

Cyberspazio a rischio

Virus influenzali, ma non solo «Bisogna pensare anche a evitare le pandemie informatiche»

Martinelli (Cnr): nei momenti di emergenza come questo il sistema tecnologico è molto più vulnerabile

VALERIO MARCHI

In questo periodo un'ampia fetta dell'umanità si ritrova fortemente limitata negli spostamenti e nei contatti umani diretti. Mai come adesso, di conseguenza, ci accorgiamo dell'apporto della comunicazione online, capace di soddisfare almeno in parte la basilare necessità (psicologica, affettiva, economica...) di interagire con il mondo.

Come non paventare, allora, la distopica possibilità di una pandemia virale di tipo informatico che ostacoli, o persino impedisca, l'accesso al cyberspazio? Se un'evenienza del genere si sommasse a frangenti simili a quelli che stiamo vivendo, si concretizzerebbe per tutti noi un vero e proprio incubo; ma, anche in presenza di condizioni normali di vita materiale, un blocco delle reti digitali potrebbe provocare conseguenze persino più gravi di quelle che ci stanno affliggendo con il Covid-19. Sorge spontanea la domanda, allora: è ipotizzabile qualcosa del genere? E

quali strategie preventive vengono adottate?

Lo abbiamo chiesto a Fabio Martinelli, che si occupa di cyber security da 25 anni ed è Dirigente di ricerca dell'Istituto di informatica e telematica del Consiglio nazionale delle ricerche.

«Ci dirigiamo sempre più verso la digitalizzazione di massa – osserva – e per questo la sicurezza informatica è importante forse quanto la prevenzione delle epidemie». Infatti, «negli ultimissimi decenni siamo passati dai cybercriminali al cyber terrorismo alla cyberwar sponsorizzata dagli Stati, e le tipologie di minacce si sono evolute, i pericoli sono reali»: un virus informatico può paralizzare trasporti, tribunali, ospedali, produzioni e quant'altro, e per questo «nel 2016 la Scientific Advice Mechanism della Commissione europea ha individuato quali priorità assolute di intervento la sicurezza informatica e l'inquinamento». Tra gli aspetti che fanno ritenere la cyber security prioritaria, c'è il fatto che «oggi, tramite vie informatiche, si possono cambiare i go-

verni creando attacchi, condizionando elezioni e diffondendo fake news». Si può usare l'informatica, insomma, per spargere e «pompare» notizie false, influenzando l'opinione pubblica.

Occorre inoltre rilevare un «interplay» fra virus biologici e informatici: nell'attuale contesto, infatti, «il numero delle fake news e degli attacchi informatici è cresciuto sia utilizzando email che approfittando, per veicolare gli attacchi, dell'attenzione spasmodica sul Coronavirus, sia sfruttando la maggiore vulnerabilità dei sistemi informatici, tipica dei momenti di forte emergenza». Possiamo dire che il virus biologico alimenta quello informatico, e che quest'ultimo influisce a sua volta sulla percezione e sulle dinamiche sociali del primo: ecco perché «un progetto di ricerca europeo (Sparta) studia come i virus informatici vengano usati per diffondere panico e informazioni errate sui virus biologici».

Dietro al virus informatico, però, ci sono sempre uomini. Si parla di virus biologici «intelligenti», che si modificano

per sopravvivere e diffondersi, ma l'intelligenza che sta dietro a quelli informatici «è più difficile da affrontare, perché all'origine c'è una mente che li programma e li rende molto più complessi e veloci nei loro adattamenti e movimenti».

Si tratta, dunque, di una guerra quotidiana, fra uomo e uomo? «Esattamente – risponde Martinelli – e consideriamo altresì che mentre una calamità naturale si scatena senza volontà di produrre il massimo danno all'uomo (un terremoto, ad esempio, può verificarsi in una zona deserta), gli attacchi informatici sono invece sempre mirati e rispondono colpo su colpo, razionalmente, con la potenzialità di colpire seriamente le stesse strutture di protezione».

Resta da chiarire se si investe a sufficienza in prevenzione: «I fondi ci sono, gli sforzi sono notevoli, l'allerta è alta. A livello europeo, la cyber security è una "main priority" ... nondimeno, si può e si deve fare sempre di più; gli investimenti non sono ancora pari a quelli di Stati Uniti e Cina».



Una pandemia virale di tipo informatico potrebbe impedirci l'accesso al cyberspazio, con gravi danni economici

L'ESPERTO

Creatore di gruppi di esperti nel settore della sicurezza

Fabio Martinelli è ricercatore dell'Istituto di Informatica e Telematica (Itt) del Consiglio nazionale delle ricerche (Cnr) ed è referente per le attività di cyber security dell'ente. È co-autore di numerose pubblicazioni scientifiche in atti di conferenze e riviste internazionali. I suoi interessi di ricerca riguardano la sicurezza dei sistemi distribuiti e pervasivi e gli aspetti di privacy e trust in sistemi dinamici e complessi. Fabio Martinelli ha promosso la creazione di vari gruppi di esperti nel settore della sicurezza.



Fabio Martinelli

«A livello europeo la cyber security è una "main priority" ma servono investimenti»

