SI CAU INTERNET...

Una de les excentricitats de Donald Trump en la seva cursa cap a la Casa Blanca ha sigut la proposta de deixar zones del planeta sense internet. Més enllà de si és factible, la pregunta és si estem preparats per assumir un món desconnectat

TEXT
Gina ***Tost*** */ Xavier* ***Vidal***

Fa unes setmanes, el precandidat a les eleccions presidencials als EUA Donald Trump va proposar deixar sense internet zones concretes del planeta per combatre l'Estat Islàmic (EI). El polític republicà ho va dir com si el govern del seu país tingués la capacitat de fer-ho. Arran de la idea expressada per Trump, moltes persones es van preguntar si és possible que el món es quedi sense internet, si tècnicament és factible i, si ho és, si estem preparats per assumir un món desconnectat, encara que sigui temporalment.

Revolution, una de les sèries més originals dels últims anys, produïda per J.J. Abrams, plantejava un argument basat en la caiguda global del sistema elèctric. Aquesta eventualitat deixava un món sense la majoria dels serveis més habituals, entre els quals un dels més importants, internet. Apagada elèctrica global al marge, quines són les causes que podrien produir la caiguda d'internet? Ara com ara, la qüestió prèvia és si tècnicament existeix la possibilitat que passi. Xavier Gatius, director general del Centre de Seguretat de la Informació de Catalunya (Cesicat), considera que la caiguda total d'internet és molt poc probable per "la seva naturalesa global i distribuïda". Gatius explica que per fer-ho "caldria inutilitzar tots els servidors de noms de domini [DNS] distribuïts pel món, o bé causar una caiguda general de totes les xarxes de comunicacions electròniques".

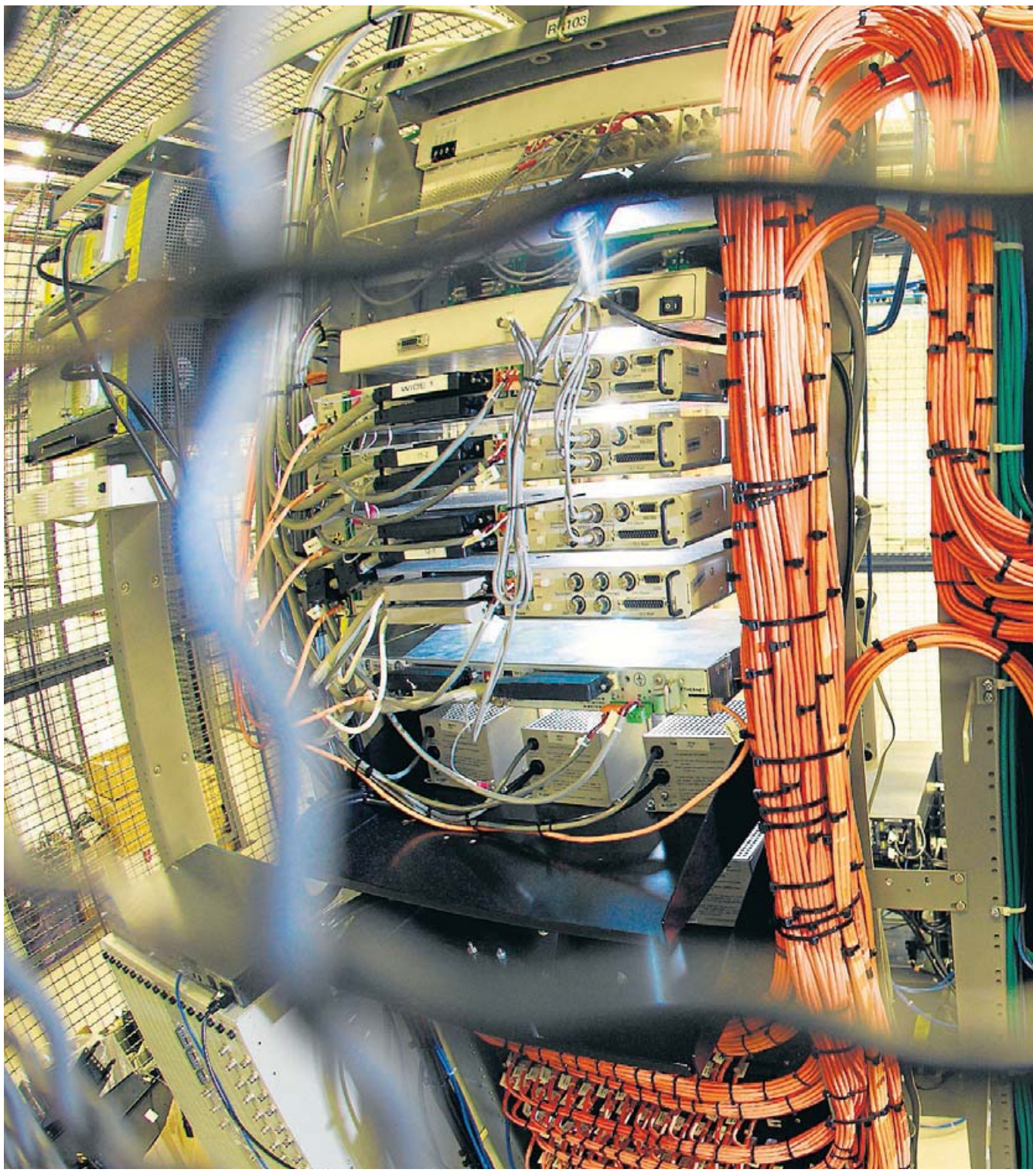
Jesús Gutiérrez, *technical support manager* de l'empresa de seguretat Sophos Iberia, explica que "la infraestructura bàsica d'internet (l'anomenada xarxa troncal o *backbone*) està formada per les xarxes de diferents empreses i organitzacions connectades entre elles, i és gairebé impossible que un problema fortuït o un hipotètic atacant afectin la connectivitat d'internet fins al punt de deixar grans àrees aïllades".

De fet, internet es va concebre com una malla descentralitzada que no fos dependent d'un ordinador central i únic. A més, el protocol de comunicació creat pel *pare* i la *mare* d'internet, Vinton Cerf i Radia Perlman, assegura que la informació sempre tindrà camins alternatius per arribar del punt d'origen al punt final. Això funciona de manera que, si un usuari demana una pàgina web que és a l'altra banda del món i el camí més directe està tallat, el protocol busca camins alternatius fins que la informació sol·licitada arriba finalment a l'usuari. Jordi Planas Manzano, membre de la delegació espanyola de la Internet Society, creu més factible la caiguda de serveis d'abast planetari com ara Facebook, que "per a molta gent seria pràcticament la caiguda d'internet, però que per a molts altres no seria una cosa gaire greu". Per tant, vist que "moltes de les funcionalitats que els usuaris esperen d'internet estan concentrades en unes quantes empreses, com ara Google, Apple i Facebook", la fallada d'aquestes grans corporacions podria equiparar-se a una caiguda de la xarxa global. De fet, el 2013 tots els serveis de Google van caure durant uns cinc minuts i el trànsit d'internet es va reduir en un 40% durant aquest breu espai de temps.

Getty

El botó d'apagada

Deixant clara la improbabilitat d'un accident tecnològic, quines altres hipòtesis podrien donar-se que provoquessin la caiguda del servei d'internet? Tornem a Trump. Diverses teories sostenen que el govern dels EUA disposa d'un sistema per anul·lar totalment el servei, l'anomenat *internet kill switch* o botó d'apagada d'internet. La idea es basa en un protocol d'actuació existent als Estats Units anomenat SOP (Standard Operation Procedure) 303 i que està dissenyat per aplicar-se en situacions d'emergència. Es tracta d'un procediment secret, aprovat el 2006, que es va usar l'any 2011 durant els disturbis socials que es van produir després que un policia matés un sensesostre a San Francisco. Les autoritats van tallar totes les comunicacions a l'àrea de les protestes durant tres hores. I ho van fer seguint el SOP 303. A més, durant la Primavera Àrab, els governs de Líbia, Egipte i Tunísia també van tallar l'accés a internet de la població per intentar controlar la revolta. Les autoritats, per tant, sí que disposarien de mètodes per deixar sense accés a la xarxa àmplies zones del món. Si la fallada es produís, tot i ser tan improbable, Xavier Gatius creu que "les conseqüències podrien ser importants sobre serveis públics, sistemes d'emergència, serveis assistencials o financers, perquè depenen en bona mesura del correcte funcionament dels sistemes d'informació i de les comunicacions electròniques".



Un atac terrorista podria col·lapsar internet? Hipotèticament, sí. O, com a mínim, podria crear un caos tal que fos impossible navegar o obrir cap servei habitual. D'una banda, es podria dur a terme atacant o bé físicament o bé a través de programari els principals servidors d'enrutament d'internet. D'altra banda, teòricament també es podria prendre el control del cervell de la xarxa, és a dir, alterar la base de dades de l'ICANN (Corporació d'Internet per l'Assignació de Noms i Números). Quan escrivim al navegador l'adreça *ara.cat*, per exemple, aquesta expressió és traduïda pel sistema en una sèrie de números (del tipus 54.170.42.201), que és el format que els ordinadors poden entendre i que ens porta fins a la web del diari. És una espècie de número de telèfon que entenen les màquines.

Totes aquestes operacions les fan només 13 servidors DNS (*domain name server*) distribuïts arreu del món. L'equivalència entre noms de domini (el nom de les webs d'internet) i adreces IP (els números que entenen els ordinadors) està emmagatzemada en la base de dades de l'ICANN. És com la llista de telèfons convencional, que relaciona noms de persones amb els seus números de telèfon. Si algú amb males intencions n'obtingués el control podria canviar aquestes equivalències, alterar tot el trànsit global i redirigir-lo on volgués. Per fer-ho, però, es necessiten set claus combinades. Aquestes claus les tenen set persones al món triades per l'ICANN i estan guardades en llocs secrets distribuïts arreu del planeta. També hi ha set persones més que fan de còpia de seguretat dels set membres primaris i que tenen una rèplica de cadascuna de les set claus. Per tant, si hipotèticament algú reunís les set claus, tindria el control global del trànsit d'internet. Sembla l'argument d'una pel·lícula de James Bond, però està basat en el funcionament real de la xarxa i la Xina va provar que es pot fer quan va desviar el 2010 el 15% del trànsit total d'internet a través dels seus servidors durant més d'un quart d'hora.

Per sort, la capacitat i la fortalesa dels 13 servidors arrel DNS que dirigeixen el trànsit del domini a nivell superior a la xarxa és molt gran. A finals de l'any passat, van suportar un misteriós assalt combinat des de nombrosos punts del planeta. Entre el 30 de novembre i l'1 de desembre els responsables van dirigir un atac global de denegació de servei contra els servidors. Aquest tipus d'atacs consisteixen a fer consultes massives als servidors fins que es col·lapsen i cauen. En aquest període, els 13 servidors van suportar gairebé cinc milions de consultes per segon durant dos dies seguits. El trànsit global d'internet només es va veure alentit, però no va arribar a fallar en cap moment. Els Fab Thirteen [Tretze Fabulosos] van suportar el bombardeig i se'n van sortir. Jesús Gutiérrez explica l'origen de la robustesa dels servidors arrel DNS en el fet que "fan servir diferents tecnologies i és pràcticament impossible que una fallada pogués afectar-los a tots".

Internet depèn de 13 servidors, que depenen de 7 claus combinades, que tenen 7 persones

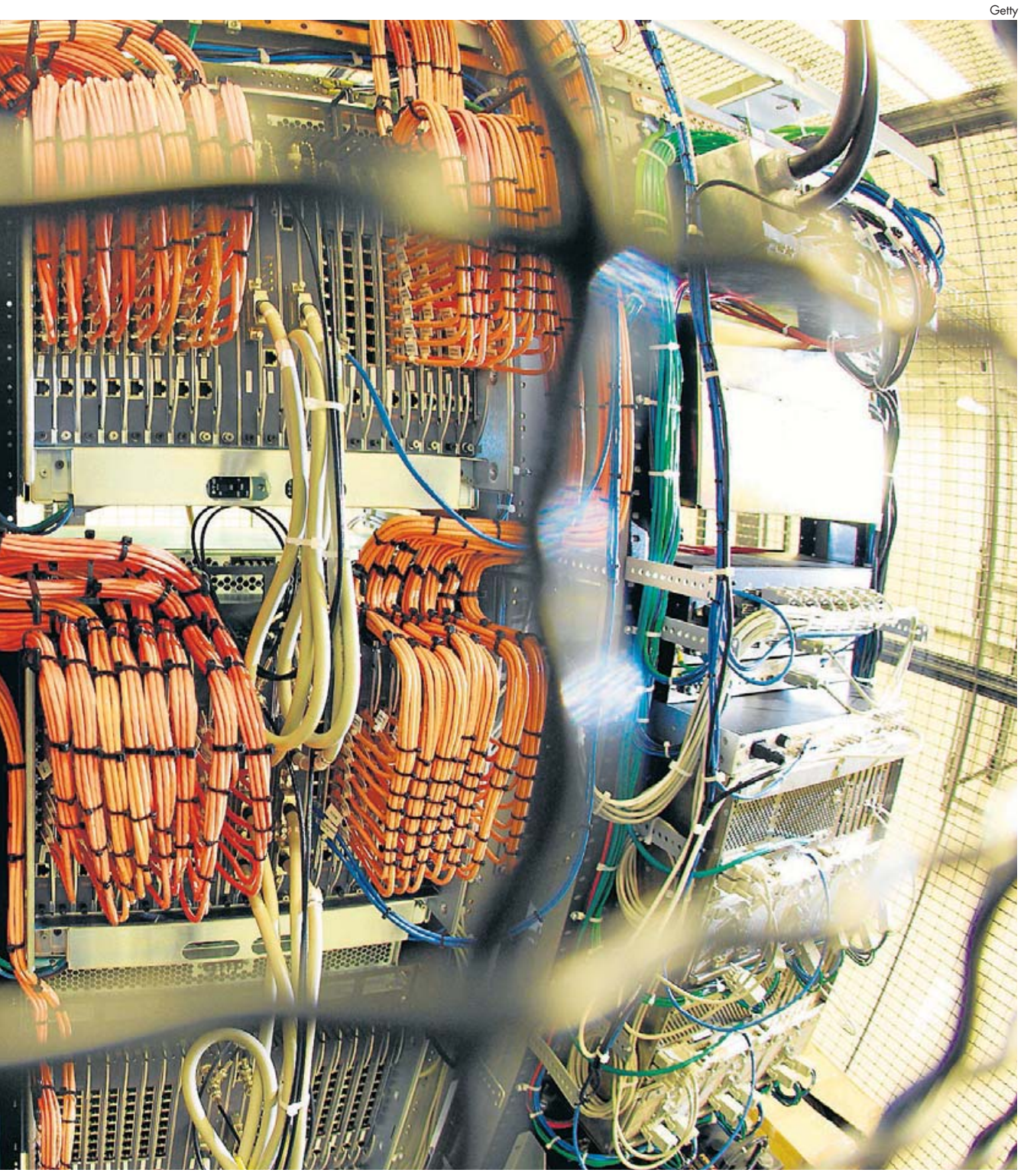
Els cables submarins

Una altra hipòtesi que podria posar en perill internet globalment seria la guerra. El 99% de la informació que viatja entre continents ho fa a través d'uns quants cables submarins. A finals de l'any passat, les autoritats nord-americanes van mostrar-se preocupades per la presència de submarins russos seguint la ruta d'alguns d'aquests cables. En una situació de tensió bèl·lica, destruir aquests cables implicaria tallar les comunicacions i internet entre continents i afectaria molts dels serveis que ara fem servir diàriament a través de la xarxa. Moltes de les grans empreses, els serveis de les quals fem servir gairebé constantment, com ara Apple, Google, Amazon i Facebook, tenen servidors al continent americà o a l'Àsia.

Si algú tallés tots o alguns dels més de 300 cables que creuen l'Atlàntic i el Pacífic, internet es convertiria en un caos. Per a Jordi Planas Manzano, que es depengui d'aquests gegants tecnològics "suposa un risc". "A mi la caiguda de Google m'afectaria molt, però, d'altra banda, l'ús que fa la joventut de la xarxa és molt més distribuït", explica Planas Manzano. L'expert de Sophos Iberia Jesús Gutiérrez detalla que si la fallada afectés tot el tronc de la xarxa simultàniament, "internet es disgregaria en segments aïllats i els usuaris d'una mateixa àrea geogràfica podrien comunicar-se entre si, però no podrien accedir a serveis allotjats en servidors d'altres zones, com ara aplicacions de missatgeria i xarxes socials proporcionades des de servidors als EUA, que no estarien disponibles a Europa".

Més enllà dels detalls tècnics, si es produís la caiguda d'internet, l'afectació social seria molt gran. Els sistemes bàsics, però, tindrien protocols

Getty



de seguretat per seguir funcionant. Xavier Gatius explica que "en el cas d'afectació a infraestructures classificades com a crítiques, hi ha mecanismes previstos per llei d'acord amb el que estableix la directiva europea 2008/114/CE, sobre la identificació i designació d'infraestructures crítiques europees". La informació i l'oci es veurien molt més perjudicats. Planas Manzano creu que "internet es fa servir majoritàriament per comunicar-se i per informar-se, i aquestes dues funcions quedarien afectades greument". A més, enumera alguns dels serveis dels quals quedaríem mancats: "Mapes per moure'ns per les ciutats, correu electrònic, agenda amb els avisos de cites, música, entreteniment multimèdia, compres *online*, planificació de les vacances... Seria fort, molt fort". I posa un exemple molt il·lustratiu: "És com l'alt executiu d'una multinacional que té secretari, cotxe, apartament, avió, departament fiscal, departament jurídic... i que, si el fan fora, es troba sol, sense casa, sense cotxe, probablement sense parella, i s'adona que sense els serveis de l'empresa no sap fer res".

Conseqüències econòmiques

A nivell econòmic, si la fallada es produís en els pròxims anys, basant-se en les estimacions d'evolució del comerç electrònic, les pèrdues es podrien acostar als 22.000 milions d'euros al dia. Els serveis financers mundials, com ara les borses, que depenen de les connexions globals, s'haurien d'aturar, amb unes pèrdues incalculables. Els serveis essencials, però, com ara hospitals i forces de seguretat, tenen xarxes pròpies que assegurarien el funcionament intern. Però seria impossible obtenir informació de fora.

L'impacte més gran a nivell d'usuari seria la impossibilitat de comunicar-nos o publicar la nostra vida digital. El diari *The Economist* va calcular les xifres diàries d'una parada d'internet i les dades són impressionants: deixaríem d'enviar gairebé 200.000 milions de correus electrònics; de pujar a Facebook i YouTube 12.000 milions de vídeos; ens quedaríem sense la informació proporcionada pels 3.000 milions de cerques que fem a Google, o sense els 500 milions de piulades que fem diàriament. Xavier Gatius està d'acord en l'efecte que tindria sobre la nostra vida quotidiana. "Si prenem com a referència que cada 60 segons a internet s'envien 21 milions de missatges de WhatsApp, es visualitzen 3 milions de vídeos a YouTube o es fan 2,4 milions de cerques a Google, es pot imaginar l'afectació que podria suposar estar sense internet durant tota una setmana", assegura.

Més enllà del que fem intencionadament a internet, hi ha la vida de les màquines que funcionen de manera autònoma comunicant-se en xarxa, com ara l'IoT (internet de les coses) i les ciutats intel·ligents. Els exemples són gairebé innumerables. Les càmeres de seguretat deixarien d'enviar senyal als ordinadors centrals, els cotxes connectats deixarien de comunicar-se amb els servidors i les ciutats intel·ligents es tornarien més tontes en quedar-se aïllades. A més, en la majoria d'oficines, treballar seria impossible perquè no es podria enviar informació entre les diferents seus, ni desar els arxius que generéssim als servidors, tret dels que tinguéssim a la mateixa empresa. Per a Jordi Planas Manzano, hi ha un tema generacional que també seria important. "Els *preinterneters* encara podríem recordar com es feien les coses abans, però penso que molts, sobretot els més joves, ho passarien molt malament", assegura.

La vida sense internet

Xavier Gatius cita el cas d'un periodista que va decidir viure sense internet durant un any per analitzar com canviava la seva vida. El reporter de la revista *The Verge* Paul Miller es va prestar a fer l'experiment amb l'objectiu de saber si som capaços de prescindir de tots els serveis i els avantatges que ens proporciona el món digital. "Passada l'eufòria inicial de descobriment d'altres maneres de relacionar-se amb les persones o amb la natura i d'utilitzar el temps –explica Gatius–, Miller va descobrir-se menys alliberat del que s'esperava i més aïllat del que hauria volgut". Realment va arribar a la conclusió que es podia viure sense internet, no de la mateixa manera, però que es podia anar passant i la seva vida diària no s'enfonsava. "És interessant observar com les coses essencials des del punt de vista social es poden fer amb internet i sense", conclou Gatius.

Tot i que la hipòtesi és socialment molt alarmant i literàriament molt llaminera, que ens puguem quedar sense internet resulta molt poc probable. Ni fins i tot situant-nos en la hipòtesi que s'intenti fer de manera intencionada i amb molts mitjans. L'expert en seguretat de Sophos Iberia Jesús Gutiérrez opina que "per la mateixa naturalesa d'internet no hi ha ningú que disposi dels recursos necessaris per llançar un atac contra la totalitat de la xarxa" que tingui la capacitat de deixar-la fora de combat. "La xarxa en essència no corre perill", sentencia Jesús Gutiérrez amb seguretat.

De moment, doncs, el perill d'una apocalipsi que plantejava J.J. Abrams a la sèrie *Revolution* està molt lluny de la realitat. ●