La ciberseguretat com a factor a considerar en els processos d'independència de nous estats al segle XXI

Jordi Mogas Recalde
Graduand en Informació i Documentació
Universitat Oberta de Catalunya
jmogasr@uoc.edu

Alexandre López-Borrull (tutor)
Professor als Estudis de Ciències de la Informació i la Comunicació
Universitat Oberta de Catalunya
alopezbo@uoc.edu

10 de juny de 2014

Treball d'investigació
Grau en Informació i Documentació

Resum
En els darrers anys s'han donat diversos casos de ciberatacs per motius polítics, cada cop més greus. Les nacions que volen esdevenir estats independents a principis del segle XXI tenen la responsabilitat de no descuidar la seva ciberseguretat per tal d'evitar-los. Aquests ciberatacs poden ser lleus però també poden representar una autèntica amenaça per als països atacats, com seria el cas d'un atac DDoS que paralitzi els serveis digitals com la banca electrònica o bé que afecti a les infraestructures crítiques nacionals, per exemple la xarxa elèctrica. Alguns dels atacs han estat fins i tot catalogats com a casos de ciberguerra. No podem preveure la gravetat de possibles ciberatacs a nacions que s'independitzin ni els efectes d'una ciberguerra, però els casos viscuts representen un toc d'alerta. En aquest article definim l'estat de la qüestió, repassem casos concrets i així posem en valor la tasca dels professionals de la informació.

Paraules clau: ciberseguretat nacional, ciberatac, ciberguerra, nació, independència.

Abstract
During the last years there have been several and increasingly serious cases of politically motivated cyber attacks. The nations that want to become independent states in the early twenty-first century have the responsibility to maximize their cybersecurity in order to avoid them. These cyber attacks can be mild but can also represent a real threat to the attacked countries, as in the case of a DDoS attack crippling digital services such as e-banking, or further affecting the national critical infrastructures, such as the electrical grid. Some of these attacks even have been classified as cyberwarfare. We can not predict the severity of possible cyber attacks to new independent nations nor the effects of a cyberwar, but the experienced cases are seen as a wake-up call. In this paper we define the state of the art, review real cases and so we value the role played by the information professionals.

Keywords: national cybersecurity, cyber attack, cyberwar, nation, independence.

1. Introducció

Conscients dels avenços tecnològics, la incremental dependència de la societat en les TIC i la constatació que els ciberatacs conformen una amenaça cada cop més preocupant, en aquest article -i com a professionals de la informació- volem donar resposta a la hipòtesi que les nacions amb aspiracions a convertir-se en nous estats del món als inicis del segle XXI necessiten extremar la seva ciberseguretat ja que, en molts casos, poden ser víctimes digitals dels seus opositors.

Per a demostrar-ho recordarem el valor de la informació en la societat moderna i com l'hem de considerar un actiu estratègic a protegir. Però no només la informació en si serà objecte d'estudi, les tipologies d'amenaça en l'ús de les tecnologies de la informació són molt variades i es poden llegir des de diferents prismes. Els estats utilitzaran hackers patriòtics per tal d'atacar els seus objectius mitjançant diversitat de tècniques que van de la intrusió i modificació de pàgines web, com va passar en moltes nacions independentistes a principis de segle, fins als casos més greus d'atacs DDoS que poden paralitzar nacions, com va passar a Estònia, el 2007, en la considerada Primera Ciberguerra Mundial.

Paradoxalment, els ciberatacs i la ciberseguretat és una preocupació general ja que es troba poc desenvolupada i legislada a nivell internacional. El professional de la informació es perfila en aquest escenari com un element d'alt valor. Les seves competències i habilitats quant a l'anàlisi, gestió i tractament de la informació i el coneixement poden ajudar en la identificació de febleses i perills de forma global; sovint cohesionant una línia interdisciplinària d'altres camps del coneixement com són la política, la informàtica o la intel·ligència militar. Els experts en ciències de la informació, doncs, han de ser considerades unes figures clau dels nous estats en favor de la seva seguretat; al servei de les noves institucions i serveis que s'han de consolidar.

2. Metodologia

La metodologia emprada per a l'elaboració d'aquest article ha estat revisió bibliogràfica, principalment en llengua anglesa. En referència a ciberseguretat nacional, ciberatacs i ciberguerra, s'ha seleccionat el coneixement que diversos acadèmics han acumulat en diferents bases de dades: Scopus, ISI Web of Knowledge, Google Scholar i altres recursos de la Biblioteca Virtual de la UOC. S'ha analitzat i filtrat el cos teòric dels articles així com tots aquells casos reals que corresponen a nacions que han viscut o busquen processos d'independència política. Finalment, s'ha contextualitzat i relacionat tota la informació recopilada i s'han afegit consideracions de casuístiques potencials per a donar resposta a la hipòtesi que la ciberseguretat és un factor a considerar en els processos moderns d'independència nacional.

3. Context informacional

Sabem que el poder de 'la informació' no és nou. Podem retrocedir fins el segle XII, per exemple, quan es documenta que el domini de la informació va permetre l'imperi mongol guanyar diverses batalles davant d'un enemic menys informat i, per tant, pitjor preparat (Arquilla i Ronfeldt, 1993).

Fet i fet, els conflictes polítics són un escenari clau per a entendre aquest actiu intangible. Fins i tot hem arribat a parlar de guerres de la informació, les primeres idees de les quals es remunten a la dècada de 1970 (Dunn, 2008), si bé les ciberamenaces d'aleshores eren accions de *hacking* poc rellevants, com ara robatoris bàsics de dades (Lakomy, 2013). Va ser a partir de l'experiència de la Guerra del Golf de 1991 quan estrategues militars van detectar una nova generació de conflictes en què la victòria ja no està garantida únicament per la força física, sinó també per la capacitat d'assegurar el domini de la informació (Dunn, 2010).

No debades, val a recordar que hi ha una creixent dependència en les tecnologies de la informació i la comunicació (TIC). Els usuaris d'Internet cada cop confiem més en aquest nou espai i creiem que és segur, però la realitat és que la manca de ciberseguretat pot afectar nacions senceres (Kallberg i Thuraisingham, 2013). Perquè les tecnologies dels països moderns també són ciberdependents. Les nacions que es volen alliberar d'estats que ara les controlen són, a més, un subjecte a considerar com a objectiu potencial davant les ciberamenaces per motius polítics.

4. Tipologies de ciberamenaça

4.1. De l'activisme al hacktivisme

Dorothy E. Denning (2001) diferencia entre l'activisme entès com a ús normal d'Internet en suport d'un programa o causa i el hacktivisme o tècniques de hacking contra llocs d'Internet amb la intenció d'interrompre les operacions normals sense causar danys greus.

L'activisme consisteix sobretot a difondre propaganda a través d'Internet (el millor exemple que podem esmentar és el *zapatismo* i la propaganda digital de l'EZLN) o bé mobilització (especialment en cas de revoltes polítiques). Recordem que les TIC es poden utilitzar per a difondre informació i també desinformació. Entenent que aquestes activitats lliures no posen en perill la ciberseguretat nacional d'una forma directa, ens centrarem en el hacktivisme.

Quan en català parlem de *hackers* acostumem a pensar en negatiu; és important conèixer l'ètica hacker entesa per molts informàtics i teoritzada per entesos com el filòsof finlandès Pekka Himanen, qui ens aclareix que el hacker és algú que té habilitats i bons coneixements de programació i que viu amb passió la informàtica sense esperit maligne. En aquest article, doncs, utilitzarem en tot moment l'anglicisme "hacker" (i derivats) per a referir-nos al que en català es podria denominar "furoner" perquè entenem que els hacktivistes actuen per a defensar uns valors i objectius particulars més que no pas de forma forassenyada o amb voluntat cega de fer mal. Reforcem així la contraposició al *cracker*, que seria el "pirata informàtic" associat al cibercrim.

Michael Dahan, a més, diferencia entre els hacktivistes i els hackers patriòtics: el primer sense motivacions tan clarament polítiques, mentre que el segon busca més repercussió mediàtica i rarament l'anonimat. Els hackers patriotes es veuen ells mateixos com a soldats irregulars que lluiten una guerra pel seu país. Fins i tot, a Israel i al món àrab el hacker patriòtic és sovint vist com un heroi defensor de l'honor nacional (Dahan, 2013). Nosaltres, tanmateix, considerarem el hacker patriota com a tipus particular de hacktivista. Poden cometre gran varietat de ciberatacs.

4.2. Ciberatacs

Un ciberatac consisteix en qualsevol acció destinada a minar les funcions d'una xarxa informàtica per a un propòsit de seguretat política o nacional (Hathaway *et al.*, 2012). Els ciberatacs són l'arma del segle XXI (Agresti, 2010) i cobreixen una àmplia gamma d'accions:

4.2.1. Bombardeig de correus electrònics

Bombardejar amb milers de missatges electrònics alhora pot provocar greus molèsties i perjudicis sobre l'afectat, com ara saturacions a la safata d'entrada i interferir en el funcionament normal del servei.

Un bombardeig de correus electrònics es va dur a terme l'any 1997 en contra el proveïdor de serveis d'Internet "Institute for Global Communications" (IGC), amb seu a San Francisco, per allotjar les pàgines web de la revista Euskal Herria, publicació que donava suport a la independència d'aquesta nació sense estat. Els atacants van reclamar que l'IGC donava suport al terrorisme ja que una secció de les pàgines web contenia material sobre ETA. Un article al diari francès Le Monde va afirmar que aquell atac representava un "conflicte sense precedents" i que "va obrir una nova era de la censura, imposada per l'acció directa de hackers anònims" (Denning, 2001).

En un altre cas, s'ha afirmat que els guerrillers tàmils van inundar les ambaixades de Sri Lanka amb milers de missatges de correu electrònic l'any 1998, amb prop de 800 correus al dia durant dues setmanes. És una de les accions de lluita nacional per part de la Liberation Tigers de Tamil Eelam, que ha estat lluitant per un país independent (Denning, 2001).

Malgrat tot, els avenços en filtratge d'spam fan pensar que aquesta tècnica d'atac ha quedat superada i obsoleta.

4.2.2. Substitució de contingut dels webs

Hi ha molts casos de hackers que accedeixen a llocs web i en substitueixen alguns dels continguts per altres de propis. Sovint, els missatges són polítics, com quan un grup de hacktivistes portuguesos va modificar els llocs web de 40 servidors d'Indonèsia, el setembre de 1998, per fer aparèixer el lema "Timor Oriental lliure" en grans lletres negres. D'acord amb The New York Times, els hackers també van afegir enllaços a llocs web que descriuen abusos de drets humans d'Indonèsia a l'antiga colònia portuguesa (Denning, 2001; Sharma *et al.*, 2011).

Un significant nombre de ciberatacs es van produir l'agost de 1999 quan l'aleshores president de Taiwan, Teng-hui Lee, va declarar en una entrevista a Deutche Welle que les relacions entre Taiwan i la Xina eren d'una natura 'd'estat a estat'. Hackers patriòtics xinesos van atacar webs governamentals taiwaneses per demostrar el seu enuig; aquestes van ser reemplaçades amb una imatge de la bandera xinesa i declaracions polítiques com "Taiwan és una part indivisible de la Xina" (Chang, 2011; Sharma *et al.*, 2011) o "Només existeix una Xina i només cal una Xina" (Denning, 2001). Com a venjança, hackers taiwanesos van respondre de la mateixa forma.

També podem recordar com el Kosovo Hackers Group, una coalició de hackers europeus i albanesos, va arribar a reemplaçar almenys cinc webs amb *baners* negres i vermells que deien: "Free Kosovo", durant el conflicte de 1999 (Denning, 2001).

En el mateix sentit, al setembre de 2000, hackers israelians van atacar i desfigurar llocs web propietat de Hezbollah i de l'Autoritat Nacional Palestina posant a la seva pàgina web principal

símbols nacionals israelians (la bandera d'Israel, grafia hebrea, i un enregistrament de l'himne nacional d'Israel). En la resposta palestina, es van atacar webs de finances i del govern israelià (Cornish *et al.*, 2009; Sharma *et al.*, 2011).

4.2.3. Redirecció de webs

És recursiu manipular el Domain Name Service (DNS) per a aconseguir redireccionar pàgines (Denning, 2001). Un truc favorit entre els hackers patriòtics durant la segona Intifada el 2001 era redirigir webs islàmics cap a webs de pornografia (Dahan, 2013).

El cas del conflicte d'Israel en confrontació als països àrabs és força més greu. Des de l'inici de la campanya de Gaza, grups de hackers del Marroc, Líban, Turquia i l'Iran han atacat llocs web israelians; un grup islàmic marroquí va irrompre al servidor del sistema de registre de domainthenet.com i va desfigurar més de 300 llocs web, incloent bancs, canals meteorològics, i notícies. En tractar d'accedir a aquests webs, els visitants eren redirigits a un lloc web que ofereix imatges de víctimes del delicte israelià contra Gaza, i missatges anti-israelians i anti-americans. Estudiants israelians van prendre represàlies atacant llocs web de Hamas (Sharma *et al.*, 2011).

4.2.4. Virus informàtics

Els virus i cucs informàtics, així com els troians, són utilitzats per a difondre missatges de protesta i danyar els sistemes informàtics. Totes elles són formes de codi maliciós (*malware*) que infecten els ordinadors i es propaguen a través de xarxes informàtiques.

El director interí de l'Oficina de Seguretat Nacional de Taiwan va dir que un ciberexèrcit xinès va llançar més de 3.100 atacs contra sistemes de govern de Taiwan el 2008. El seu propòsit es relaciona principalment amb el robatori de dades i informació sensible (Chang, 2011). Atacs similars ja s'havien produït amb anterioritat.

El cas de virus informàtic més destacat en la història, però, ha estat Stuxnet, que va infectar ordinadors en com a mínim 11 països diferents (Teixeira, 2012), si bé el 60% dels ordinadors infectats eren a l'Iran (Dunn, 2013). Es destaca que va atacar el sistema de control de la planta d'enriquiment nuclear a Natanz (l'Iran) i va desactivar temporalment 1.000 de les 5.000 centrifugadores operatives (Axelrod i Iliev, 2014). Es comporta diferent al malware alliberat d'intencions criminals: no roba informació i no embat els ordinadors infectats en els denominats *botnets* per llançar nous atacs, més aviat es busca un objectiu molt específic com ara sistemes SCADA que s'utilitzen per controlar i supervisar els processos industrials (Dunn, 2013). S'ha arribat a la conclusió que diversos països estaven darrere de l'atac, a destacar els EUA i Israel (Dunn, 2013). No és un conflicte polític però n'il·lustra la possible gravetat.

4.2.5. DDoS

La forma de ciberatac més habitual i eficaç en els darrers anys és la denegació de servei (DoS) o l'atac distribuït de denegació de servei (DDoS) consistent a efectuar un nombre elevat de peticions simultànies a un sistema informàtic de manera que aquest se sobrecarrega, no és capaç de donar resposta a l'elevat flux d'informació requerit i deixa de prestar servei.

El 2002, un lloc web construït pel "Taiwan Tea Party", que dóna suport a la independència de Taiwan, va patir DDoS continuades i greus que van paralitzar el seu funcionament. Una enorme

quantitat de correu brossa i de missatges procedents de la Xina van ser enviats a la pàgina web, aconseguint apagar-la (Chang, 2011).

El cas més destacat es remunta al 2007, quan es van produir atacs DDoS contra webs del govern d'Estònia i comercials. El fet que va motivar els atacs fou la decisió del govern estonià de moure un monument soviètic de la II Guerra Mundial al centre de Tallinn cap a un cementiri militar. Es van produir reaccions al món físic i també es van impulsar els ciberatacs (Czosseck *et al*., 2011). Aproximadament un milió d'ordinadors arreu del món van ser utilitzats per dur-lo a terme. Durant tres setmanes aquests atacs van tancar la ciberinfraestructura de l'antiga república soviètica. Es creu que l'ofensiva va ser conduïda per Rússia. Els successos van ser tan greus que s'han considerat la més destacada ciberguerra.

4.3. Ciberguerra

Arquilla i Ronfeldt (1993) són pioners a l'hora de conceptualitzar els riscs de la informació en la societat moderna i fan una primera diferenciació entre la infoguerra[1] (*netwar*) i la ciberguerra (*cyberwar*). La infoguerra (o guerra de la informació), per als autors, es refereix al conflicte relacionat amb la informació a gran nivell entre nacions o societats i inclou mesures de diplomàcia pública, propaganda i campanyes psicològiques, subversió política i cultural, interferència en els mitjans de comunicació entre altres accions que afectin les TIC. Reconeixen, això sí, que les infoguerres no seran militars ni violentes, tot i que poden abraçar dimensions que se sobreposin a la guerra militar. La ciberguerra, per contra, sí que es troba a nivell militar i té unes conseqüències majors.

Un greu atac o un conjunt d'atacs contra els sistemes informàtics d'un país amb la intenció de causar danys, i especialment amb finalitats polítiques, seran indicis per a parlar de ciberguerra. El millor test per a determinar quan un ciberatac és pròpiament considerat com a ciberguerra és si els resultats de tal atac comporten destrucció física –de vegades anomenat "efecte cinètic"– comparable a un atac convencional (Hathaway *et al.*, 2012).

El conflicte de Kosovo el 1999 s'ha caracteritzat com la primera guerra a Internet (Denning, 2001; Dunn, 2010).

Els ciberenfrontaments entre hackers xinesos i nord-americans, a més de moltes altres nacionalitats, el 2001, s'han etiquetat com la Primera Ciberguerra Mundial (Dunn, 2013). La causa va ser un reconeixement dels EUA i l'avió de vigilància que va ser obligat a aterrar en territori xinès després d'una col·lisió a l'aire amb un avió de combat xinès. Això va provocar l'inici de desfiguració a gran escala dels llocs web de la Xina i els Estats Units i atacs DDoS (Dunn, 2010).

Contradictòriament, són molts els autors que consideren els ciberatacs del 2007 contra Estònia (*veure DDoS*) com la primera ciberguerra.

4.4. Altres formes de ciberamenaça

Fins ara hem parlat de ciberatacs però dins de les amenaces que les nacions aspirants a formar-se com a estats trobem també dues activitats d'alt risc: el ciberespionatge i la censura d'Internet.

El ciberespionatge és un fenomen l'existència del qual és obertament reconeguda per part de diversos estats. És a dir, aquelles nacions aspirants a separar-se d'entitats que les dominen han

d'actuar conscients que els serveis d'intel·ligència oponents tindran tota la informació estratègica a què els sigui possible accedir.

D'altra banda, la censura. Alguns governs són reticents a exposar els seus ciutadans a material ofensiu que pot ser moralment, cultural o política perjudicial. El seu afany per dominar el ciberespai té clarament una voluntat política dominadora i pot intentar ofegar la publicitat i difusió d'activistes en favor de nous estatus polítics. Una de les censures més dures és la xinesa, que pot afectar el Tibet, Taiwan, Hong Kong i altres regions que reclamen més sobirania.

També podem recordar l'actitud de l'Estat espanyol, l'agost de 2002, quan fa forçar el tancament del lloc web de l'organització basca Batasuna. "En aquest cas es va produir un curiós conflicte jurisdiccional i fronterer, perquè el lloc web estava allotjat en servidors ubicats a França i als Estats Units" (López-Borrull, 2005).

5. Ciberseguretat nacional: contextualització

La ciberseguretat és considerada una de les claus en la seguretat nacional i, fins i tot, una prioritat nacional (Agresti, 2010). Consisteix a garantir la seguretat del ciberespai i prevenir qualsevol de les ciberamenaces i ciberatacs coneguts.

A nivell internacional, una de les conclusions de l'estudi "*Nineteen national cyber security strategies"* (NCSS) és que de tots els països analitzats només deu han definit o descrit el concepte de ciberseguretat en la seva NCSS i cadascun d'ells ho ha fet d'una manera diferent. Aquesta manca de consens en la definició portarà a confusió entre nacions quan es discuteixin enfocaments internacionals sobre les amenaces globals del ciberespai (Luiijf *et al.*, 2013).

Quan parlem de qualsevol tipus de ciberamenaces en la conceptualització de nous estats del món podem afirmar que els hacktivistes són la figura més important ja que duen a terme els ciberatacs, per iniciativa pròpia i de forma individual o bé col·laborant en grups sociopolítics. Per lliure o bé al servei d'un govern. De fet, associem les guerres amb els estats; en el cas de ciberguerres també pot existir el lligam, però els estats i governs utilitzaran hacktivistes individuals (Teixeira, 2012).

Un estat bel·ligerant podria escollir la ciberguerra com a tàctica per diferents motius, a destacar (Jenik, 2009): Permet eximir responsabilitats (no mobilitzar soldats al front, posant la vida en risc), és més econòmica que una arma convencional, és particularment difícil per a les administracions nacionals vigilar i protegir les seves fronteres digitals, i a més costa culpar un estat com a responsable dels ciberatacs.

Parlar de ciberseguretat nacional, no obstant, no deixa de connotar una limitació geogràfica que les TIC ens obliguen a superar. Els esforços realitzats en la millora de la protecció dels sectors econòmics nacionals crítics no es poden fer de manera aïllada respecte a la resta del món perquè les ciberamenaces creuen fronteres (Colesniuc, 2013). Quant a legislació, caldria que la regulació sobrepassés les fronteres estatals; es presenta com la gran paradoxa d'Internet el fet que mentre les lleis estan vinculades a un entorn geogràfic, l'accés a la informació no ho està (López-Borrull, 2005).

El fet de creuar fronteres fa la ciberseguretat una prioritat global i responsabilitat compartida (Agresti, 2010) que requereix una activa cooperació internacional (Czosseck et al., 2011). L'estudi

sobre les NCSS (Luiijf *et al.*, 2013) arriba a conclusions sobre la necessitat de tractar l'afer amb prisma internacional però es palesa que encara calen avenços. Així, ens recorden la necessitat que les nacions aprenguin unes de les altres, donada la natura global de la ciberseguretat. Constaten que a cadascuna de les NCSS li manquen elements presents a les altres.

Els hackers patriòtics poden encendre una ciberguerra entre nacions rivals amb el potencial de treure aquests estats a un conflicte armat real, tot i que normalment són els conflictes reals que es complementen digitalment (Dahan, 2013). Per posar algun exemple, davant el conflicte entre Rússia i Geòrgia per Ossètia del Sud es va afirmar que, cada cop més sovint, els ciberatacs als servidors del govern assenyalen un atac físic a la vista (Cornish *et al.*, 2009) i les accions de Kremlin Kids, hackers privats, suposadament van tancar l'Internet georgià durant la invasió russa d'Ossètia del Sud (Hathaway *et al.*, 2012).

Recordem també que el ciberespai no és només virtual ja que també es compon de servidors, cables, ordinadors, satèl·lits, etc. (Dunn, 2013).

El "problema d'atribució" és un altre factor destacable. Es refereix a la dificultat de determinar clarament aquells responsables inicials d'un. Els estats també poden negar de forma plausible estar-hi involucrats (Dunn, 2013; Kallberg i Thuraisingham, 2013). Fins i tot en els atacs contra Estònia, que es van donar a conèixer i van tenir un alt nivell de participació internacional, només es van traduir en la detenció i enjudiciament d'un ciutadà estonià, Dmitri Galushkevich (Farivar, 2009).

La ciberseguretat dels estats no està regulada per lleis nacionals ni internacionals (Lakomy, 2013). El monogràfic "*The law of cyber-attack*" (Hathaway *et al.*, 2012) ens confirma que les lleis existents només s'adrecen a un petita fracció dels ciberatacs potencials, i que gran part de la legislació aplicada no va ser dissenyada per a aquest propòsit. Hi ha diversos organismes que regulen els ciberatacs de forma directa encara que no completa; és necessari crear un nou marc legal a nivell internacional, i les noves nacions no poden obviar aquesta necessitat també a nivell nacional.

De la legislació aplicable existent, destaquem l'article 2(4) de la Carta de l'ONU, que estableix que els estats membres "s'han d'abstenir en les seves relacions internacionals de l'amenaça o ús de la força contra la integritat territorial o la independència política de qualsevol estat, o en qualsevol altra forma incompatible amb els Propòsits de les Nacions Unides", però recorda dues excepcions: accions preses en el marc d'operacions de seguretat col·lectiva i mesures adoptades en defensa pròpia. Caldria saber interpretar el paper que juguen les nacions sense estat en la seva lluita i defensa per la sobirania nacional.

6. Gravetat dels ciberconflictes polítics

S'identifiquen diverses tipologies de conseqüències als ciberatacs en general: efectes tecnològics, efectes psicològics (basats en la por i desconfiança), pèrdua financera (caigudes de negocis o danys costosos), pèrdua d'informació (robatori i publicació d'informació sensible), pèrdua de privacitat (vulneració d'informacions personals, espionatge, etc.) i pèrdua de sistemes físics (atacs a les infraestructures crítiques) (Sharma *et al.*, 2011; Axelrod i Iliev, 2014).

6.1.1. Infraestructures crítiques

La literatura especialitzada identifica tres tipus d'infraestructures: la regular, l'especial i la crítica. Aquesta última té un paper important en l'estabilitat i la seguretat dels sistemes i processos desplegats a nivell econòmic, social, polític i militar. (Popa, 2013).

Les infraestructures crítiques es defineixen generalment com a sistemes o actius vitals per a un país en què qualsevol incapacitat o destrucció d'aquests sistemes tindrien un impacte debilitant en la seguretat, l'economia, la salut i/o la seguretat pública nacional. A finals dels '80, van començar a aparèixer documents que va fer una clara relació entre les amenaces informàtiques i les infraestructures crítiques, i l'11 de setembre de 2001 va augmentar la consciència de la vulnerabilitat i la necessitat de protegir-les (Dunn, 2008). El pensament sobre vulnerabilitat dels sistemes ha evolucionat cap a la necessitat de la protecció d'infraestructures crítiques (Collier i Lakoff, 2008). En general, són un blanc fàcil ja que tenen una àmplia distribució geogràfica i en gran part resta sense protecció (Goel, 2011).

La identificació de quines són les infraestructures crítiques pot variar lleugerament entre països, però hi ha unanimitat en afirmar que els sectors més importants són l'energia, les TIC, el subministrament d'aigua, el transport i el sistema financer. De fet, però, totes les infraestructures bàsiques de la nostra societat aprofiten els avantatges dels sistemes TIC; i les TIC depenen de la xarxa elèctrica. Tot depèn de l'energia elèctrica; és crítica (Stevenson i Prevost, 2013).

6.1.2. La cinquena dimensió

Tan rellevant és el paper que els militars volen jugar en aquest àmbit que als Estats Units han sumat un cinquè domini als conflictes armats: a terra, mar, aire i espai ara s'afegeix el ciberespai. Un exemple destacat d'ús militar del ciberespai ha estat Stuxnet.

6.1.3. Teoria dels efectes catastròfics

Molts acadèmics han fet supòsits o estimacions d'efectes catastròfics a causa de grans ciberatacs o de ciberguerra. Per exemple que "el mal funcionament o la pèrdua total de les xarxes públiques d'energia, el sistema bancari, les cadenes de subministrament o de l'administració pública pot causar enormes danys econòmics i afectar nacions senceres massivament" (Skopik *et al.*, 2012).

També s'ha estimat que un ciberatac massiu podria deixar el 70% dels EUA en completa foscor sense energia elèctrica durant sis mesos (Sharma *et al.*, 2011). O que si l'energia i altres serveis poguessin ser apagats per un període de tres mesos, a causa d'un atac DDoS, el dany podria ser equivalent a 40 o 50 grans huracans colpejant alhora (Cornish *et al.*, 2009).

Centrant-nos en casos reals, Lucent Technology, una empresa que realitza negocis amb Israel, va ser atacada per un grup palestí anomenat Unitat. A la tardor de 2000, la ciberguerra entre grups pro-israelians i pro-palestins es va traduir en una caiguda d'un servidor que va fer que el mercat de valors d'Israel disminuís en un 8% (Sharma *et al.*, 2011).

A causa de la ciberguerra contra Estònia, les pàgines web del banc es van fer inaccessibles, paralitzant la major part de l'activitat financera d'Estònia. En els dies que es va trigar a lluitar contra l'atac, és probable que el país perdés bilions d'euros en la reducció de la productivitat i el temps de caiguda dels negocis (Jenik, 2009). Com a conseqüències crítiques concretes, es diu que la línia d'emergència per trucar a una ambulància o un camió de bombers estava fora de servei durant una hora (Hathaway *et al.*, 2012).

En un altre cas real, al gener de 2009, dos dels quatre proveïdors d'Internet del Kirguizistan (independitzat de l'antiga URSS) van ser atacats mitjançant DDoS. Les conseqüències van ser notables: es va discapacitar fins a un 80% de tot el tràfic d'Internet. El fet que el país tingui poca implementació de TIC va fer-lo passar desapercebut als mitjans de comunicació (Jenik, 2009; Farivar, 2009).

6.1.4. Teoria dels efectes quasi nuls

Myriam Dunn, especialista en ciberseguretat, per contra, defensa que els possibles efectes no tenen importància: "En tota la història de les xarxes informàtiques, hi ha hagut molt pocs exemples d'atacs o altres tipus d'incidents que hagin tingut el potencial per sacsejar a tota una nació o causar un xoc global" (Dunn, 2013). A més, afirma, els atacs de hacktivisme tenen un impacte polític molt qüestionable i, per tant, no estaria justificat considerar el hacktivisme com a amenaça a la seguretat nacional (Dunn, 2010).

En el cas d'Estònia, 2007, Ene Ergma, portaveu del parlament d'Estònia, va comparar els ciberatacs amb una explosió nuclear. Ara bé, aquesta qualificació ha estat contraatacada amb afirmacions que si els atacants haguessin volgut danys molt més greus no haurien cessat les seves activitats tres setmanes més tard de començar. Els atacs, doncs, significaven un missatge més que no pas una guerra (Farivar, 2009).

6.1.5. Morts en ciberguerra

Si res ha quedat clar és que la ciberguerra canvia el concepte tradicional que implica una guerra tradicional. De la mateixa manera, parlar de ciberguerra no connota la pèrdua massiva de vides humanes. Dunn (2010) fins i tot ironitza que els ciberatacs resultants amb morts segueixen sent tema de pel·lícules de Hollywood o la teoria de la conspiració.

D'altra banda, però, podem recordar el cas on l'any 2012 un hacker saudí va alliberar informació de targetes de crèdit d'almenys mig milió d'israelians a través de pàgines web. El tema va acabar amb la sospitosa mort del hacker en qüestió (Dahan, 2013). Seria aquest un cas de mort en ciberguerra?

7. Previsió de casuístiques

Fins ara hem analitzat els perills a què fan front els països que es volen independitzar mitjançant la constatació teòrica i de fets reals. Ara bé, l'objectiu que tenim és poder saber com i en quina mesura aquests casos passats afectaran als nous estats venidors. Aquestes hipòtesis no seran confirmables fins que els successos escriguin la història, però bé és cert que els professionals de la informació estem capacitats per a oferir una exposició d'escenaris plausible.

El primer que volem recordar és que al món hi ha desenes de nacions sense estat que amb major o menor suport social lluiten per independitzar-se d'estats que consideren aliens. Aquestes nacions són totes elles diferents i per tant no podem oferir respostes homogènies, però sí podem identificar trets característics que ajudaran a identificar el nivell de risc que cadascuna d'elles pateix.

Hi ha països que depenen fortament de les TIC i, per tant, durant les reclamacions sobiranistes i els seus processos constituents com a estats lliures hauran d'extremar la precaució per a evitar

ciberatacs com els exposats. Nacions que pateixen aquesta amenaça són, per exemple, Escòcia, Catalunya, el Quebec, Flandes, etc. Per contra, hi ha altres països que no depenen en absolut de la tecnologia i fins i tot la supressió temporal de la xarxa elèctrica no comportaria per a la majoria dels ciutadans un impacte catastròfic. Un bon exemple és la RASD (Sàhara Occidental).

Un altre factor rellevant és el nivell d'acceptació de l'estat dominador. El Quebec ha realitzat ja dos referèndums, en què per poca diferència han escollit romandre al Canadà; Escòcia referendarà la seva voluntat política respecte al Regne Unit el proper 18 de setembre; Flandes, Nova Caledònia i Bougainville, decidiran en sengles referèndums si s'independitzen de Bèlgica, França i Papua Nova Guinea, respectivament. Per a tots aquests països on existeix acord es pot preveure que els ciberatacs no representaran una amenaça a la ciberseguretat. Per contra, les nacions que no compten amb el suport d'un estat opressor és molt probable que vegin les seves xarxes informàtiques atacades, pàgines web hackejades i la seva infraestructura crítica amenaçada. Catalunya és advertida que la independència no és permesa i l'Estat espanyol podria veure's avalat a emprendre o donar suport ocult a accions que defensin la seva integritat territorial.

Recordem també que les nacions poden declarar-se països independents (esdevenen estats *de facto*) però això no els reconeix com a estats legalment lliures (o estats *de iure*). Posem per cas Ossètia del Sud, que s'independitzà el 1991 però és al s. XXI que alguns països la reconeixen. Destaquem, així, que hi ha països no reconeguts de manera general: oblidant altres factors, Murrawarri és un país independitzat d'Austràlia i de la Commonwealth l'any 2013 però en tractar-se d'una nació tribal aïllada no ha rebut atenció mediàtica ni política. Així mateix, Azawad és un país independitzat de Mali el 2012, però no compta amb reconeixement internacional.

Moltes nacions sense estat ho són perquè històricament el seu territori ha estat esquarterat per països invasors; o bé guerres posteriors els han reconfigurat. Així, si ens fixéssim només en el repartiment territorial podríem afirmar que el Kurdistan (amb gran extensió i població, dividit en quatre estats) és més susceptible de patir majors i més greus atacs que no nacions com ara Còrcega (més petita i només dominada per França).

Per últim, és imprescindible destacar que el suport social és clau per a preveure possibles ciberatacs. Nacions com Galiza (actualment a l'Estat espanyol), Occitània (a França) o Silèsia (a Polònia) tenen minories que demanen llibertat o un reconeixement diferenciat dins l'estat actual. Aquestes minories no poden assolir alts nivells de potencialitat i les respectives nacions corren menys perill que altres on existeix una confrontació política com a Catalunya; en gran mesura perquè ja són nacions dominades i assimilades.

8. Conclusions

Les nacions sense estat que a l'inici del segle XXI compten amb cert suport social per a canviar-ne l'estatus polític no poden ignorar que existeix una amenaça real de patir desfetes per la via cibernètica. Hacktivistes i estats detractors utilitzaran les TIC per a posicionar-se amb avantatge. Especialment en aquells casos en què les independències no són pactades es pot preveure que existiran ciberatacs més greus.

Tal com hem repassat, aquests ciberatacs poden prendre gran varietat de formes, i moltes vegades una mateixa nació és afectada per diverses d'elles. Fa una dècada predominava la intrusió en pàgines web estratègiques (govern, empreses nacionals, etc.) per a redireccionar-les o alterar-ne el

contingut, el robatori d'informació confidencial o l'ús malintencionat de virus informàtics. A hores d'ara han proliferat altres tècniques i objectius que representen una alerta superior: d'atacs DDoS que saturin els serveis fins a possibles ciberguerres que posin en perill les infraestructures crítiques com ara la xarxa elèctrica.

Ens ha quedat clar que malgrat l'exageració literària que s'ha fet dels casos viscuts, els efectes no poden ser tan catastròfics; o si més no de moment no s'han demostrat. Això no obstant, la manca de ciberseguretat es convertiria en una vulnerabilitat que podria plantejar situacions no gens desitjables. Hem pogut confirmar la hipòtesi inicial: Els països que s'independitzin properament hauran de vetllar per la seva ciberseguretat. És un dels reptes de la societat moderna.

D'altra banda, l'article ens fa reflexionar de qui són les competències davant d'aquest tipus d'escenaris. És evident que els ciberatacs poden variar molt en grau i direcció però el que centra més atenció són els ciberatacs que perpetrin els estats dominants envers els dominats: en general tenen més recursos i poden sentir-se'n moralment avalats. La ciberseguretat, per tant, s'ha de plantejar des dels governs i entitats que formaran els nous estats. Una bona estratègia i planificació serà de vital importància per no passar per alt les possibles vulnerabilitats que podrien patir els serveis digitals i les infraestructures crítiques.

Aquesta feina correspon al treball conjunt de diversos organismes i tipus de professionals: govern, equips de resposta davant d'emergències informàtiques (CERT), centres de seguretat de la informació (CSI), protecció dels centres de processament de dades (CPD), serveis d'intel·ligència nacional (CNI, CESICAT, etc.), la col·laboració activa d'organismes tant del sector públic com del privat, etc. Alguns organismes requereixen informàtics però en la majoria dels casos els professionals de la informació i del seu tractament, com els titulats en Informació i Documentació, poden desenvolupar una feina cabdal en el procés.

9. Bibliografia

Agresti, William W. (2010). "The Four Forces Shaping Cybersecurity". *Computer*, vol. 43, núm. 2 (feb.), p. 101-104. Online: <http://www.computer.org/csdl/mags/co/2010/02/mco2010020101-abs.html> [Consulta: 27/03/2014]

Arquilla, John; Ronfeldt, David (1993). "Cyberwar is Coming!". *Comparative Strategy*, vol. 12, núm. 2, p. 141-165. Online: <http://www.rand.org/pubs/reprints/RP223.html> [Consulta: 28/03/2014]

Axelrod, Robert; Iliev, Rumen (2014). "Timing of cyber conflict". *Proceedings of the National Academy of Sciences of the United States of America*, vol. 111, núm. 4 (gen.), p. 1298-1303. Online: <http://0-www.ncbi.nlm.nih.gov.cataleg.uoc.edu/pmc/articles/PMC3910638/> [Consulta: 2/04/2014]

Chang, Yao-chung (2011). "Cyber Conflict Between Taiwan and China". *Strategic Insights*, vol. 10, núm. 1, p. 26-35. Online: <https://www.academia.edu/1827575/Cyber_Conflict_Between_Taiwan_and_China> [Consulta: 30/03/2014]

Colesniuc, Dan (2013). "Cyberspace and Critical Information Infrastructures". *Informatica Economica*, vol. 14, núm. 4, p. 123-132. Online: <http://0-search.proquest.com.cataleg.uoc.edu/docview/1492882481?accountid=15299> [Consulta: 6/04/2014]

Collier, Stephen J.; Lakoff, Andrew (2008)."The vulnerability of vital systems: How 'critical infrastructure' became a security problem", p. 17-39. Online: <https://ethz.academia.edu/MyriamCavelty> [Consulta: 30/03/2014]

Cornish, Paul; Hughes, Rex; Livingstone, David (2009). "Cyberspace and the National Security of the United Kingdom: Threats and responses". London: Chatham House. Online: <http://www.chathamhouse.org/sites/default/files/public/Research/International%20Security/r0309cyberspace.pdf> [Consulta: 4/04/2014]

Cutts, Andrew (2009). "Warfare and the continuum of cyber risks: A policy perspective". *Cryptology and Information Security Series*, vol. 3, p. 66-76. Online: <http://www.ccdcoe.org/publications/virtualbattlefield/04_CUTTS_national%20cyber%20risk%20v2.pdf> [Consulta: 30/03/2014]

Czosseck, Christian; Ottis, Rain; Talihä, Anna-Maria (2011). "Estonia after the 2007 cyber attacks: Legal, strategic and organisational changes in cyber security". *10th European Conference on Information Warfare and Security 2011, ECIW 2011*, p. 57-64. Online: <http://0-search.proquest.com.cataleg.uoc.edu/docview/1010350858> [Consulta: 3/04/2014]

Dahan, Michael (2013). "Hacking for the homeland: Patriotic hackers versus hacktivists". *8th International Conference on Information Warfare and Security, ICIW 2013*, p. 51-57. Online: <http://issuu.com/acpil/docs/9781909507081_iciw_2013> [Consulta: 25/03/2014]

Denning, Dorothy E. (2001). "Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy". *Networks and Netwars: The Future of Terror, Crime, and Militancy*, Santa Monica, CA: RAND. Online: <http://www.rand.org/content/dam/rand/pubs/monograph_reports/MR1382/MR1382.ch8.pdf> [Consulta: 28/03/2014]

Dunn Cavelty, Myriam (2008). "Like a phoenix from the ashes: The reinvention of critical infrastructure protection as distributed security", p. 40-62. Online: <https://ethz.academia.edu/MyriamCavelty> [Consulta: 30/03/2014]

Dunn Cavelty, Myriam (2013). "Cyber-security". *Contemporary Security Studies*, edited by Alan Collins, p. 362-378. Online: <https://ethz.academia.edu/MyriamCavelty> [Consulta: 30/03/2014]

Dunn Cavelty, Myriam (2010). "Cyberwar" a George Kassimeris and John Buckley (eds), *The Ashgate Research Companion to Modern Warfare*, England: Ashgate Publishing, p. 123-144. Online: <https://ethz.academia.edu/MyriamCavelty> [Consulta: 30/03/2014]

Farivar, Cyrus (2009). "A brief examination of media coverage of cyberattacks (2007-present)". *Cryptology and Information Security Series*, vol. 3, p. 182-188. Online:

<http://www.ccdcoe.org/publications/virtualbattlefield/13_FARIVAR%20Web%20War%20One.pdf> [Consulta: 30/03/2014]

Goel, Sanjay (2011). "Cyberwarfare: Connecting the dots in cyber intelligence". *Communications of the ACM*, vol. 54, núm. 8 (ago.), art. núm. 1978569, p. 132-140. Online: <http://0-dl.acm.org.cataleg.uoc.edu/citation.cfm?doid=1978542.1978569> [Consulta: 3/04/2014]

Hathaway, O.A.; Crootof, R.; Levitz, P.; Nix, H.; Nowlan, A.; Perdue, W.; Spiegel, J. (2012). "The law of cyber-attack". *California Law Review*, vol. 100, núm. 4 (ago.), p. 817-885.

Jenik, Aviram (2009). "Cyberwar in Estonia and the Middle East". *Network Security*, vol. 2009, núm. 4 (abr.), p. 4-6.

Kallberg, Jan; Thuraisingham, Bhavani M. (2013)."State actors' offensive cyberoperations: The disruptive power of systematic cyberattacks". *IT Professional*, vol. 15, núm. 3, art. núm. 6471711, p. 32-35. Online: <http://0-ieeexplore.ieee.org.cataleg.uoc.edu/stamp/stamp.jsp?tp=&arnumber=6471711> [Consulta: 3/04/2014]

Lakomy, Miron (2013). "The significance of cyberspace in Canadian security policy". *Central European Journal of International and Security Studies*, vol. 7, núm. 2, p. 62-79. Online: <http://static.cejiss.org/data/uploaded/1383830201710030/cejiss_7.2_eJournal.pdf> [Consulta: 2/04/2014]

López-Borrull, Alexandre (2005). "Censura de continguts a Internet: riscos i oportunitats". *BiD. Textos universitaris de biblioteconomia i documentació*, núm. 14. Online: <http://eprints.rclis.org/18740/> [Consulta: 07/05/2014]

Luiijf, Eric; Besseling, Kim; Graaf, Patrick de (2013). "Nineteen national cyber security strategies". *International Journal of Critical Infrastructures*, vol. 9, núm. 1-2, p. 3-31. Online: <http://inderscience.metapress.com/content/c76007176206246m/> [Consulta: 30/03/2014]

Popa, Vasile (2013). "Critical infrastructure protection within the European Union". *Journal of Defense Resources Management*, vol. 4, núm. 1, p. 153-158. Online: <http://search.proquest.com/docview/1372955026?accountid=15299> [Consulta: 6/04/2014]

Sharma, A.; Mahoney, W.; Sousan, W.; Qiuming Zhu; Laplante, P. (2011). "Dimensions of Cyber-Attacks: Cultural, Social, Economic, and Political". *IEEE Technology and Society Magazine*, vol. 30, núm 1 (mar.), p. 28-38. Online: <http://0-ieeexplore.ieee.org.cataleg.uoc.edu/xpl/articleDetails.jsp?arnumber=5725605> [Consulta: 29/03/2014]

Skopik, Florian; Bleier, Thomas; Fiedler, Roman (2012). "Information management and sharing for national cyber situational awareness". *14th Information Security Solutions Europe Conference. Securing Electronic Business Processes*, p. 217-227. Online: <http://www.flosko.at/ait/2012_isse.pdf> [Consulta: 30/03/2014]

Stevenson, James; Prevost, Richard J. (2013). "Securing the grid: Information sharing in the fifth dimension". *Electricity Journal*, vol. 26, núm. 9 (nov.), p. 42-51. Online: <http://0-www.sciencedirect.com.cataleg.uoc.edu/science/article/pii/S1040619013002388> [Consulta: 2/04/2014]

Teixeira Fernandes, José Pedro (2012). "A ciberguerra como nova dimensão dos conflitos do século XXI". *Relações internacionais*, núm. 33, p. 53-69. Online: <http://www.scielo.gpeari.mctes.pt/pdf/ri/n33/n33a05.pdf> [Consulta: 4/04/2014]

Notes

[1] En aquest article seguim la traducció que Teixeira (2012) fa de *netwar* al portuguès: *infoguerra*.