El Espionaje

Pasado y presente

Pablo Jarabo Valdivieso – 8 de abril de 2015

Índice

Introducción al espionaje

Según la definición de la Real Academia Española, el significado de la palabra "**espionaje**" se refiere a la acción de espiar.

El espionaje es la obtención encubierta de datos o información confidencial.

A lo largo de la historia se han usado dos principales técnicas para llevarlo a cabo:

- La **infiltración**: técnica usada para introducir individuos en el bando del contrario o enemigo con el fin de conseguir información relativa a planes, actividades, proyectos…

  También se podría definir como la acción consistente en utilizar a una persona, denominada popularmente topo, cuya misión principal es lograr la plena confianza de los que tienen acceso a la información deseada.

- La **penetración**: la técnica cuyo objetivo es conseguir la colaboración consciente o inconsciente de un miembro de la organización o grupo contrario para que suministre datos e información secreta del grupo del que forma parte.

  Por regla general esta actividad se realiza de forma oculta y utiliza individuos a los que se les ha convencido para traicionar a su propio grupo por diversas causas o motivaciones: económicas, morales, personales…

En la actualidad estas técnicas han evolucionado considerablemente gracias a los dispositivos electrónicos. Aparece así el **espionaje informático**.

Historia del espionaje y evolución

El espionaje nació junto con la guerra y podríamos decir que sus orígenes se remontan a la propia historia del hombre. Sin embargo, al revés que en la guerra, existen muy pocos testimonios que lo verifiquen, debido a su naturaleza secreta.

Pese a esto, no sería raro pensar que en los primeros enfrentamientos entre humanos, como los de las primeras tribus del Neolítico hubiera un reconocimiento del lugar y de la población antes de realizar la incursión, lo que permitiría un eficaz ataque sorpresa.

Muestra de esto es la masacre de Asparn-Scheltz (Austria, 5000 a.C.) en donde se produjo un verdadero genocidio que se podría considerar “selectivo”, porque entre los sesenta y siete cuerpos encontrados en los yacimientos, solo cuatro corresponden a mujeres jóvenes. Esto significaría que se llevó a cabo un **raid** o incursión rápida para secuestrar a las mujeres, lo que pondría de manifiesto que los asaltantes tenían un previo conocimiento del poblado enemigo.

Lamentablemente, solo podemos tener conocimiento del uso del espionaje durante la Historia, ya que es la etapa en la que se puede encontrar documentación escrita de dicha actividad.

Edad Antigua

En **Mesopotamia**, podemos encontrar durante el III milenio a.C. las primeras muestras de la utilización de los servicios de inteligencia y espionaje, en el reinado de Sargón I de Acad, cuyo imperio comprendía desde Siria hasta el sur de Irán; este era el conocido Imperio Acadio. Para su creación, Sargón I sabía que necesitaba información confidencial fuera de sus territorios. Por ello utilizó espías a modo de exploradores para ser informado de las características de las tierras a dominar. Como prueba de ello se encontró una tablilla escrita en acadio con caracteres cuneiformes, fechada hacia el 2210 a. C., en la que se aprecia cómo Argón I se servía de mercaderes para que le proporcionasen información sobre las poblaciones que quería conquistar y así tener ventaja para llevar a cabo una incursión victoriosa.

Como el espionaje está íntimamente ligado a la guerra, en **Grecia** no podía ser de otra manera. Por ejemplo en la obra de Homero, la Ilíada, ya se habla del espionaje utilizado en la guerra de Troya.

La historia de **Roma** es, en gran parte, la historia de sus hazañas militares. Los romanos alardeaban de lograr sus victorias por su potente ejército, sin usar astucias ni engaños. Pero esto no era así. Ningún imperio de la Antigüedad se formó prescindiendo del espionaje, y Roma no sería diferente. Esto queda demostrado en obras de historiadores como Tito Livio y Sexto Julio Frontino (300 a.C.).

Edad Media

Tras la caída del Imperio romano, en **Occidente** el espionaje e inteligencia se llevaba a cabo únicamente durante los periodos de guerra. Siendo actividades muy similares de las del mundo antiguo; así, los espías seguían notificando sobre la topografía, las fortalezas, las armas, tanto ofensivas como defensivas, o las unidades enemigas disponibles, usando para ello los mismos medios que se habían utilizado en la Antigüedad.

Este espionaje puramente militar es el que se practicó en contiendas como la de Ad Decimum (533 d.C.) o la de Hastings (1066 d.C.).

En **Extremo Oriente** los sistemas de inteligencia no sufrieron tampoco muchos cambios, puesto que se siguió llevando el espionaje militar a través de los esfuerzos de exploradores y guerreros espías, tal y como hizo en Mongolia Gengis Kan, el Gran Kan.

Por el contrario en el **Japón medieval** durante la etapa Sengoku (1467-1568), surgieron dos nuevos tipos de guerreros: los samuráis, que representaban el valor ancestral del honor en la guerra; y los ninjas, también llamados shinobi, considerados guerreros espías, especializados en la ocultación, el sabotaje y la guerra encubierta.

Efectivamente, el ninja se utilizaba para obtener información y espiar al enemigo previamente a la guerra, para lo que se disfrazaban e infiltraban en terreno enemigo. Por otra parte, los shinobi también saboteaban las fuerzas enemigas mediante incendios o mediante el asesinato selectivo, probablemente la faceta por la que más se les conocía.

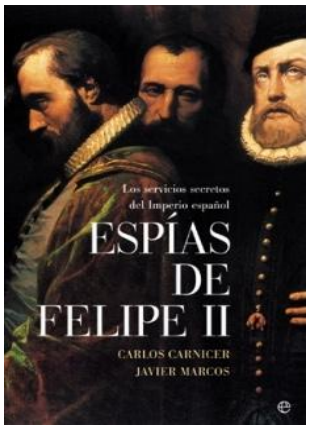
Edad Moderna

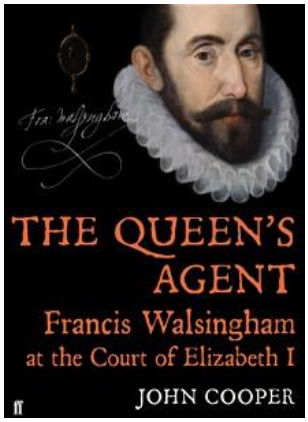
Durante los siglos XVI y XVII surgen nuevos Estados cuyo gobierno está muy burocratizado, por lo que la obtención de información por parte de los monarcas resulta una pieza clave para la supervivencia de los imperios. 'Seguridad' e 'información' son los objetivos más perseguidos en esta época.

El **imperio británico** fue el primero en crear una red de inteligencia institucionalizada. Esto fue llevado a cabo por el secretario de Estado de Isabel I, sir Francis Walsingham, que desarrolló tal cometido de 1573 a 1590.

Este maquiavélico personaje difundió su red de espías por Francia, Alemania, los Países Bajos, Italia y España.

El **imperio español** estableció, a manos de Felipe II, una gran red de espionaje cuyos centros de operaciones eran las embajadas. Aunque también participaron en esta labor el resto de altos funcionarios de la Corona, como virreyes, militares y gobernadores generales, recabando la información obtenido por lo más diversos medios.





Por su parte, los monarcas españoles de la dinastía de los Habsburgo no limitaron su actividad de espionaje al extranjero, sino que este mismo llegó a tener gran importancia dentro de las intrigas de las distintas cortes.

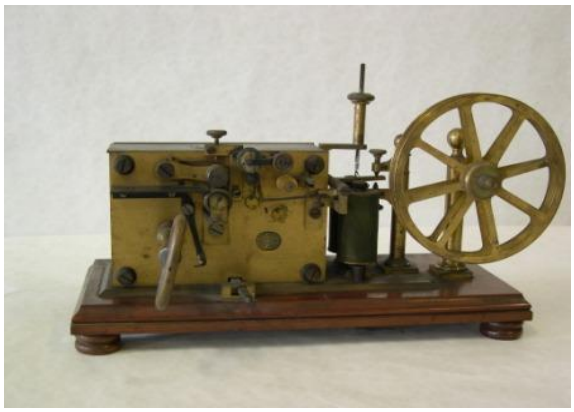
Al mismo tiempo en que se institucionalizó el espionaje en estas dos grandes potencias, otros dos grandes Estados, **Francia** y **Rusia**, pasarán a formar sus propias redes de espionaje tanto interno como externo, al participar de manera directa en el ámbito de las operaciones secretas de la política mundial.

Edad Contemporánea

En lo que respecta al espionaje, se produce un cambio de grandes dimensiones. Claras muestras de ello son las grandes guerras que tuvieron lugar en este período.

La antesala de la 1º Guerra Mundial y el ambiente bélico que se respira en Europa a finales del siglo XIX y principios del siglo XX hará que se extienda la utilización de las redes de inteligencia de manera global por todo el mundo. De esta manera se pasa de unos servicios de espionaje militar poco profesionales y con escasa formación, a unas organizaciones cada vez más especializadas y preparadas.

Se pondrán al servicio de los espías los avances tecnológicos, tanto los ya existentes –fotografía, telégrafo o teléfono– como los de más reciente aparición, el telégrafo, que aunque supuso una mejora para la comunicación militar, resultó ser un mayor factor de riesgo ya que el mensaje transmitido podía ser más fácilmente interceptado por el enemigo. En cualquier caso se redujo la aún más peligrosa utilización de espías mensajeros.



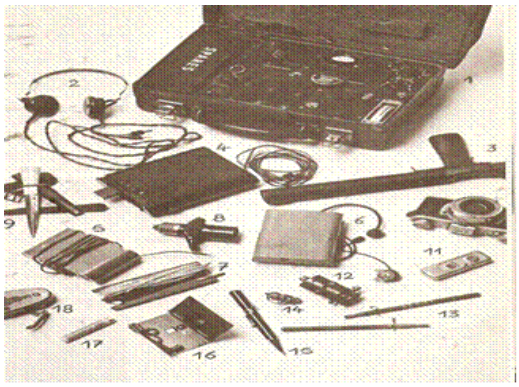
En toda Europa surgirá, incluso antes de la guerra, una gran obsesión por el espionaje; toda la población se sentirá observada, vigilada; cualquiera podría ser sospechoso de ser considerado un espía del enemigo. Aquí será trascendental la labor de los civiles, por lo que es en esta época cuando podemos hablar del nacimiento y desarrollo de los servicios de inteligencia que determinarán la historia del espionaje en el futuro.

El paulatino alejamiento de las relaciones políticas entre Gran Bretaña y el imperio alemán y la disposición beligerante de este último llevaron al imperio británico a fundar en, octubre de 1909, de la mano de William Melville, superintendente de Scotland Yard, el Secret Service Bureau, es decir la Oficina del Servicio Secreto, donde se aglutinan los diecinueve departamentos de la inteligencia militar, conocidos con las siglas que van desde el MI-1 al MI-19. Los más famosos son el **MI-5**, dedicado a la seguridad interna, es decir, al contraespionaje, y el **MI-6**, encargado de la seguridad externa, esto es, el espionaje en el extranjero.

La participación de Estados Unidos en esta guerra, aparte de ser trascendental en el desarrollo de la misma, indudablemente resultó ser un cambio fundamental para el espionaje de dicho país. De esta forma, el **FBI**, creado anteriormente por Charles Joseph Bonaparte en 1908 bajo el nombre de Oficina de Investigación, amplió sus funciones y actuaciones durante este periodo bélico. En 1916, el Congreso de los Estados Unidos permitió que el Departamento de Estado pudiese acudir al FBI en sus investigaciones.

Durante esta guerra cabe destacar la participación de las mujeres en el ámbito del espionaje, como la francesa Marie Birckel o la conocida Mata Hari.

La relevancia del espionaje durante la **2º Guerra Mundial** es mucho mayor que la que este había tenido anteriormente entre los diferentes países. Las técnicas serán cada vez más complejas. La última tecnología se pondrá a disposición del espionaje sin tener en cuenta el gasto en inversión. Así, durante el período de entreguerras cada potencia desarrollará sus propias redes de inteligencia y se distinguirán tres formas de comprender y realizar el espionaje: en primer lugar, el que se llevará a cabo por las democracias, en segundo lugar, el que realizarán los países fascistas, y, en último lugar, el de los países de ideología comunista.



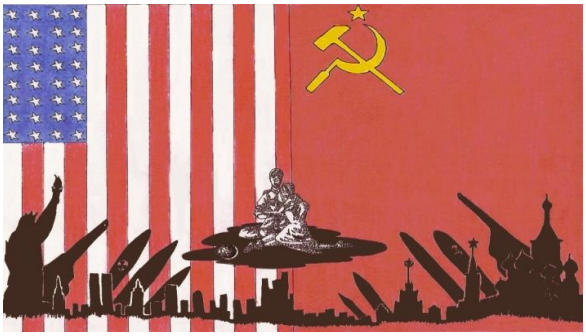
Es en esta guerra donde tuvieron importancia las llamadas operaciones de engaño, entre la que se encuentra la **"Operación Fortitude"**, en la que el espía español Juan Pujol García, al servicio de la inteligencia británica, logró engañar al ejército alemán facilitando falsa información sobre el desembarco aliado en Normandía, afirmando que este se produciría las costas de Calais.

Durante la 2º Guerra Mundial se produjeron grandes avances en el ámbito de la seguridad en las comunicaciones militares, de forma que se crearon novedosos sistemas de encriptación.

Surgieron a su vez los espías atómicos, encargados de recabar toda la información posible acerca de lo avances técnicos que se produjesen en relación con la tecnología atómica.

En la Alemania nazi, el cuerpo de policía de las SS, dirigido por el general Himmler, estructuró una red de espionaje cuyo objetivo eran los detractores del régimen y los que consideraban "impuros". Gran parte de la población colaboró en esta misión, lo que dio lugar a un ambiente de delación y sospecha.

Por último, la **Guerra Fría** tuvo como principales protagonistas del espionaje mundial, los dos países que representaban los bloques enfrentados: el capitalista encabezado por los Estados Unidos; y el comunista, por la URSS. Estos dos países infiltraron agentes para obtener información secreta relativa a la estrategia y la tecnología, hasta convertirse en una obsesión por creer tener al enemigo dentro del país. Ahora el contraespionaje es tan importante como el espionaje.

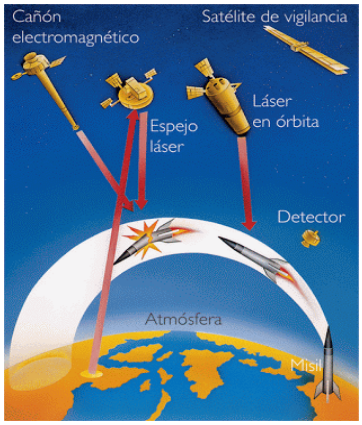


En este ambiente aparecen nuevas redes de inteligencia como son la **CIA** (Agencia Central Central de Inteligencia) en EEUU y la **KGB** (Comité para la seguridad del Estado)en la URSS. En este conflicto entre los dos bandos, los espías son eliminados al ser descubiertos o al ser delatados por traidores de su propio entorno.

El espionaje atómico tenía la misma importancia que en la 2º Guerra Mundial.

A lo largo de la Guerra Fría, se inicia la carrera espacial, el espacio se convierte en una de las principales metas del espionaje. A partir de que se lanzaran al espacio los primeros satélites espía, se logró el pleno reconocimiento de los presuntos enemigos.

Ronald Reagan, presidente de los EEUU entre 1981 y 1989, estableció una nueva forma de espionaje a partir de un proyecto que fue muy criticado: "La Guerra de las Galaxias"; denominación popular que recibió la SDI (Iniciativa de Defensa Estratégica) que consistía en defender Estados Unidos con una especie de "sombrilla espacial" que rechazara los posibles misiles soviéticos y que además permitiría espiar a la Unión Soviética. El proyecto se declaró inviable porque se entendió que la URSS lo consideraría una provocación, lo que podría traer graves consecuencias.

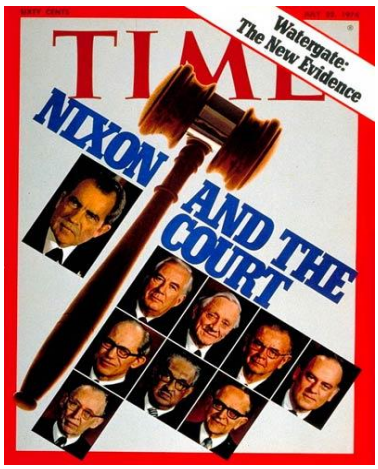


Durante la década de los setenta, los métodos usados en el ámbito militar, como vigilancia exhaustiva, pinchar teléfonos, escuchas ilegales… pasan al ámbito político, lo que se conoce como **espionaje político.** Así ocurrió en el caso más famoso a nivel mundial de toda la historia: **el caso Watergate.**


Text of Nixon's speech on Watergate

En Estados Unidos, concretamente el 17 de junio de 1973, la Oficina del comité Nacional del Partido Demócrata estadounidense del complejo de oficinas Watergate en Washington D. C., fue irrumpida por un grupo de cinco personas que serían miembros de la CIA.

Este equipo quiso mantener en secreto este allanamiento incluso seis días después del acontecimiento. Más tarde fueron descubiertos y la investigación señaló directamente a Nixon, cuando se descubrió una serie de conversaciones grabadas de forma ilegal que habían tenido lugar en los despachos de la Casa Blanca. Esas cintas a las que se les conocía como “The Smoking Gun”, lo que es, “La Pistola Humeante”, tuvieron que ser devueltas tal y como resolvió el Tribunal Supremo de Estados Unidos en noviembre de 1973.



Todas las investigaciones que se realizaron (las del FBI, las del Comité del Watergate en el Senado e incluso las de la prensa) pusieron de manifiesto que el caso Watergate era sólo la punta de un iceberg que incluía fraudes en su campaña electoral, escuchas ilegales a gran escala, auditorías de impuestos falsas y un fondo de capital secreto para sobornar a todos los implicados en estos asuntos ilegales. Ante este escándalo, el Senado de Estados Unidos inició, el 27 de julio de 1974, el segundo proceso contra un presidente en la historia de EEUU. El 8 de agosto de 1974 Nixon presentó su dimisión.

Actualmente, las innovaciones en el ámbito del espionaje se ponen al servicio de los Estados, con objetivos muy diversos como el terrorismo.

Tras el atentado de la Torres Gemelas del 11-S se inició un tipo de espionaje que incluiría operaciones encubiertas, como la que logró poner fin a la vida de Osama Bin Laden.

Esta operación conocida como **"Operación Gerónimo"**, surgió a partir de una alerta proveniente de agentes secretos paquistaníes al servicio de la CIA que situaba a uno de los mensajeros de Osama Bin Laden en la ciudad paquistaní de Peshawar. En ese momento, la CIA inicia una estrecha vigilancia hasta encontrar la mansión fortificada donde habitaba Bin Laden en Abbottabad. El seguimiento de la residencia de Bin Laden se realizó durante meses con fotografías vía satélite para tener conocimiento de todos los movimientos que se producían en la casa: habitantes, servicios de seguridad, hábitos...

Tal fue el secretismo de la operación que no tuvo conocimiento de ella ni siquiera el gobierno paquistaní.

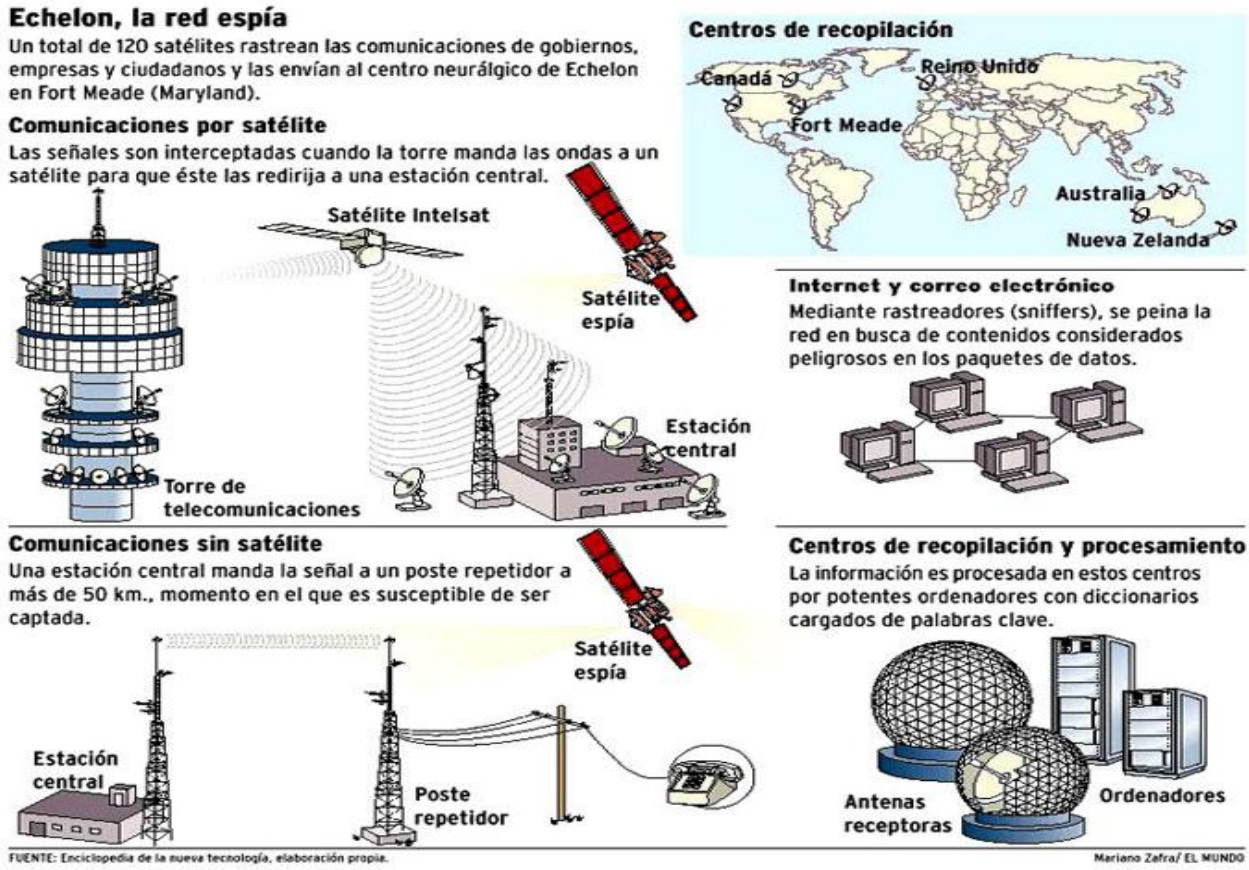
Otro objetivo es la vigilancia realizada de manera ilegal sobre otros Estados. Claro ejemplo de ello es el **caso Snowden** en el que Estados Unidos fue acusado de este tipo de espionaje tras la filtración de información del ex-técnico de la NSA Edward Snowden.

Otro conocido caso es el de la red de espionaje creada por Estados Unidos llamada **ECHELON**, también conocida como el "Gran Hermano Global".

ECHELON intercepta de manera habitual todas las comunicaciones de correo electrónico, fax y teléfono, mediante una serie de satélites espías colocados estratégicamente en la estratosfera. Una vez recabada la información, esta es enviada a una estación central.

Dicha estación cuenta con unos potentes ordenadores que están programados con unos diccionarios cargados de “palabras clave”. Cuando una de estas palabras es detectada, el dispositivo de salida es monitorizado y comienza a ser investigado.

Actualmente se conoce la participación en este proyecto de los 5 países de habla inglesa: Estados Unidos, Gran Bretaña, Canadá, Australia y Nueva Zelanda.



Hoy en día el espionaje también se puede poner al servicio de empresas privadas para llevar a cabo el poco conocido **espionaje corporativo**.

Espionaje en la actualidad

Espionaje corporativo

No se debe entender que la palabra enemigo es exclusiva de la guerra militar o política pues en los negocios empresariales y en las competencias de ventas corporativas y hasta en los deportes el espionaje es una herramienta muy usada para conseguir o robar conocimiento.

El espionaje corporativo tiene distintos nombres: espionaje industrial, espionaje empresarial, inteligencia competitiva, entre otros, pero todos se refieren a lo mismo, obtener e interpretar información de valor estratégico de la industria o de los competidores.

¿Qué es?

Es la obtención ilícita de información relativa a la investigación, desarrollo y fabricación de prototipos, mediante las cuales las empresas pretenden adelantarse a sus competidores en la puesta en el mercado de un producto novedoso.

¿Cómo se lleva a cabo?

Hay dos formas principales:

- Infiltración de personal.
- Ciberataques.

El espionaje corporativo, también conocido como espionaje industrial, ha evolucionando a través del tiempo para convertirse en un flagelo que en algunos casos utiliza las técnicas más avanzadas de espionaje conocidas. Entre las que figura la instalación de cámaras y micrófonos de forma imperceptible para el ojo inexperto en áreas sensitivas de una empresa, como pueden ser oficinas de altos mandos o salas de reuniones. Sin embargo, algunas técnicas siguen siendo simples, como rastrear información en la basura, para citar un ejemplo, uno de los métodos más sencillos de espionaje corporativo.

Es importante reconocer que gran porcentaje del valor de una compañía se basa en la información que esta posee. El robo de esta información no solo representa pérdidas económicas potenciales para las empresas, sino que también tiene repercusiones significativas en cuanto a su imagen ante sus clientes y el público en general, debido a que estos pueden percibir que su información privada podría ser vulnerada.

¿Por qué se produce?

La causa principal es el deseo de la empresa que lo lleva a cabo o el país de obtener esa información para posteriormente poder utilizarla para su propio beneficio económico.

También puede ocurrir que dicha institución lo único que quiera sea extraer la información para simplemente molestar el desarrollo del que es ataca sin después utilizarla.

Consecuencias

Legisladores de Estados Unidos han dicho que las firmas locales sufrieron pérdidas estimadas en más de 300.000 millones de dólares en concepto de robos de secretos en el 2012, gran parte de ellas vinculadas a ciberespionaje chino.

Además se producen enfrentamientos entre países involucrados, lo que no es favorable para el bienestar mundial.

Relación con China

Siempre ha sido conocida la capacidad china para el plagio de productos. Esta se puede extrapolar a las grandes empresas.

Actualmente gran nº de potencias internacionales acusan directamente a china por esta actuación considerada crimen, lo que ha causado muchas tensiones.

Ejemplos

- **Infiltración: Caso Ford**

  Objetivo: Ford Motor Company

  Espía: Empleado chino

  Duración de la operación: 2007

  Lugar: Chicago

  El ingeniero chino Xiang Dong Yu, de 47 años de edad, que trabajó durante una década en Ford Motor Company, fue detenido en octubre de 2009 por autoridades de los Estados Unidos bajo el cargo de espionaje industrial contra aquella empresa. Se le acusa de haber robado secretos comerciales, acceder a información clasificada y a archivos relacionados con montaje de motores, transmisiones, sistemas eléctricos y elementos de carrocería. Con esa información intentó obtener empleo en **Shangai Automotive** Corporation, que lo contrató en la matriz, **Beijing Automotive Corporation**. Fue sentenciado a 25 años de prisión o a pagar una multa de 50 mil dólares.

  Fuente: El Universal, México, 20 de octubre de 2009.

- **Ciberataque: Operación Aurora**

Comienzo y desarrollo

Un día diciembre del año 2009, varios empleados de Google asentados en China y otros países, recibieron correos electrónicos "extraños": los invitaba a acceder a una página de internet, a través de un link. Lo que siguió después ya se ha etiquetado como "Uno de los ciberataques más sofisticados hasta ahora registrados".

McAfee le ha bautizado con el nombre de "Operación Aurora", en el que además de Google, otras 34 empresas multinacionales (hasta ahora es el número detectado) sufrieron robo de información a través de un "**malware**" (software malicioso).

Según explica Edgar Zamudio, gerente de ingeniero de ventas de McAfee, fue algo similar al cuento del caballo de Troya: el link al que muchos empleados dieron clic provocó que dentro de sus computadoras se instalara un "**troyano**", es decir, un software malicioso que se instaló en la máquina del usuario casi en secreto, y que sin avisar, instaló un programa que permitió el acceso remoto de un usuario no autorizado (**"hacker"**) para copiar la información contenida en su computadora.

Estado chino

"El servidor de donde salió el troyano y a donde se comunicaba el software malicioso se localizó en China. Google acusa al gobierno de este país por no tener las regulaciones suficientes para proteger a las empresas que están en dicho país de un ataque de esta magnitud", dice Zamudio.

Sin embargo, la naturaleza del ataque no permite detectar con claridad de qué país o quién exactamente es el culpable: el hacker pudo haber creado el ataque desde un país determinado, con otros hackers ubicados en otros países, y simplemente "hospedó" su troyano en China. Tampoco se sabe a ciencia cierta a qué país se dirige toda la información que se pudieron robar.

Microsoft

Según se explica Zamudio, el link malicioso se abrió directamente en el Internet Explorer (de esta marca) aprovechando alguna de sus vulnerabilidades.

Google

Hasta enero de 2010, Google había sido la única víctima que había hecho público el problema, pidiendo incluso explicaciones oficiales al gobierno de China y previendo la posibilidad de salir de dicho país. Incluso, la secretaria de Estado de Estados Unidos alega que se trata de "una ola de muy sofisticados ciberataques".

Consecuencias

- Enfado de EEUU.
- Inseguridad de la población del país, ya que a partir de ese momento los ciudadanos saben que pueden estar siendo vigilados.
- Medidas de Microsoft.

  Aunque la vulnerabilidad afecta a Internet Explorer 6, 7 y 8, es recomendable actualizar el navegador a esta última versión, ya que por defecto, Internet Explorer 8 tiene activada la funcionalidad **DEP**, que previene la ejecución de datos, necesaria para la infección del sistema.

  En el día de la fecha Microsoft ha lanzando un parche oficial **MS10-002** para esta vulnerabilidad que reviste el carácter de crítico. Se debe actualizar con el mismo todas las versiones de Internet Explorer y los sistemas operativos desde Windows 2000 hasta el reciente Windows 7.

Conclusiones

Este tipo de ataques son muy fáciles de explotar cuando no se dan todas las condiciones necesarias de seguridad, ya que con el solo hecho de acceder a Internet a través de un navegador o abrir un correo electrónico y, si encuentra la vulnerabilidad, el atacante podrá acceder a información confidencial de la organización.

Teniendo en cuenta que fueron muchas y grandes las compañías afectadas a través de la Operación Aurora, lo primero que se cuestiona, es el hecho de que todavía se siga utilizando un navegar tan antiguo: aproximadamente el **20%** aún utiliza Internet Explorer 6.0.

Posibles soluciones

- "Los empleados deben ser la principal línea de defensa de la compañía" sugiere el especialista en seguridad de información Capt Raghu Rahman, CEO de Mahindra Special Sercvices Group. "Un empleado atento y capacitado es más eficiente que cualquier sofisticado sistema de seguridad y además presentan la ventaja de estar disponibles a un menor costo", agrega.
- Mayor conocimiento de los trabajadores.
- Restricción de competencias.
- Desarrollo de sistemas de seguridad.

Claves del caso Snowden

El 6 de junio de 2013 el periódico británico “The Guardian” publicó que la Agencia de Seguridad Nacional (**NSA**) tenía acceso a registros telefónicos y de internet de millones de usuarios de la operadora de telefonía Verizon en EEUU. Para justificarse la Casa Blanca defiende la necesidad de registrar las llamadas telefónicas de sus conciudadanos.

Al día siguiente, los diarios “The Guardian” y “The Washington Post” revelan información clasificada sobre dos programas de espionaje masivo que ejecuta el gobierno estadounidense: el primero (**PRISM**) le permite a la NSA y al FBI acceder a los servidores de Microsoft, Google, Apple, PalTalk, AOL, YouTube, Skype, Yahoo y Facebook de manera ilimitada y obtener así información personal de sus usuarios, monitorear correos electrónicos y el tráfico de internet; el segundo, es una herramienta que les permite rastrear y registrar datos (**Boundless Informant**) de llamadas en EEUU, con el apoyo de redes satelitales incluidas las que operan el ámbito comercial.

Estos son los principales aspectos que hay que considerar sobre este caso:

1. El 9 de junio Snowden revela que él es la fuente de ambos diarios, para ese momento se encontraba escondido en Hong Kong, desde donde había llegado procedente de Hawai.

2. El 13 de junio se inicia EEUU la persecución a Snowden penalmente por espionaje, hurto y utilización ilegal de bienes gubernamentales, justificando los programas de vigilancia con la lucha contra el terrorismo. Temen que el ex agente filtre datos a China. Snowden, haciéndole un guiño a los chinos, denuncia el espionaje estadounidense en contra de su gobierno.

3. Snowden solicita asilo a más de 20 países, más de la mitad rechazó formalmente recibirlo. Algunos de ellos se escudaron en la excusa técnica de no poder estudiar el caso por no encontrarse el solicitante dentro de su territorio.

4. Después de haber anulado una primera solicitud de asilo a Rusia, debido a la condición que Putin le impuso de no realizar actividades hostiles en contra de sus “socios estadounidenses”, al sortear las dificultades de su ruta de vuelo hacia América Latina, Snowden acepta las condiciones y solicita formalmente el asilo a Rusia.

5. En estos momentos las presiones que ha ejercido EEUU a nivel global por este caso, junto a las informaciones sobre su espionaje a múltiples gobiernos, comienzan a incomodar a diversos países. Ya diversas organizaciones, entre las que destacan las rusas y las alemanas, así como diversas personalidades, han manifestado abierta y materialmente su apoyo al ex agente de la CIA.

El espionaje en España

A lo largo de la **dictadura franquista** aparecieron las modernas de redes de inteligencia de nuestro país, al hilo del surgimiento de los movimientos sociales y estudiantiles de oposición al régimen.

Para evitar la subversión en la universidad española, el Estado Mayor decidió crear la Organización Contrasubversiva Nacional (**OCN**).

En 1969, la OCN pasa a ser el Servicio Central de Documentación (**SECED**), que depende del Ministerio de Interior, pero que fue dirigido por militares con el objetivo de vigilar los movimiento de los ciudadanos residentes en territorio español.

A partir de 1971 se amplían las competencias de este organismo. Se crean así dos departamentos junto con el dedicado a las revueltas estudiantiles: uno controlaba el mundo laboral y otro que se encargaba del ámbito intelectual, tratando de censurar toda ideología contraria o que pusiera en peligro a la dictadura.

El paso de la dictadura a la **democracia** supuso la creación de nuevos servicios de inteligencia, formándose en 1977 Centro Superior de Información de la Defensa (**CESID**) por el entonces vicepresidente del Gobierno y ministro de Defensa, el general Manuel Gutiérrez Mellado.

Su objetivo principal fue el control militar de supuestos golpes de Estado por parte de altos cargos muy descontentos con la democracia. Es por esto que después del fracasado golpe de estado del 23 de febrero de 1981, los fines del CESID se amplían.

Ahora ya no solo se encargará de la inteligencia militar sino también de cualquier posible actividad terrorista. A esto hay que añadir que entre sus competencias se encontraban también funciones de contraespionaje, es decir, controlar y mitigar las actividades de inteligencia de países extranjeros que pudieran poner en peligro la soberanía o los intereses españoles.

El atentado en el *World Trade Center* de Nueva York el 11 de septiembre de 2001, supuso el inicio de una nueva etapa en los servicios secretos mundiales, y fue el detonante para que en mayo del 2002 el CESID se convirtiera en el actual Centro Nacional de Inteligencia (**CNI**).

Los objetivos del CNI se pueden clasificar en tres grupos:

- **Espionaje exterior**, que se encarga de obtener información acerca de los intereses de España en el extranjero.
- **Contraespionaje**, que evita posibles ataques de grupos o países extranjeros.
- **Contraterrorismo**, que pretende hacer frente a actividades terroristas de cualquier índole.

En cuanto a las funciones del CNI están establecidas por la **Ley 11/2002 del 6 de mayo**, que a continuación se cita textualmente:

1. “Obtener, evaluar e interpretar información y difundir la inteligencia necesaria para proteger y promover los intereses políticos, económicos, industriales, comerciales y estratégicos de España, pudiendo actuar dentro o fuera del territorio nacional.”
2. “Prevenir, detectar y posibilitar la neutralización de aquellas actividades de servicios extranjeros, grupos o personas que pongan en riesgo, amenacen o atenten contra el ordenamiento constitucional, los derechos y libertades de los ciudadanos españoles, la soberanía, integridad y seguridad del Estado, la estabilidad de sus instituciones, los intereses económicos nacionales y el bienestar de la población.”
3. “Promover las relaciones de cooperación y colaboración con servicios de inteligencia de otros países o de Organismos internacionales, para el mejor cumplimiento de sus objetivos.”
4. “Obtener, evaluar e interpretar el tráfico de señales de carácter estratégico, para el cumplimiento de los objetivos de inteligencia señalados al Centro.”

5. “Coordinar la acción de los diferentes organismos de la Administración que utilicen medios o procedimientos de cifra, garantizar la seguridad de las tecnologías de la información en ese ámbito, informar sobre la adquisición coordinada de material criptológico y formar al personal, propio o de otros servicios de la Administración, especialista en este campo para asegurar el adecuado cumplimiento de las misiones del Centro.”
6. “Velar por el cumplimiento de la normativa relativa a la protección de la información clasificada.”
7. “Garantizar la seguridad y protección de sus propias instalaciones, información y medios materiales y personales.”

La transformación y el salto que se ha producido en los servicios secretos españoles se deben a las nuevas metas de la inteligencia mundial, ya que las principales potencias saben a ciencia cierta que los peligros a los que se enfrenta actualmente, encabezados por el yihadismo, requieren una mayor cooperación entre los servicios de espionaje de los diferentes países.

Conclusión

Podemos afirmar que el espionaje es intrínseco al ser humano, la frase, "No he podido evitar oírlo todo, tenía la oreja pegada a la puerta..." de la película "El solterón y la menor" de Irving Reis es un claro ejemplo de nuestra tendencia a conocer los secretos de los demás.

La información es poder y la posesión de esta información de forma clandestina nos otorga aún más poder, ya que nos permite adelantarnos a los movimientos del resto del mundo.

El espionaje desde sus inicios se manifiesta en el ámbito militar, es propio de los ejércitos. Ser capaz de adelantarse al rival supondría en ocasiones la victoria. A lo largo de la historia grandes ejércitos han sido derrotados por otros menos poderosos, pero que contaban con un "arma secreta", la información obtenida a través del espionaje.

El avance de la sociedad ha permitido que el espionaje se extienda también a otros ámbitos, como el político, donde regímenes autoritarios bajo la premisa de "proteger" a su pueblo, han utilizado el espionaje como aparato de control a cualquier tipo de oposición, política o social. Así ocurrió en la dictadura española o en la Alemania nazi.

Actualmente se trata de un arma muy eficaz para hacer frente a los ataques de organizaciones no gubernamentales peligrosas para los intereses del Estado, como son las organizaciones terroristas.

Por otra parte, desde hace ya varios años, los avances tecnológicos del espionaje militar han salido al mundo comercial de manera que no solo se usa como herramienta del Estado para "proteger" la sociedad, sino también con fines comerciales.

La aparición de Internet y la masificación de su uso facilita enormemente cualquier tipo de espionaje, ya que en la era digital todo queda registrado e inevitablemente dejamos huellas de casi cualquier actividad que realicemos a lo largo del día. Aunque se intente legislar se continúa llevando a cabo de manera ilícita.

Esto nos lleva a plantearnos el problema ético-moral de las actividades del espionaje.

No puede cuestionarse que en el espionaje se práctica la máxima maquiavela de "El fin justifica los medios". Cabe entonces preguntarse si sería ético permitir la utilización de medios ilegales para la consecución de estas actividades.

Es cierto que necesitamos que el Estado posea herramientas de inteligencia para protegernos, pero tenemos que ser prudentes y tratar de evitar una sobreprotección con limitación de derechos y libertades como queda perfectamente plasmado en la obra "1984" de George Orwell.

No debemos olvidar que el espionaje siempre es beneficioso si se utiliza en servicio de la colectividad y no en beneficio propio.

Bibliografía

A la hora de realizar la investigación he utilizado fuentes muy diversas que me han ayudado a completar satisfactoriamente la misma.

- Por una parte he indagado en títulos de autores como:

HERRERA HERMOSILLA, Juan Carlos. Breve historia del espionaje. Madrid, 2012.

BAUER, Eddy. Espías: Historia de la guerra secreta. San Sebastián: Buru Lan, 1971.

CARNICER, Carlos Javier. Sebastián de Arbizu, espía de Felipe II: la diplomacia secreta española y la intervención en Francia. Madrid: Nerea, 1998.

DÍAZ FERNÁNDEZ, Antonio Manuel. Los Servicios de Inteligencia españoles. Desde la Guerra Civil hasta el 11-M. Historia de una transición. Madrid: Alianza Editorial, 2005.

DVORNIK, Francis. Origins of Intelligence Services: the ancient near East, Persia, Greece, Rome, Bizantium, the Arab Muslim Empires, The Mongol Empire, China, Muscovy. New Brunswick (NJ): Rutgers University Press, 1974.

FIGES, Orlando. Mata Hari: Espía, víctima, mito. Barcelona: Edhasa, 2011.

FRATTINI, Eric. CIA, Historia de la Compañía. Madrid: EDAF, 2005.

—, KGB, Historia del Centro. Madrid: EDAF, 2005.

—, MI6, Historia de la Firma. Madrid: EDAF, 2007

HERSCH, Seymour M. Obediencia debida. Del 11 de septiembre a las torturas de Abu Ghraib. Madrid: Punto de Lectura, 2005.

JEFFREYS-JONES, Rhodri. Historia de los servicios secretos norteamericanos. Barcelona: Paidós, 2004.

JUÁREZ CAMACHO, Juan. Madrid-Londres-Berlín: espías de Franco al servicio de Hitler. Madrid: Temas de Hoy, 2005.

PASTOR PETIT, Domingo. Diccionario enciclopédico del espionaje. Madrid: Editorial Complutense, 1996.

—, Historia del espionaje. Barcelona: Aymá, 1967.

RUEDA, Fernando. Las alcantarillas del poder: las 100 operaciones de los servicios secretos españoles que marcan sus últimos 35 años de historia. Madrid: La esfera de los libros, 2011.

SÁNCHEZ-PACHECO, Felicidad. Historia del espionaje. Espías, tácticas y técnicas. Madrid: Libsa, 2009.

SHELDON, Rose Mary. Renseignement et espionnage dans la Rome Antique. París: Les Belles Lettres, 2009.

SINGH, Simon. Los códigos secretos. El arte y la ciencia de la criptografía, desde el antiguo Egipto a la era internet. Barcelona: Círculo de Lectores, 2000.

TREMPS, Enrique. El telegrama Zimmermann: el documento secreto que cambió el curso de la Primera Guerra Mundial. Barcelona: RBA, 2010.

VV. AA. Echelon. La red de espionaje planetario. Santa Cruz de Tenerife: Melusina, 2007.

ZORZO FERRER, Francisco J. «Historia de los servicios de inteligencia": el período predemocrático». En: Arbor, 2005; vol. CLXXX, n.º 709: 75-98."

- Por otra parte me he valido de blogs y páginas de la red especializadas como:

http://www.iit.upcomillas.es/pfc/resumenes/449fc6082044b.pdf

http://es.wikipedia.org/wiki/Espionaje

http://www.contextodetamaulipas.info/contenido/?p=79473

http://www.forodeseguridad.com/artic/segcorp/7208.htm

http://www.cnnexpansion.com/manufactura/2010/04/06/los-casos-conocidos

http://eleconomista.com.mx/tecnociencia/2010/01/20/operacion-aurora-ciberataque-mas-sofisticado-historia

http://www.welivesecurity.com/la-es/2010/01/21/que-es-operacion-aurora/#

http://quees.la/espionaje/

http://viva.org.co/cajavirtual/svc0362/pdfs/Articulo504_362.pdf

http://www.20minutos.es/noticia/1850380/0/caso-snowden/cronologia/espionaje-ee-uu/

http://www.bbc.co.uk/mundo/noticias/2013/11/131101_finde_historia_del_espionaje_amv

http://noticias.juridicas.com/base_datos/Admin/l11-2002.html#a4

http://www.24siete.info/nota-169343-mundo

http://www.mercaba.org/TESORO/san_cipriano.htm

http://www.fvallin.es/ckfinder/userfiles/files/Fox%202%20Bella%20Poenica.pdf

http://www.elmundo.es/america/2013/06/23/estados_unidos/1371994686.html