La realidad del espionaje económico

Pedro BAÑOS

Teniente Coronel de Infantería, Diplomado de Estado Mayor. Vicepresidente Primero de la Asociación de Diplomados Españoles en Seguridad y Defensa.

Introducción

Caso primero. Dos ilustres personajes, de gran talla intelectual, son enviados por el gobierno de su nación para espiar los adelantos científicos y tecnológicos europeos. También se les encarga que, en la medida de lo posible, entorpezcan otros desarrollos que puedan significar una ventaja para los adversarios de su país. En cumplimiento de su misión, visitan instalaciones comerciales y militares, como puertos, fábricas, minas y arsenales, haciéndose con importante información sobre diseños y procedimientos de fabricación avanzados, mejoras en la producción de alimentos y otros detalles técnicos de máxima trascendencia.

Caso segundo. Un prestigioso ingeniero y matemático se desplaza a un país vecino con el encargo de su gobierno de espiar el sistema de producción de un arma tecnológicamente muy avanzada.

Caso tercero. Debido a la fuerte crisis que sufre un sector de producción, generada por el importante retraso tecnológico, un empresario decide trasladarse a otro país con la idea de hacerse con los secretos de las capacidades técnicas y las tecnologías que son utilizadas por las industrias de este país, tan avanzadas que es imposible competir con ellas.

Ante la avalancha de noticias que acusan a China y Rusia de múltiples acciones de espionaje en los países punteros en tecnología, lo más probable es que se haya tendido a pensar que los autores de los casos citados procedían o trabajaban para uno de estos dos países.

Sin embargo, la realidad es muy otra.

El caso primero que se expone tiene como protagonistas a **Jorge Juan** y **Antonio de Ulloa**[1], enviados a mediados del **siglo XVIII** por España para espiar en buena parte de la Europa coetánea.

El segundo caso hace referencia al español **Agustín de Betancourt** (Puerto de la Cruz, 1758–San Petersburgo, 1824), primer director de la Escuela de Puertos y Caminos de Madrid. En 1993[2], se descubrió un manuscrito inédito suyo en la biblioteca del Palacio Real de Madrid, fechado en **1791** y dedicado a Carlos IV, en el que describía el sistema de fundición y barrenamiento de cañones para la marina en la fábrica francesa de Yndrid, cuyos datos, según parece, había obtenido Betancourt mediante el espionaje.

En el tercer caso[3], estamos hablando de **Bernardo de Arochena**, quien, ante el triste panorama que sufría la producción de curtidos en Sevilla en la segunda mitad del **siglo XVIII**, realiza un viaje a Londres para descubrir los motivos por los que la industria inglesa se había convertido en imbatible en este campo.

Estos ejemplos sirven para ilustrar a la perfección que el **espionaje económico** es una **práctica antiquísima.** Desde el origen de los tiempos, los hombres han pugnado por conocer los secretos de la producción de bienes que en su momento eran considerados un lujo, proporcionaban pingues beneficios o daban una gran ventaja militar. Bien fuera la fabricación de tapices, cerámicas, porcelanas, cristales o vidrieras. O la construcción de catedrales, acueductos o pirámides. Incluso el perfeccionamiento en la producción agrícola, de vinos y aceites, o la conservación de alimentos. Sin olvidar, por supuesto, el armamento y los ingenios bélicos: fundición de aleaciones, máquinas de asalto, avances revolucionarios (armas de repetición y automáticas, corazas,...), ni tampoco las tácticas y estrategias novedosas.

La mundialización del capitalismo

Como vemos, y al igual que sucede en la inmensa mayoría de los ámbitos, hay muy pocas cosas nuevas bajo el Sol, con la excepción de lo relacionado con la tecnología.

Pero, sin duda alguna, la **globalización,** con su desesperada búsqueda de **beneficios** –propia de la pura y dura aplicación del capitalismo y del liberalismo económico–, ha agudizado las realidades del espionaje, dentro de los muy diversos campos de la economía.

Hay que tener en cuenta que para conseguir esos anhelados beneficios, tanto empresas como Estados necesitan **vender** a toda costa, y cuanto más mejor. Para ello, además de la necesidad de conseguir, mantener y ampliar **mercados** solventes –en feroz pugna con una creciente competencia–, precisan de una serie de factores imprescindibles para sostener, y potenciar en lo posible, una producción industrial eficiente y rentable, generadora de bienes "vendibles": **recursos naturales** (minerales, madera,...), **energía** (principalmente hidrocarburos y electricidad) y **tecnología.**

Así las cosas, el espionaje económico, en sus diferentes versiones, actúa en todas y cada una de las fases del proceso productivo y financiero (planeamiento, diseño, producción, mercado, venta,...), así como en las necesidades que dicho proceso exige (materias primas, energía y tecnología), haciendo especial hincapié –aunque no únicamente– en la tecnología,

dado que en muchos casos esta va a ser decisiva a la hora de conseguir que un producto tenga la debida penetración comercial.

Evidentemente, el acelerado mundo en que nos movemos, en donde los productos, muy especialmente los relacionados con la alta tecnología (sean teléfonos móviles, ordenadores o vehículos), se convierten en obsoletos en plazos de tiempo cada vez menores, impulsan a las empresas a desear ser las primeras en **ofrecer la última novedad** a los consumidores, abriendo el camino a un fomento del espionaje de los competidores, en el afán por hacerse con un mercado cada vez más exigente y ansioso de primicias.

Así las cosas, los **casos de espionaje abundan**, creciendo el número de ellos de modo exponencial. Aún así, se estima que los que se dan a conocer públicamente **no son más que la punta del iceberg.** La gran mayoría de las empresas, fábricas, entidades financieras o negocios de cualquier tipo, prefieren, como norma, no hacer público que han sido víctimas de un caso de espionaje. Obviamente, esta violación de su seguridad les puede suponer un gran desprestigio, con repercusiones económicas aún mayores que las causadas por el espionaje en sí.

Incluso los propios Estados -salvo que el caso haya tenido cierta repercusión mediática o que, por el motivo que sea, interese su publicidad- prefieren que este tipo de trapos sucios queden dentro del submundo de los servicios de inteligencia, por lo que se limitan a aplicar en la sombra las medidas específicas que este sector habitúa.

Esta circunstancia, unida a la realidad de una cierta despreocupación por parte de un buen número de directivos y empleados acerca de la necesidad de adoptar eficaces medidas disuasorias y preventivas del espionaje, hace que los espías sigan campando a sus anchas, sabedores de que, con un poco de suerte, en caso de ser descubiertos, los perjuicios para ellos van a ser mínimos. De hecho, se estima que en más del 80% de las ocasiones, cuando un espía es descubierto se llega a un acuerdo "amistoso", con la mínima algarada posible[4].

Delimitando los conceptos

La primera diferenciación que debe hacerse es entre "inteligencia" y "espionaje", con indiferencia del apellido que luego se añada a estos dos términos. La **inteligencia**, además de constituir todo un proceso, no tiene porque necesariamente partir de información obtenida de forma ilegal. De hecho, puede perfectamente elaborarse exclusivamente con fuentes abiertas, de un modo transparente, como habitualmente sucede. Como norma general, consiste en realizar análisis, conclusiones y propuestas originales y valiosas a partir de datos al alcance de prácticamente cualquiera, los cuales pueden ser gratuitos o de pago.

Sin embargo, el **espionaje** siempre es una actividad ilegal, cuando menos alegal (dependiendo de la normativa de cada país), y realizada de forma encubierta, opaca y no autorizada. Trata de obtener información -que luego precisará, en la mayoría de los casos, pasar por un proceso de valoración y análisis realizado por expertos[5]-, por medios irregulares, que de otro modo sería imposible de conseguir o se tardaría mucho más tiempo en hacerse con ella.

Ante la profusión de términos empleados, y su consiguiente confusión, se va a tratar de ofrecer algunas definiciones de los principales

conceptos, aunque sin olvidar que en algunos casos se puede considerar que son sinónimos, ni tampoco que es normal que se solapen buena parte de ellos.

Espionaje bancario: ilícita obtención de información sobre posiciones y movimientos bancarios. También acerca de fusiones, adquisiciones y otras operaciones propias del sector.

Espionaje comercial: ilícita obtención de información sobre la producción, ventas, clientela, proveedores, socios, planes de expansión, fusiones, adquisiciones, directivos, empleados o cualquier otro dato relacionado, en general, con la producción y venta de una empresa.

Espionaje industrial: ilícita obtención de información sobre la planificación, investigación y fabricación de productos novedosos.

Los sectores habitualmente más afectados son los relacionados con la **alta tecnología** y los fabricantes de **productos de gran valor o con un ciclo de vida muy corto** (farmacéuticas, automóviles, biotecnología, comunicaciones, informática,...).

Espionaje fiscal: ilícita obtención de información sobre posibles evasores de fondos e impuestos, tanto dentro como fuera del territorio nacional.

Este tipo de espionaje también es cometido por los **propios Estados.** Aunque el espionaje bancario tiene una historia de más de ocho décadas –como afirma Thomas Chappot, autor de "El espionaje bancario y su rol en la adopción de disposiciones relativas al espionaje económico (1930-1935)"–, la actual crisis económica ha llevado a muchos gobiernos a potenciar la lucha contra el fraude fiscal y la evasión de capitales, incluso fuera de sus fronteras. Algo que tampoco es nuevo, pues la crisis mundial de 1929 impulsó a los países europeos a este mismo combate, como expone Chappot en los siete casos documentados que relata en su libro[6].

Posiblemente, en este sentido el país más espiado sea **Suiza**, refugio tradicional de fondos procedentes de todo el planeta. Ha habido casos recientes muy llamativos, como cuando, en diciembre de 2009, el gobierno francés reconoció que poseía información del banco HSBC conseguida por medios ilegales, en la que se recogían los nombres de 130.000 presuntos evasores de impuestos. Un año más tarde, en octubre de 2010, las autoridades de Renania del Norte-Westfalia, en Alemania, afirmaron haber pagado dos millones de francos suizos por información sobre 200 clientes del banco Julius Bär.

Probablemente por estos motivos, el Servicio de Inteligencia helvético reconoció, a principios de este año, que el espionaje económico es la principal amenaza estratégica a la que se debe enfrentar Suiza, siendo, por tanto, la protección de la información confidencial de los grandes bancos suizos una tarea prioritaria[7].

No obstante, Suiza también ha caído en la tentación de espiar[8]. En 2007, la más alta instancia judicial suiza, el Tribunal Federal, confirmó el empleo de información obtenida ilegalmente de una fiduciaria de Liechtenstein por parte de las autoridades fiscales del cantón de Berna.

Espionaje tecnológico: ilícita obtención de información relativa a patentes, desarrollo de prototipos, estudios avanzados o informes científicos.

Espionaje financiero: ilícita obtención de información sobre una empresa o persona al

respecto de su solvencia, deudas, capacidad y calidad de pago, gestiones bursátiles, especulaciones y otros aspectos relacionados con las altas finanzas.

Espionaje económico: ilícita obtención de información con la finalidad de conseguir ventajas económicas, en detrimento de la competencia, sea esta empresarial o estatal. Se puede hacer la diferenciación entre el efectuado en el ámbito de la microeconomía y en el de la macroeconomía. Igualmente, hay que diferenciar entre el producido entre empresas de un mismo país, entre industrias de países distintos y el ejercido por agentes de servicios secretos extranjeros (estatal).

En el ámbito del Estado, este tipo de espionaje puede ser parte de una verdadera guerra, pues algunas acciones extremas tienen el potencial de provocar daños enormes, con gran capacidad desestabilizadora, a un país, pudiendo destruir todo su tejido financiero de no tenerse adoptadas las medidas preventivas y correctoras precisas.

En junio de 2010, el entonces Ministro del Interior alemán, Thomas de Maizière, expuso que su gobierno preveía que en un futuro inmediato el espionaje económico se convertiría en el centro de gravedad del crimen organizado, habiéndose convertido, por tanto, en una de las grandes preocupaciones de la Oficina de Defensa de la Constitución. De Mazière también apuntó que países como Rusia y China fomentan el espionaje en la economía, la ciencia y la investigación[9].

Espionaje tecnológico-militar: ilícita obtención de información sobre las capacidades y potencialidades científicas y tecnológicas de la industria, pública y privada, de la que dispone un Estado para desarrollar nuevos equipos militares, material bélico y armamento. Concepto muy próximo al del espionaje "convencional", en el que está en juego la seguridad nacional.

Un ejemplo, de los muchos existentes, podría ser, a decir de algunos expertos, la obtención por el Mossad de los planos originales del Mirage 5, fabricado por la empresa francesa Dassault, y que sirvieron a Israel para desarrollar el avión de combate Kfir (también denominado F-21A Lion).

Más recientemente, algunas de las principales industrias armamentísticas japonesas –Mitsubishi Heavy Industries (MHI) e Ishikawajima-Harima Heavy Industries (IHI)– han denunciado el acceso no autorizado a información altamente sensible, entre la que se incluiría datos sobre submarinos, misiles y centrales nucleares[10]. MHI ha reconocido haber encontrado ocho virus en más de 80 de sus servidores. Como ya empieza a ser habitual, algunos medios japoneses dirigieron su mirada acusadora a China, pero Pekín, como también es norma, inmediatamente negó tener relación alguna con los hechos.

Guerra económica: enfrentamiento entre empresas, grupos de ellas o Estados por conseguir la supremacía en un determinado campo económico, con la finalidad de incrementar los beneficios, anular la competencia, monopolizar un mercado o producto, o bien controlar las materias primas y las tecnologías imprescindibles para desarrollos futuros. Puede tener lugar tanto en escenarios reales como virtuales (ciberespacio o mercado bursátil). Así mismo, puede desembocar, llegado el caso, en un choque violento. El espionaje forma parte importante de la amplia panoplia de medios empleados durante esta guerra en la consecución de los fines.

Histórico reciente

Aunque todavía se carezca de datos precisos[11], es bien conocido que la URSS ejerció un espionaje masivo en los países occidentales, haciéndose con información clave para el desarrollo de objetos tan variados como transbordadores espaciales, aviones de combate y hornos microondas. Uno de los casos más paradigmáticos es el del avión supersónico Tupolev Tu-144, demasiado "parecido" al Concorde como para haber sido un desarrollo totalmente independiente.

Por su parte, las noticias en las que se ha relacionado el espionaje económico con ciudadanos **chinos** o personas actuando en beneficio de **empresas chinas**, han inundado en los últimos años todos los periódicos. Algunos de los más sonados han sido:

- 2005: una becaria china obtiene de la empresa francesa Valeo información sobre el diseño de componentes para futuros automóviles.
- 2007: cinco trabajadores de fábrica coreana Kia Motors venden información confidencial a la industria china.
- 2008: un ciudadano canadiense de origen chino es condenado por un tribunal estadounidenses por vender secretos corporativos de empresas armamentísticas norteamericanas a las autoridades de China[12].
- 2010: un ciudadano estadounidense de origen chino es condenado en EEUU a 15 años de cárcel por acumular información confidencial de la compañía Boeing para proporcionársela al gobierno de Pekín. El espía podría haber estado pasando información durante 30 años sobre el trasbordador espacial, cohetes, helicópteros y aviones de combate.
- 2011: a principio de año, la empresa francesa Renault acusa a tres de sus directivos de vender información a la industria de la automoción china sobre el desarrollo del coche eléctrico, concretamente sobre el diseño de la batería. Aunque finalmente la compañía gala manifestó que había errado en su denuncia, y exoneró a su personal de la acusación de espionaje industrial, la duda sobre este caso se mantiene.
- Octubre de 2011: en EEUU, un científico de origen chino se declara culpable de robar secretos comerciales, durante cuatro años, para venderlos a China y Alemania[13].
- A primeros de octubre de este año, el presidente del Comité de Inteligencia de la Cámara de Representantes estadounidense, Mike Rogers, acusó abiertamente a China de estar robando descaradamente información comercial y propiedad intelectual[14].

Pero ni los chinos ni los rusos son los únicos implicados en el espionaje económico, a pesar de que sea a los que habitualmente se les señale con el dedo. Hay multitud de casos en los que se han visto envueltos ciudadanos y **empresas europeas y norteamericanas**. Algunos ejemplos dignos de ser citados pueden ser[15]:

- En 1993, el entonces director de la CIA, Robert Gates, acusó a Francia de espiar a EEUU en los campos industrial y comercial. Dos años más tarde, en 1995, Francia expulsó a cinco agentes de la CIA por espionaje comercial y científico –además de político–, centrado en la industria audiovisual y de comunicaciones. En ese año, y ante el creciente enfrentamiento comercial entre los dos países, el contraespionaje francés llegó a considerar a la CIA como su principal adversario[16].

- La empresa alemana SAP fue condenada a compensar con casi mil millones de euros a la norteamericana Oracle por obtener ilegalmente información de esta.
- A su vez, Oracle, una década atrás, había sido noticia por su intento de conseguir datos de Microsoft.
- La escudería McLaren fue sancionada por la Federación Internacional de Automovilismo por obtener información de su rival Ferrari.
- Coca-Cola ha denunciado reiteradamente a Pepsi por intentar hacerse con los secretos de las fórmulas de sus refrescos.
- En el altamente competitivo mundo farmacéutico, las acusaciones de espionaje son habituales. Uno de los casos más recientes fue el cometido por Novartis para hacerse con los datos del Augmentine fabricado por GSK.
- No se libra ni el mundo de la moda, donde las denuncias por el robo de diseños es muy frecuente.
- Tampoco los fabricantes de cervezas escapan de esta lacra, habiéndose dado el caso, en 2002, de que Cervezas Alhambra presentara una querella contra Heineken por presunto espionaje.
- A través de Wikileaks, se ha podido saber que la embajada de EEUU en Berlín consideraba en 2009 a Francia como el país que más espiaba la tecnología de sus aliados, en especial la de Alemania[17].
- En España, el hecho más comentado en la prensa se produjo hace un menos de un año, cuando un tribunal de Barcelona condenó a un ingeniero por robar y revelar información confidencial de su empresa[18]. En 2008, hubo otro caso, aunque con menor resonancia, cuando un joven de Iruñea fue detenido por espionaje industrial[19].

Así mismo, hay quien opina que los más avanzados en espionaje industrial siguen siendo los **japoneses**[20]. Aunque, según parece, Francia y Alemania podrían disponer de redes de espionaje conjuntas en diversas partes del mundo.

Además, no puede dejar de mencionarse que muchos son los que plantean que la mayor red de espionaje económico mundial es **Echelon**. Aunque negada oficialmente por EEUU, los expertos consideran que no solo existe, sino que tiene una capacidad para interceptar cualquier comunicación que se produzca mediante cualquier medio electrónico (sea teléfono o internet), incluyendo las transacciones comerciales. Esta red estaría controlada por la norteamericana Agencia de Seguridad Nacional (NSA, por sus siglas en inglés), y, además de EEUU, la integrarían Reino Unido, Canadá, Australia y Nueva Zelanda. Si bien su función primaria seguiría estando relacionada con los aspectos propios de la seguridad, como el terrorismo, en los tiempos actuales los intereses comerciales estarían igualmente en el foco de la atención de sus casi 400.000 empleados.

Para algunos, esta red de espionaje habría sido la responsable de que, en 1994, el grupo francés Thompson-CSF perdiera un multimillonario contrato con Brasil en beneficio de la empresa norteamericana Raytheon. Y de que, el mismo año, Airbus fracasa en su intento de negocio con Arabia Saudí, del que habrían sacado provecho Boeing y McDonnell Douglas, ambas estadounidenses[21]. También, entre 1994 y 1995, la empresa alemana de construcción de aerogeneradores Enercon GmbH habría sido espiada por Echelon a favor de su competidora Kenetech Windpower Inc.

Aunque no existen datos irrefutables acerca de su existencia o actividades, lo cierto es que,

en 2001, el Parlamento Europeo oficialmente estimó que no había motivo para dudar de la existencia de un sistema de interceptación de las comunicaciones a nivel mundial, tanto de las militares como de las privadas y comerciales, en clara referencia a la citada red Echelon.

El marco de la estrategia española de seguridad

La Estrategia Española de Seguridad, aprobada el 24 de junio de este año por el Consejo de Ministros, concede una enorme trascendencia al **espionaje económico**, como queda reflejado en las numerosas veces que cita los aspectos con él relacionados a lo largo de sus 85 páginas[22].

Ya en el Resumen Ejecutivo menciona que la **seguridad económica** es parte integral y requisito esencial de la seguridad nacional. En la misma introducción se cita que los **ciberataques** más comunes tienen **fines comerciales**, así como que las **nuevas tecnologías** ofrecen más sofisticados medios para el **espionaje**.

En la página 69 del mismo documento, hay un apartado dedicado en exclusiva al **espionaje**, al que define como las agresiones por parte de Estados, grupos o personas, con la finalidad de lograr información para obtener ventajas políticas o económicas.

También concede una particular importancia al **espionaje económico**, definido como la **adquisición ilícita de información**, patentes o tecnología críticas, e incluso la **influencia ilegal** en **decisiones políticas** de carácter económico.

Hay que destacar que este apartado concluye que el espionaje sigue constituyendo una **amenaza real y en permanente evolución**, la cual, a pesar de que su carácter clandestino hace que sea poco visible, puede tener efectos muy negativos para la seguridad.

Sistema de inteligencia económica

Para hacer frente a la amenaza que supone la inseguridad económica y el espionaje asociado, la Estrategia Española de Seguridad anuncia reiteradamente la creación de un **Sistema de Inteligencia Económica.**

De la lectura del texto se pueden deducir las **dos misiones** que se le dan a este futuro Sistema de Inteligencia Económica:

- **Analizar y facilitar información** económica, financiera y empresarial estratégica relevante, oportuna y útil para apoyar la acción del Estado y una mejor toma de decisiones en este ámbito.
- La **detección y prevención** de actuaciones contrarias a los intereses económicos, financieros, tecnológicos y comerciales de España en sectores estratégicos.

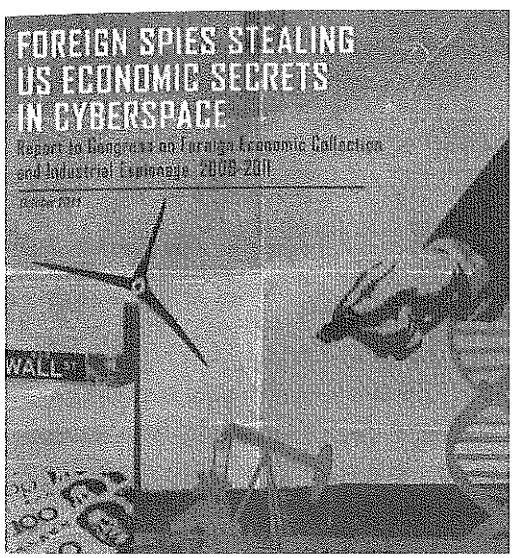
Sin duda, este Sistema es una necesidad perentoria, por lo que se espera que su puesta en marcha sea inminente. Así mismo, y debido precisamente a su enorme trascendencia, sería deseable que fuera dirigido por verdaderos expertos que hayan demostrado previamente su solvencia en el competitivo mundo económico, no necesariamente provenientes del funcionariado ni mucho menos nombrados por razones exclusivamente políticas.

Informe de la oficina nacional de contrainteligencia de EEUU[23]

A finales de octubre de este año, la Oficina Nacional de Contrainteligencia norteamericana

hizo público un informe, en el que **acusa a Rusia y China** de ser los principales responsables de los robos de secretos comerciales y tecnológicos a EEUU, empleando principalmente el ciberespacio[24].

Tras ser conocido el informe, un portavoz del Ministerio de Relaciones Exteriores de China se apresuró a rechazar de plano las acusaciones de espionaje contra su país, las cuales consideró como irresponsables y poco profesionales.



Fuente: *http://www.rtve.es/noticias/components/noticio/popup/1/7/1/3/foto473171_1240952.shtml*

En cualquier caso, este completo y detallado documento aporta valiosa información y pone de manifiesto, una vez más, la enorme importancia que está adquiriendo en los tiempos actuales todo lo relacionado con el espionaje económico. Y no solo eso, sino que augura que esta actividad se verá potenciada en el futuro inmediato, a medida que la competencia se vaya endureciendo y haya una mayor profusión de las nuevas tecnologías relacionadas con la información y las comunicaciones.

Algo que queda perfectamente claro en su resumen ejecutivo, en el que puede leerse que la obtención de información económica por parte de agentes extranjeros y el espionaje industrial representan una **importante y creciente amenaza** contra la prosperidad y la seguridad nacional. Un aspecto preocupante si se tiene en cuenta la rápida transferencia masiva de datos de una manera anónima y difícil de detectar que permite el **ciberespacio**, siendo realmente complejo atribuir la autoría.

Según el informe, las **principales áreas** espiadas son: la tecnología de la información y las comunicaciones, que constituye el núcleo central de prácticamente todas las demás tecnologías; la información financiera relativa a recursos naturales escasos; la tecnología militar, especialmente los sistemas marítimos, las aeronaves no tripuladas y las tecnologías aeroespaciales y aeronáuticas; y las tecnologías civiles y de doble uso en sectores en rápido crecimiento, tal como las energías limpias y las relacionadas con la salud y la industria farmacéutica.

También se pueden destacar las definiciones que se ofrecen:

- **Secreto comercial:** cualquier forma y tipo de información financiera, de negocios, científica, técnica económica o de ingeniería –incluyendo modelos, planes, compilaciones, programas, fórmulas, diseños, prototipos, métodos, técnicas, procesos, procedimientos, programas o códigos–, sobre la cual el propietario ha adoptado medidas razonables para mantenerla secreta, y que el hecho de que permanezca oculta implica un valor económico, actual o potencial.
- **Espionaje económico:** cuando un actor, actuando en **beneficio de un Gobierno extranjero:**
  - o (1) roba, se apropia, oculta, u obtiene mediante decepción o fraude un secreto comercial;

  - o (2) copia, duplica, reproduce, destruye, envía, descarga o transmite un secreto comercial sin autorización;
  - o (3) recibe un secreto comercial a sabiendas de que ha sido robado, apropiado, obtenido o convertido sin autorización.
- **Espionaje industrial** (o robo de secretos comerciales): cuando un actor, con la intención o a sabiendas de que causará un **perjuicio al propietario** del secreto comercial de un producto producido para colocarlo en el mercado interior o para comerciar en el extranjero, actúa con la intención de convertir ese secreto comercial en **beneficio económico** mediante:
  - o (1) robar o sin autorización apropiarse, ocultar u obtener mediante decepción o fraude información relacionada con dicho secreto;
  - o (2) copiar, duplicar, reproducir, destruir, enviar, descargar o transmitir esa información sin autorización;
  - o (3) recibir la información a sabiendas de que ha sido robada, apropiada, obtenida o convertida sin autorización.

Por otro lado, el informe aporta información sobre otros países que también sufren esta lacra, pudiéndose destacar los siguientes datos:

- **Alemania** estima que, a causa del espionaje económico, sus compañías pierden anualmente entre 28.000 y 71.000 millones de dólares y entre 30.000 y 70.000 empleos.
- **Corea del Sur** asegura que la mitad de los casos de espionaje que sufren sus empresas procede de China.
- **Japón** apunta que China está involucrada en el 60% de las filtraciones de tecnología de sus compañías.
- **Canadá** afirma que el 86% de las grandes compañías de su país sufrieron casos de ciberespionaje en 2010.

Conclusión

Como afirman todos los expertos[25], el espionaje económico se ha multiplicado en los últimos años, fomentado por la crisis económica. El escenario puede ser tanto intranacional como internacional, como ocurre con frecuencia creciente.

A nivel estatal, se puede considerar que estamos sumidos en una guerra oculta, incruenta, pero con potencial para provocar daños inmensos, no solo a las empresas sino a todo el tejido económico-industrial de un país.

Tanto la amenaza como la necesidad de hacerle frente, están claras; y la recientemente aprobada Estrategia Española de Seguridad así lo refleja, indicando el camino que debe imperiosamente seguirse para garantizar la seguridad de tan importante aspecto nacional.

La clave ahora está en que en verdad se adopten medidas efectivas para combatir eficazmente a esta gravísima amenaza. Una realidad que obliga a que no se pueda demorar por más tiempo la implementación de cuantas acciones al respeto sean precisas.

Para ello, hacen falta personas no solo con los conocimientos técnicos exigibles, sino que también dispongan de la percepción correcta de lo que supone esta realidad ya casi cotidiana. Además, por supuesto, quienes tienen las responsabilidades políticas deben disponer de la férrea voluntad de imponer las medidas disuasorias y correctoras que sean precisas, volcándose en inculcar la cultura de la protección

contra el espionaje a funcionarios, empresarios y empleados.

Especialmente cuando lo que está en juego es la seguridad nacional, como sucede cuando el espionaje económico actúa, de modo más o menos directo, en el campo macroeconómico y en beneficio de una potencia extranjera, lo que sucede con mucha más frecuencia de lo imaginable.

Notas

1. Lafuente, Antonio y Peset, José Luis (1981).
2. Samaniego (1993).
3. Autor desconocido (2007).
4. Rueda (2011).
5. En definitiva, el espionaje se podría definir como la obtención ilegal de información para su posterior conversión en un tipo de inteligencia.
6. Steiner (2010).
7. Ornelas (2011).
8. Ibíd.
9. EFE (2010).
10. RTVE/EFE (2011).
11. Autor desconocido (2009).
12. Legal Today (2008).
13. Voz de América (2011).
14. AFP (2011).
15. Para más detalles, ver Fernández (2011).
16. González (1995).
17. EFE (2011).
18. Martínez-Vares (2011).
19. EFE (2008).
20. Alpoma (2005).
21. Peredo (2008).
22. Estrategia Española de Seguridad (2011).
23. RTVE (2011).
24. Office of the National Counterintelligence Executive (2011).
25. Mars (2011).

Bibliografía

Libros

Chappot, Thomas (2010). L'espionnage bancaire et son rôle dans l'adoption de dispositions relatives à l'espionnage économique (1930-1935). Universidad de Lausanne.

Estrategia Española de Seguridad (2011). Imprenta Nacional del Boletín Oficial del Estado. Gobierno de España.
http://www.lamoncloa.gob.es

Marenches y Ockrent (1986). *Dans les secrets des princes. Stock.* Paris.

Romaña, José Miguel (1999). *Espionaje industrial.* Mensajero.

Rusbridger, James (1988). *The intelligence game*. The Bodley Head. Londres.

Shorrock, Tim (2008). *Spies for hire*. Simon & Schuster. New York.

Wright, Peter (1987). *Cazador de espías*. Ediciones B. Barcelona.

Documentos

Artículos

Álvaro, Ramón (2009). *Espionaje industrial 2.0.*
http://blog.s21sec.com/2009/03/espionaje-industrial-20.html. 16 de marzo.

Arnott, Sarah (2011). *GM boss voices concern over industrial espionage.*
http://www.newsrt.co.uk/news/gm-boss-voices-concern-over-industrial-espionage-7185.html.
11 de enero.

Cases, José Luis (2010). *¿Espionaje en trading?*
http://www.traderprofesional.com/ver/576/ESPIONAJE-EN-TRADING.html. 20 de febrero.

Corrons, Luis (2008). *Troyanos para espionaje industrial.*
http://www.revista-ays.com/DocsNum26/Industria/Corrons.pdf. Octubre.

Costas, Javier (2011). *En Renault no ha habido espionaje industrial.*
http://www.motorpasion.com/renault/en-renault-no-ha-habido-espionaje-industrial. 15 de marzo.

Davidson, Joe (1996). *Crece el espionaje económico en EE.UU.* El Tiempo.
http://www.eltiempo.com/archivo/documento/MAM-346275. 29 de febrero.

Diego (2011). *¿Qué es el espionaje industrial?*
http://www.economias.com/2011-03-15/6273/%C2%BFque-es-el-espionaje-industrial/. 15 de marzo.

Fernández, A. (2011). *Renault resucita el espionaje industrial.*
http://www.expansion.com/2011/01/07/empresas/auto-industria/1294438336.html?a=c0c82938e3abbcd8638cbc5dab2302f6&t=1320184774. 9 de enero.

González, Enric (1995). *Francia denuncia el espionaje económico de la CIA y expulsa a cinco agentes norteamericanos.*
http://www.elpais.com/articulo/internacional/ESTADOS_UNIDOS/FRANCIA/CENTRAL_INTELLIGENCE_AGENCY_/CIA/Francia/denuncia/espionaje/economico/CIA/expulsa/agentes/norteamericanos/elpepiint/19950223elpepiint_15/Tes

González Ramos, Jorge (2010). *El fraude y el espionaje industrial son los delitos más frecuentes.*
http://www.elnortedecastilla.es/v/20100322/valladolid/fraude-espionaje-industrial-delitos-20100322.html. 22 de marzo.

Guillermo, Edwin E. (2003). *Espionaje corporativo.*
http://www.gestiopolis.com/canales/gerencial/articulos/69/espicorporativo.htm.

Jiménez-Barca, Antonio (2011). *Tres altos cargos de Renault despedidos por espionaje industrial.*
http://www.elpais.com/articulo/economia/altos/cargos/Renault/despedidos/espionaje/industrial/elpepueco/20110106elpepueco_3/Tes. 6 de enero.

Lafuente, Antonio y Peset, José Luis (1981). *Política científica y espionaje industrial en los viajes de Jorge Juan y Antonio de Ulloa.*
http://www.persee.fr/web/revues/home/prescript/article/casa_0076-230x_1981_num_17_1_2348

Mars, Amanda (2011). *Espías, Sociedad Anónima.*
http://www.elpais.com/articulo/sociedad/Espias/Sociedad/Anonima/elpepusoc/20110212elpepisoc_1/Tes

Martínez-Vares, Victoria (2011). *Tres años de prisión por robar y revelar información de su empresa.* http://www.expansion.com/2011/01/05/juridico/1294267832.html?a=68891f616e07fae373b44613a4e8c3a9&t=1320185520. 6 de enero.

Noonan, Sean (2011). *Chinese espionage and French trade secrets.* http://www.stratfor.com/weekly/20110119-chinese-espionage-and-french-trade-secrets. 20 de enero.

Ornelas, Andrea (2011). *Espionaje económico e inquietud en Suiza.* http://www.swissinfo.ch/spa/economia/Espionaje_economico_e_inquietud_en_Suiza_.html?cid=30198334. 11 de mayo.
http://www.elpais.com/articulo/internacional/ESTADOS_UNIDOS/FRANCIA/CENTRAL_INTELLIGENCE_AGENCY_/CIA/Francia/denuncia/espionaje/economico/CIA/expulsa/agentes/norteamericanos/elpepiint/19950223elpepiint_15/Tes. 23 de febrero.

Pearlman, Jonathan (2009). *Spying has never been so easy.* http://www.smh.com.au/national/spying-has-never-been-so-easy-20091027-hj30.html. 28 de octubre.

Pecora, Paola (2009). *La historia del supuesto espionaje industrial de Rio Tinto.* http://forosdebolsa.com/foros/foros-de-bolsa/827198/la-historia-del-supuesto-espionaje-industrial-de-rio-tinto/. 17 de julio.

Peredo, Álvaro (2008). *Breve historia del espionaje.* http://www.aprendergratis.com/breve-historia-del-espionaje-parte-1.html. 25 de junio.

Pérez, Pablo (2011). *Renault, víctima del espionaje industrial.* http://www.lavanguardia.com/lectores-corresponsales/20110107/54098992912/renault-victima-del-espionaje-industrial.html. 7 de enero.

Pinto Jonas, Lucia. *Espionaje industrial.* http://www.aie.cl/files/file/comites/ca/articulos/abril-07.pdf

Rueda, Fernando (2011). *"Se dispara el espionaje industrial en España". Tiempo.* http://www.tiempodehoy.com/espana/se-dispara-el-espionaje-industrial-en-espana. 20 de junio.

Samaniego, F. (1993). *Un manuscrito de Betancourt desvela su espionaje industrial.* http://www.elpais.com/articulo/cultura/manuscrito/Betancourt/desvela/espionaje/industrial/elpepicul/19930317elpepicul_5/Tes. 17 de marzo.

Santamarta, José (2011). *Espionaje industrial.* http://www.evwind.com/noticias.php?id_not=8850. 28 de marzo.

Sojo, Marta G. (2011). *Juego sin amigos.* http://www.bohemia.cu/2011/10/07/internacionales/espionaje-industria.html. 7 de octubre.

Steiner, Yves. (2010). *Espionnage bancaire: rumeurs, affairs et secrets.* http://www.hebdo.ch/rumeurs_affaires_et_secrets_59745_.html. 15 de septiembre.

Autor desconocido

Autor desconocido (2007). *Espionaje industrial a través de un caso particular: la fábrica de curtidos de San Diego (Sevilla).* http://potnia.wordpress.com/2007/06/05/espionaje-industrial-a-traves-de-un-caso-particular/

Autor desconocido (2009). *¿Flagrante espionaje industrial?* http://www.ecuadorciencia.org/videos.asp?id=6588

Autor desconocido (2011). *Una historia española de espías del siglo XVIII.* http://maestrodejarcia.blogspot.com/2011/07/una-historia-espanola-de-espias-del.html. 26 de julio.

Autor desconocido (a). *Espionaje industrial.*
http://www.libreopinion.com/members/jose_marmol/Espionaje_Industrial.htm

Autor desconocido (b). *Korean court has fined TagAZ for industrial espionage.*
http://eng.russ-yug.ru/article/5761/

Agencias de noticias

AFP (2011). *Espionaje económico chino a EU es "intolerable", afirma legislador clave.*
http://feeds.univision.com/feeds/article/2011-10-04/espionaje-economico-chino-a-eeuu. 10 de abril.

EFE (2001). *La UE advierte del peligro de espionaje industrial que facilita 'Echelon'.*
http://www.elmundo.es/navegante/2001/03/07/seguridad/983985863.html. 7 de marzo.

EFE (2008). *Detenido un joven en Iruñea por espionaje industrial informático.*
http://www2.deia.com/es/impresa/2008/05/08/bizkaia/gizartea/465501.php. 8 de mayo.

EFE (2010). *Berlín advierte contra un crecimiento del espionaje económico.*
http://www.forexpros.es/news/noticias-forex/berl%C3%ADn-advierte-contra-un-crecimiento-del-espionaje-econ%C3%B3mico-53959. 21 de junio.

EFE (2011). *Francia, el gran espía industrial de la UE, según una nota filtrada por Wikileaks.*
http://www.adn.es/internacional/20110104/NWS-0948-UE-WikiLeaks-Francia-industrial-filtrada.html. 4 de enero.

Reuters (2010). *Ex empleado de Boeing, condenado a 15 años por espionaje para China.*
http://www.elmundo.es/america/2010/02/09/estados_unidos/1265734809.html. 9 de febrero.

RTVE (2011). *EE.UU. acusa a China y Rusia de ciberespionaje*
http://www.rtve.es/noticias/20111104/eeuu-acusa-china-rusia-ciberespionaje/473171.shtml

RTVE/EFE (2011). *Las mayores fabricantes de armas japonesas denuncian haber sufrido ciberataques.*
http://www.rtve.es/noticias/20110920/las-mayores-fabricantes-armas-japonesas-denuncian-haber-sufrido-ciberataques/462803.shtml

Prensa

Alpoma (2005). *Espionaje industrial.*
http://www.alpoma.net/tecob/?p=164. 28 de junio.

DW (2010). *Espionaje industrial y económico, nuevas formas de ataque.*
http://www.dw-world.de/dw/article/0,,5793831,00.html. 14 de julio.

Kioskea (2010). *El espionaje económico, un problema subestimado por las empresas.*
http://es.kioskea.net/news/12335-el-espionaje-economico-un-problema-subestimado-por-las-empresas. 28 de enero.

Legal Today (2008). *Primera condena por espionaje económico en EEUU.*
http://www.legaltoday.com/actualidad/noticias/primera-condena-por-espionaje-economico-en-eeuu. 19 de junio.

RIA Novosti (2011). *Congresista estadounidense acusa a China de espionaje económico.*
http://sp.rian.ru/international/20111005/150944978.html. 5 de octubre.

Tecnopole (2011). *Vinagre gallego y un software contra el espionaje industrial, ideas innovadoras premiadas por la USC.*
http://www.tecnopole.es/?q=es/node/1595. 11 de octubre.

Voz de América (2011). *Espía chino se declara culpable.*
http://www.voanews.com/spanish/news/usa/Espia-chino-se-declara-culpable-EEUU-132101433.html. 18 de octubre.

Organizaciones

Departamento de Justicia de EEUU (2008). *Ciudadano chino fue sentenciado por espionaje económico.*
http://www.justice.gov/archive/doj-espanol/pr/2008/June/08-nsd-545-spanish.htm. 18 de junio.

FBI. *Cómo combatir el espionaje económico.*
http://www.fbi.gov/espanol/historias/como-combatir-el-espionaje-economico

Office of the National Counterintelligence Executive (2011). *Foreign spies stealing US economic secrets in cyberspace. Report to Congress on Foreign Economic Collection and Industrial Espionage, 2009-2011.* Octubre 2011.
http://www.ncix.gov/publications/reports/fecie_all/Foreign_Economic_Collection_2011.pdf

Resumen

El espionaje ha existido desde haces siglos. Sin embargo, la globalización, con su desesperada búsqueda de beneficios ha agudizado las realidades del espionaje, especialmente dentro de los muy diversos campos de la economía. En contraposición al espionaje, siempre una actividad ilegal, se sitúa la inteligencia, además de constituir todo un proceso, que parte de información obtenida de forma legal, en muchos casos con fuentes abiertas, de un modo transparente. Además, la inteligencia es en muchos casos la única arma eficaz que tienen las empresas y los estados para hacer frente a las amenazas del espionaje.

Résumé

L'Espionnage a été tout autour depuis des siècles. Toutefois, la mondialisation, avec sa quête désespérée de profits a empiré les réalités de l'espionnage, en particulier dans les nombreux domaines de l'économie. Contrairement à l'espionnage, toujours une activité illégale, est située l'intelligence économique. Une activité qui, en plus d'être un processus, travaille avec des informations obtenues légalement, dans de nombreux cas de sources ouvertes et de manière transparente. Par ailleurs, l'intelligence est souvent la seule arme efficace pour les entreprises et l'Etat pour y répondre aux menaces d'espionnage industriel et économique.

Abstract

For centuries espionage has existed, but with today's globalization and its desperate search for benefits, espionage realities have been accentuated, especially within the very diverse fields of economy. In contrast with espionage, always an illegal activity, there is intelligence, which aside from constituting a full process; it starts with information obtained illegally, yet in many cases is transparent, with exposed and open sources. Also, intelligence is usually the only effective weapon that companies and governments have to deal with and confront espionage threats.