MATERIALS
DE TREBALL

52

El Centre Delàs d'Estudis per la Pau és membre de l'ENAAT (European Network Against Arms Trade), del WRI (War Resisters International), del IPB (International Peace Bureau) i col·laborador del SIPRI (Stockholm International Peace Research Institute)

JULIOL 2015

CENTRE DELÀS
D'ESTUDIS
PER LA PAU

SUMARI

Inseguretat nacional

Espanya basa la seva estratègia de defensa i seguretat en el manteniment i aprofundiment de la seva aliança atlàntica. L'enganyosa entrada a l'OTAN i l'incompliment de les condicions que van portar a votar afirmativament en el referèndum de 1986 a una ajustada majoria, ha tingut com a resultat una creixent militarització del territori espanyol per part de forces estrangeres aliades, sent eminentment i de forma permanent les d'EUA. L'idil·li militar nord-americà amb Espanya es remunta a temps franquistes, perquè el dictador va ser també el seu gran aliat estratègic. Amb la democràcia la relació es va consolidar i, recentment, el romanç sembla haver arribat al seu punt culminant. Espanya és un gran aliat militar dels EUA al Sud d'Europa. Quan l'Administració Obama va dissenyar l'actual sistema antimíssils a Europa, va triar la base de Rota (Cadis) per a albergar el component naval del sistema, amb el beneplàcit del govern espanyol.

A Polònia i Romania s'ubicarà el component terrestre consistent en plataformes de llançament de míssils i instal·lacions de radars. Rota allotjarà quatre destructors nord-americans equipats amb míssils i radars que patrullaran per la Mediterrània. Per si això fos poc, el Govern espanyol acaba d'aprovar per via d'urgència l'ampliació de la base de Morón de la Frontera perquè els EUA estableixin a Andalusia la seva base permanent de la força de reacció del comandament nord-americà per a l'Àfrica, amb un màxim de 2.200 marines, ampliable a 3.000, i 500 civils, que amb l'excusa de dur a terme intervencions antiter-

(pág. 2 ▶)

(▶ pág. 1) roristes pot desestabilitzar la fràgil estabilitat dels països subsaharians. La pertinença a l'OTAN i les bases nord-americanes en territori espanyol converteixen Espanya en un aliat nord-americà de primer ordre. Si a això li sumem la implicació de l'exèrcit espanyol en les invasions de l'Iraq i l'Afganistan, Espanya és percebut, no sense raó, com corresponsable de les actuacions militars de les forces armades dels EUA. Anar de la mà de la gran potència militar mundial que utilitza obertament la força de les armes com a eina de política exterior, no sembla ser la millor manera de no crear-se enemics. I crear-se enemics no és la millor manera de gestionar la seguretat d'un país. Aquest ha estat un dels pilars de l'estratègia de seguretat nacional espanyola, el punt culminant de la qual es va produir amb la famosa foto de les Açores, en què Aznar situava a Espanya al costat de Bush i Blair. Els principals atemptats contra objectius occidentals no van ser, en va, a Madrid, Nova York i Londres. És evident que l'estratègia de convertir-se en un aliat militar preferencial dels EUA no ha donat més seguretat a la població espanyola. ¿Per quan un canvi real en la política de defensa i seguretat nacional que tingui en compte les veritables necessitats de les persones?

Les noves armes digitals

Hi ha una paraula que cada cop escoltem més: ciberatac. Fa poc llegíem, segons dades del Govern espanyol, que l'any passat es van registrar més de setanta mil atacs per xarxa contra empreses, ciutadans, infraestructures critiques i institucions de l'Estat. Això situa Espanya com a tercer país al món en actes cibernètics hostils, tan sols per darrere dels Estats Units i el regne Unit. Un total de 63 d'aquests actes van ser especialment greus, amb 34 atacs a empreses energètiques i 4 a industries nuclears.

Segons el CESEDEN,[1] el ciberespai es pot definir com l'espai virtual mundial que interconnecta sistemes d'informació, dispositius mòbils i sistemes de control industrial. Un ciberatac o atac per xarxa és l'ús del ciberespai per atacar sistemes d'aquest ciberespai o bé elements i serveis no informàtics que siguin accessibles d'alguna manera des del mateix ciberespai. El seu objectiu és accedir a informació no autoritzada o bé alterar o impedir el funcionament de determinats serveis i infraestructures.

Podríem parlar de tres tipus d'atacs per xarxa o atacs informàtics. En primer lloc tenim els atacs fets per no experts. Un bon exemple serien els missatges virals contra persones concretes fets a través de les xarxes socials. És clar que no sempre tenen èxit, però quan «funcionen», poden fer molt mal: la persona concreta queda condemnada a l'ostracisme, és rebutjada, i fins i tot pot tenir problemes per trobar feina. En segon lloc podríem parlar dels atacs generats per experts informàtics que treballen individualment, els anomenats hackers. Les tècniques són molt variades. Podem parlar dels virus i cucs (programes que s'autoreprodueixen i es propaguen per la xarxa), dels troians o cavalls de Troia que s'instal·len al nostre ordinador, capten informació i l'envien al seu amo, de la suplantació d'emissors i remitents de missatges, de la tramesa massiva de correu no desitjat per bloquejar l'ordinador receptor, de la captura de paraules clau, de la suplantació d'identitat i de molts altres sistemes. En aquest cas, l'objectiu pot ser molt divers, des de simplement fer mal a robar diners o informació. Finalment, i això és el que fa més por, tenim les organitzacions, empreses i estats que han creat departaments plens de hackers especialitzats a dissenyar, preparar i executar atacs extremadament sofisticats. Són una mostra més de l'actual imbricació entre els diferents actors internacionals en un món en el qual, com diu Luis Goytisolo, els estats cada cop més s'assemblen a empreses i les empreses, a estats.

Un exemple paradigmàtic d'aquest tercer cas és el del virus *Stuxnet*, considerat la primera arma digital de la història. Amb aquest virus, els hackers de l'estructura militar de l'agència NSA dels Estats Units van poder destruir/inutilitzar el 20% de les centrifugadores que produïen urani enriquit a la central de Natanz, a Iran. L'atac va ser l'any 2009, i llavors ningú no va entendre

1. Vegeu: http://www.defensa.gob.es/ceseden/Galerias/ealede/cursos/curDefNacional/ficheros/Ciberseguridad_nuevo_reto_del_siglo_XXI_Guerra_cibernetica_aspectos_organizativos.pdf

el que passava. De fet, durant una visita dels inspectors internacionals el gener del 2010, ni els inspectors ni els tècnics iranians van poder entendre el misteri de les centrifugadores que es trencaven per excés de pressió interna, i fins després de quatre anys no es va saber el que havia passat. El virus *Stuxnet* va ser el resultat d'un projecte conjunt entre els Estats Units i Israel amb l'objectiu d'afectar els sistemes de control (fets per Siemens) de les centrifugadores. Va aconseguir infectar i controlar els sistemes informàtics d'aquestes màquines, tot i que no estaven connectades a la xarxa. L'atac es va fer en dues fases (la primera va ser d'espionatge i adquisició de dades), infectant els ordinadors d'empreses externes que subministraven equips i serveis a la central de Natanz. Aquests ordinadors infectaven els llapis de memòria dels seus usuaris amb el virus *Stuxnet*, que era invisible als sistemes antivirus. La idea clau de tot plegat era que alguns operaris acabarien anant en algun moment a la central tot portant el virus en els seus llapis. El raonament, que va funcionar a la perfecció, és que si es vol atacar un sistema molt protegit, el millor és aconseguir que els actors materials de la infecció siguin els mateixos operaris que hi tenen accés. A la primera fase, els virus que acabaven entrant en els ordinadors de control de les centrifugadores amagats en alguns dels molts llapis de memòria infectats incrementaven la seva velocitat de rotació amb l'objectiu de reduir la seva vida útil mentre informaven la sala de control de la central que tot anava bé i sense incidències i mentre enviaven informació essencial sobre aquests sistemes de centrifugat a la NSA; després, en una segona fase, els virus van anar incrementant la pressió interna del gas d'urani fins trencar les centrifugadores. Resumint: una brigada de hackers va aconseguir, sense moure's de davant dels seus ordinadors, destruir la cinquena part de les centrifugadores de Natanz.

Gràcies a Edward Snowden sabem de l'existència del programa *Politerain*. La noticia la va publicar fa pocs mesos el setmanari *Der Spiegel*. L'atac a les centrifugadores de l'Iran amb el virus *Stuxnet* va ser un dels primers resultats d'aquest programa de la famosa agència NSA, que funciona des de fa vuit anys. *Politerain* conté el grup S321, un grup de franctiradors informàtics que funcionen amb estructura militar i que treballen a la tercera planta d'un dels edificis del Fort Meade, a l'Estat de Maryland. Com diu Snowden, la seva prioritat són els atacs, no la defensa. La seva única missió és la de manipular i destruir

ordinadors i instal·lacions «de l'enemic». *Politerrain* és el viu exemple del terrorisme informàtic d'Estat, una petita mostra del que aviat veurem cada dia. És un futur que realment no tranquil·litza. Segurament no som gaire lluny de saber que hi ha armes digitals que maten gent civil.

Cada cop hi ha més casos d'atacs per xarxa, i cada vegada són més sofisticats. Podríem parlar de *Duqu, Flame o Gauss.*[2] Però també tenim un bon exemple en *l'Energetic Bear.*[3] Es tracta d'una arma digital recent, especialment dirigida a empreses i infraestructures civils. L'*Energetic Bear* s'ha mantingut estable durant quatre anys perquè utilitza xifrat de la informació. Els dos països amb més atacs han estat els Estats Units i Espanya, seguits del Japó i Alemanya. És un cavall de Troia amb una especial predilecció per les industries energètiques. No és destructiu com *Stuxnet*, però capta i espia informació, detecta llistes de contactes i paraules clau, fa captures de pantalla, recull llistes de documents i arxius, i ho envia tot als seus comandaments. *L'Energetic Bear* és tan sofisticat que encara no s'ha pogut determinar quin és el seu país d'origen.

Els atacs per xarxa no es poden evitar, és un dels peatges que hem de pagar pel fet de tenir una xarxa internet oberta. Crec que és indubtable que tots volem tenir aquesta xarxa oberta i lliure, i ens toca conviure amb virus i troians perquè ja sabem que la seguretat total és un mite. Però el que sí podem fer és ser curosos amb les nostres dades i no exposar-nos als perills de manera imprudent. No és el mateix enviar un correu electrònic a una persona concreta que enviar-li missatges de manera pública a través d'una xarxa social. Guillermo Zapata comentava, tot justificant la seva dimissió com a regidor de cultura de l'Ajuntament de Madrid, que els tuïts que ara l'han fet dimitir havien estat enviats en el context d'una conversa privada sobre els límits de l'humor. He de dir que la seva frase em va sorprendre. Per què tuïtejar converses privades en lloc d'enviar e-mails? Tot plegat em va recordar el filòsof Byung Chui Han,[4] quan diu que la peculiaritat del panòptic digital és que les persones col·laboren de manera activa en la seva vigilància i en la construcció i conservació d'aquest immens panòptic. Ho fan quan s'exhibeixen mentre despullen la seva informació a les xarxes socials.

Pere Brunet

2. Informe del CrySyS Lab 2012: http://www.rsaconference.com/writable/presentations/file_upload/br-208_bencsath.pdf
3. Informe Kaspersky 2015: https://securelist.com/files/2014/07/EB-YetiJuly2014-Public.pdf
4. Byung Chui Han, «La sociedad de la transparencia», Herder Ed. 2013

La NSA i la vigilància massiva de les telecomunicacions globals: una amenaça per als drets humans?

Google, Microsoft, Yahoo!, Facebook, Apple... ja fa alguns anys que la gran majoria de nosaltres estem molt familiaritzats amb aquestes grans corporacions. Gairebé cada vegada que accedim al món virtual amb els nostres dispositius amb connexió a Internet (ordinador personal, telèfon mòbil, tauleta tàctil...), fem ús d'alguns dels serveis que ofereixen, des dels costosos sistemes operatius (Windows i OS X) fins als serveis «gratuïts» de correu electrònic (Gmail, Outlook, Hotmail, Yahoo! Mail...), buscadors (Google, Yahoo! Search...), navegadors (Safari, Internet Explorer, Google Chrome...), xarxes socials (Google+, Facebook...), serveis de missatgeria instantània (WhatsApp) i de geolocalització (Google Maps), trucades en línia (Skype) i emmagatzematge en núvol (Google Drive, iCloud...). I, gràcies als documents filtrats al 2013 per l'exagent de la National Security Agency (NSA) Edward Snowden, ara també sabem que totes aquestes companyies han col·laborat amb l'espionatge indiscriminat de la intel·ligència americana en el marc del programa PRISM.[1] No cal dir que qualsevol de nosaltres podria haver estat objecte de vigilància en fer servir alguna d'aquestes eines.

Però donem-li a aquest espionatge aparentment abstracte (per la seva condició silenciosa) una imatge tangible: Cory Doctorow, conegut activista pels drets a Internet, comparava fa poc el potencial de vigilància de la NSA amb el de la STASI, la policia secreta de la República Democràtica Alemanya – institució que roman a la memòria col·lectiva com a eina de repressió d'un Estat obsessionat amb el control de la ciutadania. L'ambient asfixiant que suposava viure sota la mirada omniscient d'una agència d'intel·ligència amb orelles a tot arreu ha estat una figura popular en sèries de televisió, pel·lícules, videojocs i novel·les. Ara bé, la comparativa de Doctorow era la següent: cada agent de la STASI s'encarregava d'espiar 50 persones, mentre que amb els mitjans tecnològics de la NSA, *cadascun en pot vigilar fins a 10.000*.[2] Les preocupants implicacions socials d'un organisme amb el poder de controlar massivament (sense cap mena de control judicial) les comunicacions personals, les transaccions monetàries o els costums de navegació són evidents. La STASI, que confiava en aparatosos i complicats aparells per portar a terme les escoltes, ha quedat reduïda a la condició d'«artesana» de l'espionatge, que substituïa amb la seva destresa manual les limitacions en matèria tecnològica. La NSA d'avui supera en tots els aspectes els procediments l'antiquada STASI.

Que l'espionatge actual es dugui a terme silenciosament, sigui menys perceptible, no pot ser una excusa de cara a l'elaboració d'una necessària oposició política no només davant les arbitrarietats de les agències d'intel·ligència mundials, sinó també vers la percepció d'Internet (o del ciberespai) com a zona militaritzada, en la qual tothom passa a ser subjecte d'escrutini intensificat. *Digital vol dir intangible, però no irreal*: una quantitat en augment de les nostres funcions socials més elementals (tràmits amb l'administració, trucades de veu, consulta de notícies o del catàleg de la biblioteca) es trasllada ara a l'esfera virtual, a la qual cal considerar no com un simplista doble «fals» de la societat «real», sinó com una extensió de la pròpia societat, amb totes les especificitats que li poguessin correspondre. Utilitzar el ciberespai per a comunicar-nos no converteix la nostra interacció en il·lusòria (almenys, no *automàticament*), sinó que la fa subjecte de noves pautes de conducta i socialització. D'aquí que les vulneracions de drets a la xarxa hagin de ser considerades igual de rellevants que les que es fan fora de l'àmbit cibernètic. No hi ha cap diferència notable entre llegir, analitzar i emmagatzemar sense consentiment el nostre correu postal (sigui per raons polítiques o comercials) que fer-ho amb el nostre correu electrònic.

«Ningú no serà objecte d'intromissions arbitràries en la seva vida privada, la seva família, el

1. *NSA Prism program taps in to user data of Apple, Google and others* (The Guardian, 07/06/2013 – http://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data)

2. Conferència «The NSA are not the STASI: Godwin for mass surveillance» a Re:publica 2015 (https://re-publica.de/en/session/nsa-are-not-stasi-godwin-mass-surveillance)

seu domicili o la seva correspondència, ni d'atacs al seu honor i reputació. Tothom té dret a la protecció de la llei contra tals intromissions o atacs», afirma l'article 12 de la Declaració Universal dels Drets Humans. D'aquí que la naturalització a escala social de les continuades intromissions en aquest sentit formi part d'una estratègia política que pretén passar per innòcua la decisió eminentment política d'espiar indiscriminadament les telecomunicacions del total de la població. La «pesca d'arrossegament», en tant que procediment marcadament perjudicial pel sòl marí en no seleccionar els seus objectius, s'extrapola sense gaires matisos a l'entorn digital, de manera que el resultat no podia ser altre que la destrucció irresponsable de la seguretat del global de

les telecomunicacions, indistintament dels objectius que suposadament es persegueixin. El Primer Ministre del Regne Unit, David Cameron, ha arribat a exigir la prohibició del xifrat de les telecomunicacions a fi de prosseguir en la lluita contra el terrorisme (recurs utilitzat tan per WhatsApp o Telegram com per la seguretat de les transaccions financeres), una amenaça que ha comportat que diverses iniciatives destinades a oferir tecnologia compromesa amb els drets humans, com ara Ind.ie, hagin decidit marxar del país a causa de la seva oposició a introduir *backdoors*[3] deliberats en els seus productes, que no només permetrien que el govern tingués accés al contingut dels missatges,[4] sinó que els faria especialment vulnerables pel que fa a possibles atacs cibernètics.

La demanda d'un Internet lliure, democràtic i obert, absent del control i rastreig a escala massiva ha de passar a ser un dels eixos vertebradors de les organitzacions que pretenen defensar els drets humans avui, i no una qüestió que es limiti a reduïts grups de ciberactivistes o *hackers*. No podem restar indiferents davant d'un context específic en el qual les garanties democràtiques segueixin minvant, per molt que tot plegat sembli estar succeint a l'anomenat «món digital». El poder de les agències d'intel·ligència, les quals gaudeixen d'una situació privilegiada on l'escrutini democràtic és pràcticament inexistent, ha anat en augment al mateix temps que els nostres propis drets disminueixen de manera gradual. No podem ser «subjectes de dret» reals davant l'existència d'aquests poderosos mecanismes socials que actuen emparant-se en el secret més absolut i sense que nosaltres en tinguem constància oficialment.

Cal que la transcendència social que suposa l'existència de, com a mínim, una xarxa d'espionatge global de les telecomunicacions (conformat per diversos organismes d'intel·ligència dels anomenats «Five Eyes», és a dir, Estats Units, Regne Unit, Canadà, Austràlia i Nova Zelanda) es tradueixi en un pol d'oposició en defensa del dret a no ser les arbitràries víctimes de la mirada omniscient de l'Estat, que ens expropia de les garanties jurídiques fonamentals. *El rastreig i la retenció massiva de les dades personals són, pel seu component indiscriminat, del tot incompatibles amb la democràcia*. Un informe de l'Oficina de l'Alt Comissariat de les Nacions Unides per als Drets Humans va afirmar el passat 28 de maig que «el xifrat i l'anonimat proveeixen la privacitat i la seguretat necessàries per a l'exercici del dret a la llibertat d'opinió i d'expressió a l'era digital. Aquesta seguretat pot ser essencial per l'exercici d'altres drets (...)».[5] Implantar polítiques que protegeixin el xifrat i l'anonimat, en comptes de criminalitzar-lo o perseguir-lo, ha de ser una prioritat dels nostres governs en cas que vulguin fer d'Internet un vehicle de la llibertat d'expressió i no un mitjà per censurar-la.

Enric Luján

3. *Backdoor*: Mètode per accedir al sistema operatiu d'un dispositiu electrònic sense haver d'introduir cap contrasenya o seguir altres procediments que serveixin per autentificar l'usuari.
4. *So Long, and Thanks for All the Fish* (Blog d'Aral Balkan, fundador d'Ind.ie, 11/05/2015 – https://aralbalkan.com/notes/so-long-and-thanks-for-all-the-fish/)
5. *UN says encryption «necessary for the exercise of the right to freedom»* (Ars Technica, 28/05/2015 – http://arstechnica.com/tech-policy/2015/05/un-says-encryption-necessary-for-the-exercise-of-the-right-to-freedom/)

Diners, poder i opacitat a les institucions europees: un paradís per al lobby militar*

El paisatge institucional europeu està en un procés de construcció constant, com ho demostra per exemple l'evolució en les funcions del Consell, de la Comissió i del Parlament des del seu naixement fins avui. Un altre tipus d'institucions s'han anat creant paral·lelament, algunes per la pressió que exerceixen els lobbys al panorama polític europeu. Abans de detallar algunes d'elles, explicarem què és un lobby i com influeix a les polítiques europees.

La situació dels lobbys a les institucions europees

Un lobby és una estructura que representa els interessos d'un determinat grup, l'objectiu del qual és influenciar les lleis, reglamentacions i normatives, pressionant les persones o les institucions que ostenten el poder, a fi de defensar i promocionar els seus propis interessos, generalment econòmics.[1] Aquesta definició demostra el vincle que estableix amb els polítics i les institucions de poder. A Brussel·les, on es concentren moltes de les institucions europees (Comissió, Parlament, Consell, Agència Europea de Defensa (AED), Frontex...), s'estima que treballen uns 15.000 lobbistes, dels quals un 70% promou els interessos de grups industrials, un 20% defensa els interessos de les regions, ciutats i institucions internacionals i només un 10% representa els interessos d'organitzacions no governamentals, fent de la capital europea la segona ciutat del món en matèria de lobbisme, únicament després de Washington D.C.[2] La pressió dels lobbys s'exerceix aleshores sobre les institucions que tenen poder de decisió, conduint així la política europea a una situació en la qual es troba en mans dels grans grups industrials.

A la Unió Europea, la Comissió posseeix l'exclusivitat d'iniciar els projectes legislatius, a més d'haver de garantir l'interès general comunitari. Únicament la Comissió pot proposar polítiques europees pel que fa als àmbits definits pels tractats, la qual cosa fa que sigui l'objectiu privilegiat dels lobbistes. Aquests, a més de poder entrar i sortir lliurement de la Comissió, han trobat una demanda d'assessorament important per part dels propis funcionaris. Per contra, per tal d'obtenir l'accés al Parlament europeu, els lobbistes han d'acreditar-se al registre de transparència, posat en marxa de manera recent per controlar la identitat i el nombre de persones que pretenen influir als debats parlamentaris. No obstant això, tot i pretendre establir una major transparència pel que fa a les activitats de la representació dels interessos, el registre no compleix la seva funció. Ja que no és obligatori acreditar-se, aquest només serveix per saber el nombre de lobbistes que entra en contacte amb l'Eurocambra (i, en conseqüència, es desconeix el nombre de lobbistes que exerceixen pressió sobre la Comissió o altres institucions), i no estableix sancions si aquests violen el codi ètic que implica el fet de registrar-se. Tot i així, el registre permet saber quins entren en contacte amb les comissions parlamentàries encarregades de discutir els projectes legislatius de la Comissió, on s'exerceix més pressió.

Els actors europeus del lobby militar

Per promoure i defensar els seus interessos a les institucions europees, la indústria militar posseeix diversos actors que els representen. Un estudi del GRIP els classifica en quatre categories:[3] les estructures industrials, les delegacions d'empreses del sector, els *think tanks* i els grups d'experts. A continuació oferim alguns detalls pel que fa a la seva vinculació amb la indústria armamentística.

En la primera entren l'Associació Europea de la Indústria Aeronàutica Espacial i de Defensa (ASD en anglès), i la Organització Europea per a la Seguretat (EOS en anglès). Tot i que

1. GENTILUCCI, E. (2014). Le lobbying Européen de la défense et de la sécurité vis-a-vis des institutions communautaires : une approche bi-sectorielle. *Innovations: Cahiers D'économie De L'innovation*. 43, 61-83.
2. Corporate Europe Observatory (2006). Lobby Planet. Disponible a: http://www.lobbycratie.fr/documents/lobbyplanet-fr.pdf
3. BECKLEY Alexandra, *Promotion de l'industrie de la défense et de la sécurité : acteurs et pratiques*, Note d'Analyse du GRIP, 22 juin 2012, Bruxelles. Disponible a: http://www.grip.org/fr/siteweb/images/NOTES_ANALYSE/2012/NA_2012-06-22_FR_A-BECKLEY.pdf

aquestes estructures industrials no es declaren explícitament com a lobbys, les seves presentacions al web no permeten cap marge de dubte. D'aquesta manera, l'ASD presenta la seva missió general com: *«ser un centre d'intel·ligència central per a les indústries aeroespacials, de defensa i de seguretat, […] donar forma a la legislació i a les polítiques de la UE, així com la obtenció d'oportunitats de finançament en defensar posicions comunes vers les institucions europees i organitzacions internacionals de cara al benefici de les indústries europees i l'interès col·lectiu dels seus membres».*[4] De la mateixa manera, l'EOS explica que la seva missió és: *«proporcionar una plataforma de treball col·laboratiu, d'intercanvi d'idees i millors pràctiques entre les institucions europees i de la indústria europea de seguretat […] l'objectiu principal d'EOS és el desenvolupament d'un mercat de la seguretat europea harmonitzat en consonància amb les necessitats polítiques, socials i econòmiques a través de l'ús eficient dels pressupostos».*[5] L'ASD i l'EOS es troben inscrites al registre de transparència de la UE com a Grups de pressió dins de les empreses i associacions comercials, empresarials o professionals, i declaren 16[6] i 8 lobbistes[7] respectivament, la qual cosa autoritza les persones identificades a tenir un accés permanent al Parlament Europeu.

Malgrat les empreses més grans de defensa europees com Thales, BAE Systems, Finmeccanica o EADS (que també es troben entre les 10 majors empreses d'armament mundials)[8] són membres de les estructures industrials esmentades anteriorment, aquestes empreses també tenen les seves pròpies delegacions a dos passos de les institucions europees a Brussel·les, segona categoria d'estructura d'influència. Així, doncs,

4. ASD (2015). Mission en Key Priorities. Disponible a: http://www.asd-europe.org/about-us/missions-key-priorities/. Consulta: 12 de juliol de 2015.
5. EOS (2015). What is EOS? Disponible a: http://www.eos-eu.com/Middle.aspx?Page=whatiseos&tID=1. Consulta: 12 de juliol de 2015.
6. Veure registre de transparència de la UE. Disponible a: http://ec.europa.eu/transparencyregister/public/consultation/displaylobbyist.do?id=72699997886-57. Consulta: 12 de juliol de 2015.
7. Veure registre de transparència de la UE. Disponible a: http://ec.europa.eu/transparencyregister/public/consultation/displaylobbyist.do?id=32134385519-64. Consulta: 12 de juliol de 2015.
8. SIPRI (2015). The SIPRI top 100 arms producing and military services companies, 2013. Disponible a: http://www.sipri.org/research/armaments/production/recent-trends-in-arms-industry/Fact%20Sheet%20Top100%202013.pdf. Consulta: 12 de juliol de 2015.

al registre de transparència podem trobar els noms i cognoms de les persones acreditades per entrar permanentment al Parlament Europeu, i que pretenen influenciar les polítiques de defensa a favor dels objectius corporatius que defensen. Thales té 6 lobbistes,[9] EADS 10,[10] Finmeccanica 3[11] i BAE Systems 1.[12]

A més de les dues primeres categories que ja hem exposat -i que podem etiquetar d'industrials-, altres entitats no industrials treballen a fi de defensar els interessos del sector. Aquest és el cas dels *think tanks*, organitzacions la funció de les quals és la de reflexionar i investigar sobre determinats assumptes. En l'àmbit que ens interessa, el Security & Defense Agenda (SDA) es presenta com l'únic *think tank* especialitzat en qüestions de defensa i de seguretat. El lobby se situa en un dels llocs més prestigiosos de Brussel·les i al centre del barri europeu (a la biblioteca Solvay), la qual cosa reflecteix el poder d'influència de la organització, el finançament de la qual prové en gran part de la indústria del sector (especialment de les dues majors empreses d'armes a escala mundial: Lockeed Martin i BAE Systems[13]), i en menor mesura del sector públic (OTAN, UE, governs nacionals, entre d'altres) i privat (fundacions, ONG...). Més enllà dels seus recursos econòmics, és el renom dels membres de la seva *advisory board* el que atorga una fama especial a la organització. Amb personalitats com Javier Solana (exdirector de l'Agència Europea de Defensa, EAD en anglès), o Claude-France Arnould (també exdirectora de la EAD), la SDA posseeix diversos perfils d'autoritats del sector de la defensa, que a més il·lustren el fenomen de les portes giratòries, simptomàtic de les grans esferes de poder.[14]

L'última categoria del lobby militar europeu, els grups d'experts, són unes entitat de caràcter consultiu el rol de les quals consisteix en oferir assessorament i coneixements especialitzats a la Comissió i als seus departaments, en el marc de l'elaboració de propostes legislatives i iniciatives polítiques.[15] És la Comissió Europea la que posa en marxa aquest tipus d'organització amb l'objectiu de cobrir les carències que té sobre algunes qüestions. Malgrat tot, com bé explica Berkeley a l'informe del GRIP, l'interès general que ha de garantir la Comissió en el si de la Unió es confon amb l'interès industrial quan la composició d'aquests grups no inclou la societat civil i és acusada d'opacitat.[16] Al sector de la defensa i seguretat, destaca el rol del grup STAR 21 en el desenvolupament d'una estratègia aeroespacial europea. Amb un total de 15 persones, aquest es compon de 8 membres de les institucions europees i governs nacionals i 7 representants de la indústria militar, sense que portaveus de centres d'investigació especialitzats, universitats o societat civil puguin contribuir en l'elaboració de les iniciatives polítiques que representen l'interès general.[17]

Un exemple de la influència del lobby militar: la creació de l'Agència Europea de Defensa

Com ja hem dit, l'acció del conjunt dels actors que formen el lobby militar a Brussel·les està orientada cap a determinades institucions europees, com per exemple la Comissió, l'Eu-

9. Veure registre de transparència de la UE. Disponible a: http://ec.europa.eu/transparencyregister/public/consultation/searchControllerPager.do?declaration=Thales&search=search. Consulta: 12 de juliol de 2015.
10. Veure registre de transparència de la UE. Disponible a: http://ec.europa.eu/transparencyregister/public/consultation/displaylobbyist.do?id=2732167674-76. Consulta: 13 de juliol de 2015.
11. Veure registre de transparència de la UE. Disponible a: http://ec.europa.eu/transparencyregister/public/consultation/displaylobbyist.do?id=02550382403-01. Consulta: 12 de juliol de 2015.
12. Veure registre de transparència de la UE. Disponible a: http://ec.europa.eu/transparencyregister/public/consultation/searchControllerPager.do?declaration=BAE+systems&search=search. Consulta: 12 de juliol de 2015.
13. SIPRI (2015). The SIPRI top 100 arms producing and military services companies, 2013. Disponible a: http://www.sipri.org/research/armaments/production/recent-trends-in-arms-industry/Fact%20Sheet%20Top100%202013.pdf. Consulta: 12 de juliol de 2015.
14. GENTILUCCI, E. (2014). Le lobbying Européen de la défense et de la sécurité vis-a-vis des institutions communautaires : une approche bi-sectorielle. *Innovations: Cahiers D'économie De L'innovation.* 43, 61-83.
15. Comisión Europea (2015). Naturaleza y funcionamiento de los grupos de expertos. Disponible a: http://ec.europa.eu/transparency/regexpert/index.cfm?do=faq.faq&aide=2&Lang=ES. Consulta: 12 de juliol de 2015
16. BECKLEY Alexandra, *Promotion de l'industrie de la défense et de la sécurité : acteurs et pratiques*, Note d'Analyse u GRIP, 22 juin 2012, Bruxelles. Disponible a: http://www.grip.org/fr/siteweb/images/NOTES_ANALYSE/2012/NA_2012-06-22_FR_A-BECKLEY.pdf
17. BECKLEY Alexandra, *Promotion de l'industrie de la défense et de la sécurité : acteurs et pratiques*, Note d'Analyse u GRIP, 22 juin 2012, Bruxelles. Disponible a: http://www.grip.org/fr/siteweb/images/NOTES_ANALYSE/2012/NA_2012-06-22_FR_A-BECKLEY.pdf

rocambra o bé l'Agència de Defensa Europea (EAD), i arriba a dibuixar el paisatge institucional europeu. De fet, la creació d'aquesta última hauria estat una fita del lobby de defensa com a tal, com exposa el Corporate Europe Observatory al seu blog.[18] Allà s'explica com Michel Troubetzkoy, cap de la delegació d'EADS a Brussel·les, es vanagloriava de la creació de l'Agència de Defensa Europea, el «nen petit d'EADS». Aquest es felicitava de la facilitat per entrar en contacte amb polítics i influenciar-los per a que presentin al Consell els textos legislatius que ells mateixos redacten. Segons les seves pròpies paraules, el text presentat per a la creació de l'Agència de Defensa Europea era un 95% idèntic al document originari, lliurat per EADS.

La descripció del lobby militar europeu que hem realitzat en aquest article és només una breu introducció a la complexitat de les dinàmiques que permeten que aquestes potents organitzacions influeixin en les polítiques de defensa i de seguretat europees. Enfront els seus mitjans, la societat civil no és capaç de compensar la representació d'interessos econòmics en les institucions i promoure els interessos socials i mediambientals. Malgrat tot, algunes organitzacions vigilen l'activitat dels lobbys a Brussel·les, investigant i organitzant campanyes per

a sensibilitzar l'opinió pública respecte el seu caràcter nefast. Pel que fa al lobby de la defensa i de la seguretat, destaca l'activitat «Lobby tour militar» de l'associació *Agir pour la Paix*, basada en un treball del Corporate Europe Observatory, que permet els ciutadans adonar-se de les maquinacions del sector militar a les institucions i polítiques europees. Mentre aquest hi pretengui influir per defensar els seus interessos corporatius que desencadenen guerres, violències i injustícies, estarem treballant per denunciar les seves actuacions i procurar empoderar la societat civil.

Chloé Meulewaeter

18. Corporate Europe Observatory (2015). The Silent Bubble. Disponible a: http://blog.brusselsbubble.eu/2008/12/silent-bubble.html. Consulta: 13 de juliol de 2015.

** L'autora agraeix la disponibilitat i la informació proporcionada a Stéphanie Damblon, de l'associació Agir pour la Paix, durant el «lobby tour militar» a Brussel·les.*

CENTRE DELÀS D'ESTUDIS PER LA PAU

Equip de redacció: Jordi Calvo i Pere Ortega.

Han col·laborat en aquest número: Pere Brunet, Enric Lujan i Chloé Meulewaeter.

D.L.: B-18996-2010 · ISSN edició impressa: 2013-8121· ISSN edició en línea: 2013-9764

Ajuntament de Barcelona

COM COL·LABORAR

- **Forma part del nostre equip d'investigació.**
- **Ajuda'ns en tasques de comunicació, gestió i campanyes..**
- **Fes las pràctiques dels teus estudis al nostre Centre.**
- **Feste soci des de la nostra web: www.centredelas.org**

CENTRE DELÀS D'ESTUDIS PER LA PAU · Carrer Erasme de Janer, 8 (entresol) · 08001 Barcelona [Despatx nº9]
www.centredelas.org · info@centredelas.org