro a dodici anni e con la multa da euro 1.032 a euro 15.493.* […]".

[21] FATF Report, *Emerging Terrorist Financing Risks*, Ottobre 2015. Disponibile al link: http://www.fatf-gafi.org/media/fatf/documents/reports/Emerging-Terrorist-Financing-Risks.pdf Si segnala che già nel 2013 la FATF aveva realizzato una guida sulle nuove e relativamente nuove modalità di pagamento: *Guidance for a risk-based approach, 'Prepaid cards, mobile payments and internet-based payment services'*, giugno 2013, http://www.fatf-gafi.org/media/fatf/documents/recommendations/Guidance-RBA-NPPS.pdf.

d'Europa era stato il primo che aveva rivolto lo sguardo al dominio cyber attraverso la Convenzione di Budapest sul Cybercrime (23 novembre 2001)[22], adesso ritroviamo uno sguardo più attento sia sul fronte investigativo che su quello normativo. Sul primo aspetto, a livello internazionale vi è ad esempio un costante impegno di Interpol[23] che ha tra l'altro creato, con Europol e il *Basel Institute on Governance,* un *Working Group on Digital Currencies* per la raccolta di dati e l'analisi sull'uso di valute digitali per attività di riciclaggio da parte dei criminali nonché per lo sviluppo di strategie per indagini e recupero di proventi criminali digitali. Nell'ambito di questa collaborazione, a gennaio 2017 si è tenuta a Doha la prima *Global Conference on Money Laundering and Digital Currencies*. Tuttavia anche a livello nazionale va riscontrato l'occhio vigile della nostra Direzione investigativa antimafia, la quale già per il primo semestre del 2016 ha dovuto riscontrare che il "fascino criminale" delle criptovalute ha attirato l'interesse della 'ndrangheta.

Sul fronte normativo, invece, nessun governo ha dichiarato illegale il bitcoin – sebbene Paesi come la Cina stiano iniziando a mettere in atto alcuni divieti[24] – per cui le attività ad esso connesse sono tutte considerate lecite; ciononostante, le criptovalute hanno iniziato ad essere attenzionate dalle normative antiriciclaggio. L'Italia, prima tra gli Stati membri dell'Unione Europea, ha recepito la IV Direttiva antiriciclaggio (Direttiva UE 2015/859) attraverso il d.lgs. 25 maggio 2017 n. 90[25], in vigore dal successivo 4 luglio e che modifica *in toto* la normativa del 2007 (d.lgs. 231). Con essa l'Italia ha anticipato alcune disposizioni inserite nella proposta presentata dalla

[22] Testo al link: https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680081561.

[23] Interpol ospita, inoltre, all'interno del *Global Complex for Innovation* (IGCI) il programma di supporto alle polizie di 190 Paesi nel perseguire i crimini digitali (*Global Cybercrime Programme*).

[24] *China bans companies from raising money through ICOs, asks local regulators to inspect 60 major platforms*, Cnbc, 4 settembre 2017. https://www.cnbc.com/2017/09/04/chinese-icos-china-bans-fundraising-through-initial-coin-offerings-report-says.html.

[25] Attuazione della direttiva (UE) 2015/849 relativa alla prevenzione dell'uso del sistema finanziario a scopo di riciclaggio dei proventi di attività criminose e di finanziamento del terrorismo e recante modifica delle direttive 2005/60/CE e 2006/70/CE e attuazione del regolamento (UE) n. 2015/847 riguardante i dati informativi che accompagnano i trasferimenti di fondi e che abroga il regolamento (CE) n. 1781/2006. (17G00104). G.U. Serie Generale n. 140 del 19.6.2017 – Suppl. Ordinario n. 28.

Commissione[26] per la modifica della IV Direttiva: ha reso infatti gli *Exchangers* (considerati operatori non finanziari, ex art. 5.5 d.lgs. 231/2007 come modificato dal d.lgs. 90/2017) soggetti destinatari delle normative antiriciclaggio, imponendo l'obbligo – già vigente da tempo negli Stati Uniti – di iscrizione in apposito registro come "cambiavalute virtuali"[27].

Difatti, il sistema bitcoin nasce – come detto – decentralizzato ed è resiliente alle normative, ma è possibile regolamentarne alcuni attori ed è in questa direzione che i legislatori nazionali e internazionali si stanno muovendo. Nell'ecosistema delle criptovalute, che conta almeno altri tre soggetti principali[28], gli *Exchangers* sono costituiti dalle piattaforme di scambio in cui avviene la conversione delle valute virtuali in o verso valute a corso legale (vi rientrano anche gli ATM). Si tratta dunque di soggetti che operano nel punto di congiunzione[29] tra il mondo delle monete legali e il mondo delle

[26] COM(2016) 450 final, Proposta di Direttiva del Parlamento Europeo e del Consiglio che modifica la direttiva (UE) 2015/849 relativa alla prevenzione dell'uso del sistema finanziario a fini di riciclaggio o finanziamento del terrorismo e che modifica la direttiva 2009/101/CE, 5 luglio 2016. Disponibile al link: https://ec.europa.eu/transparency/regdoc/rep/1/2016/IT/1-2016-450-IT-F1-1.PDF.

[27] L'art. 1 del d.Lgs. 231/2007 (come modificato dal d.Lgs. 90/2017) definisce:
"*ff) prestatori di servizi relativi all'utilizzo di valuta virtuale: ogni persona fisica o giuridica che fornisce a terzi, a titolo professionale, servizi funzionali all'utilizzo, allo scambio, alla conservazione di valuta virtuale e alla loro conversione da ovvero in valute aventi corso legale;*
q) valuta virtuale: la rappresentazione digitale di valore, non emessa da una banca centrale o da un'autorità pubblica, non necessariamente collegata a una valuta avente corso legale, utilizzata come mezzo di scambio per l'acquisto di beni e servizi e trasferita, archiviata e negoziata elettronicamente".
Si tratta di definizioni analoghe a quelle contenute nella proposta emendata COM (2016) 450 della Commissione Europea, dove per "*Exchangers*" s'intendono "*prestatori di servizi la cui attività principale e professionale consiste nella fornitura di servizi di cambio tra valute virtuali e valute legali*" e per "*valuta virtuale*" s'intende "*una rappresentazione di valore digitale che non è né emessa da una banca centrale o da un ente pubblico né è legata a una valuta legalmente istituita, non possiede uno status giuridico di valuta o moneta, ma è accettata da persone fisiche e giuridiche come mezzo di scambio, ed eventualmente per altri fini, e può essere trasferita, memorizzata o scambiata elettronicamente*".

[28] Secondo la proposta COM (2016) 450, gli altri operatori sono: a. gli utenti (investitori, *merchants*, consumatori che usano le valute virtuali per effettuare pagamenti o acquistare beni o servizi); b. minatori (*miners*), che validano le transazioni ricevendo valute virtuali quali compensazioni per il loro servizio; c. fornitori di portafoglio (*wallet providers*) dove gli utenti tengono i loro conti virtuali, suddivisibili in *software wallet provider* (es. applicazioni di accesso al network) e *custodial wallet providers* (i.e. quelli che detengono la chiave privata degli utenti, controllando quindi le valute virtuali).

[29] In particolare, essi possono ritrovarsi a operare in diverse situazioni in cui i rischi sono altrettanto diversi: 1) vendita di bitcoin contro strumenti tracciati (ossia provenienti da altro

criptovalute e sono gli unici (sebbene la Commissione europea abbia proposto l'estensione della normativa anche ai *wallet providers*) su cu si possa operare efficacemente, dal momento che – come già sottolineato – è impossibile associare nomi e cognomi agli indirizzi bitcoin, e quindi individuare gli utenti.

Tuttavia, vi è dibattito giuridico sul fatto che si possa parlare effettivamente di cambiavalute e applicare, dunque, la normativa riferita alle valute giacché il bitcoin – così come le altre criptovalute – non è riconosciuto come valuta avente corso legale. Allo stato attuale, infatti, l'Unità di Informazione Finanziaria (UIF) istituita presso la Banca d'Italia ha ribadito, rifacendosi a quanto precedentemente affermato da *European Banking Authority* (EBA)[30], *Financial Action Task Force* (FATF)[31] e Banca Centrale Europea(BCE)[32], che "le valute virtuali […] non costituiscono moneta legale né sono assimilabili alla moneta elettronica"[33]. Ciononostante esse hanno indubbiamente finalità di "mezzo di pagamento[34] e possono, inoltre, assumere altro valore giuridico a seconda della funzione svolta: sono beni mobili e immateriali (dato che non esistono fisicamente)[35]; sono considerabili *commodity* (come i metalli o i

operatore cui si applica la normativa AML); 2) vendita di bitcoin contro strumenti non tracciati (contanti); 3) acquisto di bitcoin pagando con strumenti tracciati; 4) acquisto di bitcoin pagando con strumenti non tracciati.

[30] *EBA Opinion on 'virtual currencies'*, 4 luglio 2014. Disponibile al link: http://www.eba.europa.eu/documents/10180/657547/EBA-Op-2014-08+Opinion+on+Virtual+Currencies.pdf.

[31] FATF Report, *Virtual Currencies*, giugno 2014. Disponibile al link: http://www.fatf-gafi.org/media/fatf/documents/reports/Virtualcurrency-key-definitions-and-potential-aml-cft-risks.pdf.

[32] ECB - *Virtual Currency Schemes*, ottobre 2012. Disponibile al link: http://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf.

[33] Banca d'Italia, Unità di Informazione Finanziaria, *Comunicazione sull'utilizzo anomalo di valute virtuali,* 30 gennaio 2015.

[34] Corte di Giustizia Europea, sentenza del 22 ottobre 2015, causa C-264/14, *Skatteverket c. David Hedqvist*, consultabile al link: http://curia.europa.eu/juris/document/document.jsf?text=&docid=170305&pageIndex=0&doclang=IT&m ode=lst&dir=&occ=first&part=1&cid=581757.

[35] Tale considerazione ha le sue conseguenze giuridiche nel momento in cui si verificano "furti" di criptovalute in seguito ad attacchi hacker. Difatti, ai sensi dell'art. 624 del nostro codice penale il reato di furto è così definito: "*Chiunque s'impossessa della cosa mobile altrui, sottraendola a chi la detiene, al fine di trarne profitto per sé o per altri, è punito con la reclusione da sei mesi a tre anni e con la multa da euro 154 a euro 516*", ma richiedendo il concetto di "cosa" il requisito della materialità ed essendo invece la criptovaluta immateriale, si deve propendere per la configurazione del reato di furto di identità digitale, giacché è attraverso questa identità che viene controllata la criptovaluta (vedi art. 640-ter CP: "*1. Chiunque, alterando in qualsiasi modo il funzionamento di un sistema informatico o telematico o intervenendo senza diritto con qualsiasi modalità su dati, informazioni o programmi contenuti in un sistema informatico o telematico o ad esso pertinenti, procura a sé o ad altri un ingiusto*

carburanti)[36] in quanto bene fungibile prodotto da un'attività umana e riconosciuto da una determinata comunità quale valore; strumento finanziario (*securities*) in quanto la valutazione dipende da domanda e offerta ed è scambiato in un mercato. A fronte poi del tentativo estone di creare una criptovaluta centralizzata e statale, il presidente della BCE Mario Draghi ha rifiutato qualunque autorizzazione, giacché secondo il diritto comunitario nessuno Stato membro può introdurre una propria valuta e ha, al contempo, dichiarato che la BCE non è competente da trattato a occuparsi di criptovalute[37].

In attesa di poter analizzare i primi effetti della normativa, si segnala infine una delle risposte che gli Stati Uniti forniscono al fenomeno del riciclaggio di denaro attraverso le criptovalute: il 1° ottobre 2017 è entrata in circolazione Aml Bitcoin, dove "Aml" sta per "Anti-money laundering". Si tratta della prima criptovaluta che rispetta *in toto* le leggi americane in materia di antiriciclaggio, antiterrorismo, segreto bancario e contro i crimini finanziari in generale. Inventata in California dall'imprenditore Marcus Andrade e controllata dalla Nac Foundation Llc, da questi fondata nel 2014 per sviluppare un protocollo identico a quello dei Bitcoin originali (i.e. la blockchain), essa ha l'ambizione di ispirare sicurezza, credibilità e fiducia tra le organizzazioni, le istituzioni finanziarie, gli individui e le parti interessate per essere riconosciuta come la moneta digitale preminente nel mondo.

Al momento è stato inevitabile iniziare la lotta a questi fenomeni estendendo al dominio cibernetico la normativa pensata per fenomeni simili ma differenti; tuttavia, sarà sempre più necessario calarsi nel mondo cyber e approfondirne la conoscenza per poter effettivamente produrre risposte preventive, normative e repressive efficaci in quanto adeguate alle peculiarità proprie di questo nuovo mondo.

profitto con altrui danno, è punito con la reclusione da sei mesi a tre anni e con la multa da lire centomila a due milioni. (…) • *3. La pena è della reclusione da due a sei anni e della multa da euro 600 a euro 3.000 se il fatto è commesso con furto o indebito utilizzo dell'identità digitale in danno di uno o più soggetti*".

[36] Gli Emirati Arabi Uniti lo hanno qualificato per legge come commodity. Vedi Cnbc, *Abu Dhabi regulates ICOs for cryptocurrency funding — but warns of 'many risks'*, 9 ottobre 2017. https://www.cnbc.com/2017/10/09/abu-dhabi-regulates-icos-for-cryptocurrency-company-funding.html.

[37] Cnbc, *Cryptocurrencies like bitcoin are not 'mature' enough to regulate, ECB chief Mario Draghi says*, 19 ottobre 2017. https://www.cnbc.com/2017/10/19/cryptocurrencies-are-not-mature-enough-ecb-chief-mario-draghi.html.

10. DIRETTIVA NIS E ORDINAMENTO GIURIDICO-ECONOMICO ITALIANO. PER NON DIMENTICARE LA VULNERABILITÀ DELLE PICCOLE E MEDIE IMPRESE DA ATTACCHI CYBER

di *Marco Mariscoli*[*]

Il presente elaborato si prefigge di esaminare le possibili ripercussioni sul tessuto imprenditoriale e sull'Ordinamento giuridico italiano della Direttiva del Parlamento Europeo e del Consiglio n. 1148/2016 recante "*misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione*" cosiddetta Direttiva NIS[1]. La Direttiva dedicherà una particolare attenzione al rapporto fra i "fornitori di servizi essenziali"[2], soggetti che dovranno essere individuati dai singoli stati membri e che meriteranno una tutela particolare in caso di attacchi ai rispettivi Sistemi informatici[3]. Alla luce di quanto sino ad ora esposto, nel nostro tessuto imprenditoriale prevalentemente basato su piccole e medie imprese (PMI) – soggetti per la maggior parte non rientranti nella categoria dei "fornitori di servizi essenziali" – sussiste una consistente componente di rischio in caso di attacco cibernetico mirato a queste determinate categorie, che potrebbe portare alla paralisi non solo del settore vittima, ma anche di altre categorie professionali e/o aziendali.

La problematica che ci stiamo accingendo a disaminare appare tanto più attuale e urgente alla luce degli attacchi cibernetici perpetrati contro i sistemi informatici di alcuni operatori di servizi essenziali in diversi Stati Membri dell'Unione Europea ed in Gran Bretagna, fra i quali appunto il Servizio

[*] Avvocato penalista.
[1] Acronimo di "*Network and Information Security*".
[2] Per fornitore di servizi essenziali si intende "*Un soggetto che deve garantire un servizio che è essenziale per il mantenimento di attività sociali e/o economiche fondamentali*".
[3] Per la definizione di Sistema Informatico si rimanda alla Convenzione del Consiglio di Europa del 23 novembre 2001 nella quale viene affermato che deve intendersi un Sistema Informatico: "*qualsiasi apparecchiatura o gruppo di apparecchi interconnessi o collegati uno o più dei quali svolge un trattamento automatico di dati su indicazione del programma*".

Sanitario Nazionale Britannico o la Renault in Francia, che hanno bloccato completamente le strutture citate e non solo. La tecnologia del *ransomware*, tipologia di *malware* utilizzato in questo caso dagli hacker, è già stata utilizzata su larga scala ed in diverse occasioni e si sta diffondendo molto rapidamente, diventando già a partire dal 2017, un problema grave tanto quanto gli attacchi DDoS (Distributed Denial of Service)[4]. Per compiere tali attacchi, gli hacker hanno utilizzato un ransomware denominato "WannaCry" un virus che, come i Cryptocker, è stato creato da *scammer* con conoscenze elevate nel campo della programmazione informatica. Gli *scammer* possono infiltrarsi in un PC attraverso diverse modalità, ad esempio mediante un allegato di una mail infetta o attraverso il browser in caso di apertura di un sito web infettato.

Come si può percepire dall'etimologia inglese, la parola *ransom* implica la richiesta di un riscatto da pagare per rimuovere la limitazione ed ottenere il ripristino della possibilità di accedere al PC , di fatto perpetrando una vera e propria estorsione mediante l'utilizzo del sistema informatico; è quindi evidente l'insorgere di un rischio consequenziale, per coloro che cedono a quanto richiesto dagli estortori, di alimentare un canale di finanziamento di associazioni criminali occulte e di organizzazioni terroristiche .

A livello internazionale, la problematica in esame è stata affrontata dal Consiglio di Sicurezza dell'ONU, con la Risoluzione 2341/2017, nella quale, gli Stati Membri delle Nazioni Unite sono stati incoraggiati a coordinarsi fra loro tramite lo scambio reciproco di informazioni relative ad attacchi perpetrati nel Web. Sul punto appare però interessante quanto affermato da Jurgen Stock, Capo dell'Interpol, il quale ha lamentato uno scollegamento strutturale che al momento sussiste fra gli Stati Membri delle Nazioni Unite.

Per quanto riguarda le strutture critiche, i recenti attacchi hanno dimostrato che mentre in Europa si dibatte sulla necessità di censire le infrastrutture critiche e di adottare misure di sicurezza idonee a renderle resilienti agli attacchi cibernetici, simili eventi dimostrano quanto siano fragili le infrastrutture esposte in rete nei confronti di minacce di modesta entità. Infatti, un *ransomware* come WannaCry sfruttando una falla zero-day, ovvero non nota al momento dell'attacco e per questo motivo estremamente pericolosa"[5], ha generato un effetto su larga scala di dimensioni impreviste.

[4] David Gubiani, Security Engineering Manager di Check Point.
[5] Pierluigi Paganini, op. cit.

Il ruolo chiave nella prevenzione agli attacchi cibernetici sembra risiedere proprio nella cooperazione fra settore pubblico e privato ed è stato perciò formulato l'auspicio di realizzare un interscambio fra gli Stati Membri in merito alle informazioni sui dati acquisiti. Appare *ictu oculi* come nella Direttiva NIS si auspichi più volte ad una cooperazione fra gli Stati Membri in tema di sicurezza in rete e ciò non fa altro che rimarcare quanto lo scambio di informazioni fra i Paesi membri, e quindi il dialogo fra differenti ordinamenti giuridici, possa rivelarsi fondamentale per limitare attacchi cibernetici[6]. Il dialogo fra i diversi ordinamenti in tema di reati informatici e il conseguente interscambio di informazioni sono già da molto tempo presenti nel nostro Ordinamento Giuridico; la Legge n. 38/2006 ha istituito e normato il funzionamento del Centro Nazionale per il Contrasto alla Pedopornografia On-Line in seno alla Polizia di Stato, anche se nel presente caso il "link" fra i vari Ordinamenti Giuridici è posto in essere dai sistemi Europol ed Eurojust.

Il 2016, come affermato da Gabriele Faggioli[7], sarà ricordato nei successivi decenni come l'anno chiave della cooperazione fra stati membri a livello europeo sul tema della sicurezza informatica. Il futuro di questa tematica in Europa è essenzialmente riconducibile alle norme di un ampio pacchetto di riforme dell'Unione Europea, che prevede sia la direttiva NIS sia il Regolamento n. 679/2016, Regolamento Generale sulla Protezione dei Dati (GDPR).

Il GDPR, entrato in vigore il 24 maggio scorso e obbligatorio a partire dal 24 maggio 2018, sostituirà la Direttiva 95/46/CE in tema di tutela dei dati personali[8], mentre la Direttiva n. 1148/2016, Direttiva Network and Information Security (Direttiva NIS), entrata in vigore l'8 agosto scorso, riguarda

[6] La Direttiva NIS afferma che: "*che gli stati membri cooperino tra loro, istituendo un gruppo di cooperazione – composto da rappresentanti degli Stati membri, dalla Commissione e dall'Agenzia dell'Unione europea per la sicurezza delle reti e dell'informazione (ENISA)- al fine di sostenere e agevolare la cooperazione strategica fra gli Stati membri in relazione alla sicurezza delle reti e dei sistemi informativi e facilitare lo scambio di informazioni tra gli stati membri, in modo da accrescere la fiducia. Essi dovranno anche creare una rete di gruppi di intervento per la sicurezza informatica in caso di incidente (rete CSIRT) allo scopo di promuovere una cooperazione operativa rapida ed efficace su specifici incidenti e condividere le informazioni relative ai rischi*".

[7] Ceo Partners4innovation e presidente Clusit, nell' Articolo Sicurezza, "Ecco come l'Europa vuole rendere il cyberspazio più sicuro" articolo di Alessandro Longo pubblicato nel *Corriere della Sera* del 22 settembre 2017 (www.ilsole24ore.com).

[8] Direttiva 95/46/CE del Parlamento europeo e del Consiglio, del 24 ottobre 1995, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati.

l'adozione di misure mirate a creare un livello comune di sicurezza delle reti e dei sistemi informativi nell'Unione.

Dal testo della Direttiva emerge la necessità da parte degli Stati membri di assicurare che le amministrazioni pubbliche ed i gestori del mercato adottino misure tecniche ed organizzative appropriate alla gestione dei rischi per la sicurezza delle reti e dei sistemi informativi utilizzate nelle loro operazioni. In particolare, devono essere sviluppate dagli stati membri firmatari, misure in grado di prevenire e ridurre al minimo l'impatto degli incidenti sulla rete e sul sistema di informazione riguardante i servizi di base forniti. La Direttiva contiene disposizioni efficaci, pratiche e volte a perdurare almeno per l'arco di una generazione, dense di riferimenti tecnico-informatici che permettono di fornire un quadro in grado di affrontare le sfide imposte dalle nuove tecnologie nella protezione dei dati e nella sicurezza dei sistemi e delle reti.

Come ha affermato Antonello Salerno[9], Il futuro della cyber security in Italia potrebbe declinarsi in funzione di due aspetti chiave: prendere ad esempio la Pubblica Amministrazione (PA) per sviluppare iniziative private oppure creare dei centri di eccellenza di formazione. Il tutto accompagnato, ovviamente, ad investimenti adeguati per proteggere il settore delle infrastrutture critiche.

Se da un punto di vista formale, la direttiva NIS, è ancora da recepire, sul piano sostanziale l'Italia è già allineata a molte delle nuove prescrizioni e potrà ora concentrarsi sui dettagli per rendere più efficace la strategia nazionale. I cardini sono quelli del Decreto del Presidente del Consiglio dei ministri del 24 gennaio 2013[10], che contiene un primo modello di *governance* sulla cyber security e indica nel Dipartimento per le informazioni della sicurezza (DIS) e nel Comitato interministeriale per la sicurezza della Repubblica (CISR) i principali riferimenti di coordinamento.

Ai sensi della Direttiva NIS, gli Stati Membri dovranno individuare i settori interessati, vale a dire, tutti quegli ambiti che, se colpiti da un attacco,

[9] Giornalista presso il *Corriere delle Comunicazioni*, articolo del 17 febbraio 2017.

[10] Il decreto in esame definisce all'articolo 1 (Oggetto), che lo scopo dello stesso è volto a definire l'architettura istituzionale deputata alla tutela della sicurezza nazionale relativamente alle infrastrutture critiche materiali e immateriali, con particolare riguardo alla protezione cibernetica e alla sicurezza informatica nazionali, indicando a tal fine i compiti affidati a ciascuna componente ed i meccanismi e le procedure da seguire ai fini della riduzione della vulnerabilità, della prevenzione dei rischi, della risposta tempestiva alle aggressioni e del ripristino immediato della funzionalità dei sistemi in caso di crisi.

potrebbero bloccare un settore cruciale per la vita ed il funzionamento della nazione. L'obbligo di notifica degli attacchi riguarda soltanto i grandi player di carattere nazionale, quali ad esempio ministeri, gli operatori del Sistema Sanitario Nazionale, i grandi operatori del privato; in tale maniera la maggior parte del tessuto imprenditoriale italiano, composto prevalentemente da piccole e medie imprese (PMI), rimane escluso. Estendere tale obbligo anche a questi attori, che contano su bacini d'utenza ampi ed il cui contributo su scala nazionale è significativo, potrebbe essere una buona soluzione per far fronte alla settorialità della direttiva.

La Pubblica Amministrazione potrà giocare un ruolo interessante a questo proposito, grazie all'istituzione di meccanismi di *compliance*, e contribuire a fungere da volano di cambiamento per il settore privato come è successo in passato su altri versanti, ad iniziare per esempio dalla fatturazione elettronica.

Il settore pubblico è chiamato a rendere le proprie infrastrutture e i propri sistemi di gestione conformi a standard internazionali, pertanto alle aziende interessate a lavorare per la Pubblica Amministrazione potrebbe essere richiesta l'applicazione degli standard di sicurezza richiesti a quest'ultima, innescando così un circolo virtuoso che coinvolgerà il settore privato attraverso la certificazione della filiera della PA.

Il rischio di subire attacchi cibernetici per le imprese che operino in qualsiasi settore economico è elevato. Commenta il Prof. Pierluigi Paganini, "i sistemi industriali oggi continuano ad essere principalmente esposti a minacce generiche, dato allarmante se pensiamo che un attacco progettato per colpire questi sistemi potrebbe avere effetti disastrosi. Stuxnet prima[11], ed i più recenti attacchi in Ucraina, con il *malware* BlackEnergy, hanno dimostrato l'efficacia di un *malware* in un'offensiva contro un sistema industriale presente in un'infrastruttura critica". Da quanto appena riportato, ulteriore rischio per le imprese sembrerebbe derivare proprio dall'utilizzo di supporti informatici quali *smartphone* e *tablet* forniti da aziende pubbliche e/o private ai propri dipendenti. Negli ultimi quattro anni l'uso dello *smartphone* è

[11] È un virus informatico appositamente creato e diffuso dal Governo statunitense (nell'ambito dell'operazione "Giochi Olimpici", promossa da Bush nel 2006, che consisteva in un "ondata" di "attacchi digitali" contro l'Iran) in collaborazione col governo israeliano. Lo scopo del software era il sabotaggio della centrale nucleare iraniana di Natanz. In particolare, il virus doveva disabilitare le centrifughe della centrale, impedendo la rilevazione dei malfunzionamenti e della presenza del virus stesso (Fonte Wikipedia – Wikijus).

cresciuto del 394% mentre quello del *tablet* addirittura del 1.700%; non stupisce quindi che anche gli attacchi contro questi dispositivi mobili siano in costante aumento. Secondo il Security di Check Point Software Technologies LTS[12], un dipendente aziendale su cinque sarà autore di un caso di violazione dei dati personali della propria azienda tramite un *malware* mobile o un Wi-Fi dannoso, entrambi vettori di attacco altamente efficaci sui dispositivi mobili in assenza di un update degli antivirus utilizzati.

Recentemente, ci sono stati attacchi che hanno coinvolto i cellulari di alcuni giornalisti, dimostrando come queste tecniche d'attacco siano ormai comuni e quindi sempre più fruibili dai criminali informatici. La sicurezza mobile rimane, dunque, una sfida per le imprese, un *push-pull* tra produttività, privacy e protezione.

Oggigiorno, un ulteriore problema è dato dalla diffusione di attacchi informatici tramite l'*Internet of Things* industriale, quindi mediante altre svariate tipologie di *device* funzionali, come ad esempio le stampanti. La convergenza tra le tecnologie informatiche (IT) e la tecnologia operativa (OT) sta rendendo entrambi gli ambienti più vulnerabili. Pertanto, si renderà necessario estendere i controlli dei sistemi operativi e della sicurezza fisica allo spazio logico ed implementare soluzioni di prevenzione delle minacce negli ambienti IT e OT.

Infrastrutture critiche, comprese centrali nucleari, reti elettriche e di telecomunicazioni, rimangono altamente vulnerabili a possibili attacchi informatici. Quasi tutte le infrastrutture italiane sono infatti state progettate e costruite prima dell'avvento della minaccia di attacchi informatici e, per questo motivo, anche i più semplici principi di sicurezza informatica, nella maggior parte dei casi, non sono stati presi in considerazione all'interno dei progetti. A tal proposito è interessante e altresì preoccupante quanto è emerso nell'elaborato citato del Prof. Pierluigi Paganini che riportando quanto è emerso dalla ricerca dell'US – ICS CERT afferma che: "[…] il settore energetico è quello maggiormente preso di mira, dato che trova conferma nei numerosi attacchi osservati negli scorsi mesi da parte di gruppi di criminali e *nation-state actors*"

Secondo una recente analisi pubblicata da IBM Managed Security Services il numero di attacchi contro sistemi industriali è aumentato del 110% rispetto allo scorso anno. Gli esperti di IBM hanno osservato un aumento

[12] Report del 2016.

significativo di attacchi di tipo brute-force contro sistemi SCADA. Gli USA guidano la graduatoria delle cinque principali nazioni più colpite dagli attacchi, un dato non sorprendente se consideriamo che negli Stati Uniti è presente il maggior numero di sistemi ICS"[13].

Solo ad inizio 2016 è stato segnalato il primo blackout causato intenzionalmente da un attacco informatico[14]. I responsabili della sicurezza delle infrastrutture critiche devono dunque prepararsi alla possibilità che le loro reti e i loro sistemi possano essere attaccati in modo sistematico da diversi attori statali. Nel Security report di Check – Point del 2016 è stato evidenziato che: "Queste tecnologie sono infatti ormai parte integrante del nostro modo di fare business e i criminali informatici hanno di conseguenza innovato le loro tecniche di hackeraggio. Gli hacker sono diventati più intelligenti quando si tratta di *malware* e *ransomware*, rilasciando ogni minuto nuove varianti". L'epoca degli antivirus *signature based* per individuare il *malware* è dunque ormai lontana[15].

Per garantire convergenza nell'attuazione dell'articolo 14 della direttiva NIS, gli Stati membri della UE incoraggiano l'uso di standard e/o specifiche tecniche relative alle reti e alla sicurezza delle informazioni; in aggiunta, la legislazione degli Stati Membri individua le Autorità competenti sia nella tutela dei dati sensibili sia nell'individuazione dei Computer *Security Incident Response Team* (CSIRT). La direttiva NIS estende il compito, richiedendo agli Stati Membri di individuare anche le autorità competenti in materia di salvaguardia dei dati personali, visto il crescente numero di violazioni di quest'ultimi.

È previsto che la NIS sia diretta solamente ai fornitori di servizi essenziali e di servizi informatici mentre la normativa in tema di privacy e tutela dei dati personali, regolamento GDPR, si rivolga anche ai soggetti privati. Le normative in esame possono tuttavia sovrapporsi nei casi in cui un incidente informatico implichi anche una violazione di dati personali. In tale scenario,

[13] Pierluigi Paganini, *op. cit*.

[14] Nell'attacco di dicembre 2015, i criminali avevano come obiettivo quello di causare grandi blackout in diverse regioni ucraine. Rispetto agli ultimi attacchi non è stato utilizzato il famoso BlackEnergy ma delle versioni modificate di una backdoor open-source. Lo scenario dell'attacco in se non è cambiato molto rispetto alle precedenti campagne. I criminali hanno inviato alle potenziali vittime email di phishing contenenti come allegato un file XLS pericoloso e dei contenuti HTML con un link a un file .PNG posto in un server remoto; in questo modo i criminali erano in grado di ricevere una notifica che la mail era stata spedita e aperta dalla vittima.

[15] Check Point Report del 2016 (pages.checkpoint.com/security-report.htm).

i soggetti colpiti dovranno attivarsi per notificare gli incidenti ai sensi della due direttive.

L'auspicio è che, in una prospettiva *de jure* condendo ed in fase di recepimento nel nostro Ordinamento Giuridico di entrambe le direttive, le Autorità deputate alla sorveglianza ed alla gestione di attacchi cibernetici nonché alla tutela della preservazione dei dati personali, emanino delle linee guida che possano agevolare le imprese nel far fronte agli incidenti di sicurezza, in modo da garantire ed assicurare il rispetto di entrambe le normative.

Fermo restando che la direttiva NIS si applica solamente alle "macro categorie", mentre il Regolamento n. 679/2016 si applica a tutte le imprese, considerato il sopracitato tessuto industriale italiano, è auspicabile, la creazione, di strutture atte a recepire notizie su eventuali incidenti accaduti ai propri associati all'interno delle varie associazioni di categoria quali Confindustria, Confagricoltura, Confartigianato ecc., affinché vengano comunicate ai CSIRT competenti. Le costituende entità, dovrebbero ricalcare in sostanza la struttura dei CSIRT stessi assumendo una duplice funzione: in primis, tutelare le PMI da eventuali attacchi informatici che possano danneggiare o, addirittura, bloccare la produzione, violando ; in secundis, valutare l'affidabilità delle aziende consociate pervenendo, per tale via, all'elaborazione di una sorta di "rating di affidabilità informatica" sia sulla prevenzione di incidenti informatici sia sul contrasto agli stessi, e garantendo così un elevato livello di tutela dei dati sensibili.

Per garantire il completo funzionamento di quanto descritto, si porrebbe l'esigenza che i "mini CSIRT o CSIRT di categoria", fossero collegati ad uno CSIRT nazionale, a sua volta collegato con la rete CSIRT a livello comunitario.

Inoltre, in un'ottica top-down, gli "CSIRT di categoria", venuti a conoscenza di un incidente accaduto ad un proprio associato, dovrebbero comunicare l'incidente non solo al CSIRT nazionale ma anche agli altri iscritti alla categoria rispettando la segretezza richiesta per ragioni di reputazione aziendale. Le aziende, inoltre, dovrebbero predisporre, con cadenza biennale, un piano di prevenzione dagli attacchi informatici riguardanti anche la tutela dei dati sensibili contenuti nei propri server. Conseguentemente, ogni due anni, il CSIRT di categoria potrebbe stilare una lista delle aziende associate predisponendo un rating di affidabilità delle stesse in base al livello di prevenzione dagli incidenti informatici raggiunto. Ciò contribuirebbe sensibilmente a tutelare i membri dell'associazione ed a migliorare la prevenzione verso gli

attacchi cibernetici sia le azioni di supporto in caso di attacco subito. Tale sistema, che peraltro rimanda ad un dovere di cooperazione sancito a livello mondiale oltre che comunitario, potrà garantire ad imprese pubbliche, soggetti privati, ed agli utenti dei servizi prodotti, sistemi informatici sempre più sicuri ed idonei ad affrontare attacchi di hackeraggio non abbandonando le vittime e i loro utenti al loro destino, senza specifici punti di riferimento.

In conclusione, riprendo quanto affermato dal Prof. Pierluigi Paganini[16] "… ricordando che la sicurezza delle nostre infrastrutture dipende anche dalla postura di noi cittadini. Dobbiamo imparare a conoscere le minacce informatiche e come difenderci da esse. Siamo nodi di una rete globale con la quale scambiamo un quantitativo enorme di informazioni, falle o errori di configurazione nei sistemi che quotidianamente usiamo potrebbero portare a situazioni di rischio per l'intera collettività". Aggiungo che, come nel contrasto nel caso dei reati perpetrati da minorenni in Rete, è fondamentale, l'aspetto dell'educazione e della prevenzione. Bisogna entrare una volta per tutte nell'ottica che nessuna realtà può ormai sentirsi immune da attacchi. È necessario, dunque, creare una cultura dell'educazione rispetto a ciò che succede nel mondo virtuale che ha sempre più forti ripercussioni nel mondo reale.

[16] Dal caso Wannacry alla Direttiva NIS, le infrastrutture critiche sono ancora troppo vulnerabili.

11. L'IMPORTANZA DI INTERNET NEGLI ADEMPIMENTI FISCALI: VANTAGGI E CRITICITÀ

di *Luca Serafino De Simone*[*]

Internet è diventato ormai uno strumento di uso comune, essenziale per il normale svolgimento della vita quotidiana.

Il massiccio uso di internet, per quanto sicuramente comodo, rapido e vantaggioso per compiere operazioni quotidiane, presenta anche delle criticità legate alla sicurezza personale, per esempio per quanto riguarda i siti internet nei quali navighiamo, siti che rischiano sempre più di essere violati da attacchi hacker.

In questo mio elaborato ho analizzato il problema della sicurezza in rete relativa alla protezione dei dati fiscali. Internet è diventato ormai uno strumento fondamentale nel rapporto che intercorre tra l'Agenzia delle Entrate – l'ente che si occupa della riscossione dei tributi – e i singoli contribuenti, tanto che qualsiasi operazione, a partire dalla segnalazione della propria situazione debitoria fino ad arrivare alla rottamazione delle cartelle esattoriali, si fa tramite l'utilizzo dello strumento informatico. Ho affrontato l'argomento partendo e dai vari episodi di violazione dei server dell'Agenzia delle Entrate e di Equitalia da parte di attacchi hackers, evidenziando la loro permeabilità e tutti i rischi ad essa connessi, considerando soprattutto che tali server contengono dati particolarmente sensibili e riservati, quali quelli di tutti i contribuenti, sia persone fisiche che giuridiche, della Nazione.

Successivamente mi sono soffermato su quelle che sono le iniziative legislative adottate a livello sovranazionale, che dovranno poi essere recepite dal Governo Italiano, per poter garantire una tutela dei sistemi informatici che sia unica ed omogenea in tutta l'Unione Europea, tutela che, però, non deve mai perdere di vista il rispetto della privacy dei dati sensibili dei cittadini dell'Unione. Si tratta ovviamente di un discorso complesso ed in divenire: il pieno recepimento della normativa europea da parte degli stati membri, tra i quali l'Italia, verrà completato nel mese di maggio 2018 e,

[*] Avvocato tributarista.

successivamente, occorrerà che la Pubblica Amministrazione da una parte e le banche, gli operatori finanziari e le imprese dall'altra si dotino di efficaci sistemi di protezione contro attacchi cyber, con lo scopo di favorire soprattutto la prevenzione e l'interscambio di informazioni pratiche ed innovative in campo cibernetico.

11.1. Il ruolo di Internet nella vita dei contribuenti: vantaggi e criticità

È chiaro che internet ormai riveste un ruolo fondamentale nel rapporto che intercorre tra l'Agenzia delle Entrate, e i cittadini, , Ad esempio il sito di Equitalia, diventata dal 1° luglio 2017 "Agenzia delle Entrate Riscossione", è un portale in cui è possibile verificare la propria situazione fiscale e debitoria, i provvedimenti o procedure in atto come sgravi, fermi amministrativi o ipoteche, ma è anche possibile pagare debiti, sospendere la riscossione, quando consentito dalla legge, ed ottenere la rateizzazione dei debiti.

A riprova di ciò occorre dire che a ottobre 2016 il sito dell'allora Equitalia ha registrato un raddoppio di utenti ed ingressi rispetto allo stesso periodo dell'anno precedente. Sono stati 600 mila gli accessi, 5,5 milioni le pagine visitate e sono state registrate operazioni finanziarie per alcune decine di milioni di euro.

L'area riservata del sito dell'Agenzia delle Entrate Riscossione, ad esempio, è uno dei canali attraverso il quale fornire ai debitori i dati necessari per individuare i carichi ammessi alla rottamazione delle cartelle.

Così come è avvenuto per alcuni operatori di servizi essenziali, pubblici e privati, che sono in funzione in diversi Stati membri dell'Unione Europea, anche i sistemi operativi di Equitalia, e dell'Agenzia delle Entrate sono stati vittima di attacchi hacker.

Nel mese di novembre del 2016 infatti, il portale di Equitalia è stato bombardato da attacchi informatici provenienti dall'estero che, fortunatamente, non ne hanno alterato la sicurezza e non ne hanno intaccato l'area riservata. A distanza di pochi giorni, lo stesso attacco è stato subito dal portale dell'Agenzia delle Entrate che, per quarantacinque minuti, ha visto così limitata la funzionalità del proprio sito internet[1].

In entrambi i casi vi è stato un attacco di tipo *Distributed Denial of Service* (DDoS), ossia si è trattato di un'offensiva coordinata che prevede l'invio

[1] Franco Grilli, Equitalia, sito down: "Un attacco hacker", in *Il Giornale*, articolo on line del giorno 21 novembre 2016.

contemporaneo di migliaia di richieste al server centrale che ospita il così detto "sito bersaglio", in modo tale da sovraccaricarlo e renderlo, così, inutilizzabile. Richieste di questo tipo sono solitamente gestite da una rete composta da computer infettati con dei *malware* (software dannoso) che viene comandata a distanza per scopi illegali. Il nome che viene dato alla singola rete è quello di "botnet" mentre i singoli computer infettati che la compongono vengono comunemente chiamati "bot" oppure "pc zombie".

Nel dicembre 2011, ci fu in tutta Italia una cyber-truffa consistente nell'utilizzo illecito di mail con il nome ed il logo dell'Agenzia delle Entrate nelle quali veniva indicato, come oggetto "Notifica di rimborsi fiscali". Questa comunicazione invitava il destinatario a scaricare e compilare un modulo con la finalità di ottenere un presunto rimborso fiscale richiedendo, tra le altre informazioni, anche tutti i dati della carta di credito.

In questo caso si trattò di un tentativo di *phishing*, ossia una truffa informatica architettata per entrare in possesso, in modo illecito, dei dati personali dei vari destinatari delle mail[2].

Un evento simile è stato denunciato nel mese di agosto 2017 dal Commissariato di Polizia di Stato[3].

In aggiunta, il 25 settembre 2017, si è diffusa la notizia che nei giorni precedenti era stata scoperta una falla nella piattaforma dell'Agenzia delle Entrate che riguardava la riservatezza dei dati sensibili. Tale problema consentiva a chiunque avesse le credenziali del portale (commercialisti e contribuenti) di spiare tutti dati fiscali in esso registrati, relativi sia alle persone

[2] In truffe di questo tipo vi sono dei dettagli che possono aiutare i destinatari a capire che la mail ricevuta non è una comunicazione ufficiale; come prima cosa è importante soffermarsi sull'incipit del messaggio, che porta la dicitura "*spettabile contribuente*" seguita dal nome. Ebbene, se si presta attenzione, si nota che tra il nome della persona e l'altra parola intercorre molto spazio, questo perché si tratta di una email standard inviata a tutti e, proprio per questo motivo, lo spazio dipende solo dalla lunghezza del nome. La caratteristica di questo tipo di email è proprio quella di presentare molti spazi tra una parola e l'altra, proprio perché servono per inserire i nostri dettagli personali, che cambiano da una persona all'altra e che servono per far cadere nella trappola. In queste finte email si viene esortati a cliccare su due link per aggiornare i propri dati personali e, in seguito a una "verifica", risultano delle incongruenze sui profili dei vari utenti, invitando ad aggiornare le proprie informazioni per evitare una multa superiore ai mille Euro. Ovviamente tutto questo non è vero, la minaccia della sanzione serve a spaventare le persone per farle cliccare sul link in modo che il computer venga così infettato con conseguente sottrazione dei dati personali. Questi messaggi vanno immediatamente segnalati e cancellati, è importante sapere infatti che L'Agenzia delle Entrate comunica con i cittadini solo attraverso canali standard come le raccomandate con ricevuta di ritorno e le comunicazioni nell'area riservata del proprio sito internet.

[3] Francesca Milano, "Non aprite quella mail": Equitalia sotto attacco phising, in *Il Corriere della sera*, articolo *on line* del giorno 24 agosto 2017.

fisiche che giuridiche[4].Una volta effettuato l'accesso nel sistema infatti era sufficiente inserire il codice fiscale di un qualsiasi contribuente con l'obbligo di trasmissione telematica delle fatture per accedere a tutti i suoi dati fiscali trasmessi all'Agenzia delle Entrate. Occorre specificare che non erano presenti solamente i dati del singolo contribuente, ma anche quelli dei clienti e fornitori a lui collegati o, nel caso in cui veniva inserito il codice fiscale di un commercialista, era possibile risalire a tutti i dati dei suoi assistiti.

A causa di questa falla, la piattaforma dell'Agenzia delle Entrate è rimasta in manutenzione dal 22 settembre, al 26 settembre, costringendo l'Ente a concedere una proroga dal 28 settembre al 5 ottobre della scadenza per presentare gli adempimenti fiscali. Una delle conseguenze di questo buco nella piattaforma dell'Agenzia delle Entrate è stata che la Società Sogei, che si occupa della gestione del servizio telematico, è finita sotto accusa[5].

Gli attacchi di tipo DDoS sono tra i più diffusi metodi di attacco ai servizi web e costituiscono oggi circa il 90% dei tentativi di hackeraggio che spesso colpiscono i siti di istituzioni o di società[6].Anche i server della Commissione Europea sono stati, in passato, oggetto di tali tipi di attacco con il risultato di un evidente disservizio. Per di più, la massiccia diffusione di dispositivi dell'*Internet of Things* (IoT)[7] ha avvantaggiato di molto gli hacker ed i pirati informatici in quanto tali dispositivi presentano problemi di sicurezza causati da carenze nella progettazione dell'hardware e del software che ne gestisce le funzionalità e le comunicazioni con gli altri dispositivi di rete (i così detti "*device*")[8].

11.2. Le criticità in merito alla tutela dei dati sensibili

Questa rapida diffusione dei dispositivi IOT ha attirato le attenzioni degli hacker poiché, una volta trovata una falla nel sistema di sicurezza di uno

[4] *Ibidem.*
[5] Lo stesso Giacomo Portas, Presidente della Commissione di Vigilanza sull'Anagrafe Tributaria e Antonello Soro, Garante della Privacy, ovviamente hanno chiesto spiegazioni circa l'accaduto.
[6] Franco Grilli, *op. cit.*
[7] L'espressione "Internet of things" è un acronimo che sta a significare, letteralmente, "internet delle cose" ed è stata utilizzata per la prima volta nel 1999 da K. Ashton, ricercatore presso il Massachussets Institute of Technology, per descrivere l'interconnessione tra gli oggetti che, attraverso appositi sensori, si connettono alla rete internet, trasferendo dati (e, quindi, informazioni) attraverso un proprio indirizzo IP che ne consente l'individuazione univoca.
[8] Franco Grilli, *op. cit.*

specifico prodotto, è possibile colpire poi migliaia di dispositivi contemporaneamente[9].

In riferimento alla materia tributaria, già nel marzo del 2016 i tecnici del Garante della Privacy rilevarono come l'Anagrafe Tributaria, ossia una delle più importanti e rilevanti banche dati pubbliche, presentasse delle preoccupanti criticità in merito alle misure di sicurezza informatica sottolineando come non fosse particolarmente difficile, per ipotetici pirati informatici, riuscire ad accedere abusivamente ai dati sensibili, non solo patrimoniali, ma anche ritrovabili nelle dichiarazioni fiscali compilate online. L'Autority della Privacy ha segnalato tali criticità in due lettere inviate all'allora Direttore dell'Agenzia delle Entrate, Rossella Orlandi, ed al Ministro dell'Economia, Pier Carlo Padoan sostenendo che, in seguito ad alcune attività ispettive avviate a seguito di specifiche segnalazioni, era emerso come vi fossero "*numerose ed importanti criticità riguardo a misure tecnologiche ed organizzative che non possono in alcun modo essere sottovalutate*"[10].

L'Agenzia delle Entrate e la Commissione di Vigilanza sull'Anagrafe Tributaria in un comunicato congiunto precisarono come "*alcune criticità sono già state risolte attraverso l'adozione di misure correttive introdotte seguendo una valutazione di priorità*", facendo rientrare tra queste misure il fatto che, per accedere alla dichiarazione precompilata, fosse necessario inserire sia la password che il pin, in modo da poter visualizzare tali dati solo tramite le procedure di sicurezza rafforzata. Il Garante per la privacy replicò definendo poco soddisfacenti tali dichiarazioni e affermando che "*pur riconoscendo la volontà da parte dell'Agenzia delle Entrate di provvedere alla rimozione delle difficoltà*", ci sarebbe stato "*il proseguimento di un'istruttoria complessa e che richiederà approfondimenti ulteriori*". Il punto è particolarmente complesso e delicato se si pensa che la realizzazione di un sistema fiscale che possa dirsi moderno, efficiente e semplificato nei confronti del contribuente, necessita della creazione di nuove banche dati o del potenziamento di quelle già esistenti.

Con il passare del tempo, le disposizioni legislative che si sono susseguite in materia fiscale e tributaria hanno determinato la creazione di flussi ingenti di dati riferiti ai singoli contribuenti, consentendo a diversi soggetti di averne

[9] Basta pensare, come esempio, a quanto accaduto il 21 ottobre 2016, quando i dispositivi realizzati da XiongMai Technologies (società cinese tra i maggiori produttori al mondo di dispositivi economici destinati alla navigazione in internet) sono stati violati da un attacco DDoS da oltre 600 gigabit al secondo. La cosa ha costretto la Xiongmai a ritirare i prodotti incriminati dal commercio, cosa questa che ha causato un grosso danno d'immagine.
[10] Antonello Soro, *Lettera del giorno 17 febbraio 2017.*

accesso. Di conseguenza, si è sviluppata la necessità di proteggere tali dati particolarmente delicati. Su questa questione, secondo il Codice in materia di protezione dei Dati personali (d.lgs. 30 giugno 2003, n. 196) i sistemi di trattamento dei dati sono al servizio della persona e lo stesso trattamento deve da un lato, rispettare le libertà, i diritti fondamentali, la vita privata e la dignità dei cittadini e dall'altro, contribuire al progresso economico e sociale, allo sviluppo degli scambi e al benessere degli individui[11].

Anche la nozione di privacy intesa come tutela della riservatezza dei dati sensibili dei cittadini nella società contemporanea sussiste nel giusto ed equilibrato bilanciamento tra queste due sfere di valori.

Portando questo discorso da un quadro generale a un quadro più particolareggiato quale quello della normativa tributaria è importante sottolineare come occorra sempre ricercare un giusto equilibrio tra quelle che sono da una parte, le esigenze perseguite dall'azione amministrativa di equità fiscale e di semplificazione della vita dei contribuenti e, dall'altra, la necessità di assicurare una protezione efficace dei dati fiscali che, per ovvie ragioni, sono molto delicati e possono essere soggetti ad utilizzi illeciti e/o impropri[12].

In materia fiscale non può essere messa in discussione l'esigenza di disporre di informazioni utili per realizzare un interesse costituzionalmente protetto (l'art. 53 della Costituzione infatti dice che "Tutti sono tenuti a concorrere alle spese pubbliche in ragione della loro capacità contributiva") ma tale esigenza deve sempre coesistere con stringenti misure tecniche e organizzative per garantire l'emissione dei dati, degli accessi a questi dati e della loro conservazione.

11.3. Le iniziative legislative in tema di sicurezza dei dati sensibili

I casi che ho narrato in precedenza dimostrano come ad oggi, in Italia, sia ancora sottovalutato il rischio correlato alla sicurezza informatica e questo tanto da parte della Pubblica Amministrazione quanto da parte dalle aziende private, soprattutto le piccole e medie imprese.

Sul tema della cyber security, dal punto di vista sovranazionale sono molte le iniziative in corso, le principali sotto l'egida dell'ONU, del G7, dell'OSCE ed a livello europeo dell'UE e del Consiglio d'Europa. Per quanto riguarda quella che è l'analisi in corso, è importante citare la risoluzione del

[11] Antonello Soro, *Commissione parlamentare di vigilanza sull'Anagrafe Tributaria – Camera dei Deputati*, Audizione del giorno 25 marzo 2015.
[12] Antonello Soro, *op. cit.*

Consiglio di Sicurezza dell'ONU n. 2341/2017 (che evidenzia come per prevenire i cyber attacchi sia fondamentale la cooperazione tra i settori pubblici e privati), la direttiva NIS (che si rivolge prevalentemente alla Pubblica Amministrazione e agli operatori di servizi essenziali[13]) entrata in vigore l'8 agosto 2016 e che dovrà essere recepita, dai vati Stati che aderiscono all'Unione Europea, entro maggio 2018, ed il Regolamento Generale sulla Protezione dei Dati n. 679/2016 (GDPR), che si applica a tutte le imprese, di piccole, medie e rilevanti dimensioni ed è entrato in vigore il 24 maggio 2016[14].A partire da quella data tutti i fornitori di servizi essenziali e i fornitori di servizi digitali saranno chiamati a rispondere della mancata protezione dei dati sensibili e si vedranno costretti ad adottare una strategia per la loro difesa, cosa non affatto scontata considerato che, soprattutto le piccole e medie imprese, a causa dei costi da sostenere per la gestione della loro attività, spesso non possono disporre in azienda di esperti in materia di sicurezza informatica e protezione dei dati personali.

La peculiarità della direttiva NIS è data dal pesante regime sanzionatorio previsto per chi non si conformerà alle disposizioni. Nello specifico, la direttiva NIS presenta tre punti chiave: 1) il miglioramento della capacità di cyber security di ciascun stato dell'Unione Europea; 2) l'aumento del livello di cooperazione tra gli stati membri; 3) l'obbligo di gestione dei rischi e di riportare gli incidenti di una certa entità da parte degli operatori di servizi essenziali e dei fornitori di servizi digitali. Inoltre, gli Stati membri dovranno rispettare una serie di prescrizioni: 1) dotarsi di una strategia nazionale di cyber security che definisca gli obiettivi strategici e le misure di regolamentazione per perseguire tali obiettivi, le politiche adeguate e le priorità nazionali; 2) designare uno o più *Computer Security Incident Response Team* (CSIRT) responsabili del monitoraggio degli incidenti a livello nazionale, fornendo allarmi tempestivi, avvisi e annunci, con lo scopo di diffondere informazioni ed analisi su rischi e incidenti e soprattutto aumentare il grado di consapevolezza circa le minacce di cyber attacchi; 3) prevedere a livello europeo un sistema di riferimento unico in tema di sicurezza informatica, con misure coerenti di gestione del rischio e una sistematica segnalazione degli incidenti; 4) avere delle regole puntuali in tema di cyber security a livello

[13] Si tratta di quei soggetti, pubblici e privati, che forniscono servizi essenziali per il mantenimento di attività sociali e/o economiche fondamentali, utilizzando allo scopo la rete e i sistemi operativi. Come esempi si possono citare i soggetti che forniscono servizi in ambito di: energia, trasporti, settore bancario, settore sanitario, fornitura e distribuzione di acqua potabile, infrastrutture digitali, infrastrutture dei mercati finanziari.

[14] Tale regolamento ha come oggetto la protezione delle persone fisiche con specifico riguardo al trattamento dei dati personali ed alla libera circolazione di tali dati.

nazionale; 5) promuovere la protezione delle infrastrutture critiche in settori come trasporti, energia, bancario, finanziario e sanitario, con una serie di obblighi a carico degli operatori del settore affinché riescano a mettere in piedi sistemi capaci di resistere ai cyber attacchi.

Volendo ora analizzare la situazione dal punto di vista della sicurezza fiscale italiana, va detto che questa è una materia nella quale è particolarmente sensibile la tematica del rapporto tra sicurezza informatica e trattamento dei dati personali, soprattutto se si considera che quest'ultima deve sempre necessariamente comprendere anche la riservatezza dei dati personali dei singoli contribuenti[15]. Sul punto, occorre sottolineare, riprendendo quanto prescritto dalla risoluzione ONU n. 2341/2017, come sia fondamentale la presenza di una stretta collaborazione tra il settore pubblico e privato, per prevenire qualsiasi tipo di cyber attacco che vada a danneggiare i singoli contribuenti. È quindi necessario che vi sia collaborazione da una parte tra l'Anagrafe Tributaria, l'Agenzia delle Entrate e l'Agenzia delle Entrate – Riscossione (che si è trasformata da ente privato in ente pubblico) che, in quanto fornitori di servizi essenziali sono destinatari diretti delle prescrizioni della direttiva NIS, dall'altra tra operatori finanziari e le banche, che sono tra i destinatari del Regolamento Generale sulla Protezione dei dati n. 679/2016 (GDPR).

Questi uffici dovranno dunque essere monitorati da un CSIRT al fine di prevenire eventuali attacchi informatici e fornire avvisi e annunci sui rischi connessi. Si troveranno così immesse in un sistema di cooperazione a livello comunitario e avranno l'onere di adottare delle regole precise in tema di cyber security, soprattutto per quanto riguarda la capacità di mettere in piedi sistemi informatici idonei a resistere ai cyber attacchi ed a segnalare eventuali incidenti. Lo scopo è quello di trovare il giusto equilibrio tra i due interessi in gioco, ossia quello della sicurezza informatica da una parte e della riservatezza del trattamento dei dati fiscali dall'altra, ed è ovvio che con internet la superficie di attacco è ormai aumentata. Infatti il mettere on line qualunque cosa, compresi i dati fiscali dei contribuenti, amplia di molto la possibilità di essere attaccati.

In tema di protezione dei dati personali, già dal 2015 il Garante per la privacy ha emanato una serie di prescrizioni volte ad una maggiore tutela degli stessi. Nello specifico l'Agenzia delle Entrate avrebbe dovuto predisporre dei canali telematici idonei a comunicare una quantità di dati molto elevata quali, per l'appunto, quelli fiscali, dovendo privilegiare un contatto diretto con le banche e gli istituti finanziari (enti privati). L'Agenzia aveva

[15] Antonello Soro, *op. cit.*

inoltre l'obbligo di fornire ai vari operatori finanziari tutte le indicazioni e gli accorgimenti necessari circa i file da inviare[16].

Relativamente all'Anagrafe Tributaria, che ha al suo interno una sezione chiamata "Archivio dei rapporti finanziari" nella quale vengono racchiusi tutti i dati fiscali dei contribuenti, si è sentita l'esigenza di specificare i tempi di conservazione dei dati (sei anni dalla presentazione delle dichiarazioni dei redditi), prevedendo che, alla loro scadenza, essi fossero cancellati del tutto e in maniera autonoma. È stato inoltre previsto, con il Decreto Legislativo "Salva Italia" (D.L. n. 201/2011), che la trasmissione dei dati contabili non debba più avvenire, come era stato inizialmente prescritto, attraverso il vulnerabile servizio telematico Entratel, ma tramite una struttura informatica nuova, ossia il (SID) il quale consente la realizzazione di procedure di trasmissione del tutto automatizzate e che, proprio per tale motivo, necessitano di una protezione adeguata.

Per quanto riguarda gli operatori finanziari e le banche, gli stessi dovranno cooperare con l'Anagrafe Tributaria e gli altri Enti pubblici che si occupano della materia fiscale e, in base alla normativa GDPR, saranno tenuti ad adottare meccanismi di cifratura dei dati per scongiurare il rischio di una loro alterazione e dei protocolli sicuri per tutte quelle trasmissioni interne allo stesso operatore finanziario, limitando l'accesso ai file ad un numero ristretto di incaricati che potranno, a loro volta, accedere ai dati solo in virtù della mansione svolta.

Tutti questi soggetti, pubblici e privati, saranno inoltre tenuti ad aggiornare costantemente i sistemi operativi e i software antivirus e antintrusione, dovendo prevedere un'eventuale conservazione dei dati cifrata.

Da quanto esposto si evince come sia complessa e soprattutto in continua evoluzione la materia dello sviluppo dei sistemi informatici in ambito fiscale, anche se si considera il fatto che la Direttiva NIS e il GDPR sono ancora in fase di attuazione e non sono stata pienamente recepiti.

Proprio per tale complessità, è di primaria importanza assicurare elevati standard di sicurezza per quanto riguarda sia i dati sia i sistemi nei quali questi sono racchiusi.

Le informazioni di natura fiscale e tributaria ormai necessitano sempre più di essere condivise e, per tale motivo, i rapporti e i flussi informativi sono diventati più complessi. Questo ha portato a un aumento dei rischi circa possibili attacchi a banche dati strategiche per il Paese, la cui violazione andrebbe a provocare danni enormi, soprattutto se si considera la qualità e l'ingente quantità di dati archiviati, con il duplice effetto di violare la vita privata

[16] Antonello Soro, *op. cit.*

di milioni di cittadini e di compromettere tutti quegli interessi pubblici che sono alla base della creazione e dell'esistenza di tali strutture.

È chiaro che si tratta, dal punto di vista legislativo, di un percorso complesso e in divenire, composto da una serie di punti quali: 1) il pieno recepimento da parte dell'Italia della Direttiva NIS e del GDPR; 2) l'adozione, da parte dell'Italia, di tutte le misure atte ad attuare le prescrizioni della Direttiva NIS e del GDPR; 3) l'adozione, da parte della Pubblica Amministrazione, di quelli che saranno tutti gli accorgimenti necessari per rispettare le prescrizioni normative che deriveranno dal pieno recepimento della Direttiva NIS; 4) l'adozione, da parte degli operatori finanziari e delle banche, di tutti gli accorgimenti necessari per rispettare le prescrizioni che deriveranno dal pieno recepimento del GDPR.

Sarebbe dunque appropriato realizzare un sistema lineare in cui vi sia un pieno collegamento tra il settore finanziario privato (le banche) e la Pubblica Amministrazione, creando delle apposite strutture aventi il compito di segnalare, prima all' interno di ogni singolo ente, poi a livello nazionale e, successivamente, a livello comunitario, eventuali minacce o incidenti informatici che possano mettere a repentaglio la sicurezza dei dati sensibili dei singoli contribuenti.

Lo scopo infatti è quello di creare un vero e proprio scambio di informazioni tra tutte queste entità circa le minacce informatiche e la maniera più efficace di combatterle, cosa che si potrà realizzare pienamente solo favorendo sistemi di prevenzione basati sull'interscambio di informazioni e di pratiche innovative in campo cibernetico.

LISTA DEGLI ACRONIMI

AML – Anti Money Laundering
APT – Advanced Persistent Threat
BCE – Banca Centrale Europea
BYOD – Bring Your Own Device
CENTCOM – United States Central Command
CEO – Chief Executive Officer
CHF – Franco Svizzero
CIA – Central Intelligence Agency
CISO – Chief Information Security Officer
CISR – Comitato interministeriale per la sicurezza della Repubblica
CONSOB – Commissione Nazionale per le Società e la Borsa
CSIRT – Computer Security Incident Response Team
DCS – Distributed Control Systems
DDoS – Distributed Denial of Service
DIS – Dipartimento per le informazioni della sicurezza
DL – Decreto Legge
DPA – Data Protection Authority
DPCM – Decreto del Presidente del Consiglio dei Ministri
EBA – European Banking Authority
ENISA – European Network and Information Security Agency
EUROPOL – European Police Office
FATF – Financial Action Task Force
FINMA – Autorità Federale per la Vigilanza sui Mercati Finanziari (svizzera)
G7 – Great Seven
GDPR – General Data Protection Regulation
GIFCT – Global Internet Forum per la lotta al terrorismo

ICS – Industrial Control Systems
ICS – Industrial Control Systems
IoT – Internet of Things
IS – Islamic State
ISIS – Stato Islamico dell'Iraq e della Siria
IT – Informatic Technologies
NIS – Directive Network and Information System
NSA – National Security Agency
ONU – Organizzazione delle Nazioni Unite
OSCE – Organizzazione per la Sicurezza e la Cooperazione in Europa
OT – Operative Technology
PA – Pubblica Amministrazione
PLC – Programmable Logic Controller
PMI – Piccole e Medie Imprese
R&D – Research and Development
ROI – Return on Investment
SCADA – Supervisory Control And Data Acquisition
SID – Sistema di interscambio dati
UE – Unione Europea
UIF – Unità di Informazione Finanziaria
USB – Universal Serial Bus

RIFERIMENTI BIBLIOGRAFICI

Abu Dhabi regulates ICOs for cryptocurrency funding – but warns of 'many risks', 9 ottobre 2017. https://www.cnbc.com/2017/10/09/abu-dhabi-regulates-icos-for-cryptocurrency-company-funding.html.

Agenzia delle Entrate, Risoluzione 72/E, 2 settembre 2016, consultabile al link: http://www.agenziaentrate.gov.it/wps/wcm/connect/52bf008f-fab5-46f6-9d64-f334f1f3119a/RISOLUZIONE+N.+72+DEL+02+SETTEMBRE+2016E.pdf?MOD=AJPERES&CACHEID=52bf008f-fab5-46f6-9d64-f334f1f3119a.

Andreas M. Antonopoulos, *Mastering Bitcoin. Unlocking Digital Crypto-Currencies*, O'Reilly Media, aprile 2014.

At risk: the energy and utilities sector infrastructure, IBM X-Force Research. Available at: https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=SEL03135USEN&.

Banca d'Italia, Unità di Informazione Finanziaria, Comunicazione sull'utilizzo anomalo di valute virtuali, 30 gennaio 2015.

Banca d'Italia, Unità di Informazione Finanziaria, Quaderni dell'antiriciclaggio: Analisi e studi, Casistiche di riciclaggio e di finanziamento del terrorismo, dicembre 2016, https://uif.bancaditalia.it/pubblicazioni/quaderni/2016/quaderni-7-2016/quaderni_7_2016.pdf.

Bitcoin 'Ought to Be Outlawed,' Nobel Prize Winner Stiglitz Says, Bloomberg, 29 novembre 2017, https://www.bloomberg.com/news/articles/2017-11-29/bitcoin-ought-to-be-outlawed-nobel-prize-winner-stiglitz-says-jal10hxd.

"Bitcoin a briglia sciolta, quotazioni impazzite fino a 19mila dollari", in *Il Sole 24 Ore*", 7 dicembre 2017.

Bonderud D., *Leaked Mirai Malware Boosts IoT Insecurity Threat Level*, Security Intelligence, 4th October 2016. Available at: https://securityintelligence.com/news/leaked-mirai-malware-boosts-iot-insecurity-threat-level/.

Borger J., "Top Senate intelligence duo: Russia did interfere i 2016 election", *The Guardian*, 4 ottobre 2017, Disponibile online: https://www.theguardian.com/world/2017/oct/04/senate-intelligence-committee-russia-election-interference.

Campensato G., *Equifax, l'attacco hacker fa saltare la testa del ceo Smith*, in *CorCom, Quotidiano on line dell'economia digitale e dell'innovazione*, 7 dicembre 2011. Articolo online: https://www.corrierecomunicazioni.it/cyber-security/equifax-l-attacco-hacker-fa-saltare-la-testa-del-ceo-smith/.

Cavelty M.D., *The Militarisation of Cyberspace: Why Less May Be Better*, in: C. Czosseck, R. Ottis, and K. Ziolkowski (eds), 2012, Proceedings of the 4th International Conference on Cyber Conflict, Tallinn.

Cavelty M.D., *The Militarization of Cybersecurity as a Source of Global Tension*, in: Daniel Möckli (ed.), Strategic Trends 2012, Center for Security Studies: ETH Zurich.

China bans companies from raising money through ICOs, asks local regulators to inspect 60 major platforms, Cnbc, 4 settembre 2017. https://www.cnbc.com/2017/09/04/chinese-icos-china-bans-fundraising-through-initial-coin-offerings-report-says.html.

CIRT Programme: http://www.itu.int/en/ITU-D/Cybersecurity/Pages/Organizational-Structures.aspx.

Clark P., *Your biggest cyber threat? It's not who you think it is*, Financial Times, 9 ottobre 2017, Disponibile online: https://www.ft.com/content/b69fc21e-a9d6-11e7-93c5-648314d2c72c

Cnbc, Cryptocurrencies like bitcoin are not "mature" enough to regulate, ECB chief Mario Draghi says, 19 ottobre 2017. https://www.cnbc.com/2017/10/19/cryptocurrencies-are-not-mature-enough-ecb-chief-mario-draghi.html

COM(2016) 450 final, Proposta di Direttiva del Parlamento Europeo e del Consiglio che modifica la direttiva (UE) 2015/849 relativa alla prevenzione dell'uso del sistema finanziario a fini di riciclaggio o finanziamento del terrorismo e che modifica la direttiva 2009/101/CE, 5 luglio 2016. Disponibile al link: https://ec.europa.eu/transparency/regdoc/rep/1/2016/IT/1-2016-450-IT-F1-1.PDF.

Corte di Giustizia Europea, sentenza del 22 ottobre 2015, causa C-264/14, Skatteverket c. David Hedqvist, consultabile al link: http://curia.europa.eu/juris/document/document.jsf?text=&docid=170305&pageIndex=0&doclang=IT&m ode=lst&dir=&occ=first&part=1&cid=581757.

Council of Europe, Convention on Cybercrime, Budapest, 23.XI.2001, http://www.europarl.europa.eu/meetdocs/2014_2019/documents/libe/dv/7_conv_budapest_/7_conv_budapest_en.pdf.
Deibert R., Rohozinski R., *The new cyber military-industrial complex*, The Globe and Mail, 2011.
Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union: http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L1148&from=EN.
Direttiva (UE) 2016/1148 del Parlamento europeo e del Consiglio, del 6 luglio 2016, recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione. Disponibile online: http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016L1148&from=IT.
Direttiva 95/46/CE del Parlamento europeo e del Consiglio, del 24 ottobre 1995, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati, http://ec.europa.eu/justice/policies/privacy/docs/95-46-ce/dir1995-46_part1_it.pdf.
EBA Opinion on 'virtual currencies', 4 luglio 2014. Disponibile al link: http://www.eba.europa.eu/documents/10180/657547/EBA-Op-2014-08+Opinion+on+Virtual+Currencies.pdf.
ECB – Virtual Currency Schemes, ottobre 2012. Disponibile al link: http://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf.
Elezioni USA, è il giorno della convention democratica: Bloomberg si schiera con Hillary, Repubblica.it, 24 luglio 2016. Disponibile online: http://www.repubblica.it/esteri/elezioni-usa/primarie2016/2016/07/24/news/elezioni_usa_e_il_giorno_della_convention_democratica_per_hillary_arriva_l_endorcement_di_bloomberg-144753795/?ref=search.
Equifax data breach: credit rating firm replaces key staff, BBC News, 16 settembre 2017, disponibile online: http://www.bbc.com/news/technology-41291643.
FATF Report, Emerging Terrorist Financing Risks, Ottobre 2015. Disponibile al link: http://www.fatf-gafi.org/media/fatf/documents/reports/Emerging-Terrorist-Financing-Risks.pdf.
FATF Report, Virtual Currencies, giugno 2014. Disponibile al link: http://www.fatf-gafi.org/media/fatf/documents/reports/Virtualcurrency-key-definitions-and-potential-aml-cft-risks.pdf
Gori U., Martino L. (a cura di), *Intelligence e Interesse Nazionale*, Aracne, Roma, 2015.

Graham D., "Cyber Threats and law of war", *Journal of National Security Law and Policy*, pp. 4:87.

Green J.A., *Cyber Warfare: A multidisciplinary Analysis*, Routledge, 2015.

Grilli F., Equitalia, sito down: "Un attacco hacker", in *Il Giornale.it*, 21 novembre 2016. Articolo online: http://www.ilgiornale.it/news/cronache/equitalia-sito-down-attacco-hacker-1334193.html.

Guidance for a risk-based approach, 'Prepaid cards, mobile payments and internet-based payment services', giugno 2013, http://www.fatf-gafi.org/media/fatf/documents/recommendations/Guidance-RBA-NPPS.pdf.

Healey J.M., *Confidence-Building Measures in Cyberspace – A multistakeholder approach for stability and security*, Atlantic Council, 2014.

Hollis D., *Cyberwar Case Study: Georgia 2008*, Small Wars Journal, 2011.

Hunt K., *Middle East freezes out Qatar: what you need to know*, CNN, 27 luglio 2017, disponibile online: http://edition.cnn.com/2017/06/06/middle east/qatar-middle-east-diplomatic-freeze/index.html.

Internet Policy, *UN Group of Governmental Experts: Developments in the Field of Information and Telecommunications in the Context of International Security*, Council on Foreign Relations,2015, retrieved from: http://www.cfr.org/internet-policy/un-group-governmental-experts-developments-field-information-telecommunications-context-international-security/p36949.

INTERPOL, Research identifies illegal wildlife trade on the Darknet, 14 June 2017https://www.interpol.int/News-and-media/News/2017/N2017-080.

Jacobs P., *Top Democrat blasts Twitter: Presentation to congressional Russia investigators 'inadequate on almost every level'*, Business Insider, 28 settembre 2017, Disponibile online: http://www.businessinsider.com/mark-warner-blasts-twitter-russia-testimony-2017-9?IR=T.

"Le tasse universitarie a Cipro si pagano in Bitcoin", in *Il Sole 24 Ore*, 21 novembre 2013; Zugo, la capitale del Bitcoin: sarà possibile pagare sanità e trasporti, in *La Repubblica*, 11 maggio 2016.

Leary J., Verizon's Enterprise Unit Suffers Major Data Breach, Identity Force, 25th March 2016, Available at: https://www.identityforce.com/blog/verizon-enterprise-data-breach.

Leb L., NotPetya Operators Installed Three Backdoors on M.E.Doc Software Server Before Activating Malware, Security Intelligence, 10th July 2017. Available at: https://securityintelligence.com/news/notpetya-operators-installed-three-backdoors-on-m-e-doc-software-server-before-activating-malware/.

Lever R., Huge hack of US government data affected 21.5 mn, Yahoo, 9th July 2015. Available at: https://www.yahoo.com/news/21-5-million-affected-us-government-data-breach-194354188.html.

Levin S., *Mark Zuckerberg: I regret ridiculing fears over Facebook's effect on election*, 28 settembre 2017, Disponibilie online: https://www.theguardian.com/technology/2017/sep/27/mark-zuckerberg-facebook-2016-election-fake-news.

Longo A., "Sicurezza, Ecco come l'Europa vuole rendere il cyberspazio più sicuro", Il sole 24 Ore online, 22 settembre 2017. Disponibile online: http://www.ilsole24ore.com/art/tecnologie/2017-09-22/sicurezza-ecco-come-l-europa-vuole-rendere-cyberspazio-piu-sicuro--085913.shtml?uuid=AEeG5PXC.

Mallonee, M.K., Hackers publish contact info of 20,000 FBI employees, CNN Politics, 9th February 2016. Available at: http://edition.cnn.com/2016/02/08/politics/hackers-fbi-employee-info/index.html.

Manzin M., "Gli hacker rubano 70 milioni in bitcoin", *Il piccolo*, 9 dicembre 2017, http://ilpiccolo.gelocal.it/trieste/cronaca/2017/12/09/news/gli-hacker-rubano-70-milioni-in-bitcoin-1.16217024.

Mason R., "Xi Jinping state visit: UK and China sign cybersecurity pact", *The Guardian*, 21st October 2015, Available at: https://www.theguardian.com/politics/2015/oct/21/uk-china-cybersecurity-pact-xi-jinping-david-cameron.

Maurer T., Morgus R., *Compilation of Existing Cybersecurity and Information Security Related Definitions*, New America, 2014.

Meulenbelt S., *The 'Worm' as a Weapon of Mass Destruction*, The RUSI Journal, 2012, 157:2, pp. 62-67.

Meyer P., "Diplomatic Alternatives to Cyber-Warfare: A Near-Term Agenda", *The RUSI Journal*, 2012, 157:1, pp. 14-19.

Milano F., "'Non aprite quella mail': Equitalia sotto attacco phising", in *Il Sole 24 Ore*, 28 marzo 2017. Articolo on line: http://www.ilsole24ore.com/art/norme-e-tributi/2017-03-28/non-aprite-quella-mail-equitalia-sotto-attacco-phishing-155710.shtml?uuid=AEXvGzu.

NATO CCDCOE, *Cyber Security Strategy Documents*, retrieved from: https://ccdcoe.org/cyber- security-strategy-documents.html.

Paganini P., "Dal caso Wannacry alla Direttiva NIS, le infrastrutture critiche sono ancora troppo vulnerabili", *Startup Italia*, 22 maggio 2017. Disponibile online: http://cybersecurity.startupitalia.eu/54714-20170522-dal-caso-wannacry-alla-direttiva-nis-le-infrastrutture-critiche-ancora-vulnerabili.

Pagliery J., *The inside story of the biggest hack in history*, CNN Tech, 5 agosto 2015, disponibile online: http://money.cnn.com/2015/08/05/technology/aramco-hack/index.html.

Peterson A., *The Sony Pictures hack, explained*, The Washington Post, 18 dicembre 2014, Disponibile online: https://www.washingtonpost.com/news/the-switch/wp/2014/12/18/the-sony-pictures-hack-explained/?utm_term=.6f8636d971b6.

Rabinovits D., Phishing Scams: How to Protect Yourself, Identity Force, 5th November 2014. Available at: https://www.identityforce.com/blog/phishing-scams-how-to-protect-yourself.

Rapporto CLUSIT 2017 sulla sicurezza ICT in Italia. Disponibile online: https://clusit.it/wp-content/uploads/download/Rapporto_Clusit%202016.pdf.

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance): http://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:32016R0679.

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation): http://ec.europa.eu/justice/data-protection/reform/files/regulation_oj_en.pdf.

Rijtano R., "Cinque bancomat bitcoin in Italia: 'Tanta curiosità, poche transazioni, nessuna regola'", Repubblica.it, 20 ottobre 2014 http://www.repubblica.it/tecnologia/2014/10/20/news/bitcoin_italia-98573671/.

Roscini M., *Cyber Operations and the Use of Force in International Law*, Oxford University Press 2014.

Salerno A., *Cybercrime 2018, supply chain sotto attacco hacker*, Corriere delle Comunicazioni 17 Febbraio2017. Disponibile online: https://www.corrierecomunicazioni.it/.../cybercrime-2018-supply-chain-sotto-attacco.

Sang-Hun C., *North Korean Hackers Stole U.S. – South Korean Military Plans, Lawmaker Says*, The New York Times, 10 ottobre 2017, disponibile online: https://www.nytimes.com/2017/10/10/world/asia/north-korea-hack-war-plans.html.

"Sesso, droga e armi: la faccia cattiva del web", in *la Repubblica*, 11 aprile 2012. Disponibile al link: www.repubblica.it/tecnologia/2012/04/11/news/sesso_droga_e_armi_la_faccia_cattiva_del_web-33089682/.

Siddiqui T., *In wake of mass panic, India blames Pakistan- backed cyber attack*, The Christian Science Monitor, 24 agosto 2012, disponibile online: https://www.csmonitor.com/World/Asia-South-Central/2012/0824/In-wake-of-mass-panic-India-blames-Pakistan-backed-cyber-attack.

Soro A., *Audizione presso la Commissione parlamentare di vigilanza sull'Anagrafe Tributaria – Camera dei* deputati, 25 marzo 2015.

Soro A., *Comunicazione inviata presso l'Agenzia delle Entrate e il Ministero dell'Economia*, 17 febbraio 2017.

The Crypto-Currency. Bitcoin and its mysterious inventor, in "The New Yorker", 10 ottobre 2011, www.newyorker.com/magazine/2011/10/10/the-crypto-currency.

There's an $814 Million Mystery Near the Heart of the Biggest Bitcoin Exchange, Bloomberg, 5 dicembre 2017, https://www.bloomberg.com/news/articles/2017-12-05/mystery-shrouds-tether-and-its-links-to-biggest-bitcoin-exchange.

"Trump full of praise for Duterte's brutal drugs crackdown, leaked call reveals", *The Guardian*, 24 maggio 2017, Disponibile online: https://www.theguardian.com/us-news/2017/may/24/trump-duterte-us-philippines-drugs-crackdown.

United Nations, General Assembly, *Developments in the field of information and telecommunications in the context of international security*, Report of the Secretary-General, 2015 retrieved from: http://undocs.org/A/70/174.

United Nations, General Assembly, *Developments in the field of information and telecommunications in the context of international security*, Report of the Secretary-General, 2013 retrieved from: http://undocs.org/A/68/98.

United Nations, General Assembly, *Developments in the field of information and telecommunications in the context of international security*, Report of the Secretary-General, 2016 retrieved from: http://www.un.org/ga/search/view_doc.asp?symbol=A/71/172.

Valentino-DeVries J., Thuy Vo L., Yadron D., "Cataloging the World's Cyberforces", *The Wall Street Journal*, 2015.

Zampetti R., *Minacce cibernetiche alla sicurezza nazionale*, SIS. N. 1/2015, gennaio 2015. Disponibile online: www.archiviodisarmo.it/index.php/en/publications/magazine/magazine/finish/.../1329).

Zetter K., *An unprecedented look at Stuxnet, the world's first digital weapon*, WIRED 2014.

Zetter K*., Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid*, WIRED, 2016.

Università: economia

Ultimi volumi pubblicati:

CLAUDIO CACCIAMANI, ALESSANDRA FIORELLI (a cura di), *Il crowdfunding* (disponibile anche in e-book).

MATTEO COTUGNO, SEBASTIANO MAZZÙ, STEFANO MONFERRÀ (a cura di), *Corporate & investment banking.*

GUIDO MIGLIACCIO, GIUSEPPE NAPOLI, CLAUDIO RISPOLI, LUIGI UMBERTO ROSSETTI, *Tecnica amministrativa e ragioneria*. Strumenti per l'apprendimento.

CONFARTIGIANATO ANCONA PESARO E URBINO, UNIVERSITÀ POLITECNICA DELLE MARCHE, *Artigianato e piccole imprese patrimonio per i territori.* Nuove traiettorie di sviluppo (disponibile anche in e-book).

CLAUDIO CACCIAMANI, GIUSEPPE GIUDICI (a cura di), *Compagnie di assicurazioni e finanziamento alle imprese* (disponibile anche in e-book).

FEDERICO COLTRO, RAFFAELE D'ARIENZO, SILVIA MARINI, *Antiriciclaggio.* Teoria e pratica per professionisti (disponibile anche in e-book).

MARILENA BONGIOVANNI, PINA TRAVAGLIANTE (a cura di), *La medicina narrativa strumento trasversale di azione, compliance e empowerment* (disponibile anche in e-book).

FLAVIO SANGALLI, *Il sindacalista e Galileo.* Miglioramento e capacità realizzativa nella nuova prassi sindacale: l'esperienza di FP CISL Lombardia (disponibile anche in e-book).

SILVIO MENGHINI (a cura di), *La filiera della birra artigianale toscana.*

SERGIO BRANCIARI (a cura di), *Indagine sui bilanci delle piccole imprese.* La banca dati del Confidi Ancona (2003-2012) (disponibile anche in e-book).

CENTRO STUDI POLITICO SOCIALI J.F. KENNEDY (a cura di), *La difesa dell'ambiente e il riordino dei livelli istituzionali e dei corpi tecnici territoriali* (disponibile anche in e-book).

TULLIO CHIMINAZZO, *Etica ed economia.* Verso il nuovo umanesimo economico (disponibile anche in e-book).

FRANCESCA PIRLONE, *I borghi antichi abbandonati.* Patrimonio da riscoprire e mettere in sicurezza (disponibile anche in e-book).

CHIARA MIO (a cura di), *La rendicontazione sociale negli atenei italiani.* Valori, modelli, misurazioni (disponibile anche in e-book).

CENTRO STUDI SINTESI (a cura di), *Territori, aree vaste, competitività.* La nuova configurazione economica e strategica di Emilia Romagna, Lombardia e Veneto (disponibile anche in e-book).

REGIONE SICILIANA, *Annuario statistico regionale.* Sicilia 2015 (disponibile anche in e-book).

VALERIA MAIONE (a cura di), *Insiemesipuò.* Gli stati generali delle Donne nelle regioni italiane (disponibile anche in e-book).

LUCA BASSO, LUCA JEANTET, MICHELE PAOLO PASTORE, ANDREA VAROLI, *La ristrutturazione.* Linee guida e strumenti di composizione della crisi d'impresa (disponibile anche in e-book).

Pier Giovanni Bresciani, Alessandra Sartori, *Innovare i servizi per il lavoro: tra il dire e il mare.* Apprendere dalle migliori pratiche internazionali (disponibile anche in e-book).

Giuseppe Bortolussi, Riccardo Dalla Torre, Andrea Favaretto, Catia Ventura (a cura di), *Per la competitività del turismo nell'Alto Adriatico.* Il turismo al centro dello sviluppo (disponibile anche in e-book).

Francesca Pirlone, *I rifiuti e i piani di gestione urbana all'interno della governance* (disponibile anche in e-book).

Ilaria Delponte (a cura di), *Historical city markets: a set of guidelines* (disponibile anche in e-book).

Azienda Speciale della Camera di Commercio di Imperia PromImperia (a cura di), *Dieta Mediterranea Mediterranean Diet.* Atti del Forum Imperia 13-16 novembre 2014 (disponibile anche in e-book).

Maria Francesca Kainich, Massimo Saita, Paola Saracino, *Economia delle aziende biotecnologiche.*

Guido Cutillo, Franco Fontana (a cura di), *Compendio sulla normativa relativa ai compensi degli amministratori e dei manager aziendali - 2015* (disponibile anche in e-book).

Valerio De Luca, Dominick Salvatore (a cura di), *La sfida europea.* Riforme, crescita e occupazione (disponibile anche in e-book).

Giuseppe Bortolussi (a cura di), *Le Province: operazione verità.* Il caso Friuli Venezia Giulia (disponibile anche in e-book).

Ermeneia, *Shoe Report 2015.* Settimo Rapporto Annuale sul contributo del settore calzaturiero al rafforzamento del Made in Italy (disponibile anche in e-book).

Centro Studi Sintesi (a cura di), *La mappa dell'economia e le nuove direttrici dello sviluppo.* Emilia Romagna, Lombardia e Veneto dentro le trasformazioni (disponibile anche in e-book).

Regione Siciliana, *Annuario statistico regionale.* Sicilia 2014 (disponibile anche in e-book).

Pier Giovanni Bresciani (a cura di), *Risorse umane nell'organizzazione.* Giovani e donne nelle Banche di Credito Cooperativo (disponibile anche in e-book).

Fondazione Leone Moressa, *Il valore dell'immigrazione* (disponibile anche in e-book).

Marco Canesi, *Egemonismo del capitale e autodeterminazione dei popoli.* Una proposta per il Centro America e i Caraibi (disponibile anche in e-book).

Guido Migliaccio, *La dimensione quantitativa della gestione.* Aspetti teorici e applicativi.

Riccardo Pastore, *Il marketing del vino e del territorio: istruzioni per l'uso.*

Claudio Cacciamani, Lara Maini (a cura di), *Credito e fideiussioni.* Situazione e prospettive (disponibile anche in e-book).

Eupolis Lombardia, Ipres, Ires Piemonte, Irpet, Liguria Ricerche, Srm, *La finanza territoriale.* Rapporto 2014 (disponibile anche in e-book).

Giuseppe Bortolussi (a cura di), *Il sistema camerale in Italia.* Ruolo, valore e identità (disponibile anche in e-book).

Centro Studi Sintesi (a cura di), *Impegno e responsabilità delle professioni a servizio del territorio.* Il contributo dei professionisti allo sviluppo sociale ed economico della provincia di Venezia (disponibile anche in e-book).

FEDERICA PALAZZI, *Medie imprese italiane, sviluppo e corporate finance.* I valori del capitalismo personale (E-book).

CARLO CIPRIANI (a cura di), *Economia e management delle imprese calzaturiere.* Prospettive e strumenti per la competitività dell'industria marchigiana (disponibile anche in e-book).

GUIDO CUTILLO, FRANCO FONTANA (a cura di), *Compendio sulla normativa relativa ai compensi degli amministratori e dei manager aziendali 2012* (disponibile anche in e-book).

ÉUPOLIS LOMBARDIA, IPRES, IRES PIEMONTE, IRPET, LIGURIA RICERCHE, SRM, *La finanza territoriale in Italia.* Rapporto 2012 (disponibile anche in e-book).

PIER GIOVANNI BRESCIANI (a cura di), *Capire la competenza.* Teorie, metodi, esperienze dall'analisi alla certificazione (disponibile anche in e-book).

ERMENEIA, *Beauty Report 2012.* Terzo Rapporto sul valore dell'industria cosmetica in Italia (disponibile anche in e-book).

ERMENEIA, *Shoe Report 2012.* Quarto Rapporto Annuale sul contributo del settore calzaturiero al rafforzamento del Made in Italy (disponibile anche in e-book).

REGIONE SICILIANA, *Annuario statistico regionale.* Sicilia 2011 (disponibile anche in e-book).

A.DI.G.E.-ASSOCIAZIONE PER LA DIFFUSIONE DELLA GIURISPRUDENZA ECONOMICA, *Rivista di giurisprudenza ed economia d'azienda n. 9 - 2011* (disponibile anche in e-book).

ÉUPOLIS LOMBARDIA, IPRES, IRES PIEMONTE, IRPET, SRM, *La finanza locale in Italia.* Rapporto 2011 (disponibile anche in e-book).

STEFANO GUIDANTONI, IRENE SANESI, *Creatività cultura creazione di valore.* Incanto economy (disponibile anche in e-book).

FRANCESCA VITALI, *I luoghi della partecipazione.* Una ricerca su donne, lavoro e politica (disponibile anche in e-book).

MARISA ARGENE VALLERI, STEFANO CARAGNANO, *Appunti teorici e pratici di programmazione locale e regionale.*

BERNARD REY, *Ripensare le competenze trasversali.*

FABRIZIO BIENTINESI, *La parziale eccezione.* Costi comparati e teorie del commercio internazionale in Italia dalla metà dell'Ottocento alla seconda guerra mondiale (disponibile anche in e-book).

MASSIMILIANO DONA (a cura di), *Etica delle imprese e dei consumatori.* Atti del Premio Vincenzo Dona, voce dei consumatori 2010 (disponibile anche in e-book).

A.DI.G.E.-ASSOCIAZIONE PER LA DIFFUSIONE DELLA GIURISPRUDENZA ECONOMICA, *Rivista di Giurisprudenza ed Economia d'Azienda n. 8 - 2010* (disponibile anche in e-book).

FLAVIO SANGALLI, *Manufatti organizzativi.* Modelli e percorsi di sviluppo organizzativo di Confartigianato Imprese in Lombardia (disponibile anche in e-book).

ERMENEIA, *Beauty Report 2011.* Secondo rapporto sul valore dell'industria cosmetica in Italia (disponibile anche in e-book).

SVILUPPO BRIANZA, *I 5 fattori dello sviluppo locale.* Cultura, produzione, lavoro, leadership e megatrends nel futuro della Brianza (disponibile anche in e-book).

REGIONE SICILIANA, *Annuario statistico regionale.* Sicilia 2010 (disponibile anche in e-book).

ERMENEIA, *Shoe Report 2011.* Terzo Rapporto Annuale sul contributo del settore calzaturiero al rafforzamento del Made in Italy (disponibile anche in e-book).

FrancoAngeli/Riviste

tutte le modalità
per sceglierci in digitale

Più di 80 riviste consultabili in formato digitale su **pc** e **tablet**:

1. in *abbonamento annuale* (come ebook)
2. come *fascicolo singolo*
3. come singoli *articoli (*acquistando un *download credit)*

Più tempestività, più comodità.

Per saperne di più: **www.francoangeli.it**

Questo volume nasce in seguito al convegno “Il ruolo dell’Italia nella sicurezza cibernetica dopo il G7” organizzato dalla Fondazione Luigi Einaudi di Roma ed AISES, sponsorizzata da CSE CybSec SPA.
Si tratta di una raccolta interdisciplinare di interventi che mira a fornire un quadro generale dello stato dell’arte della cyber security in Italia, considerata l’attualità della tematica e la crescente attenzione nei confronti della materia. I temi trattati spaziano su tutti i settori: da un’analisi delle opportunità e delle minacce inerenti al cyberspace, alle iniziative portate avanti a livello internazionale, agli effetti della rivoluzione digitale sui sistemi nazionali ed i possibili sviluppi futuri. Hanno partecipato alla redazione alcuni tra i massimi esperti italiani del settore, fornendo un quadro completo ed esaustivo della realtà italiana.

Giulio Terzi di Sant’Agata ha prestato servizio all'Ambasciata a Parigi, a Ottawa, è stato Console Generale a Vancouver, Primo Consigliere Politico alla Rappresentanza Permanente alla NATO e Ministro Consigliere alle Nazioni Unite a New York. Ambasciatore in Israele tra il 2002 e il 2004, ha avuto per un quadriennio l'incarico di Direttore Politico del Ministero degli Affari Esteri assumendo poi quello di Rappresentante Permanente alle Nazioni Unite a New York, di Ambasciatore a Washington, e quindi nominato nel Novembre 2011 Ministro degli Affari Esteri con il Governo Monti.
Presiede attualmente il “Global Committee for the Rule of Law- Marco Pannella”, il Dipartimento Relazioni Internazionali della Fondazione Luigi Einaudi a Roma, è membro di Advisory Boards e Consigli di Amministrazione di ThinkTanks italiani e stranieri per la pace, la sicurezza internazionale, i diritti umani e lo stato di diritto.

Valerio De Luca è Presidente esecutivo e fondatore dell'Accademia Internazionale per lo Sviluppo Economico e Sociale, e Segretario Generale dell'istituzione Diplomatia. Fondatore e Direttore Esecutivo del Global Sustainability Forum, e Presidente del Forum del Mediterraneo di Roma. E’ Direttore del Dipartimento Relazioni Internazionali della Fondazione Einaudi Onlus, Direttore del Global Security and Foreign Affairs Programme, Centro Studi Americani in collaborazione con AISES, e co-direttore del Sustainable Finance and Market Regulation Project, Sapienza Università di Roma. Già Visiting Fellow presso la Yale Law School e la London School of Economics, è dottore di ricerca, avvocato e consulente con esperienza alla Commissione Europea, in società quotate e presso la CONSOB dove ha lavorato dal 2006 al 2012. E' Visiting Professor del Center for Sustainability Leadership e membro del comitato scientifico della Strathmore Business School University di Nairobi, nonché della Fondazione Bruno Visentini e della Fondazione Sapienza – Cooperazione Internazionale. E’ autore e curatore di volumi e di pubblicazioni.

Francesca Voce laureata in Scienze internazionali e diplomatiche all’Università degli Studi di Trieste e specializzata in Diritto internazionale grazie ad un anno trascorso alla Facoltà di Diritto dell’Università Pantheon Sorbonne di Parigi. Sta per conseguire il Master in International Security Studies alla Scuola Superiore Sant’Anna e all’Università degli Studi di Trento. Collabora con il Center for Cyber Security and International Relations Studies dell’Università degli Studi di Firenze.

FrancoAngeli
La passione per le conoscenze