Ciberterrorisme. Concepte i aproximació al fenomen

PID_00272035

Josep Maria Tamarit Sumalla
M. del Carme Guirao Cid

Temps mínim de dedicació recomanat: 3 hores

Universitat Oberta de Catalunya

Josep Maria Tamarit Sumalla

Catedràtic de Dret Penal a la Universitat Oberta de Catalunya, on és director del màster de Ciberdelinqüència. La seva activitat de recerca s'ha centrat bàsicament en aspectes relacionats amb la victimologia, la justícia restaurativa i el sistema de sancions penals. També ha escrit diverses publicacions relacionades amb la delinqüència de motivació ideològica i els delictes d'odi. És coordinador del grup consolidat de recerca sobre el sistema de justícia penal.

M. del Carme Guirao Cid

Graduada en Criminologia per la UOC i màster de Drets Humans per la mateixa universitat. És becària predoctoral a la Universitat de Lleida, on realitza la seva tesi doctoral sobre adoctrinament i victimització terrorista, un tema sobre el qual ha publicat dos articles (2018; 2019).

L'encàrrec i la creació d'aquest recurs d'aprenentatge UOC han estat coordinats pel professor: Josep Maria Tamarit Sumalla (2020)

Primera edició: febrer 2020

Av. Tibidabo, 39-43, 08035 Barcelona
Realització editorial: FUOC

Índex

Introducció

Les tecnologies de la informació i la comunicació (TIC) són en l'actualitat una poderosa eina per a extremistes i grups terroristes, que aprofiten la versatilitat de la xarxa per promoure la seva ideologia i ampliar el cercle de les seves futures víctimes. Una de les principals amenaces del ciberterrorisme és que es produeixi un ciberatac contra una infraestructura crítica, com pot ser un centre de telecomunicacions, un aeroport, una central nuclear o un centre d'intel·ligència, per contenir informació sensible i estratègica. Però no han de passar desapercebuts altres riscos que un adequat estudi del fenomen pot revelar-nos.

En els propers apartats explicarem el ciberterrorisme centrant-nos en les accions perpetrades per organitzacions terroristes de base religiosa, com Al-Qaeda i Daesh per ser els seus màxims exponents en l'actualitat i pel temor i la inseguretat que suscita pensar que algunes de les ciberamenaces poguessin materialitzar-se. De fet, algunes sèries de ficció, com *El Príncipe*, emesa per una cadena de televisió espanyola, han emulat la possibilitat que un grup d'aquest tipus acabés cometent un ciberatac contra instal·lacions crítiques. No obstant això, resulta fins a cert punt contradictori, o almenys paradoxal, que grups que es dediquen a combatre els països occidentals per concebre'ls massa moderns i transgressors per mitjà d'un discurs basat en l'islam més tradicional, hagin decidit utilitzar les TIC per lluitar contra el progrés.

El mòdul s'estructura en quatre apartats. El primer està dedicat a conceptualitzar el terme *ciberterrorisme*, a extreure els seus aspectes més característics i a diferenciar-lo d'altres ciberconductes. En els apartats segon i tercer descriurem les estructures mitjançant les quals actuen les organitzacions terroristes, així com les activitats que hi realitzen. Finalment, descriurem en profunditat com es duu a terme el procés de la radicalització per la xarxa, la ciberradicalització.

Objectius

Els objectius que es pretenen aconseguir amb l'estudi del present mòdul sobre aspectes conceptuals del ciberterrorisme són els següents:

1. Definir el ciberterrorisme i quines són les seves característiques distintives.

2. Diferenciar el ciberterrorisme d'altres modalitats cibercriminals.

3. Conèixer quines són les estructures mitjançant les quals actuen les organitzacions terroristes.

4. Conèixer els tipus d'activitats que duen a terme les organitzacions terroristes.

5. Conèixer en profunditat el procés de ciberradicalització i els perfils dels cibervictimaris i les cibervíctimes.

1. El ciberespai: noves oportunitats per als delictes de terrorisme

1.1. Factors de risc al ciberespai

La creació del ciberespai ha procurat una àmplia disponibilitat d'eines de desenvolupament efectives, i de baix cost, que han contribuït a generar noves oportunitats per a la comissió de delictes. En l'àmbit del terrorisme, la disponibilitat de coneixement gratuït en línia ha permès a les organitzacions terroristes desenvolupar els seus mètodes i realitzar activitats il·legals i atacs de manera remota, tot causant danys a béns jurídics per aconseguir els seus objectius.

L'entorn en línia té unes característiques que el fan més atractiu que el fora de línia, en permetre al cibervictimari realitzar els seus actes més enllà dels límits que li imposa l'espai físic. Com assenyala Wall (2007), aquests «nous» delictes han passat a formar part de les agendes polítiques dels estats, ja que el que més preocupa d'ells no és el fet que puguin cometre's des d'ordinadors o mitjans portables, sinó que tots estan connectats al ciberespai, un àmbit de comunicació transnacional que permet operar independentment de les variables espaciotemporals, és a dir:

> El cibervictimari pot actuar des de qualsevol lloc i cap a qualsevol lloc, independentment de la distància. Fins i tot pot cometre delictes simultàniament en diferents llocs, provocant així xarxes distribuïdes de víctimes (Miró, 2011; Jahankhani, Al-Nemrat i Hosseinian, 2014).

Com sabem, les persones solem actuar impulsades per la consecució d'un objectiu i sobre la base d'una motivació. No obstant això, no està garantit que puguem aconseguir els objectius pretesos a causa de les barreres (tant externes com internes) que ens ho dificulten o ens ho impedeixen. Autors com Suler (2004) i Agustina (2014) han estudiat el paper que té l'entorn «ciber» per desenvolupar una major desinhibició en els individus. D'aquesta manera, han identificat les següents característiques de la comunicació en el ciberespai:

1) Anonimat dissociatiu: s'erigeix com l'efecte principal de la desinhibició, per ser el responsable que puguem navegar per la xarxa sense por de ser descoberts. Les característiques de les arquitectures digitals han desenvolupat un conjunt de mecanismes que garanteixen l'anonimat al victimari, dificultant així la tasca dels cossos de seguretat per rastrejar les seves dades. Això ha permès crear noves varietats d'amenaces criminals.

Una conseqüència directa que deriva de l'anonimat dissociatiu és la possibilitat que es brinda a l'individu de poder separar el «jo» real del «jo» digital, permetent-li actuar per mitjà d'una representació virtual d'ell. Això afavoreix que l'individu construeixi un segon jo, que tampoc té per què ser l'únic, sinó que, fruit de les característiques que presenta la xarxa, se li permet elaborar més d'un, la qual cosa desencadena identitats múltiples (Becoña, 2016).

2) Invisibilitat: d'una banda, permet al subjecte actuar sabent que difícilment se li podrà atribuir l'autoria de la conducta. D'altra banda, sap que pot visualitzar continguts privats d'altres individus sense que aquests ho sàpiguen. Aquesta característica ha portat Jahankhani, Al-Nemrat i Hosseinian (2014) a parlar de «sinopticisme i panopticisme», referint-se a la capacitat de vigilància que atorga el ciberespai al victimari per controlar les seves víctimes de manera remota.

3) Comunicació asincrònica: si bé les TIC han permès eliminar les variables d'espai i temps de la comunicació interpersonal, això no garanteix que les reaccions a la conducta de l'emissor es produeixin de manera immediata per part del receptor, i poden demorar-se de minuts a hores, o fins i tot dies.

4) Introjecció solipsista: l'absència d'interacció física afavoreix la consolidació de llaços i la desindividualització del subjecte a favor d'una identitat grupal. Quan la persona rep un missatge o llegeix una aportació realitzada en un fòrum, percep aquesta informació com l'«única» existent i veraç. A partir d'aquest moment, es posa en dubte tota informació que prové d'una font externa a l'endogrup.

5) Minimització de l'estatus i de l'autoritat: al món fora de línia, l'autoritat i el poder són dues de les qualitats que descriuen un tipus determinat de personalitat que pot arribar a ser anhelada. Al ciberespai, el pes que tenen tots dos elements es redueix, fent que qualsevol persona tingui les mateixes oportunitats si els aconseguís. De fet, la màxima d'internet és «tots som iguals a la xarxa». Tothom pot compartir les seves opinions lliurement amb els altres (Suler, 2004).

La suma d'aquests factors contribueix a disminuir el llindar de risc percebut pel subjecte i a augmentar la probabilitat que acabi cometent un delicte.

Vegeu també

Les estructures web utilitzades per les organitzacions terroristes seran objecte d'estudi a l'apartat 1 del mòdul 2.

1.2. L'atractiu del ciberespai per a l'organització terrorista

A l'apartat anterior hem descrit les característiques generals del ciberespai. Ara, partint de l'estudi de Weimann (2017), ens centrarem en l'atractiu que troben els ciberterroristes en el seu ús. Com podrem veure, algunes ja s'han descrit anteriorment.

- Les aplicacions i els mitjans que ofereix internet suposen un **abaratiment** dels costos en comparació amb els mètodes terroristes tradicionals, ja que

l'única cosa que es requereix és un ordinador, un mòbil o una tauleta amb connexió a internet. Són mitjans que en l'actualitat estan a la disposició d'un amplíssim nombre de persones. No calen armes o explosius.

- El terrorisme dut a terme per la xarxa permet la **circulació lliure i l'anonimat** als perpetradors mitjançant l'ús de sobrenoms en línia o la possibilitat de connectar-se amb perfils falsos, la qual cosa dificulta a les agències de seguretat rastrejar les veritables identitats dels terroristes.

- La falta de límits de la xarxa ha permès a les organitzacions descobrir nous mitjans d'adquisició de materials per perpetrar atemptats al món real (materials per fabricar explosius, armes, drogues, etc.); per exemple, per mitjà de la ***darknet***.

- El ciberterrorista pot dirigir des del seu ordinador la seva acció contra **multitud d'objectius**, ja siguin governs, individus o serveis públics o privats, una vegada detectades les seves febleses, sent les més vulnerables les instal·lacions d'energia elèctrica a causa de la complexitat de les seves infraestructures i sistemes informàtics.

- Les característiques de la xarxa permeten **eixamplar el cercle de possibles víctimes**, que poden classificar-se en tres grups:
  - el primer englobaria partidaris i simpatitzants de l'organització, que es tornen més vulnerables a ser reclutats i adoctrinats;
  - el segon englobaria institucions i sistemes d'infraestructures crítiques de la comunitat internacional; i,
  - el tercer englobaria individus o col·lectius tradicionalment concebuts com a «enemics».

- Els atemptats poden executar-se de **manera remota**, la qual cosa significa que al ciberterrorista ja no se li requereix entrenament físic, i les possibilitats de morir durant l'atemptat disminueixen, fet que garanteix la supervivència de l'organització.

2. Què és el ciberterrorisme

2.1. Evolució de la presència d'organitzacions terroristes a la xarxa

L'amenaça ciberterrorista ha anat gestant-se amb el pas dels anys. A continuació resumirem els seus inicis fins a situar-nos al moment actual.

La primera aparició d'organitzacions terroristes a la xarxa la trobem a la segona meitat de la dècada dels noranta, coincidint amb la fundació de l'organització Al-Qaeda. És en aquest moment quan apareixen els **primers llocs web amb continguts de caràcter islamista radical**, però sense que la seva presència generés cap tipus d'alarma. Més aviat van passar desapercebuts a Occident, ja que estaven editats en àrab i l'incipient desenvolupament de la xarxa va contribuir al fet que les tasques de difusió es realitzessin al món físic.

El 2002 s'inicia un nou període, que podríem denominar «professionalitzador», caracteritzat per l'abandó progressiu (però no la desaparició) de les webs. En aquest període, les organitzacions prefereixen destinar els seus recursos a **crear les seves productores de comunicació** amb l'objectiu de controlar l'elaboració, l'edició i la distribució del material ideologitzador. Al-Qaeda funda As Sahab, i Daesh funda Al Hayat i Al Furqan, encara que en aquest cas s'estima que el nombre de productores superaria la trentena, la qual cosa demostra el poder logístic de l'organització. En tots dos casos, el material s'elabora en diversos idiomes, dels quals els més utilitzats són l'anglès, el francès, l'alemany i el rus. Aquest canvi de perspectiva a l'hora de gestionar la difusió del seu missatge va fer que es produís un augment de contingut a la xarxa, així com un increment del nombre de seguidors, la qual cosa va contribuir a un creixent interès per materials amb contingut extremista radical. Un altre fet que es produeix en aquesta etapa és el **desenvolupament de fòrums i de xats** destinats a promoure l'intercanvi d'informació entre els usuaris, i cadascun d'aquests pot actuar com a agent radicalitzador, que al seu torn és adoctrinat per altres membres, i deriven així en una espiral adoctrinadora. En aquest cas, les comunicacions que es duen a terme en aquests espais són en àrab, fet que constitueix un element de seguretat enfront de possibles intromissions per part de les forces de seguretat.

Més recentment, des de 2007, cal descriure una tercera etapa que es correspon amb **el sorgiment o auge de les xarxes socials** (com ara Facebook, Twitter, Instagram o Telegram), així com la major popularitat de plataformes audiovisuals com YouTube. Això ha permès que les organitzacions es dotessin de millors eines a l'hora de difondre el seu missatge i arribar a un nombre cada vegada més gran d'individus. Fins i tot, com veurem amb més profunditat

Vegeu també

Les modalitats de captació, reclutament i adoctrinament per internet seran objecte d'estudi a l'apartat 4 d'aquest mòdul.

quan analitzem el procés de la ciberradicalització, la interacció virtual ofereix a l'organització l'oportunitat de dirigir-se directament, de manera selectiva, a aquells simpatitzants que per la informació que publiquen o les respostes de suport que reben en els seus perfils són més receptius al seu missatge, i per tant els converteix en individus més vulnerables a la captació i a la posterior radicalització. És el que denominem «radicalització passiva». A més, i continuant amb la finalitat per la qual van ser creats els fòrums, la majoria de les xarxes socials incorporen aplicacions de xat i de missatgeria mitjançant les quals els membres d'aquests perfils poden interactuar entre ells i compartir informació escrita (documents o missatges escrits), visual (gràfics, infografies, imatges), auditiva (per exemple, *nasheeds*) i audiovisual (vídeos).

2.2. Terrorisme, TIC i nadius digitals. Una amenaça real

El terrorisme no constitueix una fenomenologia criminal homogènia. A l'interior dels grups hi ha discrepàncies que poden fraccionar-los i donar lloc a altres de nous. Un exemple d'això és el naixement d'Estat Islàmic (també denominat EIIL, EI o Daesh) el 2010 com a escissió d'Al-Qaeda en plena guerra siriana, que fins llavors era el grup hegemònic. L'auge de Daesh difícilment pot entendre's sense analitzar el paper que han tingut les noves tecnologies. Sense elles segurament no haurien pogut reclutar tantes persones, obtenir donacions i presentar-se com un desafiament superior enfront d'enemics militaritzats i més ben capacitats que ells. Una mostra de la importància que donen a les TIC rau en el fet que els membres de l'organització dedicats a la seva gestió reben el títol d'emirs i un salari superior a la resta, a més d'altres beneficis (Torres, 2016). Per tot això, es considera que Daesh ha estat l'organització terrorista que ha aconseguit el grau més elevat de sofisticació i eficàcia, i es poden comparar les seves produccions amb l'estètica pròpia de Hollywood. No obstant això, després d'anys de guerra i la pèrdua de control territorial, Daesh ha quedat afeblit i això ha contribuït al renaixement de l'organització Al-Qaeda amb el fill d'Osama bin Laden, Hazam bin Laden, com a capdavanter.

Les productores de comunicació

Aquestes productores no solament elaboren i distribueixen el material, sinó que estudien la millor manera de difondre'l amb l'objectiu que arribi al màxim nombre de persones.

El primer grup terrorista que va utilitzar la xarxa per al seu benefici va ser Al-Qaeda, quan el 2011 va fer una crida als seus seguidors mitjançant el vídeo *For Incitement and Publishing: You Are Held Responsible Only for Yourself, Parts 1 and 2*, perquè qualsevol musulmà amb coneixements informàtics realitzés ciberatacs contra llocs web i xarxes electròniques de les grans empreses «enemigues dels musulmans». No obstant això, la fundació d'un cibercalifat capaç de realitzar ciberatacs no té lloc fins a dates més recents. Això es deu, segons Torres (2018), a dos motius:

- En primer lloc, les organitzacions terroristes no s'atreveixen a apostar pel món virtual fins que perceben l'èxit que són capaços d'aconseguir grups hacktivistes, com Anonymous o Wikileaks.

- En segon lloc, per realitzar aquest tipus d'accions es requereix el desenvolupament d'una determinada capacitat operativa i humana que el grup ha d'anar desplegant.

És freqüent assenyalar que, si bé el ciberterrorisme comença a preocupar cada vegada més a les institucions, especialment als països occidentals, de moment no s'han reportat accions terroristes significatives al ciberespai, la qual cosa no significa que no s'observin any rere any increments d'aquestes activitats. Ni Al-Qaeda ni cap altra organització terrorista sembla haver tractat d'organitzar, de moment, un ciberatac greu. No obstant això, podem localitzar la primera acció ciberterrorista amb una notable envergadura el 2007, amb l'atac cibernètic que van sofrir els llocs web d'algunes institucions estonianes i la programació del canal francès *TV5 Monde*, les emissions del qual van quedar interrompudes durant divuit hores, incidents que van provocar l'emissió d'un comunicat per part del Parlament Europeu. Aquestes accions posen de manifest la capacitat que comencen a tenir les organitzacions terroristes a la xarxa.

De moment, s'estima que a Europa l'organització terrorista Daesh ha aconseguit captar 35.000 individus, dones i homes, per la xarxa. En el cas concret d'Espanya, segons dades del Ministeri de l'Interior publicats en l'informe *Ciberamenaces i tendències* de 2017, les organitzacions terroristes han interferit en el funcionament normal o fins i tot han aconseguit el control momentani d'algunes empreses o instal·lacions del sector públic i privat, limitant-se a desconfigurar els llocs web, redirigir les seves adreces o realitzar petits actes maliciosos.

Al març de 2019, els mitjans de comunicació van informar que el califat de l'organització Daesh havia sucumbit després de la pèrdua de l'últim bastió sirià que tenien en possessió. No obstant això, aquest fet no sembla que freni la seva activitat, atès que el terreny físic perdut ha estat substituït pel virtual. És a dir, la destrucció de santuaris físics ha anat acompanyada de la creació de santuaris virtuals (Cano, 2019), una realitat que va vaticinar Abdel Bari Atwan el 2015 en defensar que sense la tecnologia digital seria bastant improbable que organitzacions terroristes com aquestes poguessin arribar a existir o subsistir. Segons Cano, la majoria dels que se senten atrets per continguts propers al ciberterrorisme són adolescents, la qual cosa no sorprèn si es té en compte que un 89 % d'ells té un comportament actiu a la xarxa i un 70 % usa diàriament els mitjans socials, passant un total de dinou a vint hores setmanals connectats. Aquestes característiques suposen un avantatge per a l'organització, ja que els seus integrants responen al perfil de «**nadius digitals**» de Prensky (2011). El citat autor adverteix que aquests individus pertanyen a una generació que ha nascut i s'ha format amb les noves tecnologies, la qual cosa els fa ser individus que prefereixen:

- rebre informació en format audiovisual (preferiblement en gràfics i imatges) i en un termini immediat;
- aprendre de forma autodidacta i en un mitjà lúdic;

- treballar en xarxa; i
- accedir per un únic document a uns altres, mitjançant enllaços directes.

El perfil d'aquests joves és oposat al dels «immigrants digitals», subjectes que han hagut d'aprendre a utilitzar les TIC per néixer en una època prèvia a elles, i que tendeixen a continuar utilitzant les eines d'interacció del món fora de línia. En l'àmbit econòmic i de seguretat, disposar de nadius digitals resulta beneficiós per a l'organització. D'una banda, no es requereix invertir grans quantitats de temps ni de diners en la seva formació en entorns digitals, i, d'altra banda, s'adquireix més capacitat operativa respecte a l'evolució tecnològica, la qual cosa els permet escapar al rastreig de les forces de seguretat.

Hi ha veus que llancen alarmes que en un futur proper, si les organitzacions continuen centrant els seus esforços en el ciberespai, podrien consolidar la **incipient gihad cibernètica** i provocar greus perjudicis econòmics, socials i de seguretat, en poder afectar instal·lacions tan sensibles com les centrals nuclears, que estan controlades per dispositius tecnològics susceptibles de ser atacats; alguns experts, no obstant això, consideren exagerades les alarmes donat el nivell de seguretat dels centres nuclears enfront dels ciberatacs (Weimann, 2004; Ruiz, 2016).

2.3. Definició i característiques principals

L'ús d'internet per part de grups terroristes com a mitjà per aconseguir algunes de les seves finalitats és conegut des de principis dels anys noranta. El 1999, l'Agència d'Intel·ligència de la Defensa nord-americana va avisar de la seva imminent irrupció. No obstant això, no es va parlar del terme *ciberterrorisme*, sinó que es va preferir utilitzar el de *guerra informàtica* (*infowarfare*). Malgrat això, en la dècada dels vuitanta **Barry Collin**, investigador principal de l'Institut de seguretat i intel·ligència de Califòrnia, ja va utilitzar el terme per fer referència a «la convergència de la cibernètica i el terrorisme». És a dir, la convergència entre el món virtual i el real. Després dels atemptats de l'onze de setembre, el ciberterrorisme es va considerar una amenaça real i global. Per exemple, després de la seva comissió, les institucions encarregades de vetllar per la seguretat van haver de canviar la concepció de terrorista per adoptar una altra en la qual el ciberespai tenia un paper rellevant. A partir d'aquest moment, algunes plataformes vinculades al gihadisme van ser objecte de ciberatacs, o el seu contingut va ser bloquejat (Torres, 2016). Així i tot, avui dia manquem d'una definició. Els motius que expliquen aquesta realitat són principalment tres (Brickey, 2012; Luiijf, 2014; Mayer, 2018):

- El primer resideix en la mateixa **naturalesa del concepte**, per ser el resultat de la unió de dos termes diferents, *ciber* i *terrorisme*.

- El segon el trobem en l'**interès** que va generar el seu estudi entre 1997 i 2001, per part de diferents disciplines, la qual cosa va derivar en una àmplia gamma de definicions.

- El tercer va ser la **confusió terminològica** entre el terme *ciberterrorisme* i uns altres de naturalesa similar (hi aprofundirem en el proper punt).

Per entendre el concepte, la millor opció és analitzar el significat de cadascun dels termes que el conceben. D'aquesta manera, entendrem ***ciber*** com el prefix que s'utilitza per indicar que l'acció es duu a terme al ciberespai i que implica l'ús de mitjans electrònics o d'internet; portat a l'àmbit del terrorisme, ens condueix a afirmar que internet es converteix tant en un objectiu com en una arma utilitzada per part dels terroristes, ja que usen el ciberespai per a tasques d'organització, control, intercanvi, planificació d'informació, recaptació de fons i intents d'augmentar el seu suport, difusió de propaganda ideologitzadora i per a tasques de reclutament (Luiijf, 2014). Entenem el ciberespai com el domini global dins de l'entorn de la informació format per xarxes i infraestructures interdependents que inclouen internet, les xarxes de comunicació i els sistemes informàtics (Ruiz, 2016).

Per ***terrorisme*** ha d'entendre's «l'ús o l'amenaça d'una acció dirigida a influir el govern o per intimidar el públic, o una secció del públic, amb el propòsit de promoure una causa política, religiosa, racial o ideològica» (UK Terrorism Act, 2000) o «la creació i explotació deliberada de la por mitjançant la violència o l'amenaça de violència en la cerca del canvi polític» (Hoffman, 2006).

De la unió de tots dos deriva el terme *ciberterrorisme*, que segons Denning (2000, 2001) és

> «la convergència del terrorisme i del ciberespai. S'entén que significa atacs il·legals i amenaces d'atac contra ordinadors, xarxes i informació que hi és emmagatzemada quan la finalitat que es persegueix és intimidar o coaccionar un govern o la seva gent en compliment d'objectius polítics o socials. A més, per qualificar un acte de ciberterrorisme hauria de produir-se amb violència contra persones o propietats, o almenys causar suficient dany per generar por».

Segons l'autora, els atacs contra infraestructures crítiques podrien ser un exemple d'actes constitutius de ciberterrorisme, però no els atacs que interrompen serveis no essencials o que causen petites molèsties. D'aquesta manera, dona suport a aquells que consideren que el terme *ciberterrorisme* és inadequat, perquè un ciberatac generalitzat pot simplement provocar molèsties, no terror. No obstant això, molts altres creuen que els efectes d'un atac generalitzat a la xarxa informàtica serien impredictibles i podrien causar suficient interrupció econòmica, por i morts de civils per considerar-se adequat qualificar-los de terrorisme. Per aquest motiu hi ha dues perspectives per mitjà de les quals es defineix el terme (Rollins i Wilson, 2007):

- **Segons els efectes** que produeix el ciberterrorisme, solament pot considerar-se com a tal si els danys que produeixen els ciberatacs adquireixen la magnitud suficient per generar una por comparable a un acte físic (o fora de línia) de terrorisme.

- **Segons la intenció**, el ciberterrorisme existiria quan les finalitats que persegueixen són il·legals o es realitzen per intimidar o coaccionar un govern o persones, promoure un objectiu polític, o per causar un dany greu en l'economia d'un país.

Lectura obligatòria

L'informe del Consell d'Europa *Ciberterrorisme: l'ús d'internet amb finalitats terroristes* està disponible a l'apartat «Recursos de l'aula». El document és material obligat d'estudi per a aquest primer bloc de l'assignatura.

Altres autors, com Lewis (2002) i Mantel (2009), defineixen el ciberterrorisme com l'ús de les eines que ofereix la xarxa per part de determinats grups amb la finalitat d'atacar infraestructures crítiques o per coaccionar o intimidar un govern o un individu de la població. Per la seva banda, Mshvidobadze (2011) ho defineix com el conjunt d'actes cibernètics o ciberatacs que es duen a terme per fomentar el terror o la desmoralització en una societat.

Si s'examina el sentit que s'ha donat al terme ciberterrorisme en els documents emanats de diverses institucions, el 2004 l'**FBI** s'hi refereix com

> «un atac premeditat i políticament motivat contra informació, sistemes computacionals, programes de computadores i dades que pugui resultar en violència contra objectius no combatents per part de grups subnacionals o agents clandestins».

El 2008, l'**OTAN** va definir el ciberterrorisme com

> «un atac cibernètic que utilitza o explota xarxes informàtiques o de comunicació per causar la destrucció suficient per generar por o intimidar una societat amb un objectiu ideològic».

Aquest mateix any, el **Consell d'Europa** va publicar l'informe *Ciberterrorisme: l'ús d'internet amb finalitats terroristes*, i ho va definir com «qualsevol activitat que es realitza per part d'una cèl·lula o individu terrorista mitjançant internet». El 2011, l'informe de la Primera Comissió de Desarmament i Seguretat Internacional de l'**Assemblea General de les Nacions Unides** ho defineix com les accions realitzades mitjançant una xarxa informàtica que poden causar violència o generar temor entre les persones, o provocar una destrucció greu per problemes polítics o socials.

Entre les diferents definicions de ciberterrorisme, adoptarem la de Luiijf (2014) per ser la més exhaustiva i que ens porta a entendre-ho com l'ús, els preparatius o l'amenaça d'una acció dissenyada per part d'un grup terrorista per dur-se a terme per la xarxa, amb la finalitat de provocar un canvi en l'ordre social, crear un clima de por o intimidació entre el públic, o influir en la presa de decisions polítiques per part del govern i promoure una causa política, religiosa, racial o ideològica. Això s'aconsegueix mitjançant ciberatacs dirigits contra infraestructures o sistemes, prèviament seleccionats, atès l'elevat valor en termes de seguretat que contenen les informacions que aquests alberguen.

A partir d'aquesta definició, podem observar que les característiques bàsiques del ciberterrorisme són les següents:

- **El context legal**: el ciberterrorisme és la materialització d'un acte delictiu o amb un propòsit delictiu.

- L'acció, o ciberatac, és duta a terme per **un grup o un individu** pertanyent o simpatitzant amb una ideologia que pretén la consecució d'objectius polítics per mitjans il·legals i **sense autoritat legal** per realitzar-la.

- L'objectiu que es persegueix és **coaccionar, controlar o provocar un dany a gran escala** contra una infraestructura crítica, que indirectament **genera sensació de por, terror o inseguretat** en la societat.

- L'acció està **motivada** per raons polítiques, ideològiques, religioses o socials.

- El **ciberespai** és l'arma i l'objectiu de les accions perpetrades pels grups terroristes. Els grups terroristes aprofiten les opcions que donen les noves tecnologies per aconseguir les seves finalitats.

- La **interferència o interrupció d'un sistema electrònic**.

- Els actes provoquen **efectes psicològics** de gran abast per al públic assenyalat com a objectiu.

2.4. Ciberterrorisme i altres termes relacionats

Com hem comentat a l'apartat anterior, un motiu pel qual encara no disposem d'una definició consensuada sobre què és el ciberterrorisme és la confusió terminològica que ens porta a confondre'l amb altres termes com *ciberguerra*,

cibercrim, *ciberactivisme* (o *hacktivisme*), *ciberextremisme*, *terrorisme cibernètic*, *gihad virtual*, *gihad en línia* o *gihad electrònica*, que malgrat la seva similitud etimològica descriuen realitats diferents.

Per als objectius d'aquesta assignatura diferenciarem el ciberterrorisme del hacktivisme, el terrorisme cibernètic i el delicte cibernètic.

1) Hacktivisme: fa referència a les activitats en línia amb la finalitat de revelar, manipular o explotar vulnerabilitats en sistemes operatius per aconseguir objectius polítics, com poden ser promoure o privilegiar una ideologia política per sobre d'una altra (Weimann, 2004), o, dit d'una altra manera, utilitzar els coneixements informàtics amb finalitats polítiques. Per a això, els activistes disposen de diversos mitjans: bloquejos virtuals, atacs de correu electrònic, pirateria informàtica i robatoris informàtics, virus informàtics, o redireccionament de llocs web. Al seu torn, hem de diferenciar aquestes accions del ***hacking***, que respon a l'acció que duu a terme qualsevol persona amb coneixements informàtics amb la finalitat d'introduir-se, sense autorització, en sistemes aliens per manipular-los o obtenir informació, entre altres accions, amb finalitats ètiques, antiètiques o fins i tot neutrals, com la simple diversió.

Exemple de hacktivisme

Les accions del grup Anonymous.

2) Terrorisme cibernètic: és un terme que sol utilitzar-se a la premsa i als mitjans de comunicació de masses per esmentar els ciberdelictes de motivació no terrorista que causen greus alteracions en el funcionament de les infraestructures d'un país, i que generen temor o inquietud entre els ciutadans. Aquesta tendència a la utilització extensiva i fins i tot provocadora i hiperbòlica del terme terrorisme es detecta també quan des de certs sectors s'usa per referir-se a conductes vials extremadament perilloses (terrorisme vial), per condemnar accions pernicioses contra el medi ambient (terrorisme ecològic) o per suscitar el màxim retret contra certes formes de violència en la parella (terrorisme domèstic).

Exemple de terrorisme cibernètic

L'espionatge o el robatori de comptes bancaris.

Per tant, quan s'utilitza el concepte *terrorisme cibernètic* darrere s'amaga una finalitat sensacionalista que busca expandir les connotacions pejoratives de l'acció terrorista a accions de diferent naturalesa.

3) Delicte cibernètic: l'element que el diferencia del ciberterrorisme és la motivació que es persegueix amb la comissió del delicte. Mentre que el ciberdelicte o delicte cibernètic persegueix una finalitat, econòmica o d'un altre tipus, sense que això suposi posar en perill la vida dels ciutadans, la motivació del ciberterrorisme va més enllà de voler provocar un dany massiu per imposar unes creences, una ideologia o una governabilitat, a més d'aprofitar els beneficis de les TIC per a finalitats de captació, reclutament i radicalització d'individus que, posteriorment, es mostrin disposats a realitzar atemptats al món real.

3. Ús de les TIC per part de grups terroristes

3.1. Mitjans d'actuació

Des de la comissió dels atemptats de l'onze de setembre de 2001 contra les Torres Bessones i el Pentàgon, s'ha tingut més constància de l'ús de les TIC per part de les organitzacions terroristes. Si bé part del seu èxit es deu a les facilitats del mitjà tecnològic en termes de vulnerabilitat i escassa formació en ciberdelinqüència per part dels agents de seguretat, igual que va succeir amb les accions terroristes al món fora de línia, les organitzacions han sabut adaptar-se al ciberespai i anar explorant noves maneres de mantenir i propagar el seu missatge.

Per aconseguir les seves finalitats, les organitzacions es doten de diferents infraestructures que, donat l'ampli abast dels continguts que poden distribuir-s'hi, han potenciat la capacitat de difusió directa del contingut per mitjà d'internet, disminuint així la dependència dels canals tradicionals de comunicació.

Mentre que abans els continguts només podien distribuir-se per mitjans físics (per exemple, mitjançant el suport CD, VHS o DVD) a un públic relativament limitat, l'ús d'internet els ha permès distribuir-los per una àmplia gamma d'eines. Recordem que l'organització Al-Qaeda, l'any 2000, va ser la primera que va fundar la seva pròpia productora audiovisual, As Sahab, mitjançant la qual ha difós més de set-cents arxius de material audiovisual. Aquesta iniciativa va ser i és també utilitzada per altres organitzacions terroristes com ara Daesh que, com s'ha indicat, compta amb més de trenta productores que elaboren, a més de vídeos, la revista oficial *Dabiq* i que gestionen un canal de televisió i una emissora de ràdio, *Bein HD4* i *La veu del califat*, respectivament.

Les infraestructures més utilitzades són les següents:

1) Llocs web: els llocs web van ser els primers canals pels quals les organitzacions es van donar a conèixer. En aquests, es posa a la disposició de l'individu un conjunt de recursos (vídeos, revistes, enllaços externs, etc.) que es poden visualitzar en línia o ser descarregats. A conseqüència de l'auge de les xarxes socials, les webs han anat perdent força, i això ha permès una descentralització de la informació.

Exemples de webs

AQ/QA, Al-ansar o *Muslims news*, entre altres.

2) Xarxes socials i aplicacions de missatgeria instantània: les organitzacions han creat perfils a les diferents xarxes socials existents, de les quals Facebook i els canals de Telegram (Nikolái i Pável Dúrov) són les més recurrents; especialment Telegram per la seguretat i la privadesa que brinda, ja que, a part del xifrat complet, els missatges són eliminats al cap de poques hores; a més, la majoria dels terroristes arrestats a Europa ho han estat després de rastrejar la seva activitat en aquesta plataforma. També coincideix el fet que les reivindicacions que fan les organitzacions després de la comissió d'algun atemptat per part d'algun dels seus membres es realitzin per aquest mitjà, com va succeir el desembre de 2016 després de l'atemptat contra un mercat nadalenc a Berlín.

Actualment es considera que les xarxes socials són la porta d'entrada al terrorisme, així com els mitjans de connexió entre les organitzacions terroristes i els simpatitzants, donat el seu accés fàcil i ràpid i al fet de guardar una aparença de certa horitzontalitat entre ambdues parts. A més, el seu ús els garanteix que un nombre important de seguidors siguin joves. No oblidem que aquestes xarxes són consumides, principalment, per aquest sector de la societat, un aspecte que les organitzacions coneixen i aprofiten per impactar sobre la seva autoestima mitjançant reforços positius.

Exemple de reforç positiu a seguidors joves

Un individu que participi activament a les xarxes i comparteixi informació en el seu compte personal té més possibilitats de rebre una insígnia virtual en la qual se li concedeixi el rang de «membre destacat» o «membre sènior», per exemple (Halopeau, 2014).

La immediatesa de la comunicació afavoreix que el subjecte estigui informat a tota hora, així com interaccionar amb altres individus per les aplicacions de xat de què disposen. Un altre aspecte que cal ressaltar és que les xarxes socials són eines més difícils de controlar i de tancar per part dels cossos de seguretat, i en el cas que així es produís, el grup podria crear nous perfils en qüestió d'escassos minuts.

3) Fòrums i xats: permeten al grup mantenir la seva informació constantment actualitzada i es converteixen en una potent plataforma a la qual poden acudir persones amb la mateixa manera de pensar del grup (independentment de la seva ubicació geogràfica) i compartir, entre altres coses, mètodes, tècniques o coneixements operacionals específics amb la finalitat de cometre actes de terrorisme. Per aquest motiu, aquestes estructures són considerades autèntiques «caixes de ressonància» de la ideologia de l'organització.

No obstant això, per accedir-hi, la majoria requereixen claus d'accés que solament són remeses per part d'algun membre de l'organització quan ha pogut assegurar-se que el subjecte els serà útil i fidel. Aquesta restricció d'accés (o barrera tecnològica) no només afegeix un grau més de dificultat a les operacions antiterroristes, fent necessari recórrer a la infiltració d'algun dels seus agents per conèixer el contingut de les converses que es mantenen, sinó que també genera en el subjecte un sentiment d'«exclusivitat» que pot contribuir a reforçar la seva autoestima i el desig de pertànyer al grup, la qual cosa origina forts llaços d'amistat que poden acabar derivant en un microcosmos digital (Cohen-Almagor, 2017). Halopeau (2014) afirma que la manera de controlar aquests fòrums ha evolucionat. Si bé en el passat cadascun solia estar controlat per un sol administrador, en l'actualitat són gestionats entre diversos admi-

nistradors. D'aquesta manera, s'intenta evitar que els agents policials puguin identificar-los i arrestar-los i que el fòrum deixi de funcionar, ja que en cas d'arrestar o condemnar-ne un, els altres poden continuar amb la tasca.

4) Videojocs: per mitjà de les possibilitats audiovisuals que ofereixen, els videojocs són capaços d'emular o de traslladar situacions socioculturals del món real al virtual, i fer sentir l'individu com el veritable protagonista després de la creació del seu avatar. És a dir, el subjecte ha de fer del seu «jo» un element gràfic que el representi en el joc. No obstant això, aquest no ha de reproduir fidelment les característiques de la persona, sinó que pot modificar els aspectes que menys li agraden per uns altres.

Si bé hi ha diferents tipus de videojocs, atenent diferents variables, ens centrarem en els videojocs massius (*massively multiplayer online role-playing game*, MMORPG) de temàtica bèl·lica, com poden ser les sèries de *Call of Duty: Black Ops* o *Grand Theft Auto*. Aquests videojocs són els més utilitzats per les organitzacions terroristes per captar futurs membres, ja que requereixen poc desgast mental. S'ha observat que algunes organitzacions terroristes han elaborat els seus propis videojocs, o modificat els comercials, afegint opcions que els facin més propers a l'estil gihadista.

Exemple d'opcions properes a l'estil gihadista

Executar persones al crit d'*Allahu Akbar*, dissenyar escenaris que reprodueixen els carrers de Síria, o introduir com a vestimenta el vestit taronja característic dels presos de Guantánamo.

Per jugar a un MMORPG el subjecte ha d'interactuar amb altres jugadors simultàniament, que igual que ell estan connectats a la xarxa (Carbonell, Torres i Fuster, 2016). En tractar-se d'un món no físic, el subjecte sap que la violació de les normes del joc no li reportarà un càstig real, la qual cosa allunya el jugador del cost real que tindria la seva conducta si es dugués a terme al món fora de línia.

5) Revistes en línia: les organitzacions terroristes veuen en les opcions multimèdia un canal excepcional pel qual difondre la seva ideologia i captar nous individus per a les seves files. En aquestes revistes:

- es presenten manifests;
- es publiquen cartes o testaments de mujahidins caiguts en combat amb l'«enemic» amb l'objectiu de glorificar i de banalitzar la mort;
- es realitzen crides contra els enemics; o
- s'explica com elaborar material explosiu, utilitzar armes blanques o vehicles per cometre atemptats als seus països de residència.

De fet, com assenyalen Lemieux, Brachman, Levitt i Wood (2014), els atemptats de la marató de Boston, el 2013, van ser planificats seguint les indicacions de fabricació d'explosius que es descrivien en un nombre de la revista d'Al-Qaeda, *Inspire*. Com hem explicat anteriorment, el tractament visual i gràfic que es duu a terme del seu contingut és impecable, i cerca en tot moment un impacte capaç de captar l'atenció del lector. No obstant això, aquesta organització no ha estat l'única a recórrer a l'edició i difusió de revistes amb l'objectiu d'ampliar les seves bases. Daesh, després de l'autoproclamació del califat, tam-

bé ho ha fet amb les revistes *Dabiq*, *Dar al-Islam*, *Istok* i *Konstantiniyye*, publicades per Al-Hayat Media Center i redactades en anglès, francès, rus i turc, respectivament. Destaca el fet que aquestes publicacions són de fàcil accés i elaborades en diversos idiomes, els més utilitzats dels quals són l'anglès, el francès i el rus, a part de l'àrab.

Malgrat que es dirigeixen a un públic masculí, des de 2015 la secció femenina de Daesh, formada per la Brigada al-Khansaa i la Brigada d'Umm al-Rayan, té reservat un espai en *Dabiq* sota el títol «Per a les nostres germanes» en què, recorrent a un llenguatge col·loquial, s'emfatitza en el rol fonamental que tenen les dones en el califat, així com es desmenteix la informació que des d'Occident es dona sobre el rol real de la dona en l'organització. Encara que aquest material s'edita des del Pròxim Orient, el missatge va dirigit principalment a noies i a dones residents en països de majoria no musulmana amb l'objectiu que es desplacin cap al califat per servir a l'organització. Tot això es basa en la creença que el paper fonamental de la dona no és un altre que el de la maternitat i la cura de la llar, però, lluny de la promesa d'una vida plena com a esposes i mares dels futurs màrtirs, aquestes acaben sent esclaves sexuals.

La Brigada al-Khansaa i la Brigada d'Umm al-Rayan

Aquestes brigades estan integrades per dones d'edats compreses entre els divuit i els vint-i-cinc anys, que es dediquen exclusivament a vigilar la preservació de l'ordre a l'espai públic i a fer complir (de manera expeditiva) les estrictes normes de la xaria a totes les dones que viuen al territori del califat. A canvi, reben un sou, l'accés a serveis i una manutenció.

6) ***Nasheed***: amb aquest nom es fa referència al gènere musical musulmà que consisteix a cantar *a cappella*, o amb l'acompanyament d'algun instrument quan es tracta d'un enllaç matrimonial, un poema o part d'ell. No obstant això, després de l'esclat de la Primavera Àrab i l'autoproclamació de l'autodeclarat Estat Islàmic per part de Daesh, aquestes formes d'expressió han aconseguit un èxit que fins llavors no tenien, i s'han convertit en autèntics himnes per als simpatitzants de la ideologia gihadista, així com en elements fonamentals de la seva propaganda, atès que la seva principal funció és la mobilització i la radicalització dels oïdors.

A diferència de les *nasheeds* originals, i a pesar que la seva estructura està pautada (per exemple, la seva melodia no ha d'incitar al ball i no ha de distreure l'oïdor de la seva tasca d'estudiar l'Alcorà, entre altres), les actuals són cantades per un cor de veus masculines que repeteixen reiteradament (gairebé com mantres):

- narracions de tipus bèl·lic (*nasheeds* de batalla);
- narracions d'al·legoria o de commemoració a un màrtir caigut en combat amb l'«enemic» (*nasheeds* de martiri); o
- narracions d'exalçament de les característiques del mujahidí (*nasheeds* de lloança).

A més, l'idioma no sempre és l'àrab; es pot emprar també el francès, l'anglès o l'alemany (Said, 2012).

D'altra banda, la reacció que es pretén aconseguir en el receptor està manipulada per programes informàtics. És a dir, la peça musical obtinguda és tractada pels productors (membres de l'organització que formen l'equip d'unitat propagandístic Al-Ajnad Foundation), com si fos un disc comercial. Aquests individus s'encarreguen d'ajustar les veus, d'harmonitzar-les, de controlar els temps d'aparició, i d'inserir sons militars (per exemple, el so de passos marxant o d'armes de foc carregant-se), per finalment distribuir-la pels mitjans de l'organització, els principals canals dels quals són les seves xarxes socials i fòrums, encara que també se n'han localitzat milers al canal YouTube, les reproduccions del qual aconsegueixen xifres molt elevades. Donades les característiques i el fàcil accés que qualsevol persona pot tenir-hi, el seu control és una tasca molt complicada.

Exemple de producció de *nasheed*

Una de les produccions musicals més importants, i que s'ha convertit en senyal d'identitat del grup, és la que porta per títol *My Ummah, Dawn has Appeared*, que compta amb més de 220.000 reproduccions a YouTube.

3.2. Activitats principals del ciberterrorisme

Les organitzacions utilitzen les diferents estructures que acabem de veure per aconseguir finalitats diverses. L'Oficina de les Nacions Unides contra la Droga i el Delicte (UNODC) va assenyalar sis maneres de com pot utilitzar-se internet per a activitats terroristes: difusió de propaganda; captació, reclutament, adoctrinament i radicalització; finançament; formació; planificació i ciberatacs.

1) Difusió de propaganda: les organitzacions terroristes fan servir internet amb finalitats propagandístiques. Per a això s'utilitza el terme *gihad mediàtica*. Les organitzacions saben que amb una publicitat potent que emfatitzi la seva imatge, la brutalitat en l'acció i les seves victòries tàctiques, poden projectar una imatge de poder i d'ambició il·limitada (Torres, 2016). La propaganda es duu a terme mitjançant comunicacions d'imatge, àudio o vídeo, amb què es difon ideologia, es promouen activitats terroristes i es proporciona una justificació. En aquests materials es mostra la capacitat del grup per realitzar operacions (com atacs suïcides), publicar declaracions amb les seves intencions o els testaments de terroristes, així com mostrar els col·lectius que donen suport a la seva causa mitjançant la publicitació dels patrocinadors. La infraestructura els permet accedir, autopublicar i actualitzar informació contínuament. No obstant això, el que determinarà que una publicació es consideri, o no, propaganda terrorista i no un acte emparat pel dret a la llibertat d'expressió internacionalment reconegut, serà una avaluació subjectiva. Com se sap, el dret a la llibertat d'expressió garanteix a les persones poder compartir una opinió o distribuir contingut que pot ser considerat ofensiu per altres, a reserva de certes excepcions limitades previstes per llei com són la distribució de contingut sexualment explícit o la promoció i incitació a la violència, una cosa que constitueix una pràctica recurrent en la propaganda d'aquests grups.

2) Captació, reclutament o radicalització: aquesta utilitat està estretament relacionada amb l'anterior, ja que l'organització necessita propaganda amb un contingut que s'adapti a les característiques dels grups més vulnerables, i perquè internet pugui erigir-se com un mitjà capaç d'establir relacions amb les persones més receptives a la propaganda amb l'objectiu de captar-les, adoctrinar-les i radicalitzar-les amb la finalitat que acabin cometent un acte terrorista. Per aquest motiu, el missatge amb el qual es bombardeja un subjecte es caracteritza per contenir un elevat grau de violència (visual o verbal) i apel·lacions als sentiments d'injustícia, exclusió i humiliació.

Si aquest procés per si mateix ja és difícil d'identificar i prevenir, es torna molt més complex quan el mitjà utilitzat és la xarxa. El procés d'adoctrinament s'estructura en diverses fases, per mitjà de les quals es generen els tres elements necessaris que, segons la teoria de la recerca de la significança (*significance quest theory*, SQT), es requereixen perquè un individu completi la fase de radicalització en una ideologia extremista i decideixi fer el pas cap a l'acció terrorista. Aquests elements són els següents: la necessitat, la narrativa i la xarxa de suport (Kruglanski, Jasko i LaFree, 2016; Kruglanski, Webber, Chernikova i Molinario, 2018).

A Espanya, l'any 2011 la Fiscalia General de l'Estat va publicar la Circular núm. 2/2011, de 2 de juny, i el 2015 el Ministeri de l'Interior va fer públic un informe en el qual s'estimava que el 80 % de la captació i de l'adoctrinament es produïa en llocs físics, com ara mesquites o centres universitaris, i sempre amb la presència d'un agent radicalitzador físic. En l'actualitat, aquest predomini ha estat reemplaçat per internet, fins al punt de convertir-se en el centre virtual de l'extremisme (Cano, 2008; Reinares i García-Calvo, 2017; Reinares, García-Calvo i Vicente, 2018). No obstant això, com defensa Vicente (2018), actualment l'adoctrinament per mitjà, únicament, del ciberespai (sense intervenir interacció física) sembla poc viable. En la majoria dels casos documentats a Europa i a Amèrica, l'estadi de la radicalització va requerir un contacte cara a cara amb algun membre de l'organització a la qual pertanyia l'individu.

La captació i radicalització per la xarxa també s'ha utilitzat en el cas de les dones. El 2015, la Brigada al-Khansaa va publicar en pàgines web i fòrums afins a l'organització terrorista Daesh, un manifest de caràcter propagandístic dirigit a la comunitat femenina musulmana resident en països àrabs, amb la finalitat de reclutar dones. Aquest document, sota el títol *Les dones a l'Estat Islàmic: manifest i estudi de cas*, està estructurat en tres seccions en què es pretén descriure el paper de la dona musulmana a la seva comunitat, així com l'estil de vida que ha de portar si vol seguir les directrius del Profeta. L'objectiu és que quan la dona acabi la lectura tingui la sensació que portar una vida legítima i fructífera fora del califat és impossible. D'aquesta manera, experimenta la necessitat d'abandonar el seu país i anar-hi a viure.

3) Preparació d'atemptats: la primera vegada que es va tenir consciència d'aquest ús va ser amb l'organització Al-Qaeda, quan es va comprovar l'ús de l'esteganografia per ocultar missatges en imatges i en pel·lícules. No obstant això, la quantitat d'informació que pot ocultar-se és molt limitada, per aquest motiu es va canviar de mètode (Halopeau, 2014).

L'esteganografia

És un mètode d'ofuscació que serveix per ocultar un missatge dins d'un altre missatge visual (com ara imatges) perquè a simple vista no pugui ser detectat. Algunes de les eines que permeten fer aquest xifrat són les següents: FileInyector, Our Secret o Steganographia.

Després dels atemptats al tren de Madrid l'onze de març de 2004, els detinguts van revelar que estaven utilitzant un nou mètode per evitar la detecció de les seves comunicacions. El concepte era tenir un sol compte de correu electrònic compartit entre tots els membres del grup on poguessin escriure correus electrònics i deixar-los a la carpeta d'esborranys. Avui dia, aquesta tècnica s'ha deixat d'usar per ser ben coneguda. Després es van utilitzar altres eines com PGP o TrueCrypt. Però per garantir la privadesa de la informació, el 2007 les organitzacions van començar a desenvolupar les seves pròpies eines, com Mujahideen Secrets o Mujahideen Secrets 2, que van ser utilitzades per membres d'Al-Qaeda en la planificació d'un atemptat fallit a França el 2008. Més recentment, el 2013, el Front Islàmic Global de Mitjans va llançar Asrar al-Dardashah, el funcionament i l'aparença del qual recorda les existents en missatgeria instantània. Una altra eina és Pidgin, que requereix la creació d'un compte previ a Google Talk, MSN, Yahoo, AOL Instant Messenger i Jabber o XMPP. La importància que dona l'organització a les seves xarxes arriba a l'extrem d'emular el sistema Android. La diferència és que les seves aplicacions no poden ser descarregades des d'una botiga oficial, sinó que l'usuari ha de dirigir-se expressament al lloc web de l'organització i seguir els passos indicats.

4) Finançament: les organitzacions terroristes també utilitzen internet com a mitjà per finançar els seus actes i sufragar les despeses derivades d'aquests com, per exemple, la compra d'armes, els lloguers de pisos francs, l'adquisició d'equip tècnic, etc. Per a això poden:

- demanar directament als seus simpatitzants que contribueixin a la recaptació de fons aportant donacions personals;
- utilitzar alguna secció de les seves pàgines web com a botiga electrònica en què els seus simpatitzants puguin adquirir material de l'organització o relacionat amb la seva ideologia;
- emprar serveis de pagament en línia;
- usar transferències de fons per transferència bancària electrònica, targeta de crèdit o serveis de pagament com PayPal o Skype; i

Exemples d'organitzacions que desvien fons a organitzacions terroristes

Alguns exemples contrastats són la Benevolence International Foundation, la Global Relief Foundation i la Holy Land Foundation for Relief and Development.

- rebre suport financer per part d'organitzacions aparentment legítimes o benèfiques que desviïn part dels seus fons a comptes d'organitzacions terroristes.

5) Formació: la versatilitat d'internet, unida a les múltiples oportunitats que ofereix, ha propiciat que les organitzacions el trobin un mitjà ideal per formar els reclutats, tant en ideologia com en la fabricació i la utilització d'armes mitjançant manuals en línia de fàcil accés i en diversos idiomes, fitxers d'àudio i vídeo, o materials d'informació i d'assessorament amb instruccions detallades; una autèntica biblioteca en línia que pot consultar-se en qualsevol moment i des de qualsevol lloc. D'aquesta manera, internet s'ha convertit en el substitut dels camps d'ensinistrament terrorista situats en llocs secrets de la geografia del país de l'organització.

6) Ciberatacs: no hi aprofundirem, ja que els tipus de ciberatacs que citarem a continuació ja han estat matèria d'estudi en altres assignatures. Com ja se sap, un ciberatac respon a la conducta d'explotació deliberada de xarxes informàtiques amb l'objectiu de llançar un atac mitjançant aquestes o pertorbar el seu funcionament normal. Les xarxes més utilitzades per part de les organitzacions terroristes són les següents:

- ús de programa maliciós;
- enviament de virus infectats per modificar o danyar el sistema informàtic;
- enviament massiu de correu brossa o correu no desitjat;
- suplantació de remitents de missatges mitjançant Spoofing per accedir a recursos continguts en un tercer sistema i enviament o instal·lació d'arxius espies (*keyloggers*); i
- ús de troians o d'arxius BOT per aconseguir el control remot de sistema sense el coneixement ni el consentiment de l'usuari.

Una altra ciberacció d'interès és l'ús de la tècnica *blind radars*, que permet el bloqueig del trànsit aeri interferint electrònicament en els radars i sistemes situats a les torres de control dels aeroports i heliports. Totes aquestes accions solen durar poc, i tenen com a finalitat contribuir a la missió de la gihad. Per tant, els ciberatacs tenen, avui dia, una finalitat instrumental.

Segons Torres (2016), la possibilitat que una organització terrorista desenvolupi la seva pròpia ciberarma, encara és una cosa molt a llarg termini, ja que el seu disseny no solament implicaria un elevat cost econòmic, sinó també temps per provar el programari, comprovar la seva seguretat i immunitat enfront de ciberatacs, així com avaluar la seva efectivitat en relació amb els objectius buscats per l'organització. L'altra opció que podrien barrejar seria establir contractes de col·laboració amb alguna empresa professional perquè desenvolupés la

ciberarma. No obstant això, i malgrat l'abundant guany econòmic que això podria reportar-li, les conseqüències que pogués tenir per a l'empresa (el prestigi i la visibilitat social), a llarg termini ho farien inviable.

Com es pot observar, en aquest mòdul dedicat al ciberterrorisme no entrarem a debatre o a contrastar dades epidemiològiques, ja que no hi ha consens i sí grans dificultats per determinar amb certesa si un ciberatac respon a aquesta naturalesa o és el resultat d'una acció comesa per *hackers* amb certa simpatia o inspiració gihadista, com són, per exemple, Islamic State Hacking Division, Sons Caliphate Army, Cyber Caliphate Army o Kalacnikov.TN, l'objectiu final dels quals és crear entre tots un cibercalifat (*United Cyber Caliphate*).

Mitjans / Estructures	**Usos / Activitats**
• Pàgines web • Xarxes socials i aplicacions de missatgeria instantània • Fòrums i xats • Videojocs • Revistes en línia • *Nasheed*	• Difusió de propaganda • Captació, reclutament i/o adoctrinament • Planificació d'atemptats • Finançament • Formació • Ciberatacs

4. El procés de radicalització per la xarxa

4.1. La radicalització. Definició

La radicalització s'ha definit com el procés pel qual un individu adopta actituds i creences que justifiquen, tant utilitàriament com moralment, el terrorisme inspirat en una versió radical i extremista, que té lloc després de la prèvia captació i reclutament per part d'una organització terrorista (Cano, 2008; Reinares i García-Calvo, 2017). Si bé aquest procés pot obeir a diferents motius, en el cas del terrorisme de base religiosa té com a objectiu socialitzar l'individu a una lectura i interpretació tergiversada i tendenciosa del credo islàmic. Aquest procés, com defensen Cano i Castro (2018), consta de dos components: un de caràcter **social**, atès que perquè es doni el procés es requereix la interacció (física o no) amb un altre individu, i un altre **ideològic**, en ser l'objectiu aconseguir que un individu substitueixi el seu sistema de normes i valors, incloent-hi la seva manera de pensar, pel de l'organització.

Per això és important destacar que sempre parlem d'un procés i no d'un estat, ja que una persona difícilment es desperta convertida en terrorista, sinó que s'arriba a aquest estat després de la successió de diverses etapes. Concretament, i com explicarem amb més detall en el proper apartat, en quatre etapes que són les següents (Silber i Bhatt, 2007):

- aproximació i primers contactes;
- captació, adhesió i prerradicalització;
- aïllament i adoctrinament; i
- gihadització, que podem reanomenar «cibergihadització» per produir-se en l'entorn digital.

Advertiment sobre l'adoctrinament

Abans d'aprofundir-hi, volem advertir que cap de les fases que integren el procés ha de ser entesa de manera determinista o unidireccional, en ser l'adoctrinament un procés que pot abandonar-se en qualsevol d'elles, i evitar així la seva culminació. D'una altra manera no podríem explicar per què són tan pocs els casos en què algú que ha iniciat un procés de captació i d'adoctrinament decideix finalment fer el pas i implicar-se en una activitat de tipus terrorista.

4.2. El procés de ciberradicalització i el perfil de les cibervíctimes

Els primers a advertir de l'ús de les TIC com a mitjà de radicalització van ser Sageman (2004) i Weimann (2004). A diferència de l'adoctrinament fora de línia, internet ha permès intensificar i agilitar el procés, i disminuir el període de temps necessari a solament uns mesos, ja que la xarxa possibilita estar en contacte permanent amb la ideologia i amb els agents radicalitzadors. Aquest

fenomen s'ha denominat per part de la premsa i d'alguns experts «adoctrinament exprés». Per tant, la ciberradicalització no és un procés que hagi aparegut paral·lelament a la implantació de les TIC, sinó que les organitzacions han sabut redefinir-les (Grabosky, 2001).

A continuació, descriurem cadascuna de les quatre fases que formen el procés, així com el perfil dels individus que hi intervenen. No obstant això, per entendre millor el procés hem de tenir present que al ciberespai la conducta decisional del subjecte està limitada per la ingenuïtat i la impulsivitat que comporta actuar per internet (Agustina, 2014). Això es deu al fet que els elements que constitueixen l'entorn virtual actuen directament en la via emocional del subjecte (Bouzar, 2015, 2017).

Les quatre etapes que es descriuran no han d'entendre's seqüencialment, sinó que poden presentar-se de manera discontínua, ja que no tots els individus aconsegueixen l'últim estadi passant per totes les anteriors, sense oblidar els casos en què els individus abandonen el procés. Un repte per a la recerca criminològica, de gran interès pràctic, és l'estudi dels factors que afavoreixen el desistiment i la continuïtat del procés.

1) Aproximació i primers contactes: a diferència del que succeeix en la modalitat fora de línia, aquesta fase pot produir-se de dues maneres, segons la major o menor iniciativa que mostri el subjecte en el reclutament. Per això diferenciem entre una «aproximació activa» i una «aproximació passiva» (Guirao, 2019). En la primera (aproximació activa) és l'individu qui decideix posar-se en contacte amb l'organització per mitjà d'alguna de les seves estructures; per exemple, escrivint un missatge a les seves xarxes socials. Aquest primer perfil respon a una persona jove que experimenta sentiments d'humiliació, frustració, culpa, odi, ira o indignació, com a resposta a experiències personals o per fets negatius que han succeït en el seu entorn. Tots aquests fets actuen com a factors *push* (precipitadors o potenciadors), i faciliten que l'individu prengui la iniciativa de voler ingressar a l'organització. Al seu torn, aquests factors victimògens personals són els que indiquen als «ciberulladors» que aquest subjecte pot ser un bon candidat per reclutar. Recordem que la radicalització és un procés que pot iniciar-se per una multitud de causes, ja siguin de tipus individual o social.

L'interès que mostra el subjecte pel grup ha pogut iniciar-se per mera curiositat, és a dir, el subjecte es connecta a la xarxa i comença a buscar informació gihadista sense que aquesta hagi de guardar relació directa amb una organització terrorista o amb continguts que es mostrin proclius a la violència gihadista. Així, aquests subjectes podrien considerar-se víctimes propícies passives a la cibervictimització terrorista, si prenem com a referència la tipologia de Cohen i Felson (1979). No obstant això, conductes aparentment neutrals o «innocents» com les descrites poden ser interpretades pels ciberreclutadors com a expressives de la voluntat d'entrar a formar part de l'organització.

Quan la conducta del subjecte va més enllà de la simple curiositat, la cerca no s'atura, s'incrementen les hores enfront del monitor i s'aprofundeix en el contingut que alberga la xarxa, ens trobem davant una conducta de cerca gairebé obsessiva que li permet interioritzar els postulats gihadistes. En aquest punt és quan el subjecte comença a visitar perfils d'organitzacions i a consumir material propagandístic en el qual es mostren imatges com les de la guerra a Síria o cadàvers de dones i nens assassinats per l'«enemic». Aquests materials contribueixen a l'elaboració d'una narrativa victimista que l'organització utilitza per generar en l'individu el desig de venjança i per justificar i legitimar l'ús de la violència (Trujillo, Moyano i González-Cabrera, 2006; Kruglanski, Webber, Chernikova i Molinario, 2018).

D'altra banda, la visualització d'aquest tipus de materials fa que el subjecte comenci a qüestionar-se tant el seu estil de vida com el sistema de creences en el qual ha estat socialitzat per decidir substituir-lo pel de l'organització. Tot això deriva en un pensament desindividualitzat i dicotòmic per part del subjecte, que tendeix a diferenciar entre un «nosaltres» i un «ells». Paral·lelament, mentre experimenta sentiments de ràbia i d'odi cap a Occident, desenvolupa empatia i solidaritat cap a la comunitat musulmana (*Umma*). D'aquesta manera, qualsevol conducta o comentari que es realitza sobre el poble musulmà, i que el subjecte interpreta com a «injust», «cruel» o «humiliant», ho percep com un atac a la seva identitat. Això és el que Khosrokhavar (2003) va denominar «humiliació delegada».

El concepte *gihad*

Aquest concepte pot interpretar-se de dues maneres, segons la finalitat que persegueixi. L'Alcorà diferencia, d'una banda, una interpretació espiritual que la defineix com la «gran» gihad o la gihad «interior», que es refereix a l'esforç que cada musulmà ha de realitzar en el seu dia a dia per arribar a ser millor persona, millor musulmà, allunyant-se de les conductes que el puguin corrompre; d'altra banda, tenim la interpretació bèl·lica i defensiva, la gihad «menor» o «exterior». Aquesta interpretació permet justificar l'acció violenta comesa per un individu o grup, la finalitat del qual és eliminar el *takfir* i estendre la «veritable fe» islàmica per tot el món.

En la segona modalitat (aproximació passiva), és un membre de l'organització dedicat a les tasques de captació i de reclutament en línia qui adopta el rol actiu i inicia converses amb els subjectes que han mostrat d'alguna manera interès per l'organització o per la causa que defensen. Per localitzar-los es dedica a rastrejar perfils i les seves conductes virtuals sobre els mitjans del grup.

Tot això ens fa prendre consciència que les TIC han afavorit l'emergència d'una nova relació entre el nostre cos i la màquina, una nova subjectivitat digital.

2) Captació, adhesió i prerradicalització: una vegada el ciberullador ha traspassat la informació al ciberreclutador (rol que sol assumir una dona), les converses entre aquest i l'individu passen a establir-se en fòrums o en xats privats. No obstant això, com hem comentat en apartats anteriors, el subjecte ha d'haver rebut les claus d'accés. Aquestes claus solen aconseguir-se una vegada

l'individu s'ha descarregat el programari Tor (The Onion Router) al seu ordinador per garantir que la seva navegació no deixarà petjades en el ciberespai (*cybertrails*) susceptibles de ser rastrejades per les forces de seguretat.

En les converses, a més de referir-se a sures de l'Alcorà on abunden les al·lusions a la gihad bèl·lica, al martiri, a la promesa de la glorificació i a l'accés al paradís per convèncer el subjecte que cometi un fet delictiu i justificar la violència que puguin definir les seves accions, el ciberreclutador vol conèixer les seves vulnerabilitats, el seu estil de vida, els seus problemes familiars, el seu estatus socioeconòmic, el seu nivell educacional, la seva professió, el seu cercle d'amics, les seves aficions i altres aspectes rellevants de la vida personal. La informació facilitada es tracta amb l'objectiu d'elaborar un model adoctrinador personalitzat que pugui donar solució i resposta a totes les necessitats i preguntes existencials que pertorben el subjecte (Guirao, 2019). Així és com el subjecte experimenta un major desig d'interactuar amb els membres de l'organització i d'aïllar-se de la resta de la societat, i desenvolupa en la seva psique una «societat paral·lela» (Khosrokhavar, 2003; Kandel, 2004). Una vegada l'individu sent que ha passat a formar part del grup (o cibercomunitat), desitja satisfer una nova necessitat: la de significació social. El subjecte necessita ser reconegut i respectat pel seu grup (Baumeister i Leary, 2017). Això fa que tota informació transmesa dins del grup es reinterpreti d'acord amb el seu sistema de creences i valors. Aquesta dinàmica afavoreix la consolidació del compromís dels membres amb l'organització i promou la narrativa radical, en estar tots involucrats en un procés d'aprenentatge col·lectiu en el qual la retroalimentació és constant (Kruglanski, Jasko, Webber i Chernikova, 2018). Quan això succeeix, podem entendre que el subjecte ja ha iniciat el camí que el portarà a acceptar una trobada al món fora de línia amb un membre de l'organització.

3) Aïllament i adoctrinament: una vegada la persona ha substituït el seu sistema de creences pel salafisme radical, el següent pas és aconseguir que el canvi també es generalitzi en el seu estil de vida fora de línia, però sense que això aixequi sospites en el seu entorn. Per a això, l'organització l'autoritzarà a usar el *taqiyya*. Aquest terme sorgeix de la doctrina *takfir*, i es defineix com l'acte de dissimulació mitjançant el qual es permet al creient amagar les seves creences religioses davant el temor de perdre la vida, les vides dels seus familiars o per a la preservació de la fe. En l'actualitat, el seu ús també es permet amb la finalitat d'evitar que el creient sigui descobert per les seves intencions terroristes, i passar així desapercebut en la comunitat d'«infidels» per acabar sotmetent-los.

Els canvis conductuals que es poden observar en aquesta fase són els següents:

- Abandó o canvi en determinades activitats d'oci.

- En cas d'un individu ja musulmà, deixar d'acudir a la mesquita o oratori per considerar impura o moderada la interpretació de l'islam que s'hi predica.

També entrar en conflicte amb el seu imam o amb els seus progenitors en considerar que no defensen el poble musulmà.

- En cas que el subjecte sigui convers, s'observa que comença a assistir a un oratori o a mostrar interès per la branca radical de l'islam i pels passatges més violents de l'Alcorà.

Aquesta situació s'agreuja si la figura paterna està absent o no exerceix el rol de cap de família (Bouzar, 2015). D'aquesta manera, veiem que un canvi iniciat en l'entorn en línia té un impacte en l'entorn fora de línia, corroborant així la unitat entre tots dos mons (Agustina, 2014).

4) Cibergihadització: en aquesta fase, el subjecte presenta un pensament completament dicotomitzat, així com una hipersensibilització davant qualsevol conducta o comentari susceptible d'interpretar-se com un atac contra la seva persona o contra la comunitat musulmana. Aquí es produeix la primera trobada cara a cara amb un membre de l'organització. La trobada té dos objectius:

- en primer lloc, avaluar el nivell de fidelitat del subjecte cap a l'organització; i

- en segon lloc, acabar de convèncer-lo perquè accepti les tasques que l'organització li ordeni, inclòs el suïcidi (Guirao, 2019).

Per a això, el ciberadoctrinador potenciarà les motivacions, els sentiments i les justificacions favorables a la violència.

Resum

L'estudi d'aquest primer mòdul ens ha apropat a la realitat del ciberterrorisme. Hem vist com malgrat l'amenaça que suposa, encara no hi ha consens respecte a una definició, sent la més exhaustiva la proposta per Luiijf (2014), i que ens porta a entendre'l com l'ús, els preparatius o l'amenaça d'acció dissenyats per part d'un grup terrorista, amb la finalitat de provocar un canvi en l'ordre social, crear un clima de por o d'intimidació entre el públic, o influir en la presa de decisions polítiques per part d'un govern. El terrorisme al qual ens hem referit en aquest mòdul està associat a la promoció d'una causa política, religiosa, racial o ideològica, que permet distingir-lo d'altres manifestacions, al seu torn qualificades també com a terrorisme, en les quals un grup organitzat utilitza mitjans similars per aconseguir objectius no polítics. De la mateixa manera, hem vist com els ciberatacs no es duen a terme sobre qualsevol estructura, sinó que se seleccionen aquelles els efectes de les quals podrien perjudicar greument la integritat, la confidencialitat o la disponibilitat d'informació dels sistemes d'informació i de les xarxes.

També hem comprovat com les característiques que defineixen el ciberespai han facilitat la inhibició conductual dels individus, proliferant els ciberatacs que van més enllà del ciberterrorisme, la qual cosa ens ha portat a preguntar-nos si de debò es tracta de nous delictes o simplement són la versió 2.0 dels ja coneguts.

En l'àmbit concret del ciberterrorisme, observem que els mitjans pels quals les organitzacions poden dur a terme les seves accions són diversos, i són les xarxes socials i les aplicacions de missatgeria instantània els seus principals aliats, sobretot per realitzar activitats relacionades amb la captació, l'adoctrinament i la radicalització. Aquest procés, quan es duu a terme al món virtual, rep el nom de ciberradicalització, i ha permès no solament reduir costos econòmics, sinó també el temps necessari per radicalitzar un subjecte, passant de la mitjana de dos anys a uns sis o vuit mesos. No obstant això, els estudis han demostrat que actualment perquè un subjecte arribi a l'estadi màxim es requereix, com a mínim, un intercanvi cara a cara al món real amb un agent físic.

Tant internet com les TIC han tingut, i tenen, una importància rellevant referent a la propaganda i a la difusió del discurs radical de l'organització. Hem vist com les publicacions responen a la voluntat de causar el major impacte possible en qui les consum, per augmentar les probabilitats que acabi entrant en contacte amb l'organització i es posi a la seva disposició. Una voluntat que no solament manifesten homes, sinó també dones. Així ho hem vist amb la tasca adoctrinadora que duen a terme les brigades femenines de les organitzacions terroristes.

Exercicis d'autoavaluació

Perquè pugueu comprovar el grau de consolidació aconseguit després de l'estudi del material, us proposem contestar deu preguntes tipus test. Les solucions estan a la pàgina següent. Sort!

1. Indiqueu qui va ser el primer autor que va utilitzar el terme *ciberterrorisme*.

a) Denning.
b) Barry Collins.
c) Lewis.
d) Mshvidobadze.

2. Quina és la diferència entre la gran gihad i la gihad menor?

a) La diferència és quantitativa, és a dir, mentre que la gran gihad és la duta a terme per un grup majoritari, la menor és la duta a terme per un grup minoritari.
b) La gran gihad és la que fa referència a l'esforç que cada musulmà ha de realitzar en el seu dia a dia per arribar a ser millor persona, i la gihad menor és la que defensa l'acció bèl·lica.
c) No hi ha diferència. Solament hi ha una gihad.
d) La diferència és la seva aparició o no en l'Alcorà. Mentre que la gran gihad apareix en diverses aleies, la menor no apareix en cap.

3. Indiqueu quin dels següents mitjans ha permès descentralitzar la difusió del discurs terrorista.

a) Revistes en línia.
b) Videojocs.
c) Ciberatacs.
d) Xarxes socials i aplicacions de missatgeria instantània.

4. Indiqueu quina de les següents afirmacions sobre el procés de radicalització és correcta:

a) La radicalització no és un procés, és un estat.
b) La radicalització és un procés en el qual solament interactuen l'individu i el ciberradicalitzador.
c) Les fases de la radicalització són: aproximació i primers contactes; captació, adhesió i prerradicalització; aïllament i adoctrinament i cibergihadització.
d) Els estudis han demostrat que el procés de radicalització pot concloure's sense haver existit una trobada cara a cara al món real amb un membre de l'organització terrorista.

5. Indiqueu quina afirmació sobre les característiques del ciberterrorisme és incorrecta.

a) El ciberatac és dut a terme per un individu pertanyent o simpatitzant amb una ideologia extremista radical i que actua sense autoritat legal per realitzar-la.
b) L'acció està motivada per factors polítics, ideològics, religiosos o socials.
c) Els actes que realitzen provoquen efectes psicològics de gran abast per al públic objectiu.
d) El ciberespai és l'arma i l'objectiu de les accions perpetrades pels grups terroristes.

6. Què són les *nasheeds*?

a) Són un gènere musical musulmà que consisteix a recitar un poema o una part d'ell.
b) Són cançons que s'han convertit en senyals d'identitat dels actuals grups terroristes de base religiosa.
c) Les lletres de les *nasheeds* no sempre són en àrab, també poden ser en francès, anglès o alemany.
d) Totes les respostes anteriors són correctes.

7. Tenint en compte el major o menor grau de participació del subjecte en el procés de radicalització, diferenciem entre:

a) Aproximació propera i llunyana.
b) Aproximació proactiva i reactiva.
c) Aproximació passiva i activa.

d) Aproximació superficial i profunda.

8. L'element principal per la desinhibició conductual al ciberespai és:

a) L'anonimat dissociatiu.
b) La invisibilitat.
c) La introjecció solipsista.
d) La comunicació asincrònica.

9. Indiqueu quina de les següents afirmacions caracteritza la propaganda terrorista difosa a la xarxa.

a) Solament va dirigida a nois i a homes.
b) La seva edició està molt cuidada, fins al punt de recordar-nos produccions de Hollywood.
c) Els idiomes en què s'elaboren són l'àrab i l'anglès.
d) És de difícil accés, i solament podem visualitzar-la si disposem d'una clau d'accés.

10. La diferència entre el hacktivisme i el ciberterrorisme és:

a) El hacktivisme consisteix a realitzar activitats en línia amb una finalitat política. El ciberterrorisme vol promoure o privilegiar un credo religiós per sobre d'un altre mitjançant la perpetració de ciberatacs en instal·lacions crítiques d'un país.
b) El hacktivisme consisteix a realitzar actes a la xarxa per simple diversió, com per exemple aconseguir els comptes bancaris de desconeguts. El ciberterrorisme consisteix a dur a terme accions en línia per influir en la presa de decisions polítiques d'un govern nacional o internacional.
c) El hacktivisme és una forma de ciberterrorisme motivat per finalitats polítiques, mentre que el ciberterrorisme pot al·ludir a motius polítics, ideològics, religiosos o socials.
d) El hacktivisme consisteix a realitzar activitats en línia amb una finalitat exclusivament política. El ciberterrorisme pot al·ludir a finalitats polítiques, ideològiques, religioses o socials.

Solucionari

Exercicis d'autoavaluació

1. b

2. b

3. d

4. c

5. a

6. d

7. c

8. a

9. b

10. d

Bibliografia

Agustina, J. R. (2014). «Victimización en el ciberespacio. Victimología y victimodogmática en el uso de las TIC. Desfragmentación del yo en la era digital: 'disinhibittion effect', esquizofrenia digital e ingenuidad en el ciberespacio». A: Tamarit, N.; Pereda, J. M. (2014). *La respuesta de la victimología ante las nuevas formas de victimización*. Madrid: Edisofer.

Baumeister, R.; Leary, M. (2017). *Interpersonal Development*. Londres: Routledge.

Becoña, E. (2016). «Factores de riesgo y de protección en el uso problemático de Internet». A: Echeburúa, E. (coord.). *Abuso de Internet. ¿Antesala para la adicción al juego de azar online?* Madrid: Pirámide.

Bouzar, D. (2015). *La vie après Daesh*. París: Autrement.

Brickey, J. (2012). «Defining Cyberterrorism: capturing a broad range of activities in cyberspace». *Sentiel* (vol. 5, núm. 8, pàg. 4-6). Combating Terrorism Center at West Point (CTC). Disponible a: http://bit.ly/2wm8n1s

Cano, M. Á.; Castro, F. J. (2018). «El camino hacia la (Ciber) Yihad». *Revista electrónica de Ciencia Penal y Criminología* (núm. 20, pàg. 1-36). Disponible a: http://criminet.ugr.es/recpc/20/recpc20-15.pdf

Cano, M. Á. (2019). «La expansión, intensificación y seducción del terrorismo islamista a través de internet: análisis criminológico». *Revista Científica General José María Córdova* (vol. 17, núm. 26, pàg. 271-287).

Carbonell, X.; Torres, A.; Fuster, H. (2016). «El potencial adictivo de los videojuegos». A: Echeburúa, I. (coord.). *Abuso de Internet. ¿Antesala para la adicción al juego de azar online?*. Madrid: Pirámide.

Cohen-Almagor, R. (2017). «Jihad Onlie: How Do Terrorists Use the Internet?». A: Campos, F.; Rúas, X.; Alejandro, V.; López, X. (eds.). *Media and Metamedia Management* (pàg. 55-66). Dordrecht: Springer.

Cohen, E.; Felson, M. (1979). «Social Change and Crime Rate Trends: A Routine Activity Approach». *American Sociological Review* (vol. 44, núm. 44, pàg. 588-608).

Denning, D. E. (2000). *Cyberterrorism, Testimony Before the Special Oversight Panel on Terrorism, Committee on Armed Services, U.S. House of Representatives*. Washington: House of Representatives.

Denning, D. E. (2001). *Is Cyber Terror Next?*. Washington: Social Science Research Council. Disponible a: http://www.fas.org/irp/congress/2000_hr/00-05-23denning.htm

Grabosky, P. (2001). «Virtual Criminality: Old Wine in New Bottles?». *Social & Legal Studies* (vol. 10, núm. 2, pàg. 243-249).

Guirao Cid, M. C. (2019). «La ciberradicalització: una nova forma de victimització». *IDP. Revista d'Internet, Dret i Política* (núm. 29). UOC. DOI: http://doi.org/10.7238/idp.v0i29.3171

Halopeau, B. (2014). «Terrorist usi of the internet». A: Babak, A.; Stainforth, A.; Bosco, S. *Cyber Crime and Cyber Terrorism. Investigator's Handbook*. Ed. Elsevier.

Hoffman, B. (2006). *Inside Terrorism*. Nova York: Columbia University Press.

Jahankhani, H.; Al-Nemrat, A.; Hosseinian, A. (2014). «Cyber crime Classification and Characteristics». A: Babak, A.; Stainforth, A.; Bosco, F. *Cyber Crime and Cyber Terrorism Investigator's Handbook* (pàg. 149-164). Ed. Elsevier.

Kandel, J. (2004). «Organisierter Islam in Deutschland und gesellschaftliche Integration». *Politisch Akademie der Friederich-Ebert-Stiftung* (pàg. 1-19).

Khosrokhavar, F. (2003). *Los nuevos mártires de Alá*. Madrid: Ed. Martínez Roca.

Kruglaski, A.; Jasko, K.; LaFree, G. (2016). «Quest for Significance and Violent Extremism: The Case of Domestic Radicalization». *Political Psychology* (vol. 38, núm. 5).

Kruglaski, A.; Jasko, K.; Webber, D.; Chernikova, M. (2018). «The Making of Violent Extremist». *Review of General Psychology* (vol. 1, núm. 22, pàg. 107-120).

Lemieux, T.; Brachman, J.; Levitt, J.; Wood, J. (2014). «Inspire Magazine: A Critical Analysis of its Significance and Potential Impact Through the Lens of the Information, Motivation, and Behavioral Skills Model». *Terrorism and Political Violence* (vol. 26, núm. 2, pàg. 354-371).

Lewis, J. A. (2002). «Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats». *Center for Strategic and International Studies*.

Luiijf, E. (2014). «Definitions of Cyber Terrorism». A: Babak, A.; Stainforth, A.; Bosco, S. *Cyber Crime and Cyber Terrorism Investigator's Handbook*. Ed. Elsevier.

Mantel, B. (2009). «Terrorism and the Internet. Should Web Sites That Promote Terrorism Be Shut Down?». *CQ Researcher* (pàg. 129-152).

Miró, F. (2011). «La oportunidad criminal en el ciberespacio. Aplicación y desarrollo de la teoría de las actividades cotidianas para la prevención del cibercrimen». *Revista Electrónica de Ciencia Penal y Criminológica* (núm. 13, pàg. 1-55).

Mshvidobadze, K. (2011). «State-sponsored Cyber Terrorism: Geòrgia's Experience». *Georgian Foundation for Strategic and International Studies* (pàg. 1-7).

National Research Council (1991). *Computers at Risk: Safe Computing in the Information Age*. Washington: National Academy Press.

Prensky, M. (2001). «Nativos digitales, inmigrantes digitales». *On the horizon* (vol. 9, núm. 5, pàg. 1-7).

Reinares, F.; García-Calvo, C. (2016). *Estado Islámico en España*. Madrid: Real Instituto Elcano.

Reinares, F.; García-Calvo, C. (2017). «Actividad yihadista en España, 2013-2017: de la Operación Cesto en Ceuta a los atentados en Cataluña». *Documento de trabajo 13/2017*. Madrid: Real Instituto Elcano.

Reinares, F.; García-Calvo, C.; Vicente, A. (2018). «Yihadismo y prisiones: un análisis del caso español». *ARI 123/2018*. Madrid: Real Instituto Elcano.

Rollins, J.; Wilson, C. (2007). «Terrorist Capabilities for Cyberattack: Overview and Policy issues». A: Limitin, I. V. (ed.). *Focus on Terrorism* (núm. 9, pàg. 43-63).

Ruiz, J. (2016). «Ciberamenazas: ¿el terrorismo del futuro?». *Documento de Opinión Instituto Español de Estudios Estratégicos*. Disponible a: http://www.ieee.es/Galerias/fichero/docs_opinion/2016/DIEEEO86-2016_Ciberamenazas_JRuizDiaz.pdf

Said, B. (2012). «Hymns (Nasheeds): A Contribution to the Study of the Jihadist Culture». *Studies in & conflict terrorism* (vol. 35, núm. 12, pàg. 863-879).

Silber, M.; Bhatt, A. (2007). *Radicalization in the West: The Homegrown Threat.* Police Department City of New York.

Suler, J. (2004). «The Online Disinhibition Effect». *Cyber Psychology & Behavior* (vol. 7, núm. 3, pàg. 321-326).

Torres, M. R. (2016). «Cómo contener a un califato virtual». *Cuadernos de estrategia* (núm. 180, pàg. 167-194).

Torres, M. R. (2018). «El hacktivismo como estrategia de comunicación: de Anonymous al cibercalifato». *Cuadernos de estrategia* (núm. 197, pàg. 197-224).

Torres Díaz, O. (2015). «La propagada del Daesh también es cosa de mujeres. De Umm Sumayyah Al-Muhajira en Dabiq al manifiesto de la Brigada Al-Khansaa en Internet». *Documento opinión* (núm. 121).

Trujillo, H. M.; Moyano, M.; González-Cabrera, J. (2006). «De la agresividad a la violencia terrorista. Historia de una patología psicosocial previsible (parte II)». *Behavioural Psychology* (vol. 14, núm. 2, pàg. 289-303).

UNODC (2013). *El uso de internet con fines terroristas*. Nacions Unides. Disponible a: https://www.unodc.org/documents/terrorism/publications/use_of_internet_for_terrorist_purposes/use_of_internet_ebook_spanish_for_web.pdf

Weimann, G. (2004). «Cyberterrorism. How Real Is The Threat?». *Special Report* (núm. 119). United States Institute of Peace. Disponible a: https://www.usip.org/sites/default/files/sr119.pdf