Nomos & Khaos

Rapporto Nomisma 2012-2013 sulle prospettive economico-strategiche

Osservatorio Scenari Strategici e di Sicurezza

Nomisma LIBRI PER L'ECONOMIA

4.4

Le sfide alla sicurezza nell'era digitale

Umberto Rapetto

L'ambiente digitale continua ad esser poco conosciuto, cosa che rende ardua la predisposizione di efficaci difese dal rischio cibernetico, specialmente in Paesi come l'Italia che mancano anche delle risorse necessarie e potrebbero anche non rilevare eventuali cyber-attacchi ai propri danni. Complica ulteriormente la situazione la circostanza che le offese cibernetiche possano produrre i loro effetti con un certo ritardo rispetto al momento del loro inizio, come ha dimostrato il precedente del virus "Stuxnet" impiegato contro l'Iran. Stati Uniti e Repubblica Popolare, invece, paiono già adeguatamente attrezzati ed animano da tempo un duello senza esclusione di colpi. La Casa Bianca dispone di un vero e proprio cyber-czar, mentre la Cina si è dotata di reparti militari speciali che hanno sviluppato capacità notevoli in materia di hacking e cyber-warfare. La guerra condotta sul terreno delle informazioni è ormai una realtà temuta alla stregua di un conflitto convenzionale. Non sembrano invece esserci prospettive per l'utopia della democrazia digitale. Il web è intrinsecamente anarchico e troppo instabile per poter pensare di farne uno strumento di esercizio della sovranità popolare.

Lo scenario digitale continua a riservare sorprese. Gli osservatori, anche i più attenti, continuano a commettere errori.

Il primo sbaglio sta nel sottovalutare l'assoluta permeazione del contesto quotidiano da parte degli strumenti tecnologici e dei comportamenti correlati, la cui reale portata diverge dalla percezione superficiale che i mezzi di informazione e persino gli approfondimenti di sedicenti esperti forniscono quotidianamente.

Il secondo errore consiste nel non voler affrontare il problema in maniera sistematica, forse in modo semplicemente professionale.

Lo dimostra l'incauta "libertà di parola" che consente a chiunque di disquisire di argomenti e tematiche poco conosciute nella speranza di non incappare in interlocutori in grado di smentire categoricamente qualsivoglia dichiarazione.

Simile situazione innesca un devastante "effetto domino" con l'inarrestabile depauperamento culturale destinato a stordire chi deve decidere che – leopardianamente – trova persino dolce naufragare in tale mare di letale ignoranza.

Terza cantonata, l'insistere ad etichettare come cibernetico qualunque cosa o azione che abbiano energia elettrica a farle funzionare. Lo specchio dell'analfabetismo dilagante ha sempre dinanzi qualcuno pronto a rimirare il proprio riflesso.

DECISION MAKERS SOLI O MAL ACCOMPAGNATI

La sequela delle pietre miliari del decadente percorso potrebbe impietosamente proseguire. È sufficiente aver acquisito la più elementare consapevolezza che la quasi totalità di chi chiacchiera di queste cose, generalmente ha la medesima competenza di chi al Bar dello sport dibatte e sentenzia sui risultati domenicali del campionato di calcio.

Preso atto, pur dolorosamente, del livello (basso, avrebbe detto la buonanima dell'arboriano Pazzaglia) dei guru del settore, si è subito portati a riconoscere che qualsiasi decisione in un contesto informatico difficilmente può trovare adeguata sponda.

La circostanza non è certo rassicurante perché le insidie telematiche e le minacce convenzionali amplificate dai loro ingredienti *hi-tech* sono in crescita esponenziale e possono mettere in difficoltà anche Paesi – come gli Stati Uniti – che non hanno tardato a cimentarsi con certi problemi.

In Italia si è faticosamente giunti al varo del decreto legislativo 23 gennaio 2013 per dar prova dell'attenzione istituzionale ai rischi cibernetici. Il provvedimento si chiude con un categorico riferimento alla mancanza di fondi di qualsivoglia entità per sostenere l'onere della difesa da un simile pericolo.

Ma se l'epilogo è sconcertante per chi sperava di fare business in un settore in cui la lacunosa capacità di committenza avrebbe potuto garantire affari d'oro, quel che preoccupa gli addetti ai lavori (almeno quelli veri) è la vacuità dell'intero decreto,

che si traduce nell'istituzione di entità poco distanti da demoralizzanti gruppi di lavoro (in cui inserire rappresentanti di diverse amministrazioni), nella diaspora di competenze su più articolazioni, nonché nell'individuazione dell'embrione del sistema di protezione/reazione in realtà non ancora esistenti come il Computer Emergency Response Team presso il ministero dello Sviluppo Economico.

LA SITUAZIONE OLTRE CONFINE

Oltreoceano non si è tardato a nominare un Cyber-Czar alle dirette dipendenze di Obama e a pianificare un'organizzazione militare capace di muovere nella quinta dimensione (l'informazione), mentre aldilà della Grande Muraglia da anni le Forze Armate annoverano reparti speciali con operatività spettacolare in materia di *hacking* e di *cyber war*.

Proprio tra Stati Uniti e Repubblica Popolare Cinese è in corso da anni un duello all'ultimo bit, che ha ripetutamente portato a segnalare episodi di scorrerie attraverso i gangli del sistema nervoso americano.

Nel mirino il tessuto connettivo statunitense: dalle reti elettriche intelligenti ai grandi sistemi informatici delle corporation, le moderne orde barbariche non hanno risparmiato niente e nessuno. L'obiettivo è bicipite: mettere *knockout* le imprese paralizzandone apparati di elaborazione dati e rete di comunicazione, rubare segreti industriali e commerciali così da annullare qualsiasi vantaggio economico, finanziario, produttivo.

C'è chi sostiene che a giugno fosse previsto lo scoppio di un conflitto universale, qualcosa di più di una "tradizionale" guerra mondiale. I cinesi sarebbero stati pronti ad attaccare e, in assenza di una formale dichiarazione di apertura delle ostilità (troppo *vintage* per un così futuribile campo di battaglia), il Segretario alla Difesa Chuck Hagel aveva mobilitato le truppe con un magniloquente "*Estote parati*" suffragato da una serie di attente riflessioni sul peso di un *cyber* attacco ai danni delle infrastrutture critiche americane.

Lo stesso presidente Obama non ha esitato ad invitare la collettività internazionale ad organizzare un sistema di protezione adeguato in considerazione del fatto che si vive in un mondo in cui una Nazione non è mai grande abbastanza e forte a sufficienza per maneggiare un simile problema da sola.

A parlare con toni concitati, quindi, non sono soltanto i personaggi dell'industria della sicurezza informatica come Eugene Kaspersky, che da anni sforna rapporti e relazioni inquietanti sullo stato dell'arte della protezione dai rischi in questione:

anche politici e strateghi non esitano a ribadire la pericolosità della situazione.

L'evoluzione è fibrillante: in Australia, nel biennio 2011-2012 ci sono stati ben 438 incidenti informatici di significativa gravità e gli attacchi informatici di diversa caratura indirizzati verso la Gran Bretagna sono stati oltre 44 milioni solo lo scorso anno.

Ma la sensibilità del Regno Unito su questo tema è davvero impressionante e lo comprovano due dati incontrovertibili: dal 2010 la minaccia *cyber* è considerata come uno dei quattro rischi nazionali e, soprattutto, lo specifico programma pluriennale di sicurezza ha comportato stanziamenti aggiuntivi per complessivi 650 milioni di sterline.

Dove c'è coscienza di quanto sta succedendo gli investimenti sono proporzionali al volume di fuoco che un *cyber* arsenale deve essere in grado di garantire.

E lontano dalla nostra penisola c'è anche chi si può permettere di fare filosofia. Marcus Ranum, un "veterano" della *computer security*, recentemente in Australia (al congresso AusCert 2013) ha invitato a dimenticare la parola "*guerra cibernetica*".

Quella che potrebbe sembrare una *boutade*, è invece un appello universale basato su una considerazione elementare sull'aspetto etimologico dell'espressione ogni giorno più citata. Secondo Ranum non c'è alcuna similitudine tra quello di cui stiamo parlando e un conflitto convenzionale del mondo …fisico.

Una guerra "normale" prevede infatti almeno due ingredienti: la possibilità di vincere e una serie di difese in grado di funzionare. Marcus si sofferma sul significato di "vittoria" e si chiede chi possa mai conseguirla nel *cyber*-spazio: forse una "alleanza" tra Intel, Microsoft e Cisco…

Le riflessioni hanno coinvolto l'uditorio e spinto ad ammettere che nessuna difesa è mai riuscita a fermare davvero l'aggressore.

E allora, si condivida o no il pensiero di Marcus Ranum, non si perde tempo almeno per limitare le conseguenze potenzialmente comunque catastrofiche.

IL PERIMETRO NAZIONALE

Chi crede che da noi certe cose non accadano, pecca di superbia o manifesta una lungimirante cecità. Purtroppo, un attacco digitale in Italia potrebbe non essere nemmeno rilevato o magari esser scoperto con un ritardo tale da rendere

un eventuale riscontro inutile e inconfutabile testimone dell'inefficacia nazionale sullo specifico fronte.

In luogo della capillare dispersione degli sforzi, si sente la necessità di una convergenza repentina che deve partire da una severa selezione di persone capaci per arrivare ad una rapida concentrazione delle risorse umane e tecniche in un'unica struttura.

Il solo pensiero di un solo capo, direttore e comandante può far rabbrividire chi è abituato a moltiplicare e distribuire poltrone per non scontentare né gli amici né gli amici degli amici. A dispetto di modaiole larghe intese, in questo settore occorre evitare infruttuose fatiche per trovare accordi o condivisioni: non c'è tempo (e questo fattore potrebbe bastare) per discettare a vanvera e non c'è spazio per troppa gente (serve un vertice con concreta capacità decisionale, non oligarchie su cui spalmare responsabilità in caso di insuccesso).

UN PROFONDO MUTAMENTO D'APPROCCIO DA PARTE DEGLI AGGRESSORI

Chi ricorda i tempi leggendari dei romantici pirati informatici, sa bene che certi stereotipi sono un'ossidata reminiscenza. Il briccone galantuomo, il moderno Robin Hood o altre fascinose figure appartengono ad un passato remoto che le nuove generazioni non conoscono e addirittura stentano a credere. Internet somiglia sempre meno a Sherwood.

Quelli che hanno visto competizioni sportive tra malfattori singoli o organizzati in agguerrite gang hanno ben chiaro che gli ultimi scorci di olimpioniche disfide risalgono ad almeno dieci anni fa.

Il ricordo delle classifiche delle incursioni andate a segno e delle scalate nelle graduatorie dei più "birichini" è ormai sbiadito: nessuno ha più voglia di vantare le proprie gesta, forse dopo aver compreso che un'eccessiva pubblicità può aprire pericolosi varchi verso il proprio nascondiglio e pregiudicare il destino di chi ne ha combinate troppe.

Adesso si preferisce rimanere privi di un volto e di una sigla autonoma. C'è addirittura chi agisce con un *brand* preso in *franchising* e, conformati obiettivi e *modus operandi*, predilige l'appartenenza ad Anonymous o ad altre inidentificabili organizzazioni virtuali.

Ma c'è un altro elemento che è cambiato e ha mutato radicalmente la condotta dei malintenzionati. È scomparsa la fretta di arrivare al risultato, come se qualcuno

avesse eliminato dalla lista dei pregi di un buon *hacker* le formidabili prestazioni da centometrista.

Senza immaginare un contagio (non si pensi ai soliti virus…) di apatia o la diffusione virale del "bamboccionismo", non si può non constatare che chi vuol far danno attraverso la Rete o direttamente in seno ad un sistema informatico aziendale sceglie di agire con il metodo "*low and slow*". Messi al bando dinamiche impetuose e risultati immediatamente clamorosi, chi ambisce a conquistare prede di pregio si muove lentamente e con operazioni di basso profilo.

La spiegazione è facile a trovarsi. Non si vuole inciampare lungo l'itinerario irto di ostacoli e soprattutto si pretende che nessuno sia in grado di ricostruire il come e il quando dell'avvio dell'assalto.

Un potenziale aggressore sa bene che ogni sua mossa può lasciare traccia nei diversi meccanismi implementati per controllare quel che accade nelle viscere di un ente, di un'azienda, di una infrastruttura critica.

Strumenti come i log pronti a registrare qualunque evento e gli *intrusion detection system* (IDS) capaci di segnalare qualsivoglia operazione mirata a by-passare le misure di sicurezza, sono un nemico fin troppo conosciuto dai farabutti elettronici.

La cautela – analoga a quella di un artificiere alle prese con plichi pronti a deflagrare – induce a fare piccoli passi, ma potrebbe non bastare. Se si sfugge all'IDS, meno facile è scappare dalle rigorose annotazioni dei log.

Ma non è questo ad impensierire il delinquente di turno, che sa perfettamente che è sufficiente aspettare.

Aspettare cosa? Si tratta di attendere che il log finisca il suo …quadernetto. Non è certo una novità che la conservazione delle registrazioni non è eterna: il furfante si intrufola e non si muove per mesi, differendo la stoccata anche di un anno così da veder premiato il suo stoicismo.

Quando andrà a segno, se qualcuno cercherà di ricostruire la dinamica di intrusione e il relativo momento, sarà impossibile procedere ad alcuna operazione forense.

La flemma è diventata una regola d'oro. E l'hanno appresa anche i governi con obiettivi importanti. Facciamo un esempio. E non un esempio qualunque.

IL CASO STUXNET

Molti hanno sentito parlare di "Stuxnet", il micidiale virus che ha colpito le centrali nucleari iraniane. Il percorso è stato lungo ed incredibilmente lento. Non è semplice colpire sistemi disconnessi da ogni rete telematica e chiusi in aree inaccessibili. Non è semplice, ma non è impossibile.

La tecnica adoperata ha ricalcato – con grande gioia di Giobatta Vico – la desueta modalità di contaminazione informatica che ha caratterizzato la comparsa e la propagazione dei primi virus nella seconda metà degli anni ottanta.

All'epoca il veicolo di trasmissione dei "bacilli EDP" erano i *floppy disk*: il passaggio di un disco infetto da un computer all'altro garantiva il contagio e il progressivo diffondersi dell'epidemia.

I virus poi hanno cominciato a viaggiare attraverso la posta elettronica, poi nelle pagine web e all'interno di APPS per dispositivi mobili.

Le fasi appena indicate corrispondono – piazzate su un immaginario asse temporale – all'era della connessione globale e costante inaugurata dal web e quindi dalla proletarizzazione del contesto telematico che un tempo era feudo di pochi privilegiati.

Dovendo recapitare istruzioni nocive ad una meta non raggiungibile via Internet, l'unica via è quella del supporto di memorizzazione in uso al singolo: niente il *floppy disk* (ormai scomparso), ma l'onnipresente *pendrive*.

La "pennetta USB" è una sorta di maledizione per la sicurezza, ma la sua comodità (accompagnata dalla incosciente sottovalutazione dei rischi) la rende strumento di uso quotidiano. È ovvio che un virus abilmente piazzato su una memoria di massa USB può fare il giro del mondo, ma qualcuno – magari formatosi su "Strano ma vero" o "Lo sapevate che?" di un noto settimanale enigmistico – avrebbe subito da obiettare su una simile affermazione.

"Un buon antivirus rileva istantaneamente i virus sulle pennette e quindi è impossibile!" esclamerebbe ad alta voce uno dei tanti sedicenti esperti.

Pur dovendo mortificare un così ardito slancio, non si può fare a meno di far osservare che i programmi che intercettano ed eliminano virus, *worm* e cavalli di Troia, fanno bene il loro mestiere localizzando minacce che possono anche solo impensierire il computer in uso.

È naturale che ciascun computer (con sistemi operativi Microsoft, Linux, Apple…) tenga d'occhio quanto lo può insidiare e non dia peso a codici maligni che non riconosce come letali o semplicemente pericolosi.

Nelle centrali iraniane il software installato è diverso da quello utilizzato sugli apparati dei comuni mortali e – in virtù della rarità della piattaforma usata e della mancata connessione in Rete – precauzioni a proposito di contagi lasciano a desiderare.

In poche parole il virus, nascosto in un angolo della *pendrive* come un migrante nella stiva di una nave o nel sottofondo del cassone di un camion, si moltiplica indisturbato.

Milioni di esemplari si diffondono sull'intera superficie del globo senza fare alcun danno, fino al giorno in cui una pennetta (contagiata dopo centinaia o migliaia di passaggi *pendrive*-pc-*pendrive*) arriva ad essere fortuitamente inserita in un computer che gestisce il regolare funzionamento di una centrale atomica. Tutto il resto è cronaca dei giorni nostri.

È chiaro. Un virus informatico, un tempo considerato problema circoscritto al pc infettato o a quelli in seguito contaminati, diventa un'arma e il suo impiego può richiamare regolamentazioni planetarie.

L'attacco perpetrato con "Stuxnet" nei confronti dell'Iran è stato considerato un "*atto di forza illegale*" e di dirlo è toccato a Michael Schmitt, docente di diritto internazionale all'Us Naval War College ossia la Scuola di Guerra della Marina Militare statunitense.

Schmitt – per dirla mutuando la pubblicità Stock degli anni sessanta, "*il signore sì che se ne intende*" – è uno degli estensori del documento di regole sul *cyber-warfare* redatto sulla falsariga della Convenzione di Ginevra e intitolato "Tallinn Manual on the International Law Applicable to Cyber Warfare".

L'ammissione pur ufficiosa – da parte di funzionari americani e israeliani – della creazione del *worm* che ha mandato in tilt centrali nucleari e sistemi di arricchimento dell'uranio in Iran, ha costituito il punto di partenza di una serie di valutazioni sulla reale portata dell'accaduto e sulle sue riverberazioni in termini di diritto.

Se è rimasta qualche perplessità circa il fatto che l'aggressione tecnologica in questione sia da considerare un "attacco armato", la pluralità di esperti concorda nel ritenere che ci si trovi comunque dinanzi ad un atto ostile.

È legittimo spaventarsi pensando alle conseguenze di un simile "gesto" ed è ancor più comprensibile temere "reazioni legittime" o semplicemente legittimate a fronte di offensive digitali.

La Regola n. 9 recita infatti che "*uno Stato colpito da un atto internazionalmente ritenuto iniquo può adottare proporzionali contromisure, anche di carattere cibernetico, contro il Paese responsabile*".

C'è chi trova quiete nella Regola n. 15 che stabilisce che "*il diritto al ricorso alla forza per legittima difesa scatta se un cyber-attacco è in corso o sia imminente a manifestarsi*" e sottolinea il requisito dell'immediatezza, escludendo reazioni successive a propria volta da considerarsi atti di aggressione. Ma forse c'è poco da star tranquilli.

Discussioni di questo genere non hanno precedenti: non se ne è parlato nel corso della paralisi telematica che ha bloccato l'Estonia nel 2007, non c'è stato nessun dibattito a seguito del *cyber*-conflitto tra Russia e Georgia nel 2008. Adesso, però, il tema ha cominciato una sorta di lievitazione che lo non lo fa passare inosservato.

E il vero focus non è tanto sulle operazioni militari vere e proprie, ma piuttosto sul coinvolgimento dei "civili" in un così multiforme campo di battaglia.

L'universo "laico" è bersaglio da tempo, ma da anni è bacino di reclutamento e di impiego di risorse con finalità di carattere bellico o paramilitare. Si spazia dagli *hacker* non inquadrati in reparti tradizionali ai "dormienti" che popolano organizzazioni pubbliche e private dal cui interno sono in grado di innescare le più diverse manovre. Il problema è serio, al punto che la Regola 28 paragona gli "*hacker a noleggio*" a mercenari che non godono di alcuna immunità riconosciuta a chi combatte e tantomeno il potenziale status di prigionieri di guerra…

Basteranno le regole a sedare la turbolenta atmosfera digitale? Probabilmente no. Ma una maggiore attenzione a certe questioni può già essere un significativo passo avanti. "*Fermate il mondo, voglio scendere*" esclamerebbe l'attore Giorgio Forconi nel Carosello di mezzo secolo fa. E purtroppo oggi non ci sarebbe Ernesto Calindri a rassicurarlo con un bicchiere d'amaro al carciofo.

IL FURTO DI DATI RISERVATI E LA POSSIBILE DIVULGAZIONE

L'arma che ha rivoluzionato gli odierni equilibri bellici si chiama "*leaking*" e rappresenta l'ultima frontiera dell'infinito cosmo dell' "*information warfare*".

La guerra con le informazioni ha dovuto prendere atto che le dinamiche convenzionali – che ne hanno tracciato il percorso evolutivo – sono state clamorosamente annientate da un invisibile esercito di *whistleblowers* (letteralmente quelli che fanno soffiate) adescati da un profeta della vendetta a lento rilascio.

Il *leader* carismatico di questa nuova belligeranza oggi va sotto il nome di Julian Paul Assange, ma in realtà potrebbe pirandellianamente essere uno, nessuno o centomila in considerazione che chiunque – ovviamente dotato di cervello, cultura e fantasia – potrebbe pericolosamente prenderne il posto o emularne le gesta.

La vicenda Wikileaks è una delle pagine, e forse domani sarà un capitolo, dell'ennesima guerra mondiale che si combatte attraverso il web sfruttando la pericolosa miscela detonante di carte e bit sapientemente dosati.

È la dimostrazione che le più potenti Nazioni hanno sempre meno paura della minaccia nucleare e ogni giorno più timore della "bomba I", l'ordigno carico di informazioni letali capaci di sovvertire ordine e quiete con la violenza di uno tsunami e l'irreparabilità di un olocausto.

In passato si era immaginato un possibile scontro di natura tecnologica, ipotizzando soltanto un assalto alla baionetta virtuale in danno ai sistemi di elaborazione dati che potesse portare alla paralisi delle realtà il cui ciclo biologico fosse disciplinato dal corretto funzionamento di computer e reti.

Tale rischio ha portato progressivamente allo studio e alla progettazione di soluzioni organizzative e tecniche che potessero salvaguardare da un potenziale arrembaggio le infrastrutture critiche di un Paese.

Bersagli privilegiati di una simile aggressione sono i gangli dell'erogazione dei servizi essenziali: nel mirino dell'invisibile avversario pronto a sbarcare sui lidi telematici sono le realtà del mondo creditizio, finanziario e assicurativo, le articolazioni delle strutture sanitarie, le aziende di telecomunicazioni, gli erogatori di energia, le società di trasporto pubblico principalmente aereo e ferroviario.

Una volta attivate cautele e piani di emergenza (in realtà mai sottoposti ad un reale collaudo e quindi di affidabilità meramente teorica), chi è alla *cloche* dei diversi Governi ha ritenuto di archiviare il problema come "risolto" e di considerare la situazione sotto controllo.

A prescindere dalle valutazioni – inevitabilmente caustiche – in merito a quello che e a come è stato fatto in proposito, è evidente che pochi hanno pensato ad

una minaccia "laica" che potesse pregiudicare il patrimonio informativo di entità pubbliche e private.

Si sono dedicate risorse (spesso poco qualificate o comunque sfacciatamente autoreferenziate) per affrontare una prevedibile insidia "militarizzata" schierata con un nitido percorso che parte dall'esterno e converge verso il target.

Il "nuovo" nemico è stato immaginato con fattezze molto simili al "vecchio". Soldato e agente segreto, poco importa quale ne sia il ruolo, è immaginato come qualcuno che arriva da lontano e che si avvale di modalità di condotta assolutamente prevedibili. E invece no.

Chi combatte nelle trincee digitali e chi setaccia il tessuto connettivo telematico a caccia di informazioni e notizie sempre più sovente è il *quisque de populo* che vive in mezzo a noi e magari siede alla scrivania accanto.

Assange è l'incarnazione del collettore di mille e poi mille fonti celate dietro identità anonime e impercettibili: le nuove spie non hanno *trench* con il bavero alzato, occhiali neri e barbe finte, ma vestono e si muovono con quella sobrietà che allontanerebbe i sospetti anche dei più malfidati.

Le informazioni riservate non conoscono più casseforti pronte a custodirle, ma confidano sulla robustezza dei sistemi di controllo degli accessi e di protezione crittografiche: qualunque dossier corposo e di difficile consultazione/utilizzo si è trasformato in un file di dimensioni infinitesimali e di fruizione immediata anche per i meno esperti.

Chi vuol sapere deve solo conoscere la strada che porta ai dischi e alle *directory* che contengono il tesoro che si sta cercando. Poi basta una chiavetta Usb oppure una mail a portata di mano: in un attimo documentazione oggettivamente ad elevata criticità – per i temi trattati o per i soggetti coinvolti – può scivolare via per finire nelle mani sbagliate del committente senza scrupoli che ne ha domandato copia.

Ad accelerare questo processo sono stati la progressiva maggiore economicità e la crescente facilità d'uso degli strumenti tecnologici, la comodità e l'anonimato delle comunicazioni in Rete, la velocità di trasporto dei dati in ogni angolo del mondo, la semplicità dell'occultamento delle prove del misfatto, le opportunità di *dribbling* dei controlli più severi.

Chiunque abbia un pezzo di carta o un file "compromettente" può vendicare le

amarezze la cui deglutizione è quotidiana sul posto di lavoro: un allegato in posta elettronica può essere più devastante di qualsivoglia missile e fa la fortuna di chi trova preconfezionato un prodotto che un tempo richiedeva mesi di ricerche, approfondimenti e verifiche.

L'*intelligence* – in quest'epoca – è divenuta un rituale di selezione e filtro di cose che arrivano da sole o poco costa sollecitare, e fa fiasco soltanto se l'operatore non ha reale conoscenza della galassia *hi-tech* e cade nelle inevitabili trappole della controinformazione sempre in agguato.

Se un tempo la ricerca informativa era a supporto del confronto armato, oggi ne è l'essenza. La postazione con tastiera e schermo è il *cockpit* di un astratto velivolo da combattimento con cui – già al decollo – si può far tremare l'avversario. Perché l'informazione non va nemmeno utilizzata, ma è sufficiente dichiararne il possesso. E come al tavolo verde è ammesso pure barare…

L'INSECURITY QUOTIDIANA

Lasciando i campi di battaglia convenzionali, ci si accorge dei bombardamenti virtuali le cui esplosioni sono sempre più vicine a ciascuno di noi.

Il nostro rapporto di computer-dipendenza cresce in maniera esponenziale: qualunque azione quotidiana è legata con una sorta di invisibile cordone ombelicale ad un sistema informatico, ad una rete di comunicazione, a Internet. L'operazione bancaria, la telefonata con il cellulare, la cartella clinica informatizzata, il controllo delle centrali energetiche, la circolazione dei treni, il traffico aereo: potremmo mescolare mille ingredienti diversi e il *cocktail* sarebbe comunque venefico.

In giro per il mondo i problemi connessi alla "*insecurity*" tecnologica hanno al più regalato l'opportunità di convegni e tavole rotonde. Al limite hanno saputo ispirare la costituzione di qualche gruppo di lavoro, fatto di raccomandati o *yes-men* e mai chiamato a render conto della situazione o delle prospettive.

La deflagrazione ora dovrebbe aver risvegliato la collettività e i "*decision makers*" dal torpore, come accadeva al vecchio suocero di Luciano De Crescenzo quando – nel film "Così parlò Bellavista" – sentiva pronunciare la parola "milione". Si destava dalla sonnolenza costante, sbarrava gli occhi memore di un mancato prestito di denaro, sospirava "*Nu milione, all'anema do Pat'eterno*" e si assopiva nuovamente.

Ogni giorno i numeri parlano chiaro e diventa sempre più difficile nascondersi dietro al solito dito. Si è davvero prossimi al "*redde rationem*" e l'atmosfera apoca-

littica è quella che meglio si addice al momento storico. Chi doveva difendere quei sistemi informatici perché ha fallito la sua missione? Era incapace, incosciente, superficiale? E che dire della "*culpa in eligendo*" e "*in vigilando*" del management che gli ha irresponsabilmente affidato quel compito?

Le vittime non sono le migliaia di aziende o di enti governativi cui gli *hackers* hanno strappato il cuore in un moderno rito tribale, ma i milioni di persone che hanno a che fare con quelle organizzazioni finite k.o. sul ring telematico.

Chi prima aveva sospetti o timori che i propri dati non fossero ben custoditi e che le operazioni informatiche più delicate nella gestione delle infrastrutture critiche (finanza, sanità, energia, trasporti, comunicazioni) non godessero della necessaria impermeabilità, adesso ha qualche elemento in più per fare valutazioni ragionevolmente oggettive. Non deve spaventare quel che è successo, ma terrorizzare quel che non sappiamo essere accaduto.

UN'ULTIMA CONSIDERAZIONE

Il quadro non è confortante. Lo è ancor meno se a tracciarlo è qualcuno che ha passato un quarto di secolo ad occuparsi di queste cose a tempo pieno. Non c'è più tempo da perdere. Si deve intervenire subito. E bene. Basta con gruppi di lavoro interministeriali, composti nel rispetto di quote e di posizioni gerarchiche. Basta con la lentezza del burosauro il cui incedere contrasta con la fulmineità di un pianeta a banda larga.

POST SCRIPTUM: LA GUERRA DELL'INFORMAZIONE SBARCA IN POLITICA

Dopo aver parlato di orizzonti internazionali e di conflitti planetari, viene il legittimo dubbio di aver dimenticato qualcosa. E pure qualcosa di non trascurabile, nemmeno così distante, persino sotto gli occhi di tutti.

Le recenti consultazioni elettorali italiane – le politiche prima, le amministrative poi – hanno saputo dare l'opportunità di assegnare un non trascurabile valore ponderale a Internet e all'*information warfare*.

La Rete ha palesato il suo ruolo di strumento per sondare le opinioni, maturare il consenso, indirizzare la gente, catalizzare masse eterogenee con il solo collante dell'epidemica insoddisfazione.

Il fenomeno Movimento Cinque Stelle è stato la dimostrazione della rapidità sia nell'aggregare, sia la comprova della volatilità di quanto accade nella dimen-

sione virtuale e negli immediati dintorni. Internet si è rivelato uno strumento di incredibile efficacia e per un attimo ha fatto balenare il sogno di una rivoluzionaria democrazia digitale.

Si è immaginata la politica 2.0, quella "partecipativa" al pari del coevo web in cui tutti possono generare contenuti e prospettare idee, rinunciando con soddisfazione allo stantio ruolo passivo di semplici spettatori.

Ma proprio l'ubriacatura di presunta sovranità popolare ha segnato un primo doloroso declino di questa forma di "governo".

Lo stesso palco virtuale o l'ipotetica assemblea web-popolare sono stati il teatro di poco edificanti manifestazioni di pensiero, facendo sfociare in situazioni che hanno evocato i satirici spot della Casa della Libertà interpretati da Corrado Guzzanti una quindicina di anni fa in un programma serale di Serena Dandini.

Tutti liberi di fare e dire qualunque cosa: un gratuito esercizio di turpiloquio ha sommerso blog e forum, annacquando i legittimi entusiasmi di chi sperava nel cambiamento.

I promotori dell'iniziativa – coraggiosi pionieri di una *nouvelle vague* del cimento elettorale – hanno saputo generare dal nulla e con modeste risorse qualcosa di epocale, ma in breve tempo si sono trovati nelle condizioni di Aladino alle prese con il Genio della Lampada.

Dopo alcune *performance* spettacolari e la sensazione di una sorta di rivoluzione copernicana, i fatti hanno mostrato una certa difficoltà a mantenere il controllo della situazione e del medesimo strumento.

L'entusiasmo dei risultati ottenuti e una sopravvalutazione della stabilità del mezzo impiegato hanno portato a dimenticare l'effimero di Internet e di quel che vi gira attorno.

La Rete ha due fondamentali caratteristiche.

In primo luogo è anarchica per sua natura e per le severe regole non scritte che ne hanno consentito lo sviluppo.

In secundis è un organismo vivente, così come ben sa chi si ostina a scrivere Internet con la "I" maiuscola a dispetto delle improprie classificazioni dei più recenti dizionari. E come forma di vita dall'oscura biologia va osservata con attenzione e

studiata con umiltà. La Rete non ha padroni. Non le piacciono nemmeno quelli simpatici e questo non va dimenticato. Mai.

Se la lezione sulla *cyberwar* può sembrare rinviabile, quella sulla guerra dell'informazione non la si deve marinare.

Perché non è il conflitto del domani, ma una condizione di belligeranza che ci accompagna silente da anni tormentando gli equilibri politici ed economici e cambiando il granitico corso della storia nella totale incoscienza/indifferenza dei potenziali interessati.

STUDI & RICERCHE

Gli shock che si susseguono dai tempi del crollo del Muro di Berlino integrano ormai gli estremi di un cambiamento complesso, che è destinato a proseguire ed i cui approdi non sono ancora noti.

Molti consolidati punti di riferimento stanno venendo meno, ma alcune costanti di fondo di questa fase convulsa risultano evidenti, in particolare l'adesione americana al paradigma dello *smart power* ed il confronto che oppone gli Stati Uniti alle potenze emergenti.

La novità maggiore del 2013 non è rappresentata tanto dall'inceppamento della Primavera Araba, al quale non è stata estranea un'azione di contenimento guidata dall'Arabia Saudita, quanto dall'annunciata fine della stimolazione monetaria impressa dalla Federal Reserve all'economia mondiale.

Una stretta potrebbe in effetti essere ormai alle porte e concorrere all'arresto del processo di ridistribuzione della ricchezza e della potenza politica in atto da almeno un quarto di secolo.

Per l'Europa, ciò implica un dilemma cruciale: seguire Washington su questa strada ed alzare i tassi d'interesse dell'Eurozona, rischiando tuttavia di spingere verso il default alcuni Stati membri dell'Unione, oppure svalutare l'euro, cambiando di fatto i compiti istituzionali della BCE.

Per adesso, l'Istituto di emissione europeo sembra favorire la seconda opzione. Ma non è detto che non sia indotto in futuro a cambiare atteggiamento. La scelta è in effetti della massima importanza, così come quella che concerne l'accettazione del progetto della Partnership Commerciale e degli Investimenti Transatlantica, in realtà fonte per l'Europa tanto di opportunità quanto di rischi.

Il nostro Continente potrebbe infatti divenire parte attiva di un processo di rilancio dell'Occidente, ma al prezzo della rinuncia alle proprie ambizioni di autonomia.

Come di consueto, *Nomos & Khaos* passa in rassegna gli scenari che si presentano davanti ai decisori politici ed ai *concerned citizens* europei, ponendo in risalto le connessioni esistenti tra la gestione dei fenomeni economici e le loro ripercussioni geopolitiche.

ISBN 978-88-6140-145-7

DISTRIBUZIONE AGRA EDITRICE

€ 20,00 IVA inclusa

Nomos & Khaos

Rapporto Nomisma 2013-2014
sulle prospettive economico-strategiche

Osservatorio Scenari Strategici e di Sicurezza

a cura di

GIUSEPPE CUCCHI · GERMANO DOTTORI

con i contributi di

K.F. ALLAM · ARESU · CARACCIOLO · CUCINO
DE CASTRO E DI PASQUALE · DE NARDIS · FABBRI · LOMBARDI
LUKYANOV · MAGNANI · MAGNATTI · MAGRI · MAINOLDI
MUSCARÀ · NONES E MARRONE · PASTRELLO
PELANDA · RAPETTO · SILVESTRI · SPECK
TABARELLI · TANTAZZI · VALENTE · VITALI

Nomisma LIBRI PER L'ECONOMIA

Web democrazia ? Fine di una illusione?

Umberto RAPETTO

Ho sognato che sul Palazzo della Civiltà, all'EUR, era cambiata la storica scritta. Niente più "Un popolo di poeti di artisti di eroi…" ma l'immortale frase della buonanima di Riccardo Pazzaglia: "Il livello è basso". Dietro di me qualcuno parlava di web-democrazia. E' bastato un istante. Ho immediatamente dato ragione all'indimenticabile personaggio dello show televisivo "Quelli della notte…".
Quando mi sono svegliato, ho preso la Treccani e ho cercato la definizione di democrazia, leggendo testualmente che trattasi di "forma di governo che si basa sulla sovranità popolare e garantisce a ogni cittadino la partecipazione in piena uguaglianza all'esercizio del potere pubblico". E così mi sono chiesto cosa c'entrasse il web.

IL WEB GUARITORE DI TUTTI I MALI

Sfogliando un quotidiano ho trovato la risposta. I principali personaggi politici odierni (conoscitori dell'universo tecnologico al pari di un lettore di "Strano, ma vero" delle pagine de "La Settimana Enigmistica", nonostante l'ostentata appartenenza alla generazione dei nativi digitali) identificano nel "web" la panacea per l'inguaribile paziente Italia.
Scopro così che la sovranità popolare della definizione precedente è sparita, come pure la piena uguaglianza nell'esercizio del potere pubblico. E' sopravvissuta (e fraintesa) solo una non meglio identificata sedicente "partecipazione".
Pur cresciuto in contesti coercitivi (collegio, Nunziatella, Accademia e poi trent'anni di carriera militare), e forse proprio per aver saggiato sulla mia pelle la gratuita imposizione, ho maturato la serena convinzione che la democrazia si traducesse nel poter dire, nel farsi sentire, nell'essere ascoltati, nel prender parte alle decisioni.
Internet, in cui non mi sono imbattuto casualmente e che non ho frequentato solo per essere alla moda, è senza dubbio uno strumento che può soddisfare alcuni degli appena indicati requisiti.
Il "poter dire" non manca. La maggior parte dei frequentatori addirittura abusa di quella che non è democrazia ma semplice libertà di espressione.
Il "farsi sentire" dipende da timbro e volume di ciascuno, non affidati alla potenza delle corde vocali quanto piuttosto alla capacità che il singolo ha di trovare un seguito (poco importa da chi composto e perché).
La sonorità nello scenario del web 2.0 (quello "partecipativo", quello dei social network) è portentosa perché eco, rimbombo, propagazione ed altri fenomeni acustici consentono una diffusione potenzialmente sconfinata. Retweet e condivisioni riescono a far arrivare lontano e far galleggiare nello spazio dichiarazioni e opinioni, molto più di quanto non potesse fare la normale atmosfera. E' cambiato il "fino a dove" e soprattutto "per quanto tempo". Già, la durata. Una frase, specie se improvvida o maldestra, può diventare immortale grazie alla capacità di Internet di perpetuare qualsiasi contenuto.
Ma a dispetto di una così efficace cassa armonica, la totalità dei netizen (crasi anglofona di cittadini, citizen, della rete, net) non si risparmia nel parlare senza trovare l'auspicato riscontro.

Tsunami di soliloqui si infrangono contro gli scogli della più totale indifferenza. Chi scrive, "posta", "twitta", pubblica qualsivoglia genere di contenuto è animato dalla giusta convinzione di trovarsi al centro di una gremita agorà. Il tizio, però, non fa i conti con la non trascurabile circostanza che tutti stanno blaterando contemporaneamente senza che nessuno abbia modo, tempo e voglia di ascoltare.
Il miraggio della democrazia sul web si infrange qui. E il quisque de populo che non riesce ad essere ascoltato dai presunti "amici" e "follower" (identificati come suo attento e disciplinato pubblico) è ovvio che non raggiunge chi potrebbe fare di idee, suggerimenti e contributi la base di qualcosa di buono per l'intera comunità.
Se questo è il destino dei tanti, forse troppi, ululatori alla luna, chi può mai lontanamente pensare di partecipare alle decisioni che riguardano il futuro della collettività di appartenenza?

L'OSSIMORO DI UNA DEMOCRAZIA CHE ESCLUDE

Questo genere di partecipazione, che forse soddisfa l'enunciato di Giorgio Gaber e può quindi costituire una importante libertà, certo non è democrazia.
Il fatto che la voce del cittadino non giunga a chi siede nell'Olimpo è un problema poco considerato, così come sottovalutati sono i gap culturali, tecnici ed economici che impediscono alla globalità del "demos" di tentare anche il più banale dei contatti con la "cratia".
Tra le più pervicaci idiozie che serbo in seno, c'è l'ossessionante pensiero che una vera democrazia è quella che non lascia nessuno indietro.
A guardar bene, Internet lascia indietro persino chi non si tiene semplicemente aggiornato. Figuriamoci qual è la sorte di chi non ha mai avuto modo di avvicinarsi per ragioni generazionali, per abissali lacune di conoscenza, per problemi economici che non gli permettono l'acquisto di uno strumento tecnologico, oppure per banali difficoltà tecniche di connessione. Questa vastissima platea incarna i nuovi "paria".
Alla dichiarata e strombazzata discriminazione anagrafica (che esclude i più grandi da qualsivoglia ruolo, a dispetto di esperienza e competenza), si aggiunge quella "telematica".
Se non hai un tablet, uno smartphone o qualunque altra diavoleria elettronica – tuonano le minacce e le promesse dei politicanti – non potrai più dialogare con la Pubblica Amministrazione. Non bastavano i call center con i loro "reclusi" a complicare la vita del cittadino alle prese con la burocrazia: adesso occorrerà il "PIN unico" che a detta del titolare del dicastero competente entro 1000 giorni risolverà ogni problema.
Fortunatamente certe dichiarazioni non trovano mai concreta realizzazione, ma certo – con simili orizzonti – è davvero impegnativo discettare di "web-democracy". Chi ritiene caustico questo commento e scalda i muscoli per una cocente smentita, sappia che non provo alcun turbamento e resto avvinto alla mia posizione come l'edera di Nilla Pizzi. Il 16 dicembre del 2000, un mio articolo sulla prima pagina del quotidiano Il Messaggero, mandò su tutte le furie l'allora potentissimo Ministro, temuto riformatore dell'immutabile ed immutata res publica, ancora oggi in auge come gran commis di Serie A. Titolo, "Carta di identità multiuso". Occhiello: "Sarà tessera sanitaria e bancomat. Ma chissà quando."

Qualcuno oggi parlerebbe di “gufi”. Non credo di aver “tirato alcuna sfiga” a chicchessia, ma a quattordici anni di distanza ancora aspetto di veder contraddette certe argomentate critiche.
Palesata una possente vaccinazione al folgorante “effetto annuncio”, mi sento ancora arzillo per non convenire a proposito di democrazia tramite Internet.
Ho timore che, in una società in cui gli anziani vengono esclusi dalla possibilità di “esserci” e dove gli emuli del Ku Klux Klan non indossano buffi cappucci bianchi ma sono armati di tecnologie per portare a termine la ghettizzazione, la tirannide ricalchi schemi di orwelliana memoria.
Pensare che il ricorso al web, tanto gradito ai teen-ager, sia una prova tangibile di modernità o di apertura è indizio, grave, di due possibilità: visione infantile dell’universo o pericolosa malafede.

IL SOTTILE REGIME A TRE “W”

In questi ultimi anni è stata dimostrata la potenza di Internet come strumento di catalizzazione e di aggregazione e, in ambito politico, come efficace macchina elettorale.
La socializzazione è stata travisata in impegno sociale e qualcuno ha erroneamente ritenuto che il tessuto connettivo telematico potesse diventare il sistema nervoso della democrazia. Qualcun altro, meno esperto del precedente, ha cominciato a temere il peggio e si è adeguato spostando la propria comunicazione su Twitter e su altre piattaforme endemiche.
I risultati si sono visti. E forse i “migliori” ancora si devono vedere.
Qualche migliaio di ultras del web, che partecipano a primarie di ogni genere, decidono per la totalità di persone che riconoscono “del buono” in un movimento che può cambiare le cose. Quelli che non sono d’accordo – a dispetto della democrazia digitale – o tacciono, o sanno che il loro sguardo è destinato ad incrociare un inesorabile cartellino rosso che decreta l’immediata espulsione.
D’altronde viviamo l’Eldorado dell’astensionismo. E’ catartica la circostanza che quei pochi che esprimono la loro opinione debbano sancire il destino della collettività.
E la volontà di una manciata di persone traccia la rotta salvo che non collimi con quella di un Vate o guru al vertice dell’aggregazione in cui come in certi Consigli di Amministrazione il voto del “capo” è prevalente e decisivo.
Sul ring telematico si è addirittura spostato il confronto tra leader di schieramenti in contesa.
Post e tweet sono i dardi con cui si cerca di trafiggere l’avversario. Memori della sintesi di un immortale “Vedi, Vidi, Vici”, molti hanno cominciato a ritenere che 140 caratteri di messaggistica istantanea possono segnare la storia. E possono farlo con la garanzia che la laconica comunicazione possa essere stata fraintesa e come tale smentita con la medesima fulmineità con cui aveva preso forma.
La libertà di parola e di critica, garantita a chiunque (salvo imbattersi in non piacevoli vicissitudini giudiziarie e rapidamente pentirsi di aver ecceduto nelle proprie manifestazioni di pensiero), in realtà non ha grandi ripercussioni in termini pratici, tali da far sentire il contributo dei tantissimi singoli che avrebbero potuto essere utili.
Il cittadino è libero di sbeffeggiare il potente, ma non ha alcuna possibilità di “partecipare” ad un ipotetico governo collettivo o “democratico”. Iniquità o situazioni presunte tali non vengono fermate dalla web-democrazia ma sono soltanto l’innesco di una straordinaria atmosfera goliardica che incarna

l'impossibilità di cambiare le cose. Lo sdegno e l'incredulità di una sentenza d'appello che capovolge un esito di primo grado trovano spazio su Twitter, dove si scopre che la Rete è il palco di un divertentissimo show comico ma certo non somiglia affatto ad una delle Camere parlamentari.
Ma se si vuol dare ragione a chi sostiene che tutti possono "twittare" o "whatsappare" (Dio perdoni questi biascicati virtuosismi etimologici), si fa presto a credere che tutti sono eguali. Ci vuole poco a intravedere la sospirata democrazia.
Il passo è breve e inebria istantaneamente l'ormai ritrito "uno vale uno", principio che sarebbe meraviglioso se non negasse d'un colpo qualunque meritocrazia.

WEB-DEMOCRAZIA, E-GOVERNMENT, TRASPARENZA

Chi parla – a sproposito – di web-democrazia la confonde con due sue componenti: la trasparenza garantita dell'architettura hardware e software (che permette a chiunque di vedere, tracciare e conoscere ogni singolo atto amministrativo o politico) e il cosiddetto e-government (che dovrebbe realizzare una gestione della res publica con criteri di efficienza che solo stakanovisti sistemi informatici sono in grado di concretizzare).
Lo stato di arretratezza tecnologica nazionale – a dispetto di alcune straordinarie eccellenze sul territorio che basterebbe clonare per risolvere ogni problema – non permetterebbe nemmeno di affrontare l'argomento. Ma la politica, condotta con la stessa nonchalance con cui si imbastiscono discorsi planetari al tavolino del bar con i più improbabili interlocutori, plaude a quello che Tim O'Reilly (che ha tenuto a battesimo il web 2.0) chiama "soluzionismo". Tale corrente di pensiero lieve ritiene che i problemi di un Paese possano essere risolti con una "App", qualche sensore e un immancabile sistema di feedback.
La realtà, duole constatarlo, è molto lontana.
La democrazia non si esercita con il numero di "selfie" estasiati di chi si accontenta di poco, o compiacendosi del volume di "like" raggiunto su un social network, oppure guardando con soddisfazione il numero di rimbalzi di un più o meno sconclusionato "tweet".
La trasparenza – come la fiducia per una storica azienda casearia – è una cosa seria. E scomoda. Lo hanno dimostrato mancate dirette web di eventi politici importanti, lo hanno confermato sondaggi telematici annullati per presunti attacchi di pirati informatici con il pesante sospetto che fosse accaduto altro. Lo continuano a testimoniare certe procedure di mera facciata.
Recentemente il Governo ha aperto la designazione al ruolo di Direttore dell'Agenzia per l'Italia Digitale, chiedendo candidature via Internet a chi ritenesse di avere le carte in regola. Tutto alla luce del sole, al punto di ottenere 150 curricula da personaggi più o meno illustri, molti dei quali non avevano mai avuto bisogno di piegarsi alle Forche caudine di compilare un CV in formato europeo. L'elenco dei nomi finisce in Rete e sembra che davvero inizi un nuovo corso. Tutti si aspettano di vedere online i percorsi di studio, le esperienze professionali e le carriere di chi si è messo in competizione. Niente affatto.
Una short-list dei profili più interessanti? Nemmeno quello. Una graduatoria di merito, nonostante i mai definiti criteri di valutazione e la mai comunicata "giuria"? Figuriamoci.

La scelta, in ossequio alle quote rosa, ricade su una donna che su Twitter cinguetta con il nickname "@la_pippi" e il cui magro excursus è rimpolpato (come la stampa non ha esitato a sottolineare) dalla vicinanza al PD.
Sullo sfondo, come in una pubblicità storica di un bagnoschiuma, un cavallo che corre… Ma stavolta è Incitatus, il destriero di Caligola.
E-Government? Absit iniuria verbis… Solo un suggerimento. Accaparrarsi una copia di "The Automated State" scritto da Robert MacBride nel 1967.
MacBride, quasi cinquant'anni fa, vedeva i sistemi informatici in grado di produrre "una burocrazia di capacità quasi celeste", capace di "discernere e definire le relazioni in un modo che nessun modello umano potrebbe mai sperare di fare". Non sapeva che dalle nostre parti saremmo stati capaci di "cartelle pazze" e mille altre prodezze…

SICUREZZA E AFFIDABILITA' DI UN MODELLO DI WEB-DEMOCRAZIA

La democrazia è libertà di espressione di voto. E non manca chi sogna consultazioni via Internet, magari prendendo spunto da chi già pratica questo sistema con autoreferenziato successo.
Quelli che "la vita è tutto un PIN", Frassica docet, probabilmente disconoscono le dinamiche di connessione alla Rete e ancora sono convinti che esista un anonimato non distante da quello del tradizionale segreto dell'urna.
I sistemi finora utilizzati per elezioni e selezioni online prevedevano una serie di fasi tecniche mirate a garantire il voto solo a chi fosse registrato in uno specifico elenco (le liste degli aventi diritto) e ad assicurare che la stessa persona potesse votare più di una volta. Perfetto. O, meglio, quasi perfetto.
Se la preferenza è abbinata informaticamente al codice di autenticazione dell'elettore, si saprà "chi" ha votato "cosa".
Se quel soggetto adopera un certo computer ed è riconoscibile per il suo numero IP (identificativo indispensabile per stabilire la connessione), un domani potrebbe essere "bannato" (escluso dalla possibilità di collegarsi) con semplici filtri ed escluso dal partecipare.
Si potrebbe andare oltre. Ma non ce n'è bisogno. O, forse, molto più semplicemente non c'è alcun interesse a saperlo. E se qualcuno ne avesse un briciolo, può trovare interessante "The Net Delusion" di Evgeny Morozov, pubblicato nel 2011.
La dittatura dei dati avanza e nessuno se ne preoccupa. Perché questa è la strada della web-democracy.
O almeno così l'hanno raccontata a chi con l'inglese ha poca confidenza. "A terrible history", ipse dixit.

Umberto Rapetto, generale della Guardia di Finanza in congedo, fondatore e poi comandante per 11 anni del GAT Nucleo Speciale Frodi Telematiche, è stato il Consigliere strategico di Franco Bernabè e poi Group Senior Vice President di Telecom Italia. Docente universitario, giornalista (è una delle firme de Il Sole 24 ORE, Il Secolo XIX, OGGI, Il Fatto quotidiano), autore di oltre 50 libri, antropologo digitale, è l'ufficiale che ha catturato e fatto condannare gli hacker entrati nel Pentagono, che ha scoperto la miliardaria frode all'Erario delle slot machine, che ha recuperato i dati della Costa Concordia e ha permesso l'avvio delle attività investigatiove e processuali sul naufragio all'isola del Giglio.
Adesso fa lo "startupper" e guida HKAO Human Knowledge As Opportunity srl, think tank operante nel settore della sicurezza tecnologica, della protezione dei dati, della business intelligence e del controspionaggio industriale.