Associazione BLOOMSBURY Editore

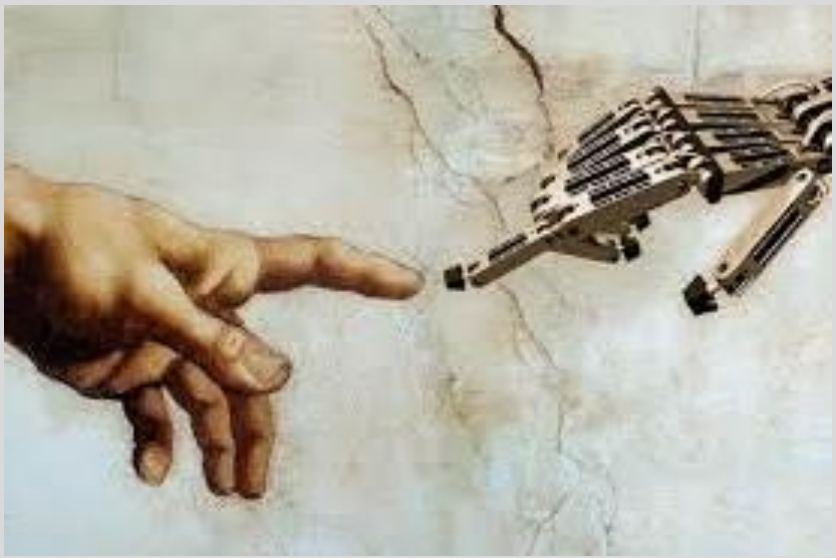
WOLF

OSCOM-ONLUS Osservatorio di Comunicazione

QUINDICINALE ON LINE autorizzazione 5003 del Tribunale di Napoli – ISSN 1874-8175 del 2002
DIRETTORE FRANCO BLEZZA **DIRETTORE RESPONSABILE CLEMENTINA GILY**
Anno XIX Numero 11 MONDO AMBIENTE WOLF 1-15 GIUGNO 2020

Sinergie sulla Cyber Security. Il ruolo della competenza diffusa

di **Vincenzo Curion**



Un meme circolato sui social durante questi mesi di lockdown, sottolineava come grazie all'emergenza virale fossero stati compiuti enormi passi avanti per la crescita delle competenze digitali. È così serpeggiata l'idea che la cittadinanza digitale fosse ormai divenuta un patrimonio del senso comune, un po' come lo dovrebbe essere diventato il lavarsi le mani accuratamente, più volte al giorno, o come lo dovrebbe essere il guardare a destra e sinistra prima di attraversare una strada. Di fatto, il senso di essere cittadini, di essere parti di una comunità, presuppone una presenza attiva all'interno di quel gruppo, per la tutela e la promozione di quel luogo e del patrimonio culturale e sociale che quell'area aggrega. Creature spaziali fin dagli esordi della nostra specie, abbiamo imparato nelle epoche, a delimitare i nostri spazi di abitazione, demarcandoli, mettendo confini e arrivando a proteggere quei confini anche a costo della vita. La storia della civiltà umana ci tramanda esempi e storie, di persone che hanno inteso la difesa di un territorio e della cultura che in esso si è stratificata attraverso le epoche, il senso ultimo delle loro vite. A queste persone, tributiamo gli onori per la loro opera e, per quanto possibile, ne traiamo ispirazione, riconoscendo che il loro servizio è un ideale a cui tutti, indistintamente dovremmo tendere. Di conseguenza, seguendo questa linea di ragionamento, non si dovrebbe mai, considerarsi completamente cittadini di un posto, ma fare in modo che, con gesti e con opere concrete, col servizio appunto, il legame tra noi ed un luogo, tra noi ed una data cultura, una data comunità, continui a rafforzarsi e rigenerarsi. "Non chiederti cosa può il tuo Paese fare per te, ma cosa tu puoi fare per il tuo Paese", ammoniva John Fitzgerald Kennedy in un suo celebre discorso, riferito agli Americani, che assolutamente avrebbero dovuto rendersi parti sollecite per il benessere della comunità tutta. Di avviso simile anche Paolo VI, quando si riferiva alla politica, nell' Esortazione Apostolica *Evangelii Gaudium*, "la politica, tanto denigrata, è una vocazione altissima, è una delle forme più preziose di carità, perché cerca il bene comune". Richiami all'impegno ed alla partecipazione per la tutela del bene comune. Fatta questa premessa, oggi che sotto la stretta del lockdown, abbiamo scoperto che anche la Rete è un bene comune, che grazie ad essa è possibile

QUINDICINALE ON LINE
DIRETTORE FRANCO BLEZZA
Anno XIX Numero 11
autorizzazione 5003 del Tribunale di Napoli – ISSN 1874-8175 del 2002
DIRETTORE RESPONSABILE CLEMENTINA GILY
1-15 GIUGNO 2020

mantenere rapporti, tessere relazioni, continuare ad usufruire di servizi, ognuno dovrebbe riconoscersi l'onore e l'onere di essere parte della Rete, usando eticamente e responsabilmente questi strumenti. Di fatto questa auspicabile "virtuosità", nell'uso di uno strumento tanto potente, non trova riscontro, se come è accaduto ed accade, durante la Pandemia sono aumentate le truffe online, i raggiri, le catene di fake news che sono schizzate all'impazzata tra le app di instant messaging ed i social network. Segno evidente dell'immaturità e della cattiva volontà di molti nel gestire questi strumenti e la comunicazione, nel volere arrecare danno agli altri utenti. Le forze dell'ordine sono intervenute come hanno potuto, con gli strumenti che avevano a disposizione. Ma come ogni fenomeno criminoso, non bisognerebbe fidare sulla repressione quanto sulla prevenzione. I cittadini dovrebbero avere competenze, tali per cui dovrebbero avere un comportamento accorto, avere una consapevolezza dei rischi della Rete; dovrebbero imparare a trattare con circospezione le potenzialità della Rete. Facendo questo, il carico di lavoro delle forze dell'ordine sarebbe meglio gestito e sarebbe anche più facile intervenire su quei più eclatanti e complessi dove conoscenze più specialistiche sono più necessarie. Facendo un confronto, nessuno si aspetterebbe che vigili, polizia e carabinieri possano essere presenti in ogni luogo della rete stradale nazionale, ma evidentemente, ogni automobilista deve essere responsabile per se stesso, cosciente dei rischi che corre e dei problemi che può causare con un comportamento imprudente alla guida. È dunque la percezione del rischio il tallone d'Achille della sicurezza in rete. Ma questa errata percezione si cura educandosi al rischio, facendo dell'apprendimento una forma di prevenzione, trasversale a tutti i livelli di partecipazione alla "vita digitale". In effetti, riflettendo sulla tipologia di attacchi, si scopre che la potenza di calcolo per queste operazioni, sovente proviene da reti di computer di ignari utenti che, avendo macchine infettate da virus informatici, si ritrovano ad essere partecipi, loro malgrado, di iniziative volte a destabilizzare la connettività, o peggio a bloccare servizi di rete. La situazione è di tale portata che da tempo gli analisti, hanno dovuto riconoscere nel cyberspace, ma più in generale nelle reti di calcolatori e device, un ulteriore campo in cui saranno combattute vere e proprie guerre. Al pari dei consolidati domini terra, acqua, aria, il cyberspace già oggi è uno spazio d'interesse nazionale, grandemente considerato dall'esercito che, nel dicembre 2019, comunicava la recente creazione del Comando Interforze Operazioni Cibernetiche e del Comando Operativo Reti, per parlare concretamente di difesa di un dominio, che è immateriale, ma le cui battaglie possono creare danni e accadimenti reali e concreti. "L'obiettivo di questi Comandi", dichiaravano le autorità

QUINDICINALE ON LINE autorizzazione 5003 del Tribunale di Napoli – ISSN 1874-8175 del 2002
DIRETTORE FRANCO BLEZZA DIRETTORE RESPONSABILE CLEMENTINA GILY
Anno XIX Numero 11 MONDO AMBIENTE WOLF 1-15 GIUGNO 2020

militari, "è di provvedere alla difesa costante del cyberspazio con una cura analoga a quella che si ha per un confine nazionale, proteggendolo persistentemente da chi lo assedia e minaccia, impegnandosi incessantemente nel contempo, a dominare la trasformazione digitale". Ma, la Rete è evidentemente una risorsa troppo importante, per lasciarla solo in mano ad un organismo, sia pure ben equipaggiato e presieduto da personale preparato e formato. Un po' come nella lotta alla Mafia ed alla criminalità organizzata, dove l'azione delle forze dell'Ordine non sarebbe da sola bastevole per arginare le forze del crimine, serve la collaborazione e l'impegno di tutti, anche nei confronti delle minacce e delle organizzazioni che agiscono attraverso il Web. Purtroppo, stando a diverse fonti, il dato sull'uso del Web, pre pandemia era sconfortante. L'uso che gli italiani facevano di questo strumento era del tutto approssimativo, con conoscenze raffazzonate ed empiriche, venute su per "sentito dire", piuttosto che per corretta applicazione, per uno studio preciso. Come possedere una formula 1, ma conoscere a stento come ingranare la prima marcia e per questo aver maturato l'accortezza, che potrebbe avere uno sfasciacarrozze per le macchine da demolire. Tutto questo nonostante, gli italiani passino in media, secondo quanto riportato dal documento *We Are Social, Hootsuite – Digital in 2018*, oltre due ore al giorno in Internet, e che gli utenti Internet siano circa il 92.5% della popolazione complessiva. Come si può allora pensare di avere una Rete sicura se non ci si adopera per conoscere meglio questo strumento? Il passaggio da arpanet a Internet, compiuto dal Dipartimento della Difesa Americana trentasette anni fa –varie fonti fanno risalire la nascita embrionale di Internet al 1983-, segnò l'inizio di una trasformazione per uno strumento, nato in ambito militare, in una tecnologia che potesse servire alla popolazione civile. Di fatto così è stato. Oggi, proprio grazie all'uso civile e commerciale della Rete, parliamo di industria 4.0 e di Internet of Things come dell'imminente futuro. Ma la conoscenza di questa evoluzione, delle sue potenti e pervasive implicazioni, delle responsabilità che ricadono su ognuno, non sono altrettanto note a tutti. Così si rischia di mettere in crisi una struttura sociale, creando potentati e microcosmi, in una sorta di far west digitale, dove la legge sarebbe quella del più forte. Già ora, in ambito internazionale, si assiste ad una spartizione di aree di controllo tra Russia e Cina che, con l'America sono le potenze che più si sono impegnate nell'organizzare strategicamente la loro influenza nel cyberspazio. Entrambe le potenze orientali, sono impegnate da anni in una riconfigurazione della propria cyber security, con accentramento del know how e con un aumento del controllo delle attività private dei singoli e delle organizzazioni produttive e commerciali, al fine di proteggere i propri interessi nello scacchiere mondiale. Gli Stati Uniti, d'altro canto, già nel 2009 hanno ufficializzato la creazione del Cyber Command Americano e, nel 2010, secondo voci diffuse, in collaborazione con Israele, avrebbero sferrato l'attacco cyber con il virus informatico Stuxnet che, secondo le indagini che furono effettuate, bloccò le ventole dell'impianto di raffreddamento delle centrali iraniane per l'arricchimento dell'uranio. Prima che l'impianto tornasse a funzionare, si stima che siano passati non meno di ventiquattro- trentasei mesi, e questo ha significato ritardi nel piano energetico ma anche militare dell'Iran, paese da tempo sulle black list americane. Per l'Italia, rispettando la Carta Costituzionale, un'azione del genere sarebbe impensabile. "L'Italia ripudia la guerra come strumento di offesa alla libertà degli altri popoli e come mezzo di risoluzione delle controversie internazionali". Ma allora, a maggior ragione, si dovrebbe agire in maniera preventiva,

QUINDICINALE ON LINE autorizzazione 5003 del Tribunale di Napoli – ISSN 1874-8175 del 2002
DIRETTORE FRANCO BLEZZA DIRETTORE RESPONSABILE CLEMENTINA GILY
Anno XIX Numero 11 MONDO AMBIENTE WOLF 1-15 GIUGNO 2020

istituzionalizzando il concetto strategico della *forward defence*, introdotta dall'esercito americano, secondo la quale *"occorre agire per contenere o respingere l'aggressione militare il più vicino possibile alla linea di contatto originale in modo da difendere l'intero territorio di una nazione o di un'alleanza"*. Ancora una volta, anche per questa strategia così raffinata, torna alla ribalta il ruolo della competenza digitale diffusa nella popolazione, perché si tratta di confrontarsi con un problema che ha più connotati della "guerriglia terroristica", piuttosto che un confronto tra truppe regolari, solite rispettare un codice di condotta militare. Occorre pensare che un virus informatico, oggi non crea solo il problema al singolo, ma può essere adoperato per mandare in crash il sistema di controllo d'un impianto, di una rete ferroviaria, i sistemi di un ospedale, i siti di diverse amministrazioni e tutti questi strumenti sono strutture d'interesse nazionale. Con un attacco da remoto che, passa attraverso il mezzo del collegamento al web esiste già da anni la possibilità di perpetrare un'azione che non ha nulla di meno dell'attacco fisico che viene comunemente sferrato alle strutture vitali di un governo nemico. Con gli strumenti informatici attuali, anche un aggressore "piccolo", lavorando con poche risorse può combattere contro un grande con la concreta possibilità di arrecare un danno significativo, cosa che invece, salvo rare eccezioni, in una guerra in campo fisico non è concepibile. Con l'aumento esponenziale di strumenti che sono connessi in rete, non è escluso che si possa creare un *distributed denial of service* ad hoc per creare destabilizzazione come e forse più che con un attacco fisico. Uno scenario del genere sarebbe l'equivalente di un'azione terroristica portata su scala nazionale. Come se le terribili stragi che hanno segnato la Storia, causate da quello o quell'altro gruppo organizzato, potessero accadere contemporaneamente, alimentando tensione sociale, sia pure non arrecando necessariamente morti. Ma quest'ultimo aspetto, quello della "mancanza di vittime umane", come direbbero gli analisti, è tutto da dimostrare visto che ad esempio, gli strumenti telecontrollati da remoto, già oggi adoperati in medicina possono essere essi stessi i mezzi che manomessi nel loro funzionamento possono creare incidenti anche gravi. In fin dei conti se è stato possibile infettare una rete di gestione di un impianto di raffreddamento, perché non dovrebbe essere possibile intervenire da remoto sui contatori dell'elettricità nelle abitazioni domestiche, su una qualsiasi struttura messa in Rete o su un pacemaker o un defibrillatore che periodicamente trasmette a distanza i valori di un paziente? Nel momento in cui venissero attaccati un numero significativo di strumenti, ecco che si potrebbe gettare nel panico o anche, nello scenario più catastrofico, nella disperazione, una parte della popolazione. Quale può essere la prima linea d'intervento attuabile da ciascun utente? Sotto osservazione andrebbe posta anche i nuovi strumenti per la domotica, dotati per giunta di intelligenza artificiale. Un microfono che ci ascolta è una finestra H24 nella privacy della nostra quotidianità. Fin dove si può parlare di benefici e dove invece iniziano i problemi? Il suggerimento degli esperti è che si debba imparare a riconoscere nella connessione di un qualsivoglia device, oltre che un'opportunità anche una minaccia. Finora tutto questo non è stato considerato, o lo è stato poco. Un'euforia di massa ha nascosto le possibili minacce celate dietro una interfaccia "amichevole". Ma si tratta di falle che vanno considerate, per non farsi trovare impreparati. Come del resto si fa con qualunque tecnologia. Chi si metterebbe in viaggio col pericolo che i freni della propria automobile possano di colpo smettere di funzionare lanciando il veicolo in una folle corsa? Evidentemente solo un incauto. Una persona responsabile, si

QUINDICINALE ON LINE autorizzazione 5003 del Tribunale di Napoli – ISSN 1874-8175 del 2002
DIRETTORE FRANCO BLEZZA DIRETTORE RESPONSABILE CLEMENTINA GILY
Anno XIX Numero 11 MONDO AMBIENTE WOLF 1-15 GIUGNO 2020

muoverebbe per tempo, facendo preventivamente almeno un controllo del proprio mezzo di viaggio, prima di partire. Questo senso di responsabilità, dovrebbe essere lo stesso ogni volta che si adopera una tecnologia, affinché possa sempre esserci una capacità di "guidare le operazioni". Pensare di lasciare solo in capo ai tecnici specializzati, il compito di fronteggiare le emergenze, dovrebbe essere visto come una "colpa grave", soprattutto perché, come si è visto in diversi casi assurti agli onori della cronaca, con i reati informatici in Rete, si può diventare facilmente corresponsabili. È il cittadino la prima linea di difesa. Occorre agire sulla competenza di ognuno, creando occasioni per incentivare o creare un senso critico digitale comune. Se un utente ha dei comportamenti attenti, evitando che la propria macchina resti alla mercé di chiunque sulla rete, egli stesso potrà far sì che quello strumento non si tramuti in una falla pericolosa, il veicolo di una potenziale infezione per tutta la Rete. Solo quando ogni navigatore avrà chiare le proprie responsabilità e saprà agire oculatamente si potrà parlare di cittadinanza digitale e non di "monadismo digitale". Fino ad allora, quando emerge la notizia di una falla, quando viene denunciata l'ennesima fake news circolata sui social, per dirla con John Donne quella è "una campana che suona anche per te".

Sitografia e Bibliografia

- https://www.garanteprivacy.it/temi/cybersecurity
- https://www.garanteprivacy.it/regolamentoue/approccio-basato-sul-rischio-e-misure-di-accountability-responsabilizzazione-di-titolari-e-responsabili#misure
- https://cybersecurity.startupitalia.eu/63206-20200201-coronavirus-esca-cybercrime
- https://cybersecurity.startupitalia.eu/63390-20200513-fbi-possibili-cyber-attacchi-della-cina-le-cure-sul-covid-19