Arreola, E. (2015) Ciberespionaje. La puerta al mundo virtual de los Estados e individuos. México. Siglo XXI

1. ¿INTELIGENCIA O ESPIONAJE?, ÉSA ES LA CUESTIÓN

Es de importancia para quien desee alcanzar con certeza en su investigación, el saber dudar a tiempo.

ARISTÓTELES

Durante la reunión del G-20 de 2013, el presidente Barack Obama justificó las acciones realizadas por su gobierno en contra de países como México y Brasil, a fin de obtener información de sus respectivos presidentes y de algunas empresas públicas, y las catalogó como actos de inteligencia. La justificación otorgada por el presidente Obama fue la respuesta oficial a un supuesto espionaje en contra de algunos funcionarios mexicanos y brasileños. Asimismo, su gobierno tomó ventaja del momento e hizo una anotación al margen, declarando que la búsqueda de "inteligencia" y no "espionaje" es algo que todos los estados llevan a cabo de manera cotidiana. Es evidente que existen dos caras de la misma moneda, pero con diferente connotación. Por un lado, la búsqueda de "inteligencia" que hasta cierto punto representa una acción regulada y aceptada por los diversos actores de la sociedad internacional. Por el otro, el "espionaje", que aunque es igualmente la búsqueda de información estratégica, se realiza de manera furtiva, ilegal e incluso violenta.

Por ello, en el ámbito de esta investigación se hace imprescindible la definición de estas dos variables conceptuales que permiten clasificar –positiva o negativamente– el acto de buscar información acerca de un individuo, organización, Estado o, en su caso, propiedad de ellos. En consecuencia y como acto inicial, enseguida se detallan las características de los conceptos de "inteligencia" y "espionaje".

INTELIGENCIA, ¿CÓMO DEFINIRLA?

En 1948, el trabajo de Sherman Kent titulado *Inteligencia estratégica para la política mundial norteamericana* estableció las bases para el pen-

samiento de inteligencia, e incluso para parte de las estructuras de inteligencia estadunidenses actualmente en funciones; además de una definición muy adecuada de lo que los EUA y algunos otros países entienden como inteligencia. Kent (1986, p. 2) definió la "inteligencia", en el prefacio mismo de dicha obra, como: "[...] el conocimiento que nuestros hombres, civiles y militares que ocupan cargos elevados, deben poseer para salvaguardar el bienestar nacional [...] Se llamaría el conocimiento *vital para la supervivencia nacional*."

La inteligencia también constituye una institución, formada ésta por seres vivos que buscan, en todo momento, una clase especial de conocimiento que les permita saber el pasado y el presente, así como predecir el futuro del resto de las naciones con base en la información estratégica que ha sido recopilada a lo largo del tiempo sobre su historia, tendencias, costumbres, etc. En palabras del propio Kent (1986, p. 2) queda como sigue:

> La inteligencia constituye una institución; es una organización física de seres vivos que persigue, como fin, una clase especial de conocimiento. Una organización semejante debe hallarse preparada para poner a los países extranjeros bajo vigilancia u observación[1] y también debe estar preparada para explicar su pasado, su presente y probable futuro. Debe tener la seguridad de que lo que se produzca en el sentido de información de esos países, sea útil a la gente que toma las decisiones, es decir, que sea apropiado para sus problemas, que sea completo, seguro y oportuno.

De igual forma, dicho autor clasifica la información estratégica como: "[...] el conocimiento sobre el cual descansan, tanto en la guerra como en la paz, las relaciones exteriores de nuestro país [...]" (p. 35). Por supuesto que lograr ese nivel de eficiencia se debe a la conformación de un equipo de gente capaz y eficaz en las tareas tanto de su campo de conocimiento como de las actividades de búsqueda de inteligencia. Kent lo plasma de la siguiente manera:

> Se desprende que tal organización [de inteligencia] posee un equipo de diestros expertos que, al mismo tiempo, conozcan cuáles son los problemas estratégicos y la política exterior corrientes, y que dediquen su pericia profesional a la producción de información útil[2] sobre los problemas (p. 35).

[1] Es aquí donde radica la justificación de los actos de espionaje o ciberespionaje.

[2] Kent hace uso de los conceptos de "inteligencia" e "información" para referirse a la obtención de información, que es donde empieza y termina el ciclo de la inteligencia.

En las palabras de este autor se encuentran los lineamientos utilizados para llevar a cabo la política exterior de los EUA y nos permite tener una visión de la importancia de la inteligencia en la conformación de dicha política durante la segunda parte del siglo XX. De igual manera, lo dicho por Sherman deja entrever las bases empleadas para dar vida al enorme sistema de inteligencia (conformado por grandes organismos gubernamentales como son la Agencia Central de Inteligencia (CIA, por sus siglas en inglés) y la NSA,[3] entre otros) con el que actualmente cuentan los EUA.

Sin embargo, ésta fue solamente la definición que los EUA decidieron adoptar, por lo que cabe acotar que en el presente, a nivel internacional, existe un amplio debate y confusión sobre el concepto de "inteligencia", lo que indica el forcejeo existente entre los diversos actores para justificar su búsqueda de información de alto valor en terrenos ajenos o extranjeros y evadir la culpa. La Oficina de las Naciones Unidas contra la Droga y el Delito (UNODC, por sus siglas en inglés) en el documento titulado *Sistemas policiales de información. Manual de instrucciones para la evaluación de la justicia penal*, ejemplifica el debate que existe para definir la inteligencia, explicando que:

> Las definiciones de qué se entiende por inteligencia varían. Algunos dicen que es la "información preparada para la acción", en tanto que hay quienes sostienen que es "información evaluada". Otros afirman que la información se transforma en inteligencia a través de un proceso analítico, en tanto que no falta quien afirme que se trata de "información importante o de importancia potencial para una indagación o posible indagación". Lo que tienen en común estas definiciones es la idea de que la inteligencia constituye un tipo especial de información con valor adicional que se reconoce o asigna mediante cierto tipo de proceso analítico (p. 1).

Si bien, a nivel internacional es difícil llegar a un consenso sobre el concepto de inteligencia, cada uno de los estados cuenta con una definición de ella. Por ejemplo, para México es conveniente señalar lo que el Centro de Investigación y Seguridad Nacional (CISEN) en-

[3] La CIA tiene su origen en la Ley Pública 253 y opera solamente fuera del territorio estadunidense; la NSA se crea en secreto en 1952 por el presidente Harry S. Truman, con objeto de mantener la seguridad de la información.

tiende por inteligencia, a fin de establecer un parámetro nacional de comparación y guía.

El CISEN, en su portal de Internet, indica que la inteligencia es: "[...] información especializada que tiene como propósito aportar insumos a los procesos de toma de decisiones relacionados con el diseño y la ejecución de la estrategia, las políticas y las acciones en materia de seguridad nacional". Definición que indica, de manera general, lo que es la inteligencia para la seguridad nacional, pero que a la vez es indicativo de dos aspectos: primero, busca cubrir todo acto o evento que estuviera incluido, pero no se conoce –lo que es vago al igual que confuso–; segundo, no se conocen los elementos vitales para la seguridad nacional ni aquellos ámbitos que se ven impactados por la falta de una definición precisa. Es claro que el núcleo de esta última es "información especializada", pero el detalle está en qué es información especializada, para quién y en qué nivel.

De alguna forma, en esta definición se recurre al concepto de seguridad nacional que justifica gran parte de, por no decir todas, las acciones menos transparentes de los estados, que ponen en riesgo los derechos humanos y que constituye un concepto que no se cuestiona. En resumen, poco ayuda la definición oficial mexicana del CISEN para el concepto de inteligencia por ser vaga, amplia y confusa, lo que en consecuencia requiere de la búsqueda de una definición clara, breve, incluyente y precisa.

En el mismo tenor, la Ley de Seguridad Nacional define a la inteligencia como: "Artículo 29. Se entiende por inteligencia, el conocimiento obtenido a partir de la recolección, procesamiento, diseminación y explotación de información, para la toma de decisiones en materia de seguridad nacional". Esto hace referencia al ciclo de la inteligencia para obtener un conocimiento, que esencialmente es información de algo o alguien. En este ciclo no se incluye, de manera explícita, el análisis de la información obtenida que se considera como una parte esencial del proceso de generación de conocimiento.

Con base en lo antes presentado y como un ejercicio de reflexión sobre el tema, se define la *inteligencia* como un tipo especial de conocimiento o información, ya sea ésta visual, virtual, oral o escrita, que cuenta con un valor agregado por el proceso de análisis, realizado por medios humanos o artificiales, que es explotada –a través de una estrategia– en un ámbito específico o general de las relaciones interpersonales, interorganismos o internacionales. Definición que será

adoptada por este trabajo, por ser clara, incluyente y acorde con lo que se expone.

Lo anterior se establece teniendo en mente que la inteligencia es sólo un componente de la seguridad nacional, que es el objetivo final de los órganos de inteligencia y la cubierta perfecta utilizada por los estados para justificar sus actividades de búsqueda de información estratégica en territorio enemigo. Se entiende que todo es válido para tener la seguridad, pero para que este término sea aplicable a cualquier situación que ponga en riesgo la seguridad de un Estado, ésta debe ser definida correctamente.

En este sentido, cabe aclarar que en el caso de México, el concepto de seguridad nacional no ha sido definido adecuadamente en la Ley de Seguridad Nacional vigente,[4] ya que deja de lado aspectos vitales para la supervivencia del Estado e incorpora aspectos triviales a su texto. Con base en esto se establece que nuestro análisis y definición del concepto de inteligencia coincide parcialmente con la definición del CISEN que, como se ha mencionado, sustenta su actuar en un concepto tan controversial y confuso en México y el mundo como es el de seguridad nacional.

La confusión que se discute da pie al desvío, con gran facilidad, de las actividades de inteligencia hacia otras esferas. Por lo tanto, es preciso agregar que, con el objeto de aplicar la búsqueda de "inteligencia" en ámbitos ajenos a la inteligencia tradicional (lucha contra los malos), pero bajo el precepto de la seguridad nacional, se han forjado diferentes variantes del término de inteligencia como son: la criminal, la estratégica y la económica, esta última de gran importancia en el mundo actual y que, de igual forma, para el presente estudio representa un tema a rescatar, ya que de acuerdo con la estrategia del *soft power* (poder suave) y los preceptos establecidos tanto por la geoeconomía como por la teoría neoliberal, hoy en día se requiere del empleo de los servicios de inteligencia para anticiparse al "enemigo" en el ámbito económico. Actitud que ha quedado plasmada en las acciones de EUA para con sus "socios comerciales" del continente americano (Brasil, México y Venezuela) y del resto del mundo (Alemania, Arabia Saudita y Japón). Por lo tanto, ya que el espionaje económico

[4] Para el efecto, el autor del presente trabajo ha realizado un análisis de la Ley de Seguridad Nacional en su trabajo de tesis de maestría titulado "Las implicaciones de la ASPAN y de la Iniciativa Mérida en la seguridad nacional de México a partir del 2005 al 2009.

es atractivo y redituable, a continuación se profundiza en la variante económica de los sistemas de inteligencia, haciendo hincapié en que, aunque dicho espionaje representa una deformación de las misiones u objetivos propuestos para los servicios de inteligencia, es en el presente una parte integral de la búsqueda de información estratégica de los potenciales enemigos. Es claro que los estados hegemónicos toman en serio la relación entre los poderes militar y económico para perdurar en el mundo actual.

Inteligencia económica

Una vez derrotado el bloque socialista y con el fin de la guerra fría, la economía de mercado resurgió con mayor fuerza para imponer sus perspectivas y formas de actuar. Desde entonces, la teoría neoliberal domina en las relaciones entre estados y, con ello, el poder económico en las relaciones internacionales ha tomado el puesto antes ocupado por la fuerza militar; es decir, se ha pasado de un realismo puro a uno de tipo económico. Evidentemente, en la "guerra económica" las necesidades de inteligencia son, en su mayoría, económicas y no militares; por lo que ahora los estados reorientan y toman ventaja de sus servicios de inteligencia para que les ofrezcan servicios de recolección de información y espionaje en materia de patentes, mercado, finanzas, etc. Como soporte de lo antes mencionado, cito lo que se establece en los *Cuadernos de estrategia 162. La inteligencia económica en un mundo globalizado*, documento editado por el Instituto Español de Estudios Estratégicos:

> Se daba así un nuevo giro a las actividades de inteligencia, naciendo el concepto de "inteligencia económica" como el conjunto de acciones coordinadas de investigación, tratamiento y distribución de la información para tomar decisiones en el orden económico. Acciones que se dirigen tanto al ámbito de la economía nacional como en el dominio empresarial, pues la globalización de los mercados pone también en riesgo a las propias empresas (p. 11).

Como se lee en la cita, esta función de la inteligencia se enfoca en la obtención de secretos comerciales e industriales que permitan obtener ventajas comparativas y competitivas en el mercado internacional. Además, se infiere que contar con este tipo de información ofrece un mundo de posibilidades para obtener mejores dividendos

en los acuerdos comerciales, en los cuales participe un Estado dado. Como resultado de ello, la información económica precisa y oportuna se convierte en poder. Aunque el poder económico ha sido utilizado desde la antigüedad para doblegar voluntades, la inteligencia económica toma nueva importancia a partir del término de la "guerra fría" y de la adopción, por parte de una vasta mayoría de países, de las teorías económicas neoliberales y de "competencia perfecta", en un mundo donde se dice predomina el libre comercio.

Al final, la inteligencia económica se ha convertido en un instrumento de presión y dominio aplicado no sólo por los estados dominantes, sino por todo aquel ente enfrascado en una competencia económica, llámese empresa transnacional o individuo millonario. Lo que se busca con la inteligencia económica es hacerse de secretos industriales y tecnológicos, así como de información estratégica sobre contratos comerciales que permitan tomar ventajas de los nichos comerciales o de las oportunidades de hacer negocio. En esencia, es una "guerra económica" para borrar del mapa a la competencia, o dejarle las migajas de un sector comercial, utilizando como armas la información, la innovación, la tecnología y, sobre todo, la anticipación.

Para dar vida a lo antes expuesto en el ámbito de esta investigación, en un primer plano se cuenta con los ejemplos del espionaje/recopilación de inteligencia económica realizado por los EUA y Canadá a la empresa Petrobras, así como al Ministerio de Minas y Energía de Brasil, respectivamente; en segundo término, el caso de México, que según los reportes presentados en los periódicos *O'Globo* (Greeenwald, 2013) y *The Guardian* (Watts, 2013), también fue objeto de espionaje en el sector energético.

Hasta el momento se ha dicho que el político y el comercial son los dos principales tipos de espionajes practicados por los servicios de inteligencia de hoy; razón por la cual, los estados invierten millones de dólares para mantener a salvo y obtener todo tipo de información estratégica en estos ámbitos. Es de llamar la atención el tira y afloja del espionaje en temas económicos, porque si bien todos los estados, organismos e individuos buscan resguardar sus fortalezas y secretos, esto no es una tarea fácil, debido a que todas las contrapartes o competidores buscan descubrir el secreto de su éxito, ya sea para emularlo o para conocer sus flaquezas.

En consecuencia, para hacerse de inteligencia político-económica, militar y, eventualmente, de cualquier otra índole, los estados (aunque también lo hacen instituciones, empresas e individuos) utilizan

una diversidad de formas e instrumentos, lo que da pie a una clasificación del tipo de inteligencia obtenida por los servicios del gobierno, de acuerdo con los recursos y técnicas empleados.

CUADRO 1.1. CLASIFICACIÓN DE LOS TIPOS DE INTELIGENCIA: SUS OBJETIVOS Y MEDIOS

Nombre	*Objetivo*	*Medios utilizados*
SIGINT	Interceptar las comunicaciones transmitidas electrónicamente.	Aparatos de intercepción.
HUMINT	Obtener información a través de personas. Es una fuente clásica.	Personas.
MASINT	Es el uso de la inteligencia para establecer informes respecto de objetivos.	Cubre el espacio de la inteligencia no atribuido a: IMINT, SIGINT, HUMINT, OSINT y agrupa otro subtipos: • Inteligencia acústica (ACINT o ACOUSTINT). • De radar (RADINT). • De infrarrojos (IRINT). • Láser (LASINT). • Nuclear (NUCLINT). • Óptica (OPINT). • Radiación no intencionada (URINT).
GEOINT	Recolección de imágenes.	Todo tipo de medio de creación de imágenes; incluye los satélites.
OSINT	Obtener información de fuentes abiertas a todo el público.	Internet, periódicos, revistas, base de datos, etcétera.
IMINT	Crear imágenes; se divide en: • OPINT: Imágenes de la región visible del espectro. • PHOINT: Espionaje fotográfico desde cámaras hasta satélites. • EOPINT: Obtenido de los fenómenos electroópticos. IRINT: Con potencial para detectar cambios de temperatura en ámbitos climatológicos adversos.	Medios de creación o edición de imágenes.

FUENTE: Elaboración propia con base en la información presentada en *Cuadernos de estrategia 162. La inteligencia económica en un mundo globalizado*, consultado en <http://goo.gl/VW1T9O> el 24 de septiembre de 2013 y en <http://goo.gl/RtdUvF> el 27 de septiembre de 2013.

Tipos de inteligencia

A fin de ilustrar las técnicas y tecnologías para la adquisición del conocimiento/inteligencia (que son utilizadas profusamente por las fuentes de información), el cuadro 1.1 (p. 20)concentra los detalles característicos de cada uno de los tipos de inteligencia empleados para conseguir la seguridad, la predominancia y el control de la información estratégica.

De este cuadro se desprende que las fuentes de inteligencia son diversas y muy variadas, atienden a todos los sentidos humanos, requieren de instrumentos de alta tecnología, y dos de ellas representan los medios fundamentales de la inteligencia –aquellas que hacen referencia a la inteligencia de señales (SIGINT) y a la inteligencia humana (HUMINT).

Hasta aquí se han presentado algunos conceptos que los Estados utilizan para realizar dichas actividades; se ha brindado uno nuevo para la inteligencia acorde con las necesidades de este trabajo de investigación; se han mencionado adjetivos que se conjugan con el concepto de inteligencia y que dan como resultado variantes predominantes en las relaciones internacionales del presente; se ha mencionado la importancia creciente de la llamada inteligencia económica, como resultado directo de que la inteligencia en el mundo moderno ha dejado de ser plenamente militar para incorporarse al ámbito comercial; se han descrito las técnicas y medios utilizados comúnmente para apoderarse de información estratégica y generar inteligencia. Ahora es momento de detallar el espionaje, que es indudablemente la contraparte del concepto de inteligencia.

ESPIONAJE, LA OTRA CARA DE LA INTELIGENCIA

Es poco frecuente identificar al espionaje como un acto nacido con el hombre mismo y considerarle como una de las profesiones más antiguas del mundo, a pesar de que, por ejemplo, en la Biblia existen diversas menciones acerca del espionaje, tanto en el Antiguo como en el Nuevo Testamento. Para muestra basta mencionar lo que dice el evangelio de San Lucas, capítulo XX, en el cual se narra cómo los fariseos infiltraron algunos espías entre aquellos que rodeaban a Jesús, para que bajo el disfraz de justos lo sorprendieran en actos "ile-

gales". Con base en lo anterior y desde una perspectiva personal, el espionaje es el arte de la observación e interpretación de la realidad que todos los individuos realizan de manera ordinaria para encontrar una respuesta mejor y más sencilla a las actividades de la vida diaria, ya que la información entra por los cinco sentidos y es procesada por el intelecto de manera natural.

La similitud en el objetivo de observar y espiar al mismo tiempo, permite clasificar dicho acto de ambas formas y explicar la situación que prevalece entre las definiciones de inteligencia o espionaje, ya que el concepto de observar, al igual que el dios Jano, cuenta con dos caras pero un solo cuerpo.

Por ello cabe preguntarse, ¿el espionaje es inteligencia o viceversa? A manera de respuesta se afirma que, en esencia, ambos son actividades de vigilancia y análisis del actuar de los estados, organismos e individuos, realizadas por sujetos, grupos antagónicos o incluso otros estados, con el objeto de identificar las fortalezas y debilidades de los diferentes actores internacionales para obtener un beneficio o ventaja en las relaciones que se sostienen con ellos. De lo que se sugiere que los dos conceptos son básicamente lo mismo.

Aunque esta sugerencia se presta a debate, es conveniente señalar que el objetivo de tales acciones es observar, vigilar y analizar[5] para obtener información especializada sobre un hecho, situación, innovación, personaje, institución o Estado. Esto se fortalece con lo expresado por Aristóteles sobre el realismo, cuando dice que el proceso del conocimiento se inicia con la observación, que es justo el punto de inicio y propósito tanto de la inteligencia como del espionaje. Por lo tanto, siendo dos caras de la misma moneda, no existe otra diferencia entre dichos conceptos que no sea la forma en la que se realiza tal actividad y en la que se obtiene la información estratégica[6] –de manera general–; mientras que las actividades de inteligencia[7] son observaciones abiertas, las de espionaje necesitan de cierto grado de clandestinidad y secrecía.

Para el efecto, es decir espiar, tanto los estados como los organismos

[5] En palabras de Sherman Kent, generador de la doctrina de la CIA, esto era poner a los países extranjeros bajo vigilancia u observación.

[6] Algunos autores sugieren que 90% de la información estratégica o especial se obtiene de fuentes abiertas, dejando solamente 10% a las actividades encubiertas o de espionaje.

[7] Es preciso señalar que el diccionario *Merriam Webster* define a la inteligencia como: "información secreta que un gobierno recolecta sobre un enemigo o posible

e individuos hacen uso de las herramientas y fuentes de obtención de inteligencia que tienen a su disposición. Es por ello por lo que:

a] Los individuos obtienen datos de su experiencia propia y de agentes investigadores.
b] Las empresas tienen grupos de analistas e investigadores de mercado.
c] Los estados cuentan con un organismo o dependencia gubernamental encargado de recopilar todo tipo de información que se convierta en inteligencia.

Los tres niveles, los organismos de investigación e inteligencia también son designados como protectores de la información personal, de los secretos comerciales y de la seguridad nacional, respectivamente. Esa doble función, descubrir y resguardar, conlleva la existencia de una delgada línea entre lo ilegal y lo legal en el proceso de obtención de inteligencia o práctica del espionaje y las actividades de contrainteligencia.

Esto nos indica que la búsqueda de inteligencia es aceptada y practicada, y hasta cierto punto se considera como una acción legal, pero que cuando las actividades de inteligencia están orientadas a tomar ventaja y robar información personal, industrial, económica, secreta o vital, utilizando principalmente medios clandestinos o ilegales, se define como espionaje. Éste requiere de acciones precisas y oportunas para contrarrestarlo.

Por ejemplo, en México, el CISEN como justificación jurídica de sus medidas de contraespionaje, aclara que la Ley de Seguridad Nacional define a las amenazas y a los riesgos que enfrenta la seguridad del Estado mexicano; tipificando en el artículo 5 al espionaje como una amenaza. En concordancia con lo que estipula dicha ley, el CISEN (*Amenazas y riesgos*, s.f.) define las amenazas como: "[...] los fenómenos intencionales generados por el poder de otro Estado o por agentes no estatales, cuya voluntad hostil y deliberada pone en peligro los intereses permanentes tutelados por la seguridad nacional, en parte o en todo el país, y cuestionan la existencia del mismo Estado [...]", lo que permite que el aparato estatal actúe contra el flagelo del es-

enemigo", lo que incluye actos de recolección de información clasificada como secreta e induce a pensar en actos de espionaje.

pionaje, ya que éste intenta sustraer, de manera furtiva, información estratégica, propiedad del Estado mexicano.

De lo antes mencionado se obtiene que la seguridad nacional busca contrarrestar el espionaje, porque este acto atenta contra la vida del Estado mismo, en este caso en particular del Estado mexicano. Al encajonar al espionaje dentro de las amenazas, la Ley de Seguridad Nacional lo condena por atentar contra la existencia del Estado; al mismo tiempo, con ello ratifica que la información es poder.

De igual forma, dicha cita reconoce que la búsqueda de información estratégica/clasificada es muy común, pero no está legalizada en el ámbito internacional; incluso dicha práctica se ve enmascarada por la diplomacia que, como lo establece Harold Nicolson (1955), desde tiempos antiguos tiene por protector al dios Hermes, muy acorde con lo que se desea puntualizar, debido a "[...] que para los antiguos simbolizaba las cualidades del encanto, la marrullería y la trampa [...]" (p. 16); el mismo autor agrega lo siguiente:

> El método de poner a los déspotas vecinos unos contra otros, hizo esencial que el gobierno de Constantinopla estuviese plenamente informado de las ambiciones, debilidades y recursos de aquellos con quien esperaba tratar [...] así que los enviados de los emperadores bizantinos llevaban instrucciones [...] también de suministrar informes completos acerca de la situación interna en los países extranjeros y de las relaciones mutuas entre dichos países. A tales fines se requerían cualidades diferentes a las del heraldo o el orador. Se necesitaban hombres dotados de facultades de observación ejercitadas, larga experiencia y sano juicio (p. 21).

Lo que se expresa en esta cita deja en claro tres puntos importantes: primero, provocar el enfrentamiento entre aquellos estados contrincantes se hacía con base en información privilegiada; segundo, la existencia del espionaje diplomático no es algo novedoso y recurre a los privilegios otorgados a sus agentes para solapar la adquisición, compra o robo de información estratégica sobre la situación de un ente antagonista; tercero, la observación y capacidad de análisis son factores determinantes en el éxito de toda empresa.

La inteligencia (como producto) y no la información por sí sola, se convierte en un elemento vital para la seguridad de los estados, ya que permite adelantarse a los movimientos de los diversos actores de la arena internacional con el fin de obtener ventajas competitivas y comparativas, cumpliendo con el viejo *cliché* que indica que la

mejor defensa es el ataque. No se olvide que la inteligencia obtenida con medios que transgreden la seguridad de otros y violentan la legislación vigente, sea nacional o internacional, debe ser considerada espionaje.

En el mismo tenor, por ejemplo, la Escuela de las Américas define al espionaje en su *Manual de contrainteligencia* (ASR, s.f.) como sigue:

> Generalmente, espionaje es el acto de obtener, dar, transmitir, comunicar o recibir información en relación con la defensa nacional con la intención o el propósito creíble de que ésta será utilizada para dañar al gobierno nacional y en beneficio o ventaja del país extranjero.[8]

Esta cita expresa el punto de vista de una de las mejores escuelas estadunidenses de formación de agentes de inteligencia de toda América Latina, en lo que respecta a la definición de espionaje, que aunque limita la información obtenida a la defensa nacional, concuerda con la forma práctica de realizar tales actividades por dicha institución. Además, condena las actividades realizadas por un país extranjero para hacerse de nuestra información de defensa nacional, evidenciando el doble juego o estándar utilizado para el acto de vigilar u observar, ya que mientras yo te observo sin problema alguno, tú no espías mis actividades ni hurgas ni robas mis secretos.

Adicionalmente, Edwin Fraumann (1997, p. 303) dice que el "espionaje" ha sido considerado como sigue: "A lo largo de la historia, el espionaje ha sido visto de forma general como una actividad conducida por espías para obtener los secretos militares de un enemigo".[9]

Ésta se convierte en una definición focalizada en el ámbito de los conflictos bélicos, misma que en años recientes se ha visto expandida por parte de los estados al emplear a sus servicios de inteligencia para obtener secretos de toda índole –en especial económicos e industriales–, bajo el supuesto de que la seguridad nacional está estrechamente vinculada con la económica. Hay que recordar que desde el fin de la guerra fría vivimos en un mundo enfrascado en una guerra económica, que necesariamente requiere de inteligencia o espionaje para su desarrollo.

Respecto a la guerra económica, en su estudio sobre espionaje en laboratorios federales, Edwin Fraumann (1997) indica que los EUA

[8] Traducción propia.
[9] Traducción propia.

han sido espiados por parte de agentes extranjeros y nacionales; como una contramedida legal, el Congreso estadunidense aprobó y firmó en 1996 el Acta de Espionaje Económico que, entre otras cosas, crea un nuevo crimen federal –el espionaje económico.[10] De nueva cuenta, en dicho texto también se encuentra el adjetivo "económico" ligado con el sustantivo "espionaje", lo que junto con el respaldo del Congreso estadunidense para castigar tales actividades, enfatiza la importancia del espionaje económico en las relaciones internacionales en el siglo XXI.

Lo contrastante es que dicha ley castiga el espionaje en territorio y contra empresas u organismos de los EUA,[11] pero no habla sobre algún castigo para el que realizan los actores económicos y gubernamentales estadunidenses a otros estados; más bien resalta que los EUA están conscientes de que son espiados por el mundo; por ello existe una estructura de contraespionaje que es liderada por el Federal Bureau of Investigation (FBI) bajo el programa Awareness of

[10] En el documento titulado Espionage Threats at Federal Laboratories: Balancing Scientific Cooperation while Protecting Critical Information, con fecha 16 de mayo de 2013, en el que el Comité de Ciencia, Espacio y Tecnología de la cámara de diputados estadunidense señala que los principales interesados en robar secretos tecnológicos han sido los rusos y los chinos. Señalando que aunque muchos de los científicos extranjeros que trabajan en territorio estadunidense son ciudadanos modelo, existen algunos otros que trabajan para los gobiernos de sus naciones de nacimiento –al respecto menciona el caso de un intento de robo por parte de los ingenieros Shanshan Du y Yu Qin de la tecnología híbrida de la compañía General Motors para venderla a un competidor chino del sector automotriz; otras compañías mencionadas son Dupont, Rockwell y Boeing. Tanto chinos como rusos se enfocan en el robo de tecnologías de carácter militar, de médico, de comunicaciones, de industria aeroespacial y de transportes que les brinden la oportunidad de lograr alcances similares a los de sus contrapartes estadunidenses. Otro aspecto importante de este documento yace en el hecho de que mucho del espionaje económico se realiza a través de la obtención de información de trabajadores, académicos e investigadores, ya que representan una población que es poco vigilada por el gobierno y que se encuentra en práctica constante en su campo de trabajo/estudio. De acuerdo con el documento, mientras que los costos de investigación son pagados por el gobierno, instituciones y empresas estadunidenses, los beneficios de sus éxitos, gracias al espionaje, llegan a otros sin costo alguno. Por ejemplo, menciona a los grupos o individuos terroristas que se apoderan, clandestinamente, de tecnología, información y materiales para construir un arma de destrucción masiva. Concluye que el control de la transferencia de tecnología y conocimiento (*know-how*) representa una cuestión de seguridad nacional, consultado en <http://goo.gl/Y8FdFc> el 13 de febrero de 2014.

[11] Tenemos el ejemplo del *hacker* escocés mencionado como el culpable de *hackear* los sistemas informáticos de la NASA, en busca de secretos que revelaran la existencia de extraterrestres, consultado en <http://goo.gl/v4dTb2> el 30 de octubre de 2013, pp. 2 y 3.

National Security and Response, con la participación de una docena de agencias federales y del sector empresarial.

Asimismo, Fraumann establece que en este programa el primer frente de ataque al espionaje económico en territorio estadunidense lo constituye el U.S. Customs Service (Servicio de Aduanas de los EUA, p. 307). Adicionalmente, en su estudio hace referencia a una clasificación simple de los métodos empleados para adueñarse de los secretos económicos (los cuales son utilizados para describir el espionaje en general) (pp. 305 y 306):

a] *Métodos intrusivos.* Accesos electrónico y físico a los ambientes protegidos, así como acceso a personal trabajando en dichos ambientes, de los cuales el primero contempla el espionaje que ha sido desarrollado y practicado en el presente por las agencias de aplicación de la ley y de seguridad nacional de los EUA.
b] *Métodos no intrusivos.* Cabe aclarar que estos actos no son considerados de espionaje por sí mismos, pues la información se obtiene de fuentes públicas.

Esta clasificación de métodos si bien es utilizada para el espionaje económico, también se usa para detallar cualquier otra actividad que se desee investigar. Con base en otros criterios, en la clasificación y el alcance del espionaje se realiza también el tipo de inteligencia puesta en práctica:

a] *Inteligencia estratégica*: es la encargada de conocer las intenciones de otros estados.
b] *Inteligencia táctica*: se encarga de los objetivos militares así como de oportunidad.
c] *Contrainteligencia*: es la responsable de preservar la protección de los sistemas de inteligencia propios y de los secretos más importantes.

Los tres tipos de inteligencia mencionados se alimentan de la información presentada y obtenida de fuentes públicas y de aquéllas no públicas –en estas últimas es donde principalmente se ubica la práctica del espionaje electrónico, marítimo, aéreo y con agentes secretos.

Desde una perspectiva personal y a manera de resumen, el espionaje –del tipo que sea– es el robo de secretos, datos, información y propiedad intelectual que se ve "legalizado" por las condiciones

imperantes de competitividad o conflicto, y que además es aceptado e inclusive alentado por los estados, organismos e individuos, como una actividad cotidiana de interacción en el mundo de hoy. Invariablemente, el espionaje es una práctica de la que todos saben pero nadie habla de forma abierta.

En consecuencia, y gracias al escándalo iniciado por los delatores de los actos de espionaje practicado por los EUA alrededor del mundo, se tiene el marco oportuno y preciso para indagar en detalle sobre los programas de espionaje/inteligencia implementados por los EUA en el siglo XXI. Aunque primero es preciso detallar lo que es un programa de espionaje y cuáles son sus características.

¿QUÉ SON LOS PROGRAMAS DE ESPIONAJE/INTELIGENCIA?

La definición otorgada por el *Diccionario de la Lengua Española* (s.f.) para "programa" establece que, entre otras cosas, es: "Anuncio o exposición de las partes de que se han de componer ciertos actos o espectáculos o de las condiciones a que han de sujetarse, reparto, etc.", o "serie ordenada de operaciones necesarias para llevar a cabo un proyecto"; para nuestra necesidad, esta última definición es más que suficiente porque establece, de forma clara, que "programa" es la conjunción ordenada de las partes para obtener un propósito previamente establecido.

Por otro lado, la definición para espionaje en la misma fuente (*Diccionario de la Lengua Española*, s.f.) es: "Actividad secreta encaminada a obtener información sobre un país, especialmente en lo referente a su capacidad defensiva y ofensiva" o "actividad dedicada a obtener información fraudulenta en diversos campos". Aunque lo anterior es breve, también es preciso para definir el fenómeno del espionaje.

De manera complementaria, por lo expuesto previamente sobre la similitud de los conceptos de inteligencia y espionaje, se toma lo que en el *Diccionario de la Lengua Española* (s.f.) se define como "inteligencia", esto es: "Conocimiento, comprensión, acto de entender", o "trato o correspondencia secreta de dos o más personas o naciones entre sí".

Con base en las definiciones anteriores, construimos la que le corresponde a "programa de espionaje/inteligencia": "Una serie ordenada de actividades, secretas o no, encaminadas a obtener información

estratégica sobre un Estado en los diversos campos del poder, a fin de conseguir el objetivo planificado en las relaciones con dicho Estado".

Esencialmente los programas de espionaje se catalogan en dos formas básicas:

1] Operación especial.
2] Conjunto de acciones específicas para apoderarse de información estratégica sobre un Estado, organismo, objeto o sujeto.

Como complemento de lo antes mencionado y como una perspectiva diferente, por un lado, el espionaje (al ser una operación especial) es también catalogado dentro de las operaciones no convencionales,[12] mismas que se definen como: aquellas operaciones que por sus características no siguen un patrón establecido para cumplir con la misión o tarea encomendada, y que comprenden lo que se conoce como:

a] *Operaciones especiales*: son aquellas acciones encubiertas, operaciones secretas, sabotaje, actos clandestinos, subversión, infiltraciones, espionaje.
b] *Operaciones psicológicas.*
c] *Operaciones cibernéticas*: éstas requieren de una alta especialización y son necesarias para las misiones de inteligencia del presente.

Por el otro lado y en palabras llanas, los programas de espionaje/inteligencia son estructurados a nivel nacional e internacional para obtener:

- Inteligencia sobre los diversos grupos antagonistas de un Estado.
- Información privilegiada referente al desempeño de los mercados internacionales.
- Secretos militares.
- Bases de datos de los particulares.
- Todo aquello que dé indicios de los movimientos, tendencias

[12] Las operaciones no convencionales son aquellas que requieren una habilidad ajena al uso exclusivo de la fuerza, esto es, que implican ciencias sociales, biológicas, económicas, tecnológicas, políticas, cibernéticas, etc. Algunas veces se les denomina únicamente como operaciones especiales.

e intenciones de los estados, organismos e individuos en la arena internacional y que haya sido obtenido de una manera "políticamente correcta y tolerada".

Por lo tanto, se infiere que como un resultado directo de sus características de clandestinidad, especialidad, flexibilidad y alcance, las acciones de "inteligencia" finalmente se convierten en programas de espionaje económico, tecnológico, político, militar, social, cultural, psicológico y digital o cibernético; por esta razón, los detalles de dichos programas son una parte que no se pasa por alto cuando se busca explicar su funcionamiento práctico.

CARACTERÍSTICAS DE LOS PROGRAMAS DE ESPIONAJE DIGITAL

Todo acto conlleva un conjunto de características que lo definen como tal o cual; por ello cuando se piensa en programas de espionaje digital se incluyen una serie de formas, actitudes, instrumentos y situaciones implementadas para lograr el objetivo –adueñarse de información estratégica y de importancia vital para un tercero, que es utilizada en su contra en el momento oportuno–, lo que confirma que el final de todo organismo, individuo o Estado llega desde sus propias debilidades una vez descubiertas. Esto me recuerda aquello que dice la Ley Miranda: "Todo lo que diga será utilizado en su contra", pero ampliado de forma exponencial, porque no sólo es lo que se hace o se dice públicamente lo que provoca la derrota, sino todo aquello que se quiere conservar entre sombras.

Generalmente, los programas de espionaje/inteligencia digital tienen por característica principal el secreto, pero también incluyen detalles únicos como:

- Ser intrusivos.
- Consistir de implante físico, virtual o una combinación de ambos.
- Ser patrocinados generalmente por las agencias de seguridad estatales o grandes empresas.
- Contar con gran capacidad de almacenamiento de datos.
- Fungir como transmisores remotos de información o como llaves maestras; con capacidades para realizar cruces de información.

- Tener una capacidad de simulación –entran a las redes como programas inofensivos o actualizaciones.
- Transgredir los derechos de los estados y humanos.
- Poner en riesgo la soberanía de los estados, organismos e individuos.
- Atentar contra la seguridad nacional.
- Manipular, alterar, destruir, negar o degradar la información contenida en computadoras, redes de computadoras o en la red de Internet misma.
- Ser de alta especialización.
- Constituir una tarea de índole multidisciplinaria.
- Usar tecnología de punta.
- Comprar o recurrir a los dobles agentes o agentes infiltrados.
- Emplear el conocimiento de *hackers* y *crackers* a cambio de un pago.
- Aprovechar el soborno y el intercambio de favores.
- Generar y requerir de capital humano altamente especializado.

Para su empleo rápido, éstas se presentan en el cuadro 1.2. De las características anteriores destacan el secreto, la flexibilidad, la persistencia y la especialización que requieren para llevarlos a buen término.

De las características antes mencionadas, aquellas que trasgreden los derechos de privacidad del hombre y de la seguridad de los estados son las que se utilizan como recurso legal para limitar el actuar de las agencias de espionaje/inteligencia alrededor del mundo. Aunque la violación de derechos de privacidad no le ha importado mucho a la NSA, pues cuenta con dos divisiones dedicadas a la implantación de las llamadas *backdoors*[13] (puertas traseras):

a] La ANT (presumiblemente Advanced or Access Network Technology).
b] La TAO (Tailored Access Operations).

La primera de ellas se ha infiltrado en casi la totalidad de la infraestructura de seguridad de los jugadores más importante de la industria de los "cortafuegos" (*firewalls*) (Appelbaum, 2013). Lo que le brinda

[13] Las llamadas *backdoors* son tanto programas de computadoras como circuitos integrados que permiten la vigilancia y control remotos con acceso a la información contenida en aquellos dispositivos que han sido intervenidos o modificados.

CUADRO 1.2. CARACTERÍSTICAS DE LOS SISTEMAS DE ESPIONAJE DIGITAL

Secretos	*Intrusivos/ no intrusivos*	*Implantes físicos o virtuales*	*Gran capacidad de almacenamiento*	*Transmisores remotos de información*
Llaves maestras de programas y sistemas operativos.	Ponen en riesgo la soberanía y seguridad de Estados, organismos e individuos.	Requieren de equipos multidisciplinarios para su diseño y operación.	Tecnología de punta.	Empleo de los grandes servidores, *hackers* y *crackers* para saltear las medidas de seguridad digital.
Multidisciplinarios.	Especializados.	Son herramientas de manipulación.	Transgreden los derechos humanos.	Buscan el control y el poder de la información.
No tienen una regulación internacional.	Promovidos por agencias estatales.	Cuentan con la participación de las empresas privadas de fabricación de componentes.	Furtivos.	Con disfraz de servicios gratuitos.
En coalición internacional.	Emplean organismos internacionales como fuentes.	Con capacidad para mutar.	De un diseño general o personalizado.	Usan las redes de internet/ intranet como su medio de conexión.
Flexibles.	Justifican acciones de seguridad.	Persistentes.[a]		

[a] El equipo de la ANT se refiere con esto al hecho de que un programa de espionaje *spyware* que ha sido instalado en un sistema operativo, sobrevive al borrado completo del disco y a la instalación de un nuevo sistema operativo. Esta persistencia sigue dando acceso a la computadora ya supuestamente limpia, consultado en <http://goo.gl/UqHxkY> el 20 de enero de 2014.

FUENTE: Elaboración propia.

acceso a nuestra vida digital de manera exclusiva a la NSA, ya que la división de ANT cuenta con una útil llave maestra que abre la puerta cuando así lo desea. Asimismo, los recursos para llevar a cabo sus actividades incluyen tanto equipo como programas de computadora con diseño personalizado/especializado para tareas específicas en ámbitos particulares.

La TAO es una agencia creada en 1997 como resultado de la aparición de Internet, que tiene por objetivo trabajar contrarreloj para diseñar y fabricar los instrumentos necesarios para interceptar e interferir las comunicaciones globales, actividad que ha sido exitosa en sistemas como los que han sido utilizados por las compañías de telecomunicaciones europeas, o en los correos electrónicos enviados a través de los servidores "BES" de *Black Berry* –equipos que eran considerados de alta seguridad por el sistema de encriptado que utilizaban.

La experiencia dice que la combinación de ambas herramientas (es decir, las secciones ANT y TAO) ofrece los mejores resultados. En esta combinación, la primera fase del proceso de piratería o robo informático (*hacking*) se realiza con las herramientas de uso común con las que cuenta la TAO,[14] y si el objetivo resiste dichos recursos entonces entra en acción la división ANT con su arsenal de herramientas especiales para penetrar en equipos de red, computadoras y teléfonos digitales. Como una prueba de la existencia de las unidades TAO y sus trabajos, la unidad TAO que se encuentra en San Antonio, Texas, tiene como área de responsabilidad cubierta al Medio Oriente, Cuba, Venezuela, Colombia y México.[15]

Como puede observarse, esta área de responsabilidad incluye a productoras importantes de petróleo y a los enemigos ideológicos por excelencia en el continente americano, como son Venezuela y Cuba, que han cedido a los designios de los EUA de una manera u otra. Lo que se convierte en un indicador de que si las herramientas con las que cuenta la TAO han sido suficientes para mantener a raya

[14] También existe evidencia de un hecho que llamó la atención pública y la de los representantes políticos en la ciudad de San Antonio, Texas; esto ocurrió cuando las puertas automáticas de los estacionamientos de las viviendas ubicadas en las cercanías de la base aérea de *Lackland* se negaron a ser abiertas por los controles remotos debido a que las antenas de la NSA –que tiene oficinas en dicha instalación militar– estaban transmitiendo en la misma frecuencia de trabajo de los controles remotos de las puertas de los estacionamientos, pero por supuesto con mucha mayor potencia.

[15] Aparece la operación Whitetamale con el objetivo de espiar a la Secretaría de Seguridad Pública, consultado en <http://goo.gl/4tmliU>.

dichas regiones, bien vale lo que se ha pagado por ellas. Sin duda, las potentes características de los programas de espionaje instalados por los EUA los convierten en un gran negocio para propios y extraños.

Por ejemplo, éste es un nicho de oportunidad comercial en el cual, durante 2011, según declaraciones del periódico *The Wall Street Journal*, el monto de las transacciones por concepto de contratos por venta de productos y servicios ascendía a 5 000 millones de dólares.[16]

Debe mencionarse que este mercado de herramientas de espionaje digital se encuentra principalmente fuera de los EUA, ya que al menos esto se realiza en el interior de la National Security Agency con medios propios diseñados por la sección TAO; éste es un grupo de la mencionada agencia que, de acuerdo con el sitio Engadget[17] (s.f.), "[...]tiene por objeto crear programas para infiltrarse en el *hardware* de la red, utilizando *software* que sobrevive actualizaciones de sistema y con capacidad para acceder a otros equipos en la misma[...]"; sin menoscabo de los cambios físicos realizados por agentes, encubiertos o no, en el material y equipo para la efectiva recolección de información.

El secreto, ser indetectables, y la persistencia son las características primordiales de los sistemas de inteligencia y espionaje digital, por lo que los sistemas de espionaje no escatiman esfuerzos para evitar ser detectados o evidenciados, siendo la criptografía la herramienta preferida para mantener intacto el secreto de los mensajes, misma que a lo largo de la historia ha echado mano de diversos métodos para transmitirlos, punto a punto, con el mayor grado de seguridad posible. Los métodos que se han empleado incluyen tintas invisibles, cartas escritas en código, grabados en el cuero cabelludo, el empleo de cifras/códigos hasta la transmisión codificada por radio.

Al respecto, cabe aclarar que, aun con los avances tecnológicos y uso de métodos diversos para la transmisión de la información estratégica, tanto el espionaje como la inteligencia utilizan elementos básicos como es la criptografía, ciencia que se emplea para mimetizar un mensaje de manera efectiva o realizar el análisis criptográfico, con el fin de encontrar los tesoros ocultos en la información transmitida a través de los diversos medios de comunicación.

Se dice que, aunque el mundo digital del presente ha dejado de

[16] Si deseas obtener mayor información consulta <http://goo.gl/1RpDDt>.

[17] Consultado en <http://goo.gl/CecVsV> el 3 de enero de 2014. Explica además que la NSA hace modificaciones internas en las computadoras, inclusive antes de la entrega de los nuevos dispositivos a sus compradores.

lado las viejas prácticas de cifrado y descifrado de mensajes utilizando la tinta y el papel para guardar o revelar el secreto, las actividades de espionaje y contraespionaje basadas en códigos y cifras no terminan, sino que al contrario, crean una competencia perpetua entre ellas. Por lo tanto, esta competencia criptográfica es el interminable juego del gato y el ratón, porque cada triunfo de los criptógrafos representa una derrota de los criptoanalistas y viceversa. Esta evidencia habla por sí sola de la importancia que tiene para los estados, organizaciones e individuos el conocer, diseñar y emplear diversos métodos criptográficos para la salvaguarda de su información estratégica.

Por ello, como una consecuencia de la importancia que tiene la criptografía para el presente trabajo, a continuación se menciona su definición, características, aplicación y métodos más representativos, así como los momentos históricos relevantes de esta ciencia del secreto.