Cybersecurity e vulnerabilità del fattore umano

Valentina De Vito, Ester Macrì, Anna Pettini, Giuliano Resce - 17/12/2018 [papers]

Abstract

In recent times decision makers have devoted a lot of attention to cyber threats since cybersecurity is a prerequisite for the good functioning of an increasing number of economic and non-economic activities. The effectiveness of legislative and control measures, however, depends on individual behaviours. In the absence of individual awareness and knowledge, increasing spaces for vulnerability open up. This paper aims to deepen the research on individual behaviours in the field of cybersecurity, in the awareness that the research does not yet devote the necessary attention to these phenomena. The results show a widespread vulnerability, even among more educated people who are supposed to be less likely fake news believers.

Cybersicurezza | *A dispetto dei luoghi comuni, cyber attacchi e furti di dati colpiscono molto anche i più giovani e i più istruiti. L'intervento pubblico è sempre più necessario.* Il ***Global Risks Report 2018*** indica che i cyber attacchi e i furti di dati occupano rispettivamente il terzo ed il quarto posto nella classifica 2018 sui rischi globali in termini di probabilità, dopo gli eventi climatici estremi ed i disastri naturali.[1] Un recente sondaggio ha stimato che circa 978 milioni di persone sono state colpite dalla criminalità informatica nel 2017.[2] Per dare un'idea della dimensione delle perdite economiche, il ***CEO*** e fondatore della società russa di cyber sicurezza Kaspersky Lab, Eugene Kaspersky, ha commentato che ogni anno il crimine informatico costa al mondo l'equivalente di "tredici volte la spesa globale per le missioni spaziali",[3] una cifra che si aggira intorno ai 600 miliardi di dollari (0,8% del PIL mondiale), stando alle stime pubblicate nel febbraio 2018 da McAfee e il Center for Strategic and International Studies. La rapida evoluzione delle tecnologie ha avuto un profondo impatto sulla società e sull'economia: accanto al miglioramento della produttività delle imprese e alla creazione di nuova occupazione - in 27 Paesi europei tra il 1999 e 2010 la digitalizzazione ha prodotto 11,6 milioni di posti di lavoro aggiuntivi[4] -, la dipendenza dalle ICTs, per la quasi totalità delle attività nelle economie avanzate, ha anche esposto le attività produttive a crescenti minacce cibernetiche. La cyber-sicurezza è un argomento complesso e la sua comprensione richiede conoscenze e competenze provenienti da varie discipline. Sebbene, chiaramente, le misure tecniche siano un elemento fondamentale, la cyber-sicurezza sta ponendo sfide tanto di natura tecnica quanto non tecnica.[5] I problemi relativi alla cyber-sicurezza sorgono a causa dell'inevitabile presenza di vulnerabilità nelle tecnologie, dell'esistenza di attori malevoli pronti ad approfittarne e della scarsa consapevolezza delle ripercussioni e dei rischi in cui si incorre attraverso quei comportamenti che prevalentemente, ma non unicamente, derivano da una conoscenza solo superficiale dei dispositivi che usiamo. Si tratta dunque di una questione che riguarda ormai ugualmente singoli individui, realtà aziendali, ma anche gli Stati nel loro intero poiché le minacce informatiche minano le identità delle persone, la tenuta economica delle aziende e la tenuta democratica dei Paesi,[6] come ha dimostrato in modo eclatante il recente caso della società Cambridge Analytica. [7] Guardando al volume di produzione giuridica, anche internazionale, e alla mole di organismi predisposti alla sicurezza dei cittadini e delle imprese, [8] pare oggi ovvio che i decision-makers, sia di ambito pubblico che privato, abbiano presente l'importanza della sicurezza cibernetica. Lo stesso non può dirsi per i cittadini che, a livello individuale, mostrano una cultura digitale largamente insufficiente. Per il singolo individuo, cybersicurezza vuol dire sicurezza dei propri dati personali, ma anche difendersi dalle notizie false che proliferano sul *web*, che diviene una delle variabili che indicano il grado di esposizione al rischio informatico. Dai risultati di uno studio recente

pubblicato su *Social Science* sulla diffusione di notizie vere e false in rete, [9] emerge infatti che lo strumento cibernetico tende a favorire la viralità delle informazioni false. Alla luce di ciò, è quindi imprescindibile sviluppare consapevolezza, capacità e strumenti per tutelare la nostra presenza nello spazio cibernetico. La ricerca sta rivolgendo crescente attenzione al ruolo che il fattore umano gioca nella sicurezza cibernetica, in particolar modo laddove le tecnologie preposte hanno fallito nel proteggere le aziende dai cyber attacchi.[10] E' infatti la composizione di fattori organizzativi, ambientali e comportamentali che determina la misura in cui i lavoratori aderiscono alle pratiche di cyber sicurezza (Herath e Rao 2009b). Alcuni studi hanno esplorato il modo in cui i diversi tratti della personalità possono impattare sull'adozione o meno di procedure di cyber sicurezza,[11] o la discrepanza tra le intenzioni di comportamento ed il comportamento effettivo, che va a minare la possibilità di predire condotte conformi (Shropshire *et al.* 2015). La ricerca sta quindi rivolgendo alcuni sforzi in una direzione sempre più necessaria ma, tuttavia, non ancora debitamente esplorata. Nel solco della ricerca sui comportamenti individuali ad uso delle pratiche di cybersicurezza, ci siamo chiesti se esista una correlazione tra le fonti di informazione di cui le persone fanno uso ed il sussistere di comportamenti digitali che le rendano più vulnerabili. L'atteggiamento più comune, nella generalità degli individui, è prestare fiducia alle informazioni generate nell'ambiente a loro contiguo (definito "pregiudizio della verità" da Bond & DePaulo, 2006). Questo, si è detto in passato, consente alle persone di gestire efficacemente la grande quantità di informazioni ricevute ogni giorno (Gilbert, 1991) al fine di evitare di dover svolgere valutazioni sistematiche per giudicare la legittimità ed affidabilità di ciascuna informazione ricevuta. Nello spazio cibernetico, la propensione alla fiducia varia in base alle conoscenze o convinzioni individuali sui potenziali rischi della comunicazione in rete e della tecnologia in generale (Corritore, Kracher, e Wiedenbeck, 2003; Wang e Emurian, 2005), ma in generale l'uso della rete si presta a dare agli utenti una percezione di anonimato che li induce a rivelare maggiori informazioni di sé rispetto a quante ne rivelerebbero *face to face* (Joinson e Paine, 2007). Per questo motivo si è scelto di osservare attraverso quali piattaforme si informassero gli intervistati, ed il grado di fiducia da essi accordato alle diverse testate. Al contempo, sono stati sondati il livello di conoscenza dei più comuni crimini informatici ed il comportamento digitale dei partecipanti. In particolare, è stato rilevato di quali cyber crimini fossero state vittime gli intervistati al fine di testare il grado di vulnerabilità effettiva. La vulnerabilità potenziale è stata, invece, controllata sulla base delle risposte ai quesiti su variabili quali la frequenza nell'aggiornamento delle password dei più comuni servizi *online* (posta elettronica, *home-banking,*…), l'utilizzo delle *app* più diffuse, la motivazione soggiacente al *download* delle *app*, la scelta dell'utilizzo del *social login*, la disponibilità a fornire la propria posizione nell'utilizzo di dispositivi dotati di GPS o di *app* per le quali il GPS è richiesto, la scelta del sistema operativo e del *browser* utilizzati con maggior frequenza. Infine, è stato esaminato anche livello di conoscenza della cybersicurezza a livello macro. **2. I dati** La ricerca è stata condotta tramite un questionario standardizzato costruito *ad hoc* per l'indagine, utilizzando il *web* come canale di somministrazione[12]. Nello specifico, il questionario è stato somministrato ai partecipanti tramite ***Facebook***, in quanto si tratta del *social network* più diffuso in Italia. [13] Dato l'argomento di indagine, la ricerca non poteva che essere condotta *online*, in modo da andare ad intercettare gli utenti privilegiati del web e quindi più interessati al tema. Per il campionamento si è quindi proceduto utilizzando un metodo non probabilistico, detto "di convenienza", proprio perché prevede la selezione del campione in base a criteri di comodità. Se, da un lato, un campione estrapolato con questo metodo è ben diverso dai canoni classici dell'inferenza statistica, dall'altro è quello che permette di intercettare al meglio la popolazione di riferimento dell'indagine, cioè persone che utilizzano internet con frequenza e sono attive sui Social Network. Visto che la tematica dell'indagine è proprio un fenomeno che ha strettamente a che fare con la rete, la *web survey* appariva l'unica strada percorribile e perfettamente in linea con l'obiettivo della ricerca. La rilevazione *web* ha avuto inizio il 21 febbraio 2018 e si è conclusa entro quasi un mese dal suo avvio, il 18 marzo

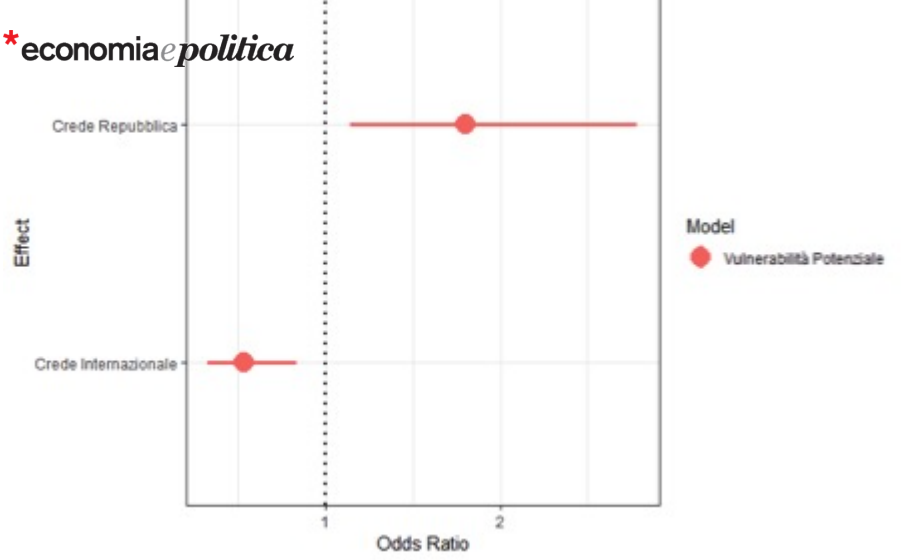
2018, con un totale di 1139 questionari compilati per intero. **2.1 I partecipanti all'indagine** Il campione ottenuto dall'indagine si è configurato come segue. Sul totale di 1139 partecipanti provenienti da tutto il territorio italiano, il 48,6% dei rispondenti è di genere maschile (n = 554) ed il 51,4% è di genere femminile (n = 585). La maggior parte dei rispondenti, ossia il 41,44%, appartiene alla fascia di età 18-24, il 21,33% alla fascia 25-29 ed il 12,20% alla fascia 30-34. Infine, un quarto dei rispondenti dichiara di avere più di 35 anni. Rispetto al titolo di studio, quasi la metà (49,78%) degli intervistati si dichiara in possesso di un diploma di istruzione superiore. Una numerosità così corposa in questo intervallo è dovuta al fatto che la maggior parte del campione appartiene alla fascia di età 18 – 24 e dunque da persone ancora troppo giovani, nella maggior parte dei casi, per aver ottenuto un titolo di studio più elevato della licenza superiore. Si fa presente, inoltre, che il test è stato somministrato anche ad una classe di circa 60 studenti al primo anno di Università e il principale canale di diffusione è stato proprio il network universitario. Pertanto, si può presupporre che il questionario abbia raggiunto molte persone attualmente iscritte ad un corso di laurea triennale. Rispettivamente il 15,89% ed il 17,38% sono quelli in possesso di laurea triennale e di laurea magistrale. Più di un decimo del campione possiede un titolo post-laurea e solo il 6,15% è in possesso di licenza media. I dati relativi all'occupazione mostrano che quasi la metà del campione è costituito da studenti. Infatti, la percentuale cumulata di studenti e studenti-lavoratori è del 49,43%. Il 38,28% degli intervistati ha un'occupazione full-time o, in minor misura, part-time. La restante parte del campione ha dichiarato di essere disoccupata, in cerca di occupazione, NEET, casalinga/o o altro. **3. Analisi dei dati** L'analisi statistica condotta per studiare l'associazione tra la vulnerabilità informatica (relativa e assoluta) e la fiducia accordata in diversa fonti di informazione quotidiana, misura l'*outcome* mediante due variabili dicotomiche:

1. Vulnerabilità Potenziale: (1) l'intervistato ha avuto almeno un comportamento potenzialmente a rischio, (0) altrimenti;
2. Vulnerabilità Effettiva: (1) essere stato oggetto di almeno un attacco e (0) altrimenti.

L'associazione tra la fiducia accordata alle diverse testate giornalistiche e la vulnerabilità potenziale e effettiva è studiata mediante delle regressioni logistiche multivariate. Al fine di mantenere solo le variabili significative nel modello finale, si procede mediante *backward stepwise selection.* Nei risultati si mostrano le determinanti della probabilità di avere una vulnerabilità potenziale e/o effettiva mediante *adjusted Odds Ratios* (aOR) con un intervallo di confidenza del 95%. In epidemiologia l'OR è la misura dell'associazione tra due fattori, per esempio tra un fattore di rischio e una malattia. Il calcolo dell'OR è dato dal confronto tra le frequenze di comparsa dell'evento nei soggetti esposti e le frequenze di comparsa dell'evento nei soggetti non esposti al fattore di rischio in studio. In questi termini, in questa analisi trattiamo la disposizione a dare fiducia a una serie di fonti informative come un fattore di rischio (o un fattore protettivo) per la vulnerabilità potenziale e effettiva. aOR =1 indica assenza di associazione tra esposizione ed evento di interesse, aOR>1 indica associazione positiva, aOR<1 indica associazione negativa. Le variabili di controllo inserite nel modello sono il genere, la classe d'età e il titolo di studio. In questo modo la forza delle associazioni mostrate nei risultati è aggiustata per queste caratteristiche individuali degli intervistati. Le analisi statistiche presentate sono eseguite con R (R Core Team, 2018). **4. Risultati 4.1 Informati da un algoritmo e disattenti** L'analisi descrittiva dei risultati mostra una forte vulnerabilità dei rispondenti a partire dai loro comportamenti digitali. La prima sfera di vulnerabilità è quella relativa all'informazione. Il 60% dei rispondenti ha dichiarato di informarsi prevalentemente attraverso i Social Media, mentre un 20% ha dichiarato di utilizzare come fonte principale di informazione i suggerimenti del browser sul proprio smartphone. Entrambi queste modalità di reperimento delle informazioni implicano per la loro stessa natura un filtro e una selezione delle notizie in base alle preferenze e al profilo dell'utente. La maggior parte dei rispondenti, perciò, ha una visione informativa della realtà selezionata da un algoritmo in

base a ciò che ha letto in passato. Ciò determina una visione parziale di ciò che accade e ha, come conseguenza, il formarsi delle c.d. *echo chambers*[14]. A questo si aggiunge che il 67,78% degli intervistati ha dichiarato di aver creduto almeno una volta ad una notizia che è stata, in seguito, smentita da fonti ufficiali. Quasi la metà di questi, ossia il 28,45%, ne ha condivisa almeno una. Rispetto al grado di fiducia accordato dal campione ad alcune delle maggiori testate di informazione, è risultato che la fonte cui è accordata maggior fiducia è l'agenzia di informazione Ansa, con il 51,10% del campione che afferma di leggervi notizie cui crede senza alcun dubbio. A seguire, ai primi posti ci sono l'Economist (37,23%), La Repubblica (34,50%), il Corriere della Sera (34,33%) e Internazionale (33,54%). Fra le varie testate di cui il campione avrebbe dovuto fornire il proprio grado di fiducia, si è scelto di introdurne due, Informare x Resistere e NewsTg24, che compaiono nella *blacklist* di Bufale.net[15], quindi etichettate come fonti dove spesso sono state pubblicate notizie false o non precise. Se, come si evince dalle tabelle, solo il 3,07% del campione crede indubbiamente a notizie lette su Informare x Resistere, ben il 25,02% ha piena fiducia in NewsTg24. Questa percentuale è più alta di quella relativa al resto delle testate suggerite nella domanda[16]. Si può facilmente ipotizzare che gli intervistati abbiano confuso NewsTg24 con SkyTg24, a conferma del fatto che una lettura veloce e disattenta, che di fatto è prevalente nella lettura su smartphone, facilita le trappole informative. **4.2 Iperconnessi e sempre tracciabili** La diffusione dei comportamenti ritenuti a rischio non si limita solo alla sfera dell'informazione. Per valutare il potenziale di rischio è stato costruito un *indice di vulnerabilità potenziale* a partire da alcuni comportamenti: tenere sempre attivo il GPS nel proprio smartphone, non cambiare la password con frequenza, connettere diversi account social tra loro, installare una APP senza prima informarsi sulla stessa. E' interessante soffermarsi su alcuni dati che emergono dalle risposte alle singole domande. Infatti, solo il 13,26% del campione, nell'installare una *app*, si preoccupa del nome della società che l'ha sviluppata. Inoltre, ben il 56,54% del nostro campione dichiara di aver optato per il *social login*, ossia aver scelto di collegare il proprio account Facebook ad altri profili, utilizzando così le stesse credenziali per l'accesso ad altri siti o *app*. Il 26,78% del campione dichiara di tenere sempre attivo il GPS nel proprio smartphone. Questo dato è sicuramente in crescita con la diffusione di nuovi strumenti di monitoraggio passi e battito cardiaco come smartwatch e fitbit a basso costo che necessitano, per funzionare, dell'attivazione costante del GPS nello smartphone. Inoltre, il 21,25% dei rispondenti si è dichiarato disposto a fornire la propria posizione a qualsiasi *app* che gli faccia ottenere lo scopo e ben il 65,76% è disposto a fornirla a Google. Questo comporta di essere sostanzialmente sempre tracciati o, comunque, tracciabili. Quello che emerge da questa prima analisi descrittiva è, dunque, che la vulnerabilità potenziale è molto diffusa, a partire dall'informazione quotidiana. Ciò trova riscontro anche nell'analisi statistica che segue. **4.3 Fiducia e vulnerabilità** In questo paragrafo si mostra l'associazione tra vulnerabilità potenziale (0 = 163, 1 = 976) e la fiducia accordata a diverse testate giornalistiche. Dopo il processo di *backward stepwise selection* restano due testate giornalistiche: La Repubblica e Internazionale. La figura 1 mostra che l'aOR è significativamente superiore a 1 per chi crede nella Repubblica. In altre parole, esiste una associazione positiva tra la fiducia ne La Repubblica e la vulnerabilità potenziale. Al contrario, l'aOR è significativamente minore di 1 per chi accorda maggior fiducia a *Internazionale*. In questo caso esiste quindi un'associazione negativa tra vulnerabilità potenziale e la fiducia nelle notizie pubblicate da Internazionale. In termini epidemiologici si direbbe che credere ne La Repubblica è un fattore di rischio, mentre credere in Internazionale ha un effetto protettivo nei confronti della vulnerabilità potenziale.

Figura 1 - adjusted Odds Ratio dell'associazione tra credere nelle diverse testate giornalistiche e vulnerabilità potenziale

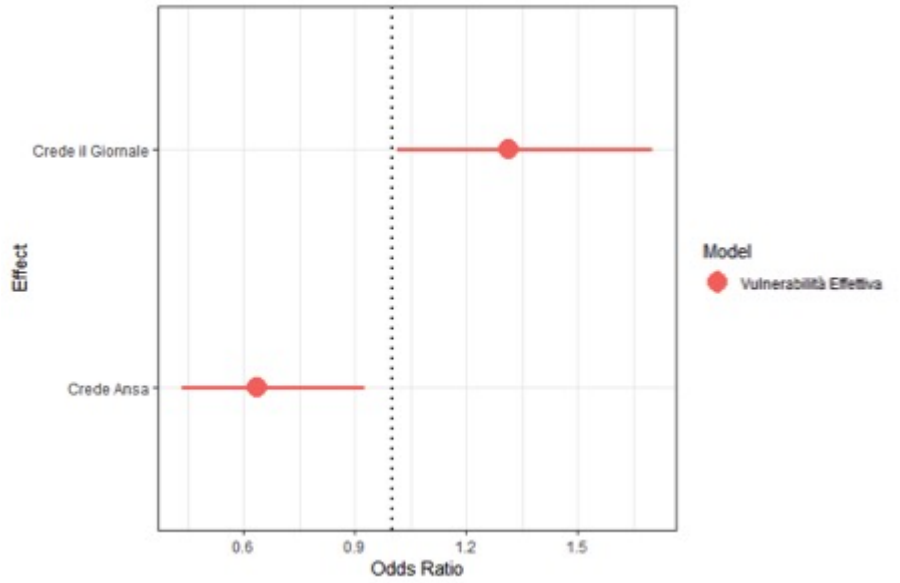


Il punto è l'aOR = probabilità di avere

vulnerabilità potenziale. Il dato, aggiustato per genere, fascia di età e titolo di studio, fornisce una misura della forza di associazione tra il credere alle diverse testate giornalistiche e la vulnerabilità potenziale. Gli estremi superiori e inferiori delle linee rappresentano rispettivamente l'*Upper* e il *Lower bound* degli intervalli di confidenza stimati al 95%. Nel grafico si mostrano solo le testate giornalistiche che mostrano una significatività dopo il processo di *backward stepwise selection.*

4.4 Associazione tra la fiducia accordata alle diverse testate giornalistiche e la vulnerabilità effettiva La forza dell'associazione tra la fiducia accordata alle testate giornalistiche e la vulnerabilità effettiva (casi osservati: vulnerabilità 0 = 377; 1 = 762). Dopo il processo di *backward stepwise selection* restano due testate giornalistiche: il Giornale e Ansa. La figura 2 mostra che per i lettori de Il Giornale c'è un'associazione positiva con la vulnerabilità effettiva. In altri termini, gli intervistati che credono ne il Giornale hanno maggiore probabilità di essere stati oggetto di almeno un attacco. Al contrario dare fiducia alle notizie Ansa ha un aOR inferiore a 1: vale a dire un effetto protettivo verso la vulnerabilità effettiva. Trattandosi di aOR tali evidenze sono al netto di fattori individuali quali genere, titolo di studio e fascia di età.

e nelle diverse testate



Il punto è l'aOR = probabilità di avere

vulnerabilità effettiva. Il dato, aggiustato per genere, fascia di età e titolo di studio, fornisce una misura della forza di associazione tra il credere alle diverse testate giornalistiche e la vulnerabilità effettiva. Gli estremi superiori e inferiori delle linee rappresentano rispettivamente l'*Upper* e il *Lower bound* degli intervalli di confidenza stimati al 95%. Nel grafico si mostrano solo le testate giornalistiche che mostrano una significatività dopo il processo di *backward stepwise selection.*

5 Commenti conclusivi Questo lavoro si occupa della relazione tra comportamenti individuali, vulnerabilità potenziale e vulnerabilità effettiva in termini di cyber-sicurezza, che si dimostra essere non solo una questione di analfabetismo funzionale (che può manifestarsi anche come vulnerabilità rispetto alle *fake news*), perché riguarda ampiamente anche la popolazione giovane e istruita, risultato confermato da una bassa significatività dell'associazione tra titolo di studio, classi di età e vulnerabilità. Il caso di studio composto da un campione di 1139 intervistati mostra che la vulnerabilità individuale potenziale, oltre che quella effettiva, sono molto diffuse anche nelle generazioni più giovani e ciò minaccia, anche in prospettiva, ogni sforzo fatto dalle autorità garanti della cyber-sicurezza. Il 60% dei rispondenti ha dichiarato di informarsi prevalentemente attraverso i Social Media, mentre un 20% ha dichiarato di utilizzare come fonte principale di informazione i suggerimenti del browser sul proprio smartphone. Inoltre, il 67,78% degli intervistati ha dichiarato di aver creduto almeno una volta ad una notizia che è stata, in seguito, smentita da fonti ufficiali. Quasi la metà di questi, ne ha condivisa almeno una. Solo il 13,26% del campione, nell'installare una *app*, si preoccupa almeno del nome della società che l'ha sviluppata. Ben il 56,54% degli intervistati dichiara di aver optato per il *social login*, ossia aver scelto di collegare il proprio account Facebook ad altri profili, utilizzando così le stesse credenziali per l'accesso ad altri siti o *app*. Il 26,78% del campione dichiara di tenere sempre attivo il GPS nel proprio smartphone. Il 21,25% dei rispondenti si è dichiarato disposto a fornire la propria posizione a qualsiasi *app* che gli faccia ottenere lo scopo e ben il 65,76% è disposto a fornirla a Google. L'analisi condotta sui dati raccolti mostra alcuni spunti degni di ulteriore indagine: per esempio esiste un'associazione positiva tra la fiducia accordata alle notizie pubblicate da La Repubblica e la vulnerabilità potenziale. Al contrario, esiste un'associazione negativa tra vulnerabilità potenziale e la fiducia nelle notizie pubblicate dal settimanale *Internazionale*. Stando a ciò che mostra questo campione, l'indicazione che si ottiene è che un comportamento più o meno consapevole sulla sicurezza in rete è legato alla fonte di informazione selezionata come più affidabile. Una differenza tra *La Repubblica* ed *Internazionale*, è che nel primo caso si tratta di un quotidiano con accento sull'opinione e l'interpretazione dei fatti, mentre il settimanale si propone come una fonte di pura osservazione sulle notizie pubblicate all'estero. Ciò può farci ipotizzare una correlazione positiva tra la neutralità e oggettività ricercata nelle fonti di informazione e il grado di attenzione e responsabilità individuale verso le proprie azioni in rete. Risultato che si ripete nel caso della vulnerabilità effettiva: gli intervistati che danno piena fiducia alle notizie pubblicate ne *Il Giornale* hanno maggiore probabilità di essere stati oggetto di almeno un attacco rispetto a coloro che propendono per assegnare fiducia alle notizie *Ansa*, caratteristica che mostra invece un effetto protettivo verso la vulnerabilità effettiva. Sebbene il caso di studio qui presentato abbia dimensioni ridotte, esso ha il senso di segnalare che esiste un tema ancora poco esplorato, ma cruciale per l'efficacia degli sforzi di garantire la cybersicurezza. Certo perchè questo arrivi ad essere utilizzabile da interventi pubblici è necessario approfondire come e quanto il *digital divide*, inteso in senso ampio, si associ alle disuguaglianze multidimensionali di vecchia e nuova generazione.

* Master's student, Scuola Superiore S.Anna, Pisa. **Data Life Lab researcher. ***Corresponding author. University of Florence, Department of Economics and Management, pettini@unifi.it ****Institute of Clinical Physiology, National Research Council of Italy (IFC-CNR).

Riferimenti bibliografici

Anwar, M., He, W., Ash, I., Yuan, X., Li, L., Xu, L., 2016. Gender difference and employees' cybersecurity behaviors. *Comput. Human Behav.* 69, 437 - 443. Bond, C. F., DePaulo, B. M., 2006. Accuracy of deception judgments. *Personality and Social Psychology Review.* 10, 214 - 234. http://dx.doi.org/10.1207/s15327957pspr1003_2

. Clark D. *et al.*, *At the Nexus of Cybersecurity and Public Policy: Some Basic Concepts and Issues* in National Research Council, The National Academies Press, Washington, 2014. Corritore, C., Kracher, B., & Wiedenbeck, S. (2003). On-line trust: Concepts, evolving themes, a model. *International Journal of Human Computer Studies*. 58, 737 - 758. http://dx.doi.org/10.1016/S1071-5819(03)00041-7 . Dhamija, R., Tygar, J. D., & Hearst, M. (2006). Why phishing works. In Proceedings of the SIGCHI conference on human factors in computing systems (581 - 590). http://dx.doi.org/10.1145/1124772.1124861 . Egelman, S., Peer, E., 2015a. Predicting Privacy and Security Attitudes. *Computers and Society: The New letter of ACM SIGCAS.* 45(1), 22–28. Egelman, S., Peer,E., 2015b. Scaling the Security Wall: Developing a Security Behavior Intentions Scale (SeBIS) (CHI'15). Proceedings of the ACM CHI'15 Conference on Human Factors in *Computing Systems*. 1, 2873–2882. Fogg, B. J., Soohoo, C., Danielson, D., Marable, L., Stanford, T., & Tauber, E. R., 2002. How do users evaluate the credibility of Web sites?. In Proceedings of the 2003 Conference on Designing for User Experiences (pp. 1e15). http://dx.doi.org/10.1145/997078.997097 . Gilbert, D. T., 1991. How mental systems believe. *American Psychologist*. 46, 107 - 119. Hadlington L., 2017. Human factors in cybersecurity; examining the link between Internet addiction, impulsivity, attitudes towards cybersecurity, and risky cybersecurity behaviours. *Heliyon*. 3. https://doi.org/10.1016/j.heliyon.2017.e00346 . Herath, T., Rao, H.R., 2009a. Encouraging information security behaviours in organizations: Role of penalties, pressures and perceived effectiveness. *Decis. Support Syst*. 47 (2), 154 - 165. Herath, T., Rao, H.R., 2009b. Protection Motivation and Deterrence: a Framework for Security Policy Compliance in Organisations. *Eur. J. Inf. Syst*. 18 (2), 106 - 125. Joinson, A. N., Paine, C. B., 2007. Self-disclosure, privacy and the internet. In A. N. Joinson, K. Y. A. McKenna, T. Postmes, & U.-D. Reips (Eds.), *Oxford Handbook of Internet Psychology* (237 - 252). Oxford, UK: Oxford University Press. ISBN: 9780199561803. Macrì, E. e Tessitore, C., 2013, "Sampling, Channels and Contact Strategies in Internet Survey", in *Advancing Research Methods with New Technologies*, IGI Global. McBride, M., Carter, L., Warkentin, M., 2012. Exploring the role of individual employee characteristics and personality on employee compliance with cybersecurity policies. RTI International Institute of Homeland Security Solutions, North Carolina. McCormac, A., Zwaans,T., Parsons,K., Calic,D., Butavicius,M., Pattinson,M., 2016. Individual differences and Information Security Awareness. *Comput. Human Behav.* 69, 151–156. R Core Team (2018). R: A language and environment for statistical computing. R Foundation for Statistical Computing, Vienna, Austria. URL http://www.R-project.org/. Shropshire, J., Warkentin, M., Johnston, A.C., Schmidt, M.B. 2006. Personality and IT security: An application of the five - factor model. Americas Conference on Information Systems (AMCIS), 3443 - 3449. Shropshire, J., Warkentin, M., Sharma, S., 2015. Personality, attitudes and intentions: Predicting initial adoption of information security behavior. *Comput. Sec.* 49, 177 - 191. Uebelacker, S., Quiel,S., 2014. The Social Engineering Personality Framework. Workshop on Socio-Technical Aspects in Security and Trust, 24–30. Vosoughi, S. *et al.*, "The Spread of True and False News Online", in *Social Science*, n. 359, Marzo 2018, pagg. 1146 – 1151. Welk, A.K., Hong,K.W., Zielinska,O.A., Tembe,R., Murphy-Hill,E., Mayhorn, C.B., 2015. Will the Phisher-Men Reel You In? in *International Journal of Cyber Behavior Psychology and Learning.* 5(4), 1–17. [1] World Economic Forum, *The Global Risks Report 2018* - 13th Edition, p. 61. http://www3.weforum.org/docs/WEF_GRR18_Report.pdf [2] Norton by Symantec, Norton Cyber Security Insight Report – Global Results 2017, Gennaio 2018. http://now.symassets.com/content/dam/norton/global/pdfs/norton_cybersecurity_insights/NCSIR-global-results-US.pdf [3] Giorgi, A., *Il cyber crime? Si combatte con la formazione. Parola di Eugene Kaspersky*, 30 gennaio 2018. http://formiche.net/2018/01/cyber-security-kaspersky-roma-luiss-sapienza/ [4] Senato della Repubblica - 11a Commissione Lavoro, previdenza sociale. *L'impatto sul mercato del lavoro della quarta rivoluzione industriale*. https://www.senato.it/application/xmanager/projects/leg17/attachments/dossier/file_internets/000/002/240/doc [5]

Clark, D. et al., 2014. [6] Longo, A., *Ignoranti in Sicurezza Digitale*, 11 febbraio 2018. http://nova.ilsole24ore.com/esperienze/diventeremo-tutti-hacker-buoni%E2%80%89/?refresh_ce=1 [7] La società è stata accusata di aver fatto uso improprio dei dati personali di circa 87 milioni di utenti, di cui 214 mila italiani, sottratti attraverso il *social login* ad un'*app* interna a Facebook chiamata "thisisyourdigitallife", allo scopo (anche) di manipolare il consenso elettorale in due delle più grandi campagne elettorali degli ultimi anni: quella del referendum pro – Brexit e quella dell'attuale Presidente degli Stati Uniti, Donald Trump. [8] Si annoverano a livello internazionale gli sforzi dell'ONU nell'ambito dell'applicabilità del diritto internazionale al cyberspazio, così come quelli del G7 per l'adozione di un approccio collaborativo fra Stati, le misure per il rafforzamento della fiducia informatica fra Stati e per la riduzione dei rischi di conflitti derivanti dall'uso delle ICTs dell'OSCE. A livello regionale europeo sono state coordinate iniziative in materia di cybersicurezza a partire dalla pubblicazione nel febbraio 2013 della *Strategia dell'Unione Europea per la Cybersicurezza* (*Network and Information Security*; *General Data Protection Regulation, etc)*. In Italia, con l'adozione del *Quadro Strategico Nazionale* e del *Piano Nazionale per la sicurezza cibernetica* (2013) si delineano, rispettivamente, l'indirizzo strategico nazionale di lungo e di breve periodo. A fronte delle evoluzioni normative in ambito europeo e della crescente sofisticazione e persistenza delle minacce, l'architettura istituzionale per la cybersicurezza predisposta inizialmente dal *DPCM Monti* è evoluta nel *DPCM Gentiloni* del febbraio 2017. [9] Vosoughi *et al.*, pp. 1146 – 1151. [10] Hadlington, 2017, Anwar et al., 2016; Herath e Rao, 2009a, b. [11] Per approfondimenti, si rimanda a Shropshire *et al.* (2006), McBride *et al*. (2012), Uebelacker e Quiel (2014), McCormac *et al.* (2016), Egelman e Peer (2015a, b), Welk *et al.* (2015) [12] Per la somministrazione del questionario online è stato utilizzato lo strumento open "Google Form". Il questionario integrale è consultabile all'indirizzo di Google Drive: https://docs.google.com/document/d/1I1Ski-WT0KONmcY4XWmeOlfa6Qoq71FMsWHRbWjAZWs/edit?usp=sharing [13] Infatti, secondo il rapporto "Digital in Italia 2018" di gennaio 2018 su una popolazione di circa 59.33 milioni di abitanti, 43.31 sono gli utenti di Internet (il 73% della popolazione) – dato in crescita del 10% rispetto al 2017. 34 milioni è, invece, il numero totale di utenti attivi su Facebook mensilmente. Secondo una suddivisione per età e sesso degli utenti del *social media*, risulta che gli utenti nella fascia d'età 18 – 24 siano 5.5 milioni (circa 2.6 le femmine e 2.9 i maschi) mentre gli utenti nella fascia 25 – 34, siano 7.6 milioni (circa, rispettivamente, 3.6 e 4). Il successo di Facebook lo rende canale privilegiato per la trasmissione rapida di informazioni e dunque terreno estremamente allettante per i ricercatori sociali. Per un approfondimento, si rimanda a Macrì e Tessitore (2013). [14] *Echo chamber* (trad. camera dell'eco) Un ambiente in cui una persona incontra solo credenze o opinioni che coincidono con le proprie, in modo che le opinioni esistenti vengano rafforzate e non vengano prese in considerazione idee alternative. https://en.oxforddictionaries.com/definition/echo_chamber [15] http://www.bufale.net/home/the-black-list-la-lista-nera-del-web/ [16] Fatto Quotidiano: 19,14%; Libero: 15,10%; La Nazione: 15,10%; Il Giornale: 10,62%; Famiglia Cristiana: 5,09%; Leggo: 4,39%.

Valentina de Vito | Cybersicurezza | Vulnerabilità del fattore umano

[caption id="attachment_9487" align="aligncenter" width="300"]

Cybersicurezza-Valentina-de-Vito[/caption]

Valentina de Vito | Cybersicurezza | Vulnerabilità del fattore umano