MATERIALES
DE TRABAJO

52

El Centre Delàs d'Estudis per la Pau es miembro de la ENAAT (European Network Against Arms Trade), del WRI (War Resisters International), del IPB (International Peace Bureau) y colaborador del SIPRI (Stockholm International Peace Research Institute)

JULIO 2015

CENTRE DELÀS
D'ESTUDIS
PER LA PAU

SUMARIO

Inseguridad nacional

España basa su estrategia de defensa y seguridad en el mantenimiento y profundización de su alianza atlántica. La engañosa entrada en la OTAN y el incumplimiento de las condiciones que llevaron a votar afirmativamente en el referéndum de 1986 a una ajustada mayoría, ha tenido como resultado una creciente militarización del territorio español por parte de fuerzas extranjeras aliadas, siendo eminentemente y de forma permanente las pertenecientes a EEUU. El idilio militar norteamericano con España se remonta a tiempos franquistas, porque el dictador fue también su gran aliado estratégico. Con la democracia la relación se consolidó y, recientemente, el romance parece haber llegado a su punto culminante. España es un gran aliado militar de EEUU en el Sur de Europa. Cuando la Administración Obama diseñó el actual sistema antimisiles en Europa, eligió la base de Rota (Cádiz) para albergar el componente naval del sistema, con el beneplácito del gobierno español.

En Polonia y Rumania se ubicará el componente terrestre consistente en plataformas de lanzamiento de misiles e instalaciones de radares. Rota alojará cuatro destructores norteamericanos equipados con misiles y radares que patrullarán por el Mediterráneo. Por si esto fuera poco, el Gobierno español acaba de aprobar por vía de urgencia la ampliación de la base de Morón de la Frontera para que EEUU establezca en Andalucía su base permanente de la fuerza de reacción del mando de EE UU para África, con un máximo de 2.200 marines, ampliable a 3000, y 500 civiles, que con la excusa

(pág. 2 ▶)

(▶ pág. 1) de llevar a cabo intervenciones antiterroristas puede desestabilizar la frágil estabilidad de los países subsaharianos. La pertenencia a la OTAN y las bases norteamericanas en territorio español convierten a España en un aliado estadounidense de primer orden. Si a ello le sumamos la implicación del ejército español en las invasiones de Irak y Afganistán, España es percibido, no sin razón, como corresponsable de las actuaciones militares de las fuerzas armadas de EEUU. Ir de la mano de la gran potencia militar mundial que utiliza abiertamente la fuerza de las armas como herramienta de política exterior, no parece ser la mejor manera de no crearse enemigos. Y crearse enemigos no es la mejor manera de gestionar la seguridad de un país. Este ha sido uno de los pilares de la estrategia de seguridad nacional española, cuyo punto culminante se produjo con la famosa foto delas Azores, en la que Aznar situaba a España al lado de Bush y Blair. Los principales atentados contra objetivos occidentales no fueron, en vano, en Madrid, Nueva York y Londres. Es evidente que la estrategia de convertirse en un aliado militar preferencial de EEUU no ha dado mayor seguridad a la población española. ¿Para cuando un cambio real en la política de defensa y seguridad nacional que tenga en cuenta las verdaderas necesidades de las personas?

Las nuevas armas digitales

Hay una palabra que cada vez escuchamos más: ciberataque. Hace poco leíamos, según datos del Gobierno, que el año pasado se registraron más de setenta mil ataques por red contra empresas, ciudadanos, infraestructuras críticas e instituciones del Estado. Esto sitúa a España como tercer país en el mundo en actos cibernéticos hostiles, tan sólo por detrás de Estados Unidos y el Reino Unido. Un total de 63 de estos actos fueron especialmente graves, con 34 ataques a empresas energéticas y 4 en industrias nucleares.

Según informes del CESEDEN,[1] el ciberespacio se puede definir como el espacio virtual mundial que interconecta sistemas de información, dispositivos móviles y sistemas de control industrial. Un ciberataque o ataque por red es el uso del ciberespacio para atacar sistemas de este mismo ciberespacio o bien elementos y servicios no informáticos que sean accesibles de alguna manera desde el mismo. Su objetivo es acceder a información no autorizada o bien alterar o impedir el funcionamiento de determinados servicios e infraestructuras.

Podríamos hablar de tres tipos de ataques por red o ataques informáticos. En primer lugar tenemos los ataques hechos por no expertos. Un buen ejemplo serían los mensajes virales contra personas concretas hechos a través de las redes sociales. Claro que no siempre tienen éxito, pero cuando «funcionan», pueden hacer daño real: la persona concreta queda condenada al ostracismo, es rechazada, e incluso puede tener problemas para encontrar trabajo. En segundo lugar podríamos hablar de los ataques generados por expertos informáticos que trabajan individualmente, los llamados hackers. Las técnicas son muy variadas. Tenemos los virus y gusanos (programas que se auto-reproducen y se propagan por la red), los troyanos o caballos de Troya que se instalan en nuestro ordenador, captan información y la envían a su dueño, la suplantación de emisores y remitentes de mensajes, el envío masivo de correo no deseado para bloquear el ordenador receptor, la captura de palabras claves, la suplantación de identidad y muchos otros sistemas. En este caso, el objetivo puede ser muy diverso, desde simplemente hacer daño a robar dinero o información. Por último, y esto es lo que más miedo da, tenemos las organizaciones, empresas y estados que han creado departamentos llenos de hackers especializados en diseñar, preparar y ejecutar ataques extremadamente sofisticados. Son una muestra más de la actual imbricación entre los diferentes actores internacionales en un mundo en el que, como comenta Luis Goytisolo, los estados cada vez más se parecen a empresas y las empresas, a estados.

Un ejemplo paradigmático de este tercer caso es el del virus *Stuxnet*, considerado la primera arma digital de la historia. Con este virus, los hackers de la estructura militar de la agencia NSA de Es-

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

tados Unidos pudieron destruir/inutilizar el 20% de las centrifugadoras que producían uranio enriquecido en la central de Natanz en Irán. El ataque fue en 2009, y entonces nadie entendió lo que pasaba. De hecho, durante una visita de los inspectores internacionales en enero de 2010, ni los inspectores ni los técnicos iraníes pudieron entender el misterio de las centrifugadoras que se rompían por exceso de presión interna, y hasta después de cuatro años no se supo lo que había pasado. El virus *Stuxnet* fue el resultado de un proyecto conjunto entre Estados Unidos e Israel con el objetivo de afectar a los sistemas de control (hechos por Siemens) de las centrifugadoras. Consiguió infectar y controlar los sistemas informáticos de estas máquinas, aunque no estaban conectadas a la red. El ataque se hizo en dos fases (la primera fue de espionaje y adquisición de datos), infectando los ordenadores de empresas externas que suministraban equipos y servicios en la central de Natanz. Estos ordenadores infectaban los lápices de memoria de sus usuarios con el virus Stuxnet, que era invisible a los sistemas anti-virus. La idea clave de todo el sistema era la premisa de que algunos operarios acabarían yendo en algún momento a la central llevando el virus en sus lápices. El razonamiento, que funcionó a la perfección, es que, si se quiere atacar un sistema muy protegido, lo mejor es conseguir que los actores materiales de la infección sean los propios operarios que tienen acceso al mismo. En la primera fase, los virus que terminaban entrando en los ordenadores de control de las centrifugadoras escondidos en algunos de los muchos lápices de memoria infectados, incrementaban su velocidad de rotación con el objetivo de reducir su vida útil mientras informaban la sala de control de la central que todo iba bien y sin incidencias y mientras enviaban información esencial sobre estos sistemas de centrifugado a la NSA; luego, en una segunda fase, los virus fueron incrementando la presión interna del gas de uranio hasta romper las centrifugadoras. Resumiendo: una brigada de hackers logró, sin moverse de delante de sus ordenadores, destruir la quinta parte de las centrifugadoras de Natanz.

Gracias a Edward Snowden sabemos de la existencia del programa Politerain. La noticia la publicó hace pocos meses el semanario *Der Spiegel*. El ataque a las centrifugadoras de Irán con el virus *Stuxnet* fue uno de los primeros resultados de este programa de la famosa agencia NSA, que funciona desde hace ocho años. Politerain incluye el grupo S321, un grupo de francotiradores informáticos que funcionan con estructura militar y que trabajan en la tercera planta de uno de los edificios del Fuerte Meade,

en el Estado de Maryland. Como dice Snowden, su prioridad son los ataques, no la defensa. Su única misión es la de manipular y destruir ordenadores e instalaciones «del enemigo». Politerain es el vivo ejemplo del terrorismo informático de Estado, una pequeña muestra de lo que pronto veremos cada día. Es un futuro que realmente no tranquiliza. Seguramente no estamos muy lejos del momento en el que conviviremos con armas digitales que matarán gente civil.

Cada vez hay más casos de ataques por red, y cada vez son más sofisticados. Podríamos hablar de los virus *Duqu, Flame o Gauss.*[2] Pero también tenemos un buen ejemplo en el llamado *Energetic Bear.*[3] Se trata de un arma digital reciente, especialmente dirigida a empresas e infraestructuras civiles. El *Energetic Bear* ha mantenido estable durante cuatro años porque utiliza cifrado de la información. Los dos países con más ataques han sido los Estados Unidos y España, seguidos de Japón y Alemania. Es un caballo de Troya con especial predilección por las industrias energéticas. No es destructivo como *Stuxnet*, pero capta y espía información, detecta listas de contactos y palabras clave, hace capturas de pantalla, recoge listas de documentos y archivos, y lo envía todo a sus jefes. El *Energetic Bear* es tan sofisticado que aún no ha sido posible determinar cuál es su país de origen.

Los ataques por red son inevitables, es uno de los peajes que tenemos que pagar por tener una red internet abierta. Es indudable que todos queremos tener esta red abierta y libre, y nos toca convivir con virus y troyanos porque ya sabemos que la seguridad total es un mito. Pero lo que sí podemos hacer es ser cuidadosos con nuestros datos y no exponerlos a los peligros de manera imprudente. No es lo mismo enviar un correo electrónico a una persona concreta que enviarle mensajes de manera pública a través de una red social. Guillermo Zapata comentaba, justificando su dimisión como concejal de cultura del Ayuntamiento de Madrid, que los tuits que ahora lo han hecho dimitir habían sido enviados en el contexto de una conversación privada sobre los límites del humor. Debo decir que su frase me sorprendió. ¿Por qué tuitear conversaciones privadas en lugar de enviar e-mails? Todo ello me recordó el filósofo Byung Chui Han[4] cuando explica que la peculiaridad del panóptico digital es que las personas colaboran de forma activa en su vigilancia y en la construcción y conservación de este inmenso panóptico. Lo hacen cuando se exhiben mientras desnudan su información en las redes sociales.

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 y la vigilancia masiva de las telecomunicaciones globales: ¿una amenaza para los derechos humanos?

Google, Microsoft, Yahoo!, Facebook, Apple... ya hace algún tiempo que la gran mayoría de nosotros estamos muy familiarizados con estas grandes corporaciones. Casi cada vez que accedemos al mundo virtual con nuestros dispositivos con conexión a Internet (ordenador personal, teléfono móvil, tableta táctil...), hacemos uso de algunos de los servicios que ofrecen, desde los caros sistemas operativos (Windows y OS X) hasta los servicios «gratuitos» de correo electrónico (Gmail, Outlook, Hotmail, Yahoo! Mail...), buscadores (Google, Yahoo! Search...), navegadores (Safari, Internet Explorer, Google Chrome...), redes sociales (Google+, Facebook...), servicios de mensajería instantánea (WhatsApp) y de geolocalización (Google Maps), llamadas en línea (Skype) y almacenamiento en la nube (Google Drive, iCloud...). Y gracias a los documentos filtrados en 2013 por el ex-agente de la National Security Agency (NSA) Edward Snowden, ahora también sabemos que todas estas compañías han colaborado con el espionaje indiscriminado de la inteligencia americana, en el marco del programa PRISM.[1] No hace falta decir que cualquiera de nosotros bien podría haber sido objeto de vigilancia al usar alguna de estas herramientas.

Pero démosle a este espionaje aparentemente abstracto (por su condición silenciosa) una imagen tangible: Cory Doctorow, conocido activista por los derechos en Internet, comparaba hace poco el potencial de vigilancia de la NSA con el de la STASI, la policía secreta de la República Democrática Alemana – institución que permanece en la memoria colectiva como una herramienta de represión de un Estado obsesionado con el control de la ciudadanía. El ambiente asfixiante que suponía vivir bajo la mirada omnisciente de una agencia de inteligencia con orejas en todos lados ha constituido una figura popular en series de televisión, películas, videojuegos y novelas. Ahora bien, la comparativa de Doctorow consistía en lo siguiente: cada agente de la STASI se encargaba de vigilar 50 personas, mientras que con los medios tecnológicos de la NSA, *cada uno puede vigilar hasta 10.000.*[2] Las preocupantes implicaciones sociales de un organismo con el poder de controlar masivamente (sin ningún tipo de control judicial) las comunicaciones personales, las transacciones monetarias o las costumbres de navegación son evidentes. La STASI, que confiaba en aparatosos y complicados aparatos para llevar a cabo las escuchas, ha quedado reducida a la condición de «artesana» del espionaje, que substituía con su destreza manual las limitaciones en materia tecnológica. La NSA de hoy supera en todos los aspectos los procedimientos de la anticuada STASI.

Que el espionaje actual se lleve a cabo silenciosamente, sea menos perceptible, no puede ser una excusa en lo que respecta a la elaboración de una necesaria oposición política no solamente frente a las arbitrariedades de las agencias de inteligencia mundiales, sino también respecto a la percepción de Internet (o del ciberespacio) en tanto que zona militarizada, en la cual todo el mundo pasa a ser sujeto de escrutinio intensificado. *Digital significa intangible, pero nunca irreal*: una cantidad en aumento de nuestras funciones sociales más elementales (trámites con la administración, llamadas de voz, consulta de noticias o del catálogo de la biblioteca) se traslada ahora a la esfera virtual, a la que debemos contemplar no como un simplista doble «falso» de la sociedad «real», sino una extensión de la propia sociedad, con todas las especificidades que le pudieran corresponder. Utilizar el ciberespacio para comunicarnos no convierte nuestra interacción en ilusoria (al menos, no automáticamente), sino que la somete a nuevas pautas de comportamiento y socialización. De ahí que las vulneraciones de derechos en la red deban ser consideradas igual de relevantes que las que se hacen fuera del ámbito cibernético. No hay ninguna diferencia notable entre leer, analizar y almacenar sin consentimiento nuestro correo postal (sea por razones políticas o comerciales) y hacerlo con nuestro correo electrónico.

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

«Nadie será objeto de intromisiones arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honor y reputación. Todo el mundo tiene derecho a la protección de la ley contra tales intromisiones o ataques», afirma el artículo 12 de la Declaración Universal de los Derechos Humanos. De ahí que la naturalización a escala social de las continuadas intromisiones en este sentido corresponda a una estrategia política que pretende pasar por inocua la decisión (eminentemente política) de espiar indiscriminadamente las telecomunicaciones del global de la población. La «pesca de arrastre», en tanto que procedimiento marcadamente perjudicial para el suelo marítimo al no seleccionar sus objetivos, se extrapola sin diferencias notables al entorno digital, de

modo que el resultado no podía ser otro que la destrucción irresponsable de la seguridad del global de las telecomunicaciones, indistintamente de los objetivos que supuestamente se persigan. El Primer Ministro del Reino Unido, David Cameron, llegó a exigir la prohibición del cifrado de las telecomunicaciones con el objetivo de persistir en la lucha contra el terrorismo (recurso que utilizan tanto WhatsApp o Telegram como las transacciones financieras para asegurar la confidencialidad de las operaciones), una amenaza que ha comportado que ciertas iniciativas destinadas a ofrecer tecnología comprometida con los derechos humanos, como Ind. ie, hayan decidido irse del país debido a su reticencia a introducir *backdoors*[3] deliberados en sus productos, que no sólo permitirían que el gobierno tuviera acceso al contenido de los mensajes,[4] sino que los haría especialmente vulnerables en lo que respecta a posibles ataques cibernéticos.

La demanda de un Internet libre, democrático y abierto, ausente del control y rastreo a escala masiva ha de convertirse en uno de los ejes vertebradores de las organizaciones que pretenden defender los derechos humanos hoy, y no una cuestión que se limite a reducidos grupos de ciberactivistas o *hackers*. No podemos permanecer indiferentes ante un contexto específico en el cual las garantías democráticas siguen disminuyendo, por mucho que todo parezca estar sucediendo en el mundo denominado «digital». El poder de las agencias de inteligencia, que gozan de una situación privilegiada en la cual el escrutinio democrático es prácticamente inexistente, ha ido en aumento al mismo tiempo que nuestros propios derechos disminuyen de manera gradual. No podemos ser «sujetos de derecho» reales ante la existencia de estos poderosos mecanismos sociales, que actúan amparándose en el secreto más absoluto y sin que nosotros tengamos oficialmente constancia de ellos.

Resulta imprescindible que la trascendencia social que supone la existencia de, como mínimo, una red de espionaje global de las telecomunicaciones (conformada por diferentes organismos de inteligencia de los llamados «Five Eyes», es decir, Estados Unidos, Reino Unido, Canadá, Australia y Nueva Zelanda) se traduzca en un polo de oposición en defensa del derecho a no ser las arbitrarias víctimas de la mirada omnisciente del Estado, que nos expropia de las garantías jurídicas fundamentales. *El rastreo y la retención masiva de los datos personales son, por su componente indiscriminado e invasivo, absolutamente incompatibles con la democracia*. Un informe de la Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos afirmó el pasado 28 de mayo que «el cifrado y el anonimato otorgan la privacidad y la seguridad necesarias para ejercer el derecho de la libertad de opinión y expresión en la era digital. Esta seguridad puede ser esencial para el ejercicio de otros derechos (...)».[5] Implantar políticas que protejan el cifrado y el anonimato, en vez de criminalizarlo o perseguirlo, debe ser una prioridad de nuestros gobiernos en caso que quieran hacer de Internet un vehículo de la libertad de expresión, y no un medio para censurarla.

Enric Luján

3. *Backdoor*: Método para acceder al sistema operativo de un dispositivo electrónico sin tener que introducir contraseña alguna o seguir otros procedimientos que sirvan para identificar al usuario.
4. *So Long, and Thanks for All the Fish* (Blog de Aral Balkan, fundador de 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/)

Dinero, poder y opacidad en las instituciones europeas: un paraíso para el lobby militar*

El paisaje institucional europeo está en un constante proceso de construcción, como lo demuestra por ejemplo la evolución en las funciones del Consejo, de la Comisión y del Parlamento desde su nacimiento hasta la fecha. Otro tipo de instituciones se crearon en el camino, algunas por la presión que ejercen los lobbies en el panorama político europeo. Antes de detallar algunas de ellas, vamos a explicar qué es un lobby y cómo influye en las políticas europeas.

La situación de los lobbies en las instituciones europeas

Un lobby es una estructura que representa los intereses de un grupo dado, cuyo objetivo es influenciar las leyes, reglamentaciones y normativas, presionando a las personas o a las instituciones que ostentan el poder, con el fin de defender y promocionar sus propios intereses, por lo general económicos.[1] Esta definición de lobby pone en evidencia el vínculo que éste tiene que establecer con los políticos y las instituciones de poder. En Bruselas, donde se concentran muchas de las instituciones europeas (Comisión, Parlamento, Consejo, Agencia Europea de Defensa (AED), Frontex…), se estima que trabajan 15.000 lobistas, de los cuales 70% promueven los intereses de grupos industriales, 20% defienden los intereses de las regiones, ciudades e instituciones internacionales y sólo 10% representan los intereses de organizaciones no gubernamentales, dejando así la capital europea en segunda posición mundial en materia de lobbismo, justo después de Washington D.C.[2] La presión de los lobbies se ejerce pues sobre las instituciones que tienen poder de decisión, llevando así la política europea a una situación en la que está en mano de los grandes grupos industriales.

En la Unión europea, la Comisión tiene la exclusividad de iniciar los proyectos legislativos, además de tener que garantizar el interés general comunitario. Únicamente ella puede proponer políticas europeas en los campos definidos por los tratados, lo cual le lleva a ser el blanco privilegiado de los lobistas. Éstos, además de poder entrar y salir a su antojo de la Comisión, encuentran una demanda de asesoramiento importante por parte de los funcionarios. Por contra, para tener acceso al Parlamento europeo, los lobistas se tienen que acreditar en el registro de transparencia, recientemente puesto en marcha para controlar la identidad y el número de personas que tratan de influir en los debates parlamentarios. Sin embargo, a pesar de tratar de establecer una mayor transparencia en las actividades de representación de intereses, el registro no cumple con su función. Como no es obligatorio acreditarse, éste sirve sólo para saber cuántos lobistas entran en contacto con la Eurocámara (por consecuente se desconoce el número de lobistas que ejercen presión en la Comisión u otras instituciones), y no establece sanciones si éstos faltan al código ético que implica el registrarse. Aun así, el registro permite saber quiénes entran en contacto con las comisiones parlamentarias encargadas de discutir los proyectos legislativos de la Comisión, dónde más presión se ejerce.

Los actores europeos del lobby militar

Para promover y defender sus intereses en las instituciones europeas, las industrias militares cuentan con varios actores que les representan. Un estudio del GRIP los clasifica en cuatro categorías[3]: las estructuras industriales, las delegaciones de empresas del sector, los *think tanks* y los grupos de expertos. A continuación damos algunos detalles en cuanto a su vinculación con la industria armamentística.

En la primera entran la Asociación Europea de la Industria Aeronáutica Espacial y de Defensa (ASD por sus siglas en inglés), y la Organización Europea para la Seguridad (EOS por sus siglas en inglés). Si bien estas estructuras

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 en: 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 en: http://www.grip.org/fr/siteweb/images/NOTES_ANALYSE/2012/NA_2012-06-22_FR_A-BECKLEY.pdf

industriales no se declaran explícitamente como lobbies, sus presentaciones en la web no dejan lugar a duda. Así, la ASD presenta su misión general como: «ser un centro de inteligencia central para las industrias aeroespaciales, de defensa y de seguridad, [...] dar forma a la legislación y a las políticas de la UE, así como la obtención de oportunidades de financiación al defender posiciones comunes hacia las instituciones europeas y las organizaciones internacionales para el beneficio de las industrias europeas y en el interés colectivo de sus miembros».[4] De la misma manera, la EOS explica que su misión es: «proporcionar una plataforma de trabajo colaborativo, de intercambio de ideas y mejores prácticas entre las instituciones europeas y de la industria europea de Seguridad [...]. El objetivo principal de EOS es el desarrollo de un mercado de la seguridad europea armonizada en consonancia con las necesidades políticas, sociales y económicas a través del uso eficiente de los presupuestos».[5] La ASD y la EOS están inscritas en el registro de transparencia de la UE como *Grupos de presión dentro de las empresas y asociaciones comerciales, empresariales o profesionales*, y declaran respectivamente 16[6] y 8 lobistas,[7] lo cual autoriza a las personas identificadas tener un acceso permanente al Parlamento europeo.

Si bien las mayores empresas de defensa europeas como Thales, BAE Systems, Finmeccanica o EADS (que también se encuentran entre las 10 mayores empresas de armamento mundiales)[8] son miembros de las estructuras industriales previamente detalladas, estas empresas tienen también sus propias delegaciones a dos pasos de las instituciones europeas en Bruselas, segunda

4. ASD (2015). Mission en Key Priorities. Disponible en: http://www.asd-europe.org/about-us/missions-key-priorities/. Fecha de consulta: 12 de junio de 2015.
5. EOS (2015). What is EOS? Disponible en: http://www.eos-eu.com/Middle.aspx?Page=whatiseos&tID=1. Fecha de consulta: 12 de junio de 2015.
6. Ver registro de transparencia de la UE. Disponible en: http://ec.europa.eu/transparencyregister/public/consultation/displaylobbyist.do?id=72699997886-57, fecha de consulta: 13 de junio de 2015.
7. Ver registro de transparencia de la Unión europea. Disponible en: http://ec.europa.eu/transparencyregister/public/consultation/displaylobbyist.do?id=32134385519-64, fecha de consulta: 13 de junio de 2015.
8. SIPRI (2015). The SIPRI top 100 arms producing and military services companies, 2013. Disponible en: http://www.sipri.org/research/armaments/production/recent-trends-in-arms-industry/Fact%20Sheet%20Top100%202013.pdf. Fecha de consulta: 12 de junio de 2015.

categoría de estructura de influencia. Así pues, en el registro de transparencia encontramos los nombres y apellidos de las personas acreditadas para entrar de manera permanente en el Parlamento europeo, y que tratan de influenciar las políticas de defensa a favor de los objetivos corporativos que defienden. Thales cuenta con 6 lobistas,[9] EADS con 10,[10] Finmeccanica con 3[11] y BAE Systems con una persona para representar sus intereses.[12]

Además de las dos primeras categorías que hemos venido detallando –y que podemos catalogar como industriales– otras entidades no industriales trabajan para defender los intereses del sector. Tal es el caso de los *think tanks*, organizaciones cuya función es la de reflexionar e investigar sobre asuntos determinados. En el ámbito que nos interesa, el Security & Defense Agenda (SDA) se presenta como el único *think tank* especializado en cuestiones de defensa y de seguridad. El lobby se encuentra en uno de los lugares más prestigiosos de Bruselas y en pleno corazón del barrio europeo (en la biblioteca Solvay), lo cual refleja el poder de influencia de la organización, cuya financiación proviene en gran parte de la industria del sector (sobre todo de las dos mayores empresas de armas mundiales: Lockheed Martin y BAE Systems[13]), y en menor medida del sector público (OTAN, UE, Gobiernos nacionales, entre otros) y privado (como fundaciones, ONG). Más allá de sus recursos económicos, es el renombre de los miembros de su *advisory board* que da una fama especial a la organización.

Con personalidades como Javier Solana (ex director de la Agencia Europea de Defensa - EAD por sus siglas en inglés), Jaap de Hoop Scheffer (ambos ex secretarios generales de la OTAN), o Claude-France Arnould (también ex directora de la EAD) la SDA cuenta con varios perfiles de autoridades del sector de defensa, que además ilustran el fenómeno de las puertas giratorias, sintomático de las altas esferas de poder.[14]

En la última categoría del lobby militar europeo, los grupos de expertos son unas entidades consultativas cuyo rol es proporcionar asesoramiento y conocimientos especializados a la Comisión y sus departamentos, en el marco de la elaboración de propuestas legislativas e iniciativas políticas.[15] Es la Comisión europea la que pone en marcha este tipo de organización para cubrir las lagunas que tiene sobre algunas cuestiones. Sin embargo, como bien explica Berkeley en el informe del GRIP, el interés general que tiene que garantizar la Comisión en el seno de la Unión se confunde con el interés industrial cuando la composición de estos grupos no incluye a la sociedad civil y está tachada de opacidad.[16] En el sector de la defensa y de la seguridad, destaca el papel del grupo STAR 21 en el desarrollo de una estrategia aeroespacial europea. Con un total de 15 personas, éste se compone de 8 miembros de las instituciones europeas y gobiernos nacionales y 7 representantes de la industria militar, sin que portavoces de centros de investigación especializados, universidades o sociedad civil puedan contribuir en la elaboración de las iniciativas políticas que representen el interés general.[17]

9. Ver registro de transparencia de la UE. Disponible en: http://ec.europa.eu/transparencyregister/public/consultation/searchControllerPager.do?declaration=Thales&search=search, fecha de consulta:13 de junio de 2015.
10. Ver registro de transparencia de la UE. Disponible en: http://ec.europa.eu/transparencyregister/public/consultation/displaylobbyist.do?id=2732167674-76, fecha de consulta: 13 de junio de 2015.
11. Ver registro de transparencia de la UE. Disponible en: http://ec.europa.eu/transparencyregister/public/consultation/displaylobbyist.do?id=02550382403-01, fecha de consulta: 13 de junio de 2015.
12. Ver registro de transparencia de la UE. Disponible en: http://ec.europa.eu/transparencyregister/public/consultation/searchControllerPager.do?declaration=BAE+systems&search=search, fecha de consulta: 13 de junio de 2015.
13. SIPRI (2015). The SIPRI top 100 arms producing and military services companies, 2013. Disponible en: http://www.sipri.org/research/armaments/production/recent-trends-in-arms-industry/Fact%20Sheet%20Top100%202013.pdf. Fecha de consulta: 12 de junio 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 en: http://ec.europa.eu/transparency/regexpert/index.cfm?do=faq.faq&aide=2&Lang=ES, fecha de consulta: 12 de junio 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 en: 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 du GRIP*, 22 juin 2012, Bruxelles. Disponible en: http://www.grip.org/fr/siteweb/images/NOTES_ANALYSE/2012/NA_2012-06-22_FR_A-BECKLEY.pdf

Un ejemplo de la influencia del lobby militar: la creación de la Agencia Europea de Defensa

Como ya hemos dicho, la acción del conjunto de los actores que forman el lobby militar en Bruselas está orientada hacia varias instituciones europeas, como por ejemplo la Comisión, la Eurocámara o bien la Agencia de Defensa Europea (EAD), y llega a dibujar el paisaje institucional europeo. De hecho, la creación de esta última sería un logro del lobby de defensa mismo, tal y como lo expone el Corporate Europe Observatory en su blog.[18] En él, explican cómo Michel Troubetzkoy, el jefe de la delegación de EADS en Bruselas, se jactaba de la creación de la Agencia de Defensa Europa, el «*bebé de EADS*». Éste se felicitaba de la facilidad para entrar en contacto con políticos, e influenciarlos para que presenten en el Consejo los textos legislativos que ellos mismos redactan. Según sus palabras, el texto presentado para la creación de la Agencia de Defensa Europea estaba idéntico en un 95% al documento facilitado por EADS.

La descripción del lobby militar europeo que hemos venido haciendo en este artículo es sólo una breve introducción a la complejidad de las dinámicas que permiten a estas potentes organizaciones influir en las políticas de defensa y de seguridad europeas. Frente a sus medios, la

sociedad civil no da la talla para compensar la representación de intereses económicos en las instituciones y promocionar los intereses sociales y medioambientales. Sin embargo, algunas organizaciones vigilan la actividad de los lobbies en Bruselas, investigando y organizando campañas para sensibilizar la opinión pública sobre su carácter nefasto. En cuanto al lobby de la defensa y de la seguridad, destaca la actividad «Lobby tour militar» de la asociación Agir pour la Paix, basada en un trabajo del Corporate Europe Observatory, que permite a los ciudadanos darse cuenta del alcance de los tentáculos del sector militar en las instituciones y políticas europeas. Mientras éstos traten de influir en ellas para defender sus intereses corporativos desencadenadores de guerras, violencias e injusticias, estaremos trabajando para denunciar sus actuaciones y procurar empoderar la sociedad civil.

Chloé Meulewaeter

18. Corporate Europe Observatory (2015). The Silent Bubble. Disponible en: http://blog.brusselsbubble.eu/2008/12/silent-bubble.html, fecha de consulta: 13 de junio de 2015.

** La autora agradece la disponibilidad y la información proporcionada por Stéphanie Damblon, de la asociación Agir pour la Paix, durante el «lobby tour militar» en Bruselas.*

CENTRE DELÀS D'ESTUDIS PER LA PAU

Equipo de redacción: Jordi Calvo y Pere Ortega.

Han colaborado en este número: Pere Brunet, Enric Lujan y Chloé Meulewaeter.

D.L.: B-19576-2010 · ISSN edición impresa: 2013-813X · ISSN edición en línea: 2013-9764

Ajuntament de Barcelona

CÓMO COLABORAR

- **Forma parte de nuestro equipo de investigación.**
- **Ayúdanos en tareas de comunicación, gestión y campañas.**
- **Haz las prácticas de tus estudios en nuestro Centro.**
- **Hazte socio desde nuestra 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