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

Informazioni per il lettore

Questo file PDF è una versione gratuita di sole 20 pagine ed è leggibile con

La versione completa dell'e-book (a pagamento) è leggibile con Adobe Digital Editions. Per tutte le informazioni sulle condizioni dei nostri e-book (con quali dispositivi leggerli e quali funzioni sono consentite) consulta cliccando qui le nostre F.A.Q.

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

INDICE

Prefazione, di *Marco Castaldo* pag. 7

Introduzione, di *Valerio De Luca* » 11

1. **La cyber security in Europa nell'attuale scenario geopolitico**, di *Giulio Maria Terzi Di Sant'Agata* » 13
2. **Lo stato dell'arte della cyber security italiana**, di *Francesca Voce* » 22
3. **Cyber diplomacy e relazioni internazionali: le iniziative diplomatiche per mitigare il rischio di escalation militare nel cyberspazio**, di *Luigi Martino* » 26
4. **Hacking, un concetto fondamentale nei conflitti moderni,** di *Pierluigi Paganini* » 36
5. **Una Convenzione Digitale di Ginevra per il Cyberspace,** di *Pier Luigi Dal Pino* » 43
6. **La cyber security nell'era cognitiva: i rischi per le imprese e per il sistema paese**, di *Domenico Raguseo* » 51
7. **Il ruolo dell'Italia nella sicurezza cibernetica: minacce, consapevolezze, risposte, speranze**, di *Giulio Massucci* » 58
8. **La sicurezza informatica è un diritto umano**, di *Arturo Di Corinto* » 75
9. **Cyber security, criptovalute e criminalità**, di *Irene Piccolo* » 86

10. Direttiva NIS e Ordinamento giuridico-economico italiano. Per non dimenticare la vulnerabilità delle piccole e medie imprese da attacchi cyber, di *Marco Mariscoli* pag. 96

11. L'importanza di Internet negli adempimenti fiscali: vantaggi e criticità, di *Luca Serafino De Simone* » 105

Lista degli acronimi » 115

Riferimenti bibliografici » 117

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);