Alumne: **Jordi Mogas Recalde**
jmogasr@uoc.edu

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

1. i 2. Sobre la ciberseguretat i els professionals de la informació[1]

*1. En el resum esmentes que es posa en **valor** la tasca dels professionals de la informació. Concreta quin és aquest valor i com és recollit a la bibliografia.*

*2. Quin perfil creus que hauria de tenir un equip de resposta a un ciberatac (dret, informàtica, Informació i Documentació)? Quines **competències** pròpies dels professionals de la informació (per exemple, les ofertes en el propi grau) caldria considerar.*

Sobre el 'valor' a la bibliografia

L'article que presento té com a principal objectiu la revisió bibliogràfica referent a la ciberseguretat, amb especial atenció als ciberatacs a països que s'han independitzat en els darrers anys i els que ho poden fer properament. S'ha creat com a treball d'investigació que justifica l'abast dels estudis en ciències de la informació, si bé es focalitza pretesament en l'objectiu adés esmentat. En conseqüència, el cos de l'article insinua el valor de la nostra professió de forma implícita i s'explicita tan sols a la introducció i a la conclusió.

La Informació i Documentació no és una disciplina aïllada de la resta de coneixements (Cobarsí i López-Borrull, 2009). En una investigació sobre les 480 assignatures de mostra d'11 plans d'estudis en Informació i Documentació de diverses universitats s'ha detectat la presència de més de 40 àrees de coneixement o departaments diferents (Moneda, 2014). A la pregunta 4, sobre la possible publicació de l'article, comprovarem com la bibliografia consultada es basa en publicacions científiques de camps com la informàtica, l'economia, etc. i un percentatge mínim s'ha recuperat dels estudis en Informació i Documentació.

No podem justificar el valor del professional de la informació al meu article només en base a la bibliografia utilitzada. En aquesta defensa tindrem l'ocasió de demostrar que el valor arguït prové sobretot de la relació entre el treball d'investigació i allò estudiat al grau.

Professionals de la informació?

És a bastament acceptat que vivim en una societat de la informació i del coneixement, on aquests intangibles són els actius clau per a l'avenç i la innovació. No ha de costar fer entendre que calen

[1] Deguda la convergència conceptual he preferit ajuntar les preguntes 1 i 2 oferint una resposta cohesionada. Així mateix, he valorat positivament la reordenació de les respostes contingudes.

persones capacitades per a assumir-ne els rols derivats. Això no obstant, diferents estudiants del Grau en Informació i Documentació de la UOC hem constatat que molta gent aliena al nostre camp del coneixement no sap realment l'abast dels estudis: hi ha qui no se'n fa a la idea i molts ens relacionen únicament amb la biblioteconomia o la documentació tradicionals.

L'any 1988 la FID va passar a anomenar-se "International Federation for Information and Documentation"; la rellevància del concepte 'informació' ja era considerada. D'aleshores ençà, la creixent dependència en TIC i la proliferació d'eines 2.0 i de *cloud computing* així com l'avenç incessant en les possibilitats dels sistemes d'informació perfilen la necessitat de professionals especialitzats. Podríem considerar-nos una disciplina moderna, fins i tot nova (en el seu estat de desenvolupament actual), que concentra les capacitats i habilitats de tractament i gestió de la informació de què fins ara s'han encarregat de manera menys organitzada i poc enfocada altres ciències. En el cas de la ciberseguretat hom pot associar-ne les responsabilitats als departaments informàtics però el cert és que nosaltres ocupem un espai propi.

Relació amb la informàtica

Es diu que "la informàtica és la ciència que estudia mètodes, processos, tècniques, amb la finalitat d'emmagatzemar, processar i transmetre informació i dades en format digital".[2] Etimològicament prové de la fusió dels mots "informació" i "automàtica".[3]

El professional de la informació té una estreta relació amb la informàtica. Moneda (2014) constata que aquesta àrea en l'oferta acadèmica dels nostres estudis representa vora el 8% del total, precedit només per les assignatures de Biblioteconomia i Documentació; percentatge que en el meu cas concret és superior. A la UOC estudiem assignatures com ara Bases de Dades, Enginyeria del Programari, Tecnologies de la Informació, Sistemes d'Informació a l'Organització, etc. De fet, jo he optat per la menció de "Gestió de Sistemes d'Informació" que comparteix assignatures amb estudiants del Grau en Enginyeria informàtica (e.g., Gestió Funcional de Serveis de SI/TI).

Ara bé, el perfil general de l'informàtic és més tècnic (programació, sistemes operatius, xarxes, etc.) i el nostre es centra en el tractament de la informació i la seva consideració com a actiu estratègic. Si l'informàtic sap desenvolupar i utilitzar *softwares*, nosaltres som els que sabem treure un millor rendiment informacional i cognitiu d'entre totes les eines que tenim a l'abast.

Seguretat de la informació i ciberseguretat

La seguretat de la informació abraça molt més que la ciberseguretat, la qual es centra només en l'àmbit digital. La nostra professió ho hauria de dominar tot, però en el meu article ens centrem en la seguretat del ciberespai, que és la més vulnerable en la hipòtesi investigada.

La ciberseguretat, també coneguda com a seguretat informàtica o seguretat de les TIC, té un alt component tècnic però és essencial que el professional de la informació en sàpiga extreure les competències pròpies i se n'encarregui; que defineixi una línia entre allò que pot ocupar l'informàtic i allò que li pertoca a ell. Hem d'identificar quines són les nostres competències concretes i aquelles tasques de què ens podem responsabilitzar.

[2] "Informàtica" a la Wikipedia en espanyol: <http://es.wikipedia.org/wiki/Inform%C3%A1tica>
[3] "Informàtica" a la Viquipèdia en català: <http://ca.wikipedia.org/wiki/Inform%C3%A0tica>

Competències del professional de la informació

Hi ha moltes competències específiques pròpies de la disciplina i comunes al grau d'Informació i Documentació que es poden associar al professional de la informació que s'ocupa de la seguretat de la informació (i en especial de la ciberseguretat). Utilitzaré la llista oficial del grau adaptada al nostre cas concret i n'afegiré d'altres:

- Identificació de les ciberamenaces als nous estats.
- Gestió del coneixement relatiu als ciberatacs viscuts en ocasions anteriors.
- Investigació proactiva en ciberseguretat i seguretat de la informació.
- Definició i aplicació de mètodes sistemàtics d'observació de l'entorn per a detectar amenaces.
- Gestió de "sistemes de gestió de la seguretat de la informació" (SGSI) al servei nacional.
- Vetllar per la disponibilitat, la integritat, la confidencialitat, l'autenticitat i l'auditabilitat o traçabilitat de la informació (i.e. seguretat de la informació).
- Aplicació de les TIC a la gestió d'informació i coneixement sobre ciberseguretat.
- Capacitat interdisciplinària de col·laboració amb organismes públics i privats per a potenciar les mesures efectives de ciberseguretat a nivell nacional i global.
- Capacitat per a oferir suport a les organitzacions que requereixin informació sobre ciberseguretat (webs institucionals, portals de banca electrònica, empreses nacionals susceptibles d'estar al punt de mira, sistemes d'informació de grups polítics, encarregats d'infraestructures crítiques, etc.).
- Disseny de productes, serveis i sistemes d'informació per potenciar la ciberseguretat.
- Gestió de la implantació i explotació de productes, serveis i sistemes d'informació.
- Definició i aplicació de polítiques, mètodes i tècniques per a protegir, conservar i preservar documents i el seu contingut informatiu per a augmentar tècniques de ciberseguretat.
- Col·laboració en la creació de polítiques d'informació sobre ciberseguretat.
- Participació amb el nou govern en el disseny i l'avaluació de polítiques públiques.
- Identificació, avaluació i validació d'informació, documents i les seves fonts.
- Aplicació de tècniques de cerca, recuperació, tractament i presentació de la informació.
- Identificació de les necessitats i els fluxos d'informació de la nació per a maximitzar la seva ciberseguretat i la seguretat de la informació en general.
- Previsió, organització, gestió i realització de projectes tècnics específics.
- Gestió i administració d'unitats organitzatives dedicades a la ciberseguretat nacional.
- Competències en informàtica.
- Treball en equip interdisciplinari.

Competències en base a les assignatures cursades

Si ens fixem en les assignatures estudiades al grau, podem associar-ne algunes directament amb les capacitats i competències que tindríem per a encarregar-nos de la ciberseguretat:

- *Polítiques d'informació*: les relatives a polítiques i estratègies com ara coneixement en la sèrie de normes ISO/IEC 27000, que proporciona un marc de gestió de la seguretat de la informació que pot ser utilitzat per qualsevol tipus d'organització. També es pot treballar en col·laboració amb el nou govern per a establir noves polítiques públiques i fins i tot amb els organismes encarregats de la creació de normatives (a l'article s'ha posat de manifest que la normativa i legislació en ciberseguretat encara està en fase incipient i que no hi ha gaire concordança internacional; els professionals de la informació podríem fer-nos-hi un lloc destacat).
- *Societat xarxa, Comportament informacional i Xarxes socials*: estudis sobre els usuaris de les xarxes socials i com aquests poden actuar. Quan els usuaris investigats s'identifiquen com a hacktivistes podem començar a detectar les conductes que posarien en risc els sistemes protegits.

Les relacions de centralitat i la identificació de paràmetres com la *closeness centrality* o la *betweenness centrality* podrien proporcionar gràfics d'alt valor estratègic per a la detecció de possibles focus de perill on investigar. També entendre les seves necessitats i comportaments serien indicadors per a preveure els tipus d'accions que poden escometre.

- *Gestió del coneixement i Organitzacions intensives en coneixement* són dues disciplines elementals en la formació del professional de la informació a l'hora de formar-lo en tècniques i metodologies per a treure el màxim rendiment de les experiències. Així, nosaltres sabem la importància d'estructurar bé el coneixement relatiu a la ciberseguretat, sabem com fer el seguiment, captura, registre, difusió, transferència, col·laboració, aprenentatge, millora i innovació en base al coneixement processat. Sabem utilitzar tècniques per a prevenir ciberatacs en base a l'aprenentatge d'experiències passades; per exemple, tècniques com quadres de comandament integral del tipus KBS o bé accions de revisió com RDA. Sabem identificar indicadors per a obtenir conclusions i poder prendre decisions.
- *Fonts d'informació i Tecniques de recerca* ens preparen per a saber extreure la informació de les fonts primàries més adients; ens preparen per a investigar més en aquells llocs d'on potser no podem extreure informació tan fàcilment però que poden ser vitals (web invisible). Sabem valorar la veracitat de la informació obtinguda, sabem presentar-la amb professionalitat, etc. Coneixem el valor de les metadades i el web semàntic. Sabem explorar amb eficàcia tots els recursos al nostre abast.

Podríem seguir amb la llista però no cal ja que la relació queda provada. Totes les assignatures del grau conformen un cos de coneixement que l'alumne assimila i que pot aplicar a l'hora d'encarregar-se de les seves tasques pròpies en ciberseguretat.

Tasques específiques per a un professional de la informació

A les conclusions dic que la ciberseguretat s'ha de plantejar des dels governs i entitats que formaran els nous estats, i afegeixo: "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.".

No em correspon enumerar les tasques i funcions de què es podria responsabilitzar un professional de la informació encarregat de vetllar per la ciberseguretat nacional de nous estats del món. Aquestes poden ser molt variades i en tot cas s'haurien de pactar entre les parts contractuals interessades. Ara bé, és interessant complementar aquesta defensa amb una primera aproximació al que podria representar la nostra pràctica professional:

- Identificació i monitoreig de les diferents tipologies de ciberamenaça, al servei d'un CERT.
- Elaboració i proposició de polítiques públiques referents a la ciberseguretat.
- Gestió de sistemes de seguretat de la informació.
- Serveis al Centre de Seguretat de la Informació de Catalunya (CESICAT): Gestió documental, administració de la seva pàgina web, protecció de dades, etc.
- Investigació i recerca sobre mecanismes de seguretat de les infraestructures crítiques nacionals. Creació d'informes per al govern del nou estat.
- Tasques d'anàlisi d'informació en suport als informàtics que desenvolupen aplicacions.
- etc.

Totes les possibles tasques es poden deduir directament de les competències llistades anteriorment.

El nostre valor

A la introducció de l'article dic: "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".

Confio que aquesta defensa hagi palesat els motius pels quals som tan importants en matèria de ciberseguretat per als nous estats. El nostre valor no és "un valor"; és tot allò que valem.

Equip de resposta a un ciberatac

Sense defugir de la pregunta clara del Tribunal Virtual, en primer lloc vull subratllar que una clau de l'article és que el lector hagi entès que es presenten els ciberatacs i altres ciberamenaces com a perills que els nous estats han d'identificar per tal de no arribar-los a patir. En la nostra professió hi ha un interès **proactiu** més que no pas reactiu i, en efecte, la bibliografia que he consultat fa valer la mateixa visió; vegem-se algun exemple:

1) Ja es va contextualitzar fa temps la necessitat d'entendre l'enfocament proactiu: "*some would argue that such a focus would simply be an extension of the current fragmented approach, which is largely reactive — as each new vulnerability is discovered, a new fix is developed — and increasingly costly and ineffective. What is needed, they say, is a strategic approach that is more preventive or even preemptive in nature rather than largely reactive and defensive*" (Fischer, 2005).
2) Martin Rudner sobre les ciberamenaces a les infraestructures crítiques insisteix que "*this approach would entail a proactive cyber-security initiative on the part of intelligence services to prevent attacks rather than merely react to them*" (Rudner, 2013).
3) Els costos també es poden considerar a l'hora de preferir descobrir i prevenir per davant de sanejar o lamentar: "*Proactive steps to mitigate over-the-horizon risks will be much less costly to commerce and national security than allowing these threats to materialize*" (Cutts, 2009).
4) Quant a la seguretat dels sistemes SCADA s'afirma que "*A strategic roadmap framework has been developed to address the security issue in a proactive manner*" (Ten *et al.*, 2010).
5) També podem esmentar l'article de Skopik *et al*. (2012), el qual ens proposa un CAIS (Cyber Attack Information System) per a Àustria amb dos tipus de *stakeholders*: el National Cyber Centre que coordina les activitats a nivell nacional i les organitzacions individuals que participen al sistema. El CAIS necessita de la feina de professionals de la informació i ajuda a prevenir ciberatacs gràcies a la col·laboració de les organitzacions.

Però és evident que tots els atacs no es poden prevenir i, per tant, també ens tocarà treballar en actitud de **reacció**. Jo mateix he esmentat la possibilitat de desenvolupar tasques en equips de resposta davant d'emergències informàtiques (CERT).

La ciberseguretat nacional no depèn només d'un perfil professional. L'estratègia de ciberseguretat nacional espanyola de 2013 proposa un comitè especialitzat en ciberseguretat que "*reflejará el espectro de los ámbitos de los departamentos, organismos y agencias de las Administraciones*

Públicas con competencias en materia de ciberseguridad".[4] Un **equip de resposta a un ciberatac** també ha de cobrir diferents àmbits i englobar perfils diversos però convergents quant a la necessitat d'actuació. Els informàtics programaran els mecanismes defensius pertinents, els governs i els cossos policials emprendran mesures, els experts en dret aplicaran la normativa penal escaient, etc. Els professionals de la informació podem tenir el paper que se'ns hagi assignat, des de funcions consultives fins a la gestió del coneixement expert; qualsevol de les tasques llistables a l'apartat anterior. En tot cas, cal formar part d'un equip heterogeni.

La seguretat de la informació com a assignatura potencial al nostre grau

El rector de la UOC ens alerta que "la possibilitat que un ciberatac pugui paralitzar tota l'activitat d'una regió o d'un país resulta aterradora [...] estem en un nou escenari de riscs i amenaces on la informació s'ha convertit en una arma estratègica i tàctica que pot arribar a qüestionar la governabilitat d'una organització o d'una nació" (Planell, 2013).

Sobre seguretat de la informació i la ciberseguretat, a la UOC hi ha l'oferta formativa del Màster interuniversitari de seguretat de les TIC (UOC-UAB-URV).

Com a assignatura als programes de grau trobem com a més destacada "Sistemes de gestió de la seguretat" per als alumnes d'informàtica.

Per a nosaltres no hi ha res específic. Això sí, a l'assignatura de Polítiques d'Informació vam explorar la importància de les polítiques públiques d'informació, incloent aquelles en matèria de seguretat a la societat de la informació. Recordem que "El desenvolupament d'una estratègia global de seguretat de la informació a escala nacional comença a ser una constant entre els estats, política habitualment centrada en la necessitat de desenvolupar eines de recerca i de conscienciació del públic pel que fa al nombre cada vegada més important d'amenaces i vulnerabilitats de la seguretat en línia" (Alamillo, 2009). Qui ha de ser el professional designat per a desenvolupar aquestes estratègies sinó el titulat en ciències de la informació?

En altres assignatures també s'hi ha fet referència sense massa detall. Val a destacar que a Auditoria de la Informació vam aprendre que "[l'auditoria] és una eina útil aplicada en l'àmbit de l'auditoria interna, la gestió documental, la seguretat de la informació, la intel·ligència competitiva o la gestió del coneixement" (Soy, 2011, p. 21). Curiosament, veiem, llista un seguit de matèries que són ofertes com a assignatures del nostre grau amb l'única excepció de la seguretat de la informació.

La seguretat de la informació –i la ciberseguretat– és un camp d'estudi completament escaient als nostres interessos i competències i del qual no tenim oferta formativa curricular. Aprofito per posar sobre la taula el meu parer quant a la conveniència que la UOC incorpori al pla d'estudis d'Informació i Documentació una assignatura optativa que permeti els estudiants aprofundir en coneixements de seguretat de la informació i ciberseguretat enfocada al nostre perfil professional.

[4] Estrategia de Ciberseguridad Nacional 2013: <http://www.lamoncloa.gob.es/NR/rdonlyres/680D00B8-45FA-4264-9779-1E69D4FEF99D/256935/20131332EstrategiadeCiberseguridadx.pdf>

3. Sobre el context informacional

Posa en relació el contingut del punt 3 de context informacional respecte dos episodis lligats a la Segona Guerra Mundial, l'existència del Ràdar i la màquina Enigma

Al contingut del punt 3, sobre el context informacional, vaig voler reforçar dues idees:

1) Hem arribat a guerres de la informació en conflictes polítics / guerres.
2) Això pren màxim sentit en l'actual estat de ciberdependència creixent.

A la Segona Guerra Mundial (1939 – 1945) el desenvolupament de TIC no era el que coneixem ara i la dependència en elles no existia, però sí que es va demostrar el poder del domini de la informació en situacions bèl·liques, que ve d'antic. Sandoval (2001) ens recorda que "*La guerra informacional puede ser dividida en tres grandes funciones: la que apunta a maximizar la superioridad informacional perjudicando a las capacidades sensoriales, analíticas y comunicacionales del enemigo; la que se enfrenta a las infraestructuras civiles enemigas (guerra electrónica e informática); por último, la que tiende a condicionar al adversario (guerra psicológica)*". La màquina Enigma encaixaria a la primera funció mentre que el radar podria classificar-se a la primera o la segona en funció de la interpretació que en fem. Quant al poder psicològic, i d'acord al meu article, consideraríem més aviat el hacktivisme que fa propaganda o bé la censura d'Internet.

El radar: Durant la dècada prèvia a la II Guerra Mundial Anglaterra, els EUA, Alemanya i França van investigar sobre la possibilitat de detectar avions enemics mitjançant l'eco i les interferències de les ones de ràdio. Watson-Watt va crear el model actual i el va desenvolupar durant aquella guerra. Cada cop s'aconseguia detectar enemics a més milles de distància.

És fàcil imaginar que així com l'imperi Mongol guanyava batalles gràcies a disposar més informació, els països que durant la II Guerra Mundial aconseguissin desenvolupar millor la tècnica de radar haurien de disposar d'informació estratègica avantatjosa quant a capacitat defensiva i per a atacar. La informació de saber on és l'enemic és estratègicament essencial.

Per a entendre-ho clar anirem més enllà amb la imaginació: Què hauria estat de les tropes napoleòniques derrotades el 1808 a Montserrat si haguessin disposat de radars o d'un missatger que els hagués donat informació real? Em refereixo, és clar, a l'episodi llegendari del timbaler del Bruc.

Enigma és una màquina existent des dels anys vint que permet xifrar missatges mitjançant un complex sistema de codificació rotativa. Era considerada indesxifrable... fins que durant la II Guerra Mundial es va descobrir el secret (tot i que es mantingué en secret); es considera que si no s'hagués descobert la guerra hauria durat almenys dos anys més.

Tan important és voler descobrir la informació sobre l'enemic com protegir la pròpia. Enigma[5] és un dels exemples més representatius en l'afany de l'home per a xifrar el llenguatge i enviar missatges a distància sense que aquests puguin ser compresos per altra part que la destinatària.

[5] Enigma: <http://es.wikipedia.org/wiki/Enigma_%28m%C3%A1quina%29>

4. Sobre la possible publicació de l'article

Per la feina duta a terme, i pel contingut, pensem que l'article podria ser perfectament publicat, per exemple, a la revista Ítem. Quins principals canvis creus que caldria dur a terme, tant de contingut com de format i presentació? En quin perfil de revista creus que es podria ajustar?

Valor afegit del meu article

L'article és publicable perquè:

- Faig una revisió bibliogràfica seriosa de caire científic quant a ciberseguretat; es recullen també els casos reals que representen un toc d'alerta.
- Relacionar ciberseguretat i ciberatacs a nacions sense estat que malden per independitzar-se conforma un enfocament diferent. La seva inclusió a les bases de dades consultades aportaria novetat atès el propòsit inèdit.
- Associar competències en ciberseguretat als professionals de la informació també es pot considerar novetat i valor afegit.
- Respecta les normes de la comunitat (citacions, rigor, novetat, etc.).

Canvis de format i presentació

No paga la pena allargar-se amb els canvis de format ja que cada revista té les seves normes. De fet, jo he pres per referència les "Instruccions per als autors" de BiD adaptant alguns aspectes al meu gust (per exemple l'alineació justificada). Si publiqués a Ítem hauria de respectar les indicacions que ells estableixen. La major part del format així com la bibliografia ja estarien preparats.

Per mor del contingut no veig convenient afegir taules, imatges, figures ni gràfics.

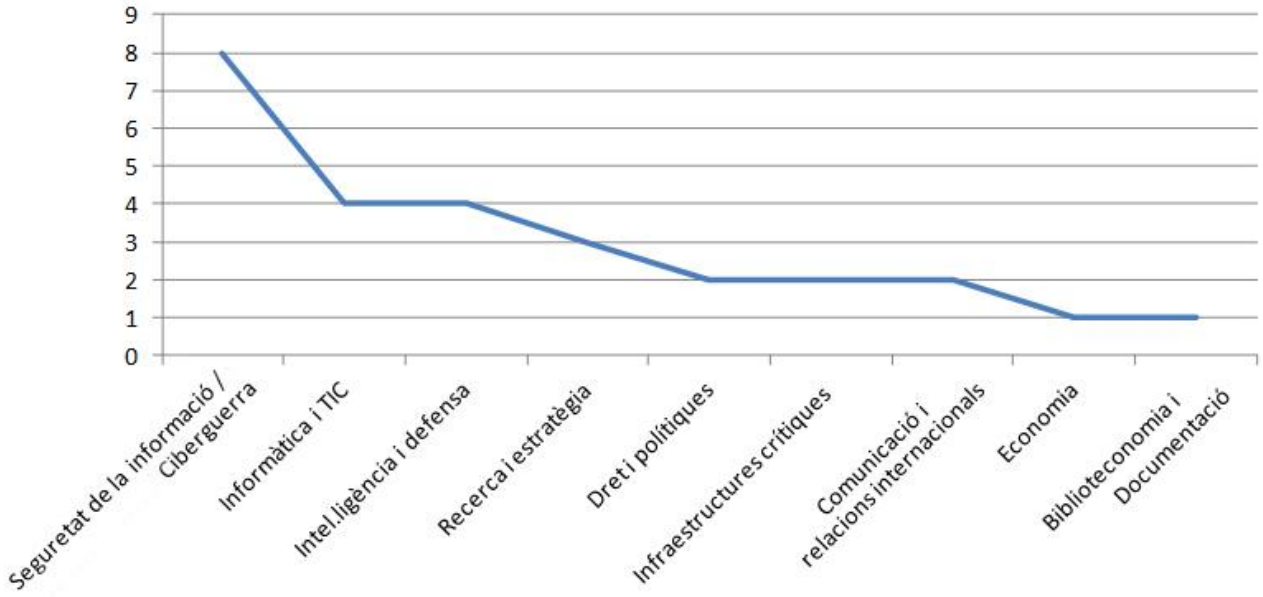
Canvis de contingut

Tot el contingut de l'article ha estat consultat, escrit, assimilat, revisat i millorat fins que l'autor (jo) ha aconseguit el resultat més immillorable d'acord a la seva capacitat. Per part meva només puc defensar el rigor i dedicació intensa que m'han permès oferir un resultat que ja no ha de menester més canvis. Seria d'agrair que lectors de l'article aportin la seva valoració crítica per tal de remarcar allò que al seu parer seria millorable o podria ser reformulat; el seu *feedback* seria la millor tècnica per a proposar canvis de contingut.

No obstant, sí que puc reconèixer que (ho he defensat a l'inici) presento un text amb l'objectiu principal d'investigar quant a la ciberseguretat en els països potencials d'independitzar-se. Per a emmarcar-lo com a treball final de grau no he pogut defugir de relacionar el contingut amb el valor del professional de la informació; Ho he fet a la introducció, a la conclusió i hi he aprofundit en aquesta defensa. Si ara arriba l'hora de publicar-lo en una revista científica del món de la Informació i la Documentació, miraria de fer-hi algunes pinzellades; conservant-ne l'essència però remarcant també en el cos del redactat el nostre valor.

Perfil de la bibliografia

Abans de decidir en quin tipus de revista puc publicar el meu article seria interessant recordar quin tipus de bibliografia he consultat. Alguns documents molt rellevants són conferències en ciberseguretat. Altres, la majoria, són articles en revistes científiques o bé reculls especials que podem categoritzar de la següent manera[6]:



Tenint en compte que el meu article es basa en una estricta revisió bibliogràfica i que només el capítol de previsió de casuístiques es distancia del constant sistema de citacions, podem afirmar que segurament el resultat obtingut és molt propi i adient d'ésser publicat en una revista sobre seguretat de la informació o seguretat informàtica. En un segon esglaó podem pensar que tindríem força acceptació en una revista d'informàtica o en una publicació sobre defensa nacional. A l'altre extrem, l'article tracta sobre economia però no al centre d'atenció i la Biblioteconomia i Documentació tampoc no conforma una font d'informació destacada en l'elaboració.

Recuperem en aquest punt la necessitat de canviar els continguts per a crear un interès especial en la nostra disciplina. Es va fer a la introducció i la conclusió però la manca de bibliografia especialitzada en documentació ens ha d'obligar a reflexionar en la necessitat de reforçar al llarg de tot el text el valor del professional de la informació.

Perfil d'una revista on publicar

Com a autor novell i tenint en compte que es tracta d'un article en català tal volta hauria de buscar una revista apropiada sense fixar-me en el factor d'impacte. La possible continuïtat de la investigació i una producció més prolífica podrien guiar-me a aquest interès més endavant.

El redactat actual seria del tot vàlid per a una revista sobre informàtica i TIC. També una publicació de ciències socials i polítiques hi trobaria un gran interès ja que s'hi han filtrat els casos de conflictes polítics d'alliberament nacional. El perfil de la bibliografia no mostra aquesta vessant però es presenta innegable. De la mateixa manera, hem decidit que l'article ha de ser publicable en

[6] Aquesta classificació és aproximada i orientativa; per posar un exemple: La revista "Informatica Economica" només s'ha classificat com a economia i no com a informàtica.

una revista científica de Biblioteconomia i Documentació perquè, independentment de la bibliografia, nosaltres hi hem remarcat (i ho podem reforçar) el valor del professional de la informació. I perquè és el que ens interessa.

Les revistes més apropiades on publicar serien *BiD* o *Ítem*, les quals són indexades / resumides a[7]:

	BiD	Ítem	UOCpapers*
DIALNET			
Directory of Open Access Journals (DOAJ)			x
e-Revistas	x		x
ISOC	x	x	
Latindex-Catálogo	x	x	x
Latindex-Directorio	x	x	x
L I S A: Library & Information Science Abstracts	x	x	
LISTA Full Text	x		
Racó	x		
Red ALyC			x
Scopus			
Social Sciences Citation Index			

* *UOC Papers* es troba en procés de refundació i no admet la presentació d'articles.

Seria possible interessar-se en revistes com *El profesional de la información* o altres en llengua anglesa però el cert és que també trobo interessant col·laborar en revistes que publiquen articles originals en la nostra llengua.

[7] Basat en les dades de http://www.latindex.org

5. Sobre la possible continuïtat de la investigació

Si disposessis de recursos materials i humans per a seguir la investigació relacionada en aquesta temàtica, quins aspectes creus que tindria sentit investigar?

Si disposés de recursos materials, humans i econòmics no dubtaria gens a aprofundir més en l'escletxa al món de la investigació que aquest treball m'ha obert. El tema investigat és d'allò més atractiu, apassionant; com un bosc amb molts arbres i secrets encara per descobrir.

Aspectes a investigar

Primer de tot m'hauria de formar bé en Seguretat de la informació: a l'elaboració de l'article no he tingut dificultats per a aprendre sobre ciberseguretat per tal d'oferir un resultat de qualitat. Però no em vull enganyar: a la UOC no he estudiat una assignatura en seguretat de la informació i sé que hi ha conceptes bàsics que caldria consolidar per tal de dotar d'una base més consistent i professional futurs articles.

Aspectes concrets on potenciar la investigació, a tall d'exemple, serien:

- Polítiques públiques en ciberseguretat: Hi ha diverses polítiques públiques, però sovint no són integrals, no tenen una projecció internacional coherent, etc. A l'article ho he explicat i ben bé és un tema on l'investigador en ciències de la informació hauria d'aprofundir per a aportar coneixement nou i creatiu.
- Gravetat dels ciberconflictes polítics: El que ha estat un apartat del meu article donaria per a investigacions molt significatives. Quin grau en les conseqüències d'un atac DDoS pot patir un país acabat d'independitzar? Quin impacte tindria en les facetes econòmica, política, estructural i social (psicològica)? Etc.
- El problema d'atribució: Tothom coincideix en la dificultat de determinar qui ha comès els ciberatacs; només s'especula. Els atacs a Estònia van ser de Rússia; no es nega ni es demostra. Aquest plantejament d'incertesa hauria de ser vist com un nínxol de coneixement potencial d'investigació. No podem pretendre demostrar allò impossible però sí utilitzar indicadors que els nous estats del món puguin utilitzar per a la ciberseguretat.
- Nivell d'integració en ciberdefensa nacional: He confirmat que el professional de la informació podria prestar els seus serveis en ciberseguretat a diferents organismes i institucions que els nous governs han de coordinar. Un aspecte a investigar seria el nivell d'intregració i/o col·laboració d'aquests ens a Catalunya: CESICAT, CPD's, CERTS's, Apdcat, Administracions i Govern, organitzacions privades en seguretat digital, etc. i en cas d'haver-hi desconnexions poc lògiques fer una proposta d'apropament.
- Ciberguerra contra Catalunya: No només com a títol que capta l'atenció, el Consell Assessor per a la Transició Nacional (CATN) ens alerta al seu informe número 5 la necessitat d'extremar la ciberseguretat del país. La periodista experta en el tema Mercè Molist ha escrit a Vilaweb sobre els perills d'una ciberguerra contra nosaltres. El meu article tenia un abast geogràfic mundial i per això Catalunya només apareix com un element més; seria molt interessant fer un nou article on aquest abast geogràfic es redueixi a la nostra nació.
- El professional de la informació en ciberseguretat: En aquesta defensa he fet una teorització de totes les competències que ens poden correspondre però ho he fet sense basar-me en l'opinió d'altres autors en la matèria. Es podria investigar formalment.
- etc.

Aspectes que no investigaria més

- Ciberatacs lleus de hacktivistes: La bibliografia recuperada m'ha conduït a parlar del hacktivisme i atacs a pàgines web, bombardeigs d'emails, etc. Una de les conclusions és que aquesta tipologia de ciberatacs és minvant; va en detriment d'altres atacs més sofisticats i perillosos com els DDoS. Molts autors ho ratifiquen. Per tant, fer una investigació expressa sobre hackeig simbòlic de pàgines web independentistes tindria més un valor periodístic que no pas un pes significatiu per a la comunitat científica.
- Països poc dependents en TIC: Tenia l'obligació temàtica d'esmentar tots els països que en major o menor grau cerquen independitzar-se, però una de les conclusions és que aquells que no fan un ús intensiu de TIC no corren perills de ciberatacs ni de ciberguerra. No val la pensa perdre massa esforços recercant casos com Murrawarri, Azawad, Sudan del Sud, la República Àrab Sahrauí Democràtica, etc.
- Infraestructures crítiques: Si parlem de ciberseguretat és obligatori considerar com a risc més destacat les infraestructures crítiques nacionals. No n'hi ha dubte. Ara bé, la producció científica en aquest àmbit és considerable i no és plenament un camp d'investigació dels professionals de la informació. Hem d'estudiar els sistemes d'informació que suporten les infraestructures crítiques tant com altres sistemes d'informació; opino que investigar-les de forma específica no donaria valor afegit.
- etc.

Hipòtesis per a nous articles

Els aspectes que tindria sentit investigar indiquen en gran mesura possibles noves hipòtesis. En recuperaré alguna i n'afegiré d'altres per a proposar idees:

- Les polítiques públiques catalanes en matèria de ciberseguretat: estat de la qüestió.
- Gravetat dels ciberconflictes polítics: les conseqüències catastròfiques de possibles atacs a nacions que s'independitzen als inicis del segle XXI.
- Organismes per a la ciberseguretat de Catalunya el 2014: revisió dels organismes públics i privats competents en ciberseguretat, funcions específiques i relació entre ells.
- Ciberguerra contra una Catalunya independent: perills i reptes.
- Competències del professional de la informació en matèria de ciberseguretat.
- La cibervigilància com a nova forma d'amenaça per a la Catalunya del segle XXI.
- etc.

***Investigar per a* El profesional de la Información**

La revista EPI en el seu número 24, 3, de maig 2015, tindrà per tema central "*Privacidad y seguridad de la información*". Hi ha temps fins el 10 de gener de 2015 per a entregar els *papers*. La possibilitat de publicar-hi seria un bon pretext per a decidir una línia d'investigació interessant de les esmentades; o una altra que pugui crear interès a mi i als lectors de la revista.

6. Sobre els estats i les nacions sense estat

En el títol planteges els processos d'independència. Quins creus, atesa la bibliografia, que són els referents similars en aquests processos que han tingut lloc en els darrers anys, on la ciberseguretat ha tingut un pes més gran? Lligat a posem per exemple el procés català, quin seria l'aprenentatge a considerar respecte a països en situacions similars?

Sobre les nacions sense estat

1) Nacions que s'han independitzat al segle XXI (nous estats):

	Nacions o regions[8]	***Independència de...***	***X***[9]
2014	**Crimea**	Ucraïna; posterior annexió a Rússia	
2013	**Murrawarri**	Austràlia	
2012	**Azawad**	Mali	
2011	**Sudan del Sud**	Sudan	
2008	**Kosovo**	Sèrbia	**X**
2006	**Montenegro**	Sèrbia	
2006	**Ossètia del Sud**	Geòrgia	**X**
2002	**Timor Oriental**	Indonèsia	**X**

2) Casos tractats que no corresponen a països independitzats aquest segle:

	Casos	
2010	**Stuxnet**	Stuxnet és el cuc informàtic maliciós més poderós de la història. S'atribueix a Israel i als EUA amb el major impacte afectant l'Iran. Tot i no ser de nacions sense estat, era imprescindible recordar-ne l'existència i efectes al meu treball.
2007	**Estònia**	Estònia va formar part de l'URSS fins l'any 1991. Estònia i Geòrgia no són països nous al segle XXI però els greus ciberatacs per part de Rússia són referents inevitables en parlar de ciberguerra.

3) Països que busquen la independència (independentment del grau reivindicatori) i han patit ciberatacs polítics deguda aquesta aspiració:

- **Taiwan** (actualment reclamat per la Xina)
- **Palestina** / Israel
- **Euskal Herria** (dominada pels estats espanyol i francès)
- **Kurdistan** (dividit en quatre estats, principalment Turquia)
- **Caixmir** (dividit entre l'Índia, el Pakistan i la Xina)
- **Tibet** (Xina)
- **Tamil Eelam** (Sri Lanka)

[8] N'hi ha que no són reconeguts de iure; en parlo a l'apartat "7. Previsió de casuístiques".

[9] Els països marcats amb una X són els que tenen alguna referència de ciberatacs al meu treball d'investigació. La resta no n'han patit o els autors consultats no en parlen. Val a matisar que Kosovo és referit al meu treball però especialment per la guerra viscuda el 1999.

4) Nacions que faran un referèndum d'independència i de què no he pogut recuperar cap referència bibliogràfica referent a ciberatacs:

- **Quebec**: vol independitzar-se del Canadà. Podria fer properament un 3r referèndum (?).
- **Escòcia**: referèndum per independitzar-se del Regne Unit el 18 de setembre de 2014.
- **Flandes**: Possible independència de Bèlgica, democràtica, sobre la taula.
- **Nova Caledònia**: referèndum per independitzar-se de França previst entre 2014 i 2019.
- **Bougainville**: referèndum per independitzar-se de Papua Nova Guinea en un futur.

5) Nacions amb minories que lluiten per la independència o per un reconeixement nacional més ampli dins l'estat actual i de les quals no tinc ciberatacs registrats:

Txetxènia, Alt Karabagh, Somalilàndia, Transnítria, Padània, República de Cascàdia, Hong Kong, Illes Fèroe, Grenlandia, Patagònia, Còrcega, Galiza, Silèsia, Astúries, Voivodina, etc.

Sobre els tipus de ciberatacs patits (per any)

	Bombardeig d'e-mails	**Substitució de contingut web**	**Redirecció de webs**	**Cucs, virus i *malware***	**DDoS**	**Ciberespionatge / censura**
Taiwan		1999		2005, 2008	2002	*Constant*
Israel / Palestina		2000, 2007, 2008, 2012	2001	2010	2001	
Euskal Herria	1997	1997				2002
Timor Oriental		1998				
Estònia					2007	
Ossètia del Sud					2008	
Kirguizistan					2005, 2009	
Kosovo	1999	1999		1999	1999	
Caixmir		2000				
Tibet						*Constant*
Tamil Eelam	1998					
Stuxnet				2010		

Alguns casos com Kurdistan o l'EZLN han estat recollits al meu article només a causa del poder mobilitzador dels hacktivistes a través d'Internet.

Països on s'ha viscut ciberguerra

No hi ha unanimitat a l'hora d'identificar la primera ciberguerra, a la bibliografia comprovem que tampoc no n'hi ha quan s'ha de considerar què és ciberguerra i què no. Sigui com sigui aquests són els casos més destacats:

1999 – "First war on the Internet": A la guerra de **Kosovo**
1999 – 2003 – Ciberguerra entre **Taiwan** i la Xina
2001 – "First Cyber World War" entre la Xina i els EUA
2007 – "First Cyberwar": **Estònia** és atacada i culpen Rússia
2008 – Geòrgia és atacada i culpen Rússia
2010 – **Stuxnet**: Iran és atacat; culpen els EUA i Israel.

Processos d'independència referents

Els subapartats precedents sintetitzen els casos disseminats al meu article i altres que es van considerar a l'inici de la investigació. Un cop revisats puc donar resposta mitjançant idees clau:

a) Dels 8 països independitzats al segle XXI, només he recollit referències de ciberatacs en 3 casos: Kosovo, Ossètia del Sud i Timor Oriental. Aquests vuit països no són grans dependents de les TIC ni econòmicament dels més avançats. Catalunya o Escòcia serien casos diferents.
b) Encara que parlem de nacions independentistes, a l'hora de tractar la ciberseguretat se'ns fa indispensable conèixer els ciberriscs generals; per això no s'han bandejat els dos casos de ciberguerra més destacats: Stuxnet i Estònia.
c) La tipologia de ciberatacs a la majoria de nacions sense estat són del que podríem considerar "hacktivisme lleu". Atacs DDoS i de ciberguerra a aquestes nacions encara no s'han produït.
d) No es destaquen ciberatacs referents a països que s'han encaminat cap a la independència de forma democràtica. Sí que hi ha ciberatacs a nacions que no compten amb l'aprovació de l'estat ocupant: Taiwan i Palestina són els casos més destacats però demostren hacktivisme lleu.

Conclusió: no podem parlar de nacions independentistes referents quant a ciberatacs patits i, per tant, basar-nos-hi per a valoritzar la necessitat de ciberseguretat. Això no obstant, hem palesat que moltes d'aquestes nacions són al punt de mira al ciberespai i són atacades. Podem parlar d'atacs de hacktivisme lleu si bé amb clar declivi en la línia cronològica: cada cop els atacs generals són més sofisticats i greus. Hem de basar la consciència en altres casos del camp de la ciberseguretat com són Stuxnet (cucs informàtics avançats) i Estònia (DDoS). La meva investigació sosté que els casos tractats són indicadors per a pensar que cap ciberseguretat nacional es pot relaxar.

Aprenentatge per al procés català

L'aprenentatge per al procés català és inequívoc: Si no protegim el nostre ciberespai correm el risc de ser atacats i patir conseqüències imprevisibles. Per experiències viscudes en processos similars sabem que aquestes conseqüències podrien anar des de la redirecció de la pàgina web de la Generalitat de Catalunya cap a una pàgina pornogràfica (com va passar a Israel) fins a atacs DDoS generals mitjançant *botnets* que aturin tots els sistemes d'informació i serveis nacionals de manera continuada (com a l'exemple d'Estònia).

Estònia 2007 és un referent que molts autors citen. Sense entrar a valorar els efectes que va tindre, hi ha la veu unànime de dir que va ser un toc d'alerta. No es pot ignorar el perill de no protegir el ciberespai. Catalunya és un país que té una aspiració independentista majoritària –del 60%–[10] i, a la defensiva, té la negació rotunda de molts espanyols (incloent el govern) que semblen somniar imperis del passat. Catalunya, sens dubte, ha de maximitzar la seva ciberseguretat nacional.

[10] "Un 60% dels catalans estan a favor de la independència, segons un sondeig del CEO", notícia publicada al diari Ara el 18/03/2014: <http://www.ara.cat/politica/sondeig-CEO-independencia_0_1103889719.html>

Bibliografia

Alamillo, Ignacio (2009). "Les polítiques públiques en matèria de seguretat a la societat de la informació". A: *«V Congrés Internet, Dret i Política (IDP). Cara i creu de les xarxes socials»* [monogràfic]. IDP. *Revista d'Internet, Dret i Política*, núm. 9, UOC. Online: <http://idp.uoc.edu/ojs/index.php/idp/article/view/n9_alamillo/n9_alamillo_cat> [Consulta: 23/06/2014]

Cobarsí Morales, Josep; López-Borrull, Alexandre (2009). "Informació i documentació: Conceptes bàsics". *Introducció a la informació i la documentació*. Barcelona: FUOC.

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]

Fischer, Eric A. (2005). "Creating a National Framework for Cybersecurity: An Analysis of Issues and Options". *Congressional Research Service*, The Library of Congress Washington DC 20540-7500. Online: <http://oai.dtic.mil/oai/oai?verb=getRecord&metadataPrefix=html&identifier=ADA463076> [Consulta: 6/04/2014]

Moneda, Mercedes de la (2014). "La interdisciplinarietat en els graus d'Informació i Documentació". *BiD: textos universitaris de biblioteconomia i documentació*, juny, núm. 32. Online: <http://bid.ub.edu/32/moneda1.htm> [Consulta: 23/06/2014].

Planell, Josep A. (2013). "I Congrés de Seguretat a la Xarxa: Ciberespionatge i Ciberseguretat". [Recurs audiovisual]. Online: <http://youtu.be/mDSgAUDVv00> [Consulta: 21/06/2014]

Rudner, Martin (2013). "Cyber-threats to critical national infrastructure: An intelligence challenge". *International Journal of Intelligence and Counter Intelligence*, vol. 26, núm. 3 (set.), p. 453-481. Online: <http://dx.doi.org/10.1080/08850607.2013.780552> [Consulta: 30/03/2014]

Sandoval, Mario (2001). "La función de la información estratégica en las relaciones internacionales". Fasoc, any 16, núm. 3 i 4. Online: <www.fasoc.cl/files/articulo/ART41083579ccf69.pdf> [Consulta: 22/06/2014]

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]

Soy i Aumatell, Cristina (2011). "Gestió de la informació i auditoria de la informació". *Auditoria de la informació*. Barcelona: FUOC.

Ten, Chee Wooi; Manimaran, Govindarasu; Liu, Chenching (2010). "Cybersecurity for critical infrastructures: Attack and defense modeling". *IEEE Transactions on Systems, Man, and Cybernetics Part A: Systems and Humans*, vol. 40, núm. 4 (jul.), p. 853-865.