Dai cercapersone di Hezbollah un avvertimento per il nostro futuro

written by Paolo Musso | 2 Ottobre 2024

L'attacco di Israele ai cercapersone e ai walkie-talkie di Hezbollah ha suscitato commenti di ogni genere, ma tutti esclusivamente in relazione alla guerra. E questo è comprensibile (a proposito, dove sono finiti quelli che "Israele non deve reagire per il suo stesso bene, perché non è più quello di una volta e non è in grado di combattere contemporaneamente Hamas e Hezbollah"?).

Ciò che è meno comprensibile è che nessuno ne abbia tratto spunto per riflettere sui rischi della internettizzazione globale, che tutti (o almeno tutti quelli che hanno voce sui mass media) considerano auspicabile o quantomeno inevitabile, l'unico problema essendo quello di "gestirla bene".

Probabilmente ciò è dovuto, almeno in parte, al fatto che gli strumenti di comunicazione usati da Hezbollah non erano connessi ad Internet, proprio per evitare che succedesse qualcosa del genere. Eppure, è successo, anche se non è ancora chiaro come. Ma, quale che sia stato il metodo utilizzato (forse una frequenza radio o un sms: attacco-hacker-a-hezbollah-cosa-sappiamo-dei-cercapersone-fatti-esplodere-da-remoto), si è trattato comunque di un segnale a distanza di qualche tipo che in pochi secondi ha fatto esplodere le batterie, forse (ma non è certo) con l'aiuto di una piccola carica di esplosivo preventivamente introdotta.

Ora, basta riflettere un attimo (sport che però non è più molto di moda…) per rendersi conto che, se questo è successo perfino con strumenti non connessi a Internet, a maggior ragione potrà succedere con quelli connessi. E ciò diventerà

sempre più probabile quanti più oggetti metteremo in rete.

Pensate cosa potrebbe accadere se, invece dei piccoli cercapersone, a esplodere o essere lanciate fuori strada o contro le case fossero le automobili (peggio ancora poi se avessero batterie all'idrogeno, che esplode con violenza 20 volte superiore alla benzina) o gli aerei – voglio dire tutte le automobili o tutti gli aerei di una città o addirittura di un'intera nazione: potremmo avere un 11 settembre moltiplicato per mille.

Per gli esperti di informatica l'unica soluzione è migliorare i sistemi di cybersecurity, come ci ripetono come un disco rotto ogni volta che qualcosa va storto, in parte per deformazione professionale e in parte (probabilmente anche maggiore) per interesse personale, dato che sono loro stessi a venderci i sistemi di cui sopra. Ma questa è una risposta del tutto inadeguata, per diversi
motivi.

Anzitutto, la cybersecurity costa cara, anche perché va continuamente aggiornata. E i nostri paesi, che sono già sull'orlo della bancarotta a causa dell'economia asfittica e dell'immenso debito pubblico (che non è un problema soltanto italiano, ma di tutti i paesi ricchi, nessuno escluso: ne parleremo presto), non possono continuare a caricarsi di spese, soprattutto di spese che nel tempo sono destinate a crescere sempre più. Inoltre, va considerato non solo il costo economico di Internet, ma anche il suo costo energetico, che, come tutti gli esperti sanno, anche se nessuno lo dice, nel giro di pochi anni diventerà la prima causa di inquinamento al mondo. Secondo, il pericolo non viene solo dall'esterno, ma anche dall'interno, cioè da possibili e sul lungo periodo inevitabili errori nella costruzione e/o nell'aggiornamento dei sistemi, contro cui la cybersecurity non serve a niente. Un esempio l'abbiamo già avuto il 19 luglio scorso, con il blocco di moltissimi sistemi informatici, dovuto a un banale errore in un file di aggiornamento, che è bastato a mandare in

tilt il trasporto aereo e una quantità di altri servizi in tutto il mondo per diversi giorni.

Terzo, la sicurezza assoluta non esiste. Di fatto, tutte le più importanti istituzioni del mondo, comprese quelle governative e militari ai più alti livelli, sono già state hackerate almeno una volta e spesso anche più d'una. L'unica eccezione è il CERN di Ginevra, ma solo perché il suo è un sistema informatico chiuso, che non comunica né con Internet né con alcun altro sistema esterno (naturalmente parlo del sistema che gestisce l'acceleratore, non dei sistemi secondari o dei computer personali dei ricercatori che ci lavorano, che però non comunicano col sistema principale).

Quarto e più importante di tutti, una volta che tutto sia online anche un solo collasso di qualche sistema importante, incidente o hackeraggio che sia, può causare una catastrofe peggiore di un attacco nucleare.

Cosa dovremmo fare, allora?

Certamente non possiamo semplicemente spegnere Internet. Ma dovremmo almeno smetterla di considerare che mettere tutto online sia buono a prescindere e, prendendo esempio dal CERN, farlo solo quando è davvero necessario, cioè quando i rischi sono palesemente inferiori ai benefici. E i benefici in questione devono essere quelli della collettività e non quelli dei giganti dell'informatica (l'ideale sarebbe che le due cose coincidessero, ma purtroppo più passa il tempo, più sembrano entrare in conflitto).

Ne riparleremo più ampiamente appena possibile. Ma intanto cominciate a rifletterci.