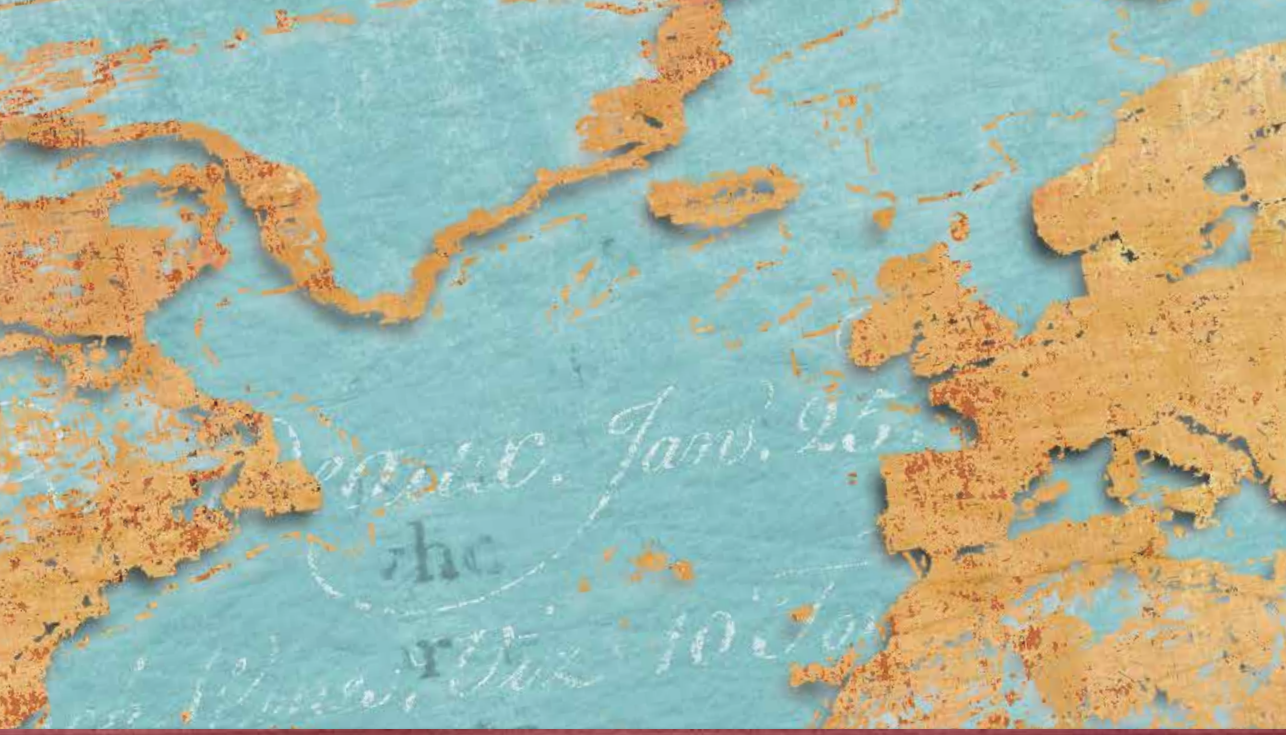

Cuadernos de Estrategia 162
La inteligencia económica en un mundo globalizado

Instituto Español de Estudios Estratégicos

ieee.es
Instituto Español de Estudios Estratégicos

MINISTERIO DE DEFENSA

Cuadernos de Estrategia 162
La inteligencia económica en un mundo globalizado

Instituto Español de Estudios Estratégicos

ieee.es
Instituto Español de Estudios Estratégicos

MINISTERIO DE DEFENSA

CATÁLOGO GENERAL DE PUBLICACIONES OFICIALES
http://publicacionesoficiales.boe.es/

Edita:

MINISTERIO DE DEFENSA
SECRETARÍA GENERAL TÉCNICA

www.bibliotecavirtualdefensa.es

NIPO: 083-13-121-3 (edición en papel)
ISBN: 978-84-9781-842-1 (edición en papel)

NIPO: 083-13-120-8 (edición libro-e)
ISBN: 978-84-9781-841-4 (edición libro-e)

Depósito Legal: M-13935-2013
Imprime: Imprenta Ministerio de Defensa
Fecha de edición: mayo 2013

ÍNDICE

Página

Introducción

INTELIGENCIA ESTRATÉGICA Y SEGURIDAD ECONÓMICA 9

Introducción 9
Globalización económica y geoeconomía 12
Inteligencia estratégica y económica 16
Modelos de inteligencia económica 19
Inteligencia estratégica y seguridad económica 23
Influencia como un elemento esencial de la inteligencia económica 27
Inteligencia económica y ciberseguridad 29
El objetivo del presente Cuaderno 31

Capítulo I

EL PAPEL DE LA INTELIGENCIA ESTRATÉGICA EN EL MUNDO ACTUAL 35

Resumen 35
Introducción 37
Ya no hay damas azules ni rojas en el nuevo tablero de juego 43
La Trinidad de Kent rediseñada 48
Organización: Matrix ya ha nacido 48
Un nuevo producto de verdad estratégico 55
Proceso estratégico: la nueva planificación 59
Conclusiones 62

Capítulo II

ESTUDIO DE LA GUERRA ECONÓMICA Y DE LAS PROBLEMÁTICAS RELACIONADAS 67

Resumen 67

Introducción 69

La emergencia de los principios fundacionales de la guerra económica 70
La violencia y la supervivencia 70
Recursos y territorios 70
Las dinámicas conflictivas ligadas a la colonización 72

Página

El control de las rutas comerciales ... 73
La imbricación de la guerra y de la economía ... 75
La influencia de los enfrentamientos económicos en la conducción de la guerra ... 75
Lucha ideológica y relaciones económicas de fuerza entre potencias ... 77
Creación de estructuras dedicadas a la guerra económica ... 78
Las justificaciones geopolíticas de la conquista ... 81
La conquista contra el imperialismo mercantil ... 81
La conquista del espacio vital ... 83
El encubrimiento de la guerra económica ... 85
Las estrategias de dominación ... 87
Las estrategias de recuperación ... 91
El cambio de paradigma de guerra económica ... 92
Las políticas de seguridad económica ... 93
El impacto de las estrategias económicas de incremento de poder ... 95
Los límites del etnocentrismo occidental ... 96
Las contradicciones entre los Estados Unidos y Europa ... 97
Los efectos perversos de la ejemplaridad liberal ... 99
Conclusiones ... 100

Capítulo III

INTELIGENCIA JURÍDICA: EL VALOR ESTRATÉGICO DEL DERECHO EN LA SEGURIDAD ECONÓMICA ... 103

Resumen ... 103
Planteamiento ... 105
El derecho como conjunto de normas ... 108
El derecho como objeto de la inteligencia ... 111
El derecho como herramienta de la inteligencia ... 116
Conclusiones ... 125

Capítulo IV

LA INTELIGENCIA PARA COMPETIR: NUEVO PARADIGMA EN LA DIRECCIÓN ESTRATÉGICA DE LAS ORGANIZACIONES EN UN MUNDO GLOBALIZADO ... 135

Resumen ... 135
Resumen ejecutivo ... 138
Introducción ... 139
IC y direccionamiento estratégico ... 141
Campo de actividad de la IC ... 142
Beneficios aportados por la IC a la organización ... 143
La IC como proceso ... 144
La IC como función organizativa o enfoque de gestión ... 146
Etapas esenciales del proceso de trabajo de la IC ... 147
Planificación ... 148
Obtención de la información ... 149
Análisis ... 150
Comunicación, puesta en práctica de lo aportado y evaluación ... 152
Cómo aparece organizada la IC ... 153
Países referentes en la práctica de la IC. La situación en España. La oferta de formación ... 154
La IC impulsada desde las instituciones ... 154
La oferta de formación ... 156
Fundamentos de la IC. Estado del arte ... 157
Implicaciones para las organizaciones. Su aprovechamiento vs. su protección ... 159
Influencia y seguridad desde la empresa ... 165

Página

El quebranto de la legalidad que plantea el espionaje industrial y sus negativas consecuencias sobre la IC en la empresa 166
Implicaciones para los territorios: la inteligencia territorial 169
Perspectivas de evolución 170

Capítulo V

LOS RIESGOS ECONÓMICOS DE LA CIBERGUERRA 177

Resumen 177
Ciberguerra y ciberconflicto: la dimensión económica 180
La cibernética como modelo de cambio del paradigma económico 186
El mundo cibernético del mañana 189
El desarrollo de las amenazas. La nueva realidad económica de la inseguridad cibernética 190
Las nuevas formas de ataque 191
El nuevo enemigo: actores colectivos del ciberconflicto 196
Medir el coste del ciberconflicto: ¿es posible cuantificarlo? 198
Los límites legales a la ciberguerra ***stricto sensu*** 200
Ciberdefensa activa y pasiva 205
Un sistema emergente de gestión integral de la ciberseguridad 206
Creación de un marco legal armonizado para combatir los ciberdelitos y ciberconflictos 207
Autoprotección 208
Diseñar para la seguridad 209
Establecimiento de estándares y buenas prácticas 210
Protección de infraestructuras críticas 211
Resistencia en la informática en la nube y los dispositivos móviles 213
Cooperación nacional e internacional en ciberseguridad 215
Una cultura de ciberseguridad: normas de conducta en la era digital 217

Composición del grupo de trabajo 223

Cuadernos de Estrategia 225

INTELIGENCIA ESTRATÉGICA Y SEGURIDAD ECONÓMICA

Eduardo Olier Arenas

Introducción

En 1992 uno de los autores del presente Cuaderno publicó el libro de título *La máquina de guerra económica*[1]. Ya en su inicio, el autor alertaba sobre la importancia de la economía en las relaciones internacionales. Una importancia que el autor llevaba hasta los tiempos del término de la Segunda Guerra Mundial y que conectaba entonces con los iniciales procesos de la globalización y de sus intercambios, los cuales estaban modificando la misma noción de conflicto. Y ya entonces alertaba sobre los efectos de la guerra económica que, contrariamente a la guerra tradicional, comporta acciones que son muchas veces invisibles y decisivas.

Acabada la Guerra Fría, Harbulot se centraba igualmente en la desaparición de la bipolarización en el mundo y la creciente hegemonía norteamericana. Desaparecida la Unión Soviética, solo quedaba uno de los jugadores, un hecho sobre el que muchos años antes, en 1968, hacía sentir su preocupación Jean-Jacques Servan-Schreiber[2], manifestando el problema de manera muy contundente: «No nos hallamos en presencia de

[1] HARBULOT, Christian. *La machine de guerre économique.* Estados Unidos, Japón, Europa: Ed. Económica, 1992.

[2] SERVAN-SCHREIBER, Jean-Jacques. *El desafío americano*. Plaza y Janés, 1968.

un imperialismo político clásico —decía—, de una voluntad de conquista, sino más mecánicamente en un desbordamiento de poder debido a la diferencia de `presión´ entre la América del Norte y el resto de mundo, comprendida Europa». Añadiendo en otro lugar del libro que: «Actuar, ¿cómo? Luchar, ¿contra quién?... Pues la General Motors no es la Wehrmacht, el caso Bull no es Múnich, y el Concorde no es Sedán. Asistimos a la primera gran guerra sin armas ni fortificaciones».

Pero no solo fueron conscientes de este problema los franceses. También los japoneses se dieron cuenta de la importancia de la economía como un nuevo espacio de dominio. Y casi desde el término de la Segunda Guerra Mundial, con sus Fuerzas Armadas, destrozadas y sin posibilidad de recomposición, iniciaron el camino de su reconstrucción industrial y de su posición como una de las potencias económicas del planeta. De manera que, con el tiempo, en los inicios de los años noventa, iniciaban su tercera revolución industrial con el potente MITI conduciendo las operaciones económicas ofensivas y defensivas. Y con los japoneses, otras naciones también desarrollaban estrategias para expandir su potencial económico, tecnológico o comercial hacia otros lugares. Una expansión que se demostró defensiva en algunos casos, sobre todo en países de menor tamaño como Suecia.

Un poco antes del libro de Harbulot al que antes aludimos, Edward Luttwak, experto reconocido en geopolítica, de origen rumano pero afincado en Estados Unidos, lanzó un nuevo concepto en la revista *The National Interest*[3]. Era la primera vez que surgía el término geoeconomía. Para Luttwak, «la geoeconomía es el mantenimiento de la antigua rivalidad existente entre las naciones utilizando medios económicos en lugar de bélicos». Lo que amplió en 1993 en su libro *The Endangered American Dream*[4], indicando que «la geoeconomía mide el progreso mediante la participación que un determinado producto alcanza en el mercado, en lugar de centrarse en el avance que una fuerza militar realiza sobre el mapa». Surgía así el entronque de la economía con la geopolítica. Las guerras económicas tomaban de esta manera carta de naturaleza como parte integrante del hecho económico. Economía y política se unían en nuevos escenarios bélicos alejados de los conflictos militares tradicionales.

Y al tratarse de nuevos escenarios, la complejidad de los mismos se multiplicaba enormemente. El arte de estas nuevas guerras se hacía mucho más sofisticado. Un hecho que, a inicios de los noventa, también desarrollaba otro teórico de la geoeconomía, Pascal Lorot.

[3] LUTTWAK, Edward. «From geopolitics to geoeconomics: Logic of conflict, grammar of commerce». *The National Interest*, verano de 1990, pp. 17-23.

[4] LUTTWAK, Edward. *The endangered American dream*. Simon & Shuster, 1994.

Lorot, fundador y director de la revista francesa *Géoéconomie,* definía en 1990 la geoeconomía como «el análisis de las estrategias de orden económico —especialmente comerciales— decididas por los Estados en el contexto de las políticas conducentes a proteger las economías nacionales o ciertos elementos bien determinados de estas, a adquirir el dominio de ciertas tecnologías claves y/o a conquistar ciertos segmentos del mercado mundial relativos a la producción o comercialización de un producto o de una gama de productos sensibles, sobre los cuales su posesión o su control confiere a los detentadores —Estado o empresa nacional— un elemento de poder o de proyección internacional y contribuye al reforzamiento de su potencial económico y social». Un poder que se llevaría a cabo según el concepto de *soft power* desarrollado por Joseph S. Nye[5].

La estrategia de *soft power* necesitaba por tanto de nuevas técnicas. Una de ellas, antigua como el arte mismo de la guerra, era la utilización de los servicios de inteligencia. Anticiparse al enemigo requería conocer su estrategia y sus movimientos con antelación. De ahí la necesidad de nuevos métodos de acuerdo con los nuevos tiempos. Aparecía con fuerza la inteligencia económica como la utilización de los servicios de inteligencia en el medio económico. Los Estados debían saber qué hacer en el nuevo mundo global que se avecinaba.

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. La defensa de los intereses económicos, por un lado, y, por otro, la necesidad de lograr ventajas respecto de los competidores —a nivel empresarial o estatal— han sido el motor decisivo del desarrollo de potentes instrumentos de inteligencia económica al servicio de los intereses nacionales y de importantes empresas transnacionales de muchos países que hoy dominan la escena económica mundial.

Y es en este contexto donde quiere moverse el presente Cuaderno del Instituto de Estudios Estratégicos, ya que la defensa de los intereses nacionales ha de incluir también los aspectos económicos, claves hoy en el mundo global en el que vivimos. Un hecho largamente olvidado en España, que solo desde hace relativamente poco tiempo se ha ocupado de la importancia que tienen los servicios de inteligencia económica, más allá de dotar de seguridad a personas o instalaciones críticas.

[5] NYE, Joseph. S*oft power: The means to success in world politics.* Public Affairs, 2004.

Globalización económica y geoeconomía

Nos hemos referido antes de manera sucinta a la geoeconomía. Volvamos de nuevo a ello.

Aunque sin expresarlo tácitamente, tanto Edward Luttwak como Pascal Lorot hacían ver que algo había cambiado en la escena mundial para que la economía fuera un elemento determinante. Quizás estos autores, expertos ambos en geopolítica, no alcanzaban a ver los movimientos de la globalización económica. Movimientos que en realidad eran el eje de estos cambios, ya que, desde el final de la Segunda Guerra Mundial y en especial con los acuerdos de Bretton Woods, aparecía un nuevo orden económico mundial –eso sí, muy dominado por los Estados Unidos–, circunstancia que, como hemos visto, movió a la preocupación a Servan-Schreiber.

La globalización económica —proceso aún en curso— es un movimiento, quizás espontáneo, por el que las naciones se han ido haciendo más interdependientes. Cierto es que en la antigüedad se dieron situaciones similares. Por ejemplo, los fenicios comerciaban por todo el Mediterráneo y los romanos extendieron sus dominios mediante imponentes calzadas de piedra para mover a sus tropas y extender su economía muy lejos de sus fronteras, desde Egipto hasta Britania –Egipto, por ejemplo, fue por décadas el granero del Imperio–. También España, el Reino Unido y Holanda extendieron sus dominios casi por todo el mundo conocido. Pero hay que decir que, en lo económico, las transacciones comerciales y los movimientos financieros fueron muy limitados. Tanto es así, que las crisis económicas estuvieron siempre localizadas y no se extendieron globalmente, una circunstancia que, de alguna manera, persiste hoy en día, cuando solo se puede hablar de globalización con sentido dentro del mundo financiero. En lo comercial, el mundo camina hacia la globalización, manteniendo las actividades comerciales en lo fundamental entre países fronterizos o regiones concretas.

Sin embargo, hay que resaltar que la globalización no se reduce a lo comercial o lo financiero; también incluye aspectos culturales, políticos y sociales, lo que da origen a un nuevo orden que se caracteriza en lo esencial por cuatro características principales[6]:

- Importantes movimientos de personas de un país a otro.
- Enorme flujo de capitales entre fronteras.
- Intensificación del comercio internacional.
- Y muy singularmente, fuerte innovación tecnológica.

[6] OLIER, Eduardo. *Geoeconomía: las claves de la economía global*. Pearson-FT-Prentice Hall. 2011.

De manera que, desde 1945 hasta hoy, se pueden identificar seis etapas[7] hacia la globalización, la última de las cuales ha constituido una nueva situación después de la crisis financiera que se extendió desde Estados Unidos en 2008 que aún no sabemos con exactitud qué evolución tomará. Estas etapas son:

1. *1945-1960. La gran maquinaria industrial.* Acabada la Segunda Guerra Mundial, la URSS, Estados Unidos y algunos países europeos se encontraron con potentes industrias crecidas al calor del conflicto bélico: automóviles, ferrocarriles, aviación, industrias electrónicas, etc. Paralelamente, surgía un *boom* inmobiliario que se unía a un enorme crecimiento demográfico: el conocido como *baby boom*. El PIB de todos los países industrializados se doblaba, al igual que lo hacían el poder adquisitivo de las clases medias y el consumo.
2. *1960-1973. Turbulencias geopolíticas*. Son años de prosperidad económica, unidos a las tensiones provocadas por la *Guerra Fría*. Es un período que culmina con el embargo del petróleo de la OPEP, la Organización de Países Exportadores del Petróleo; una década de fuerte descolonización en gran parte de África, donde surgieron más de 30 nuevos países. Además, fue una época de grandes cambios que conocía la llegada del hombre a la Luna, los movimientos revolucionarios en Sudamérica, el asesinato de Kennedy, la guerra de Vietnam, y un largo etcétera de sucesos que culminaban en 1968 con el *Mayo francés*. También es el tiempo del nacimiento de la OLP, Organización para la Liberación de Palestina, y la Guerra de los Seis Días de 1967, que culminaba con la ocupación israelí de los territorios palestinos de Gaza y Cisjordania y de los Altos del Golán en Siria.
3. *1973-1982. Estanflación de origen energético.* Estancamiento económico y fuerte inflación es lo que se denomina estanflación. El embargo de petróleo de la OPEP llevaron los precios del petróleo a crecer un 70%. Su consecuencia no se hizo esperar: enorme inflación, estancamiento económico y paro. Se acababan los días de la riqueza económica de posguerra, una situación que dio origen a múltiples privatizaciones de empresas públicas de los servicios propiedad del Estado, sobre todo en Estados Unidos. También fue el tiempo de la revolución iraní y la posterior guerra entre Irak e Irán.
4. *1982-1989. Se impone el liberalismo económico y la economía de mercado.* El presidente americano Ronald Reagan formaba gobierno en 1981. Arrancaba el *supply-side economics,* una estrategia económica dirigida a incentivar la producción de bienes y servicios en la idea de que la oferta crea su propia demanda según la ley de Say, uno de los economistas de la escuela clásica. A esto se unió la liberalización económica y la reducción de impuestos. De manera

[7] OLIER, Eduardo. *Ibíd.*

casi automática, crecieron los ingresos del Estado americano por el incremento de la productividad y el impulso del ahorro, lo que traía consigo una mayor creación de empleo y un fuerte crecimiento económico. Se reducían las tasas inflacionarias, logrando activar nuevamente el consumo y el crédito bancario. En Inglaterra, Margaret Thatcher, elegida primer ministro en 1979, seguía el mismo criterio. Una ola liberal se extendió por los países occidentales, acabando definitivamente la política keynesiana de después de la Segunda Guerra Mundial. Caía el muro de Berlín en 1989 y finalizaba la bipolarización de las dos potencias. Fue una época, sin embargo, conocedora de una de las mayores crisis financieras del siglo, la conocida crisis de deuda de muchos países latinoamericanos que se declararon incapaces de cumplir con sus compromisos de débito con los organismos internacionales, particularmente con el FMI, el Fondo Monetario Internacional.

5. *1989-2000. La sociedad interconectada.* La noche del 9 al 10 de noviembre de 1989 caía el muro de Berlín. Las consecuencias no se hicieron esperar: el 25 de diciembre de 1991 dimitía Mijaíl Gorbachov, llamado *padre de la Perestroika*. Se desintegraba la Unión Soviética, y con ella el «sistema de bloques»; un fenómeno que dio paso a la apertura de las fronteras mundiales, al uso intensivo de las tecnologías de la información y las telecomunicaciones, a la aparición de Internet y al arranque definitivo de la globalización económica. El comercio mundial se desarrolló de manera explosiva, como lo hicieron los avances tecnológicos en todos los campos, especialmente con el desarrollo de los microprocesadores electrónicos que revolucionaron la industria allá donde llegaron sus aplicaciones, incluida la medicina. La economía mundial volvió a crecer y los mercados financieros se globalizaron. El mundo conocía una nueva explosión de crecimiento económico que se detenía en cierta manera por la llamada *crisis de las puntocom*, empresas tecnológicas que indujeron una fuerte crisis de capitales, si bien contenida en el tiempo.
6. *2000-2010. El mundo globalizado en crisis financiera global.* Japón, la segunda economía del mundo detrás de Estados Unidos, había mostrado signos de agotamiento al inicio de la década de 1990 cuando sus bancos no pudieron aguantar la pérdida de valor de sus activos inmobiliarios que habían realizado años antes. Después vendrían las hipotecas *subprime* y la crisis financiera global iniciada en 2007 que se expandía por todo el mundo occidental desde Estados Unidos a partir de 2008. Las guerras económicas se veían ya de manera patente y se iniciaba un movimiento del centro de gravedad económico mundial hacia el este. Asia, cuya economía en conjunto representaba algo menos del 20% del total en 1970, superaba el 28% en 2007, mientras que la Europa comunitaria caía del 34% al 25% en el mismo período, a la vez que Estados Unidos

mantenía su peso en torno al 33%. El 11-S, con los atentados a las Torres Gemelas de Nueva York, demostraron también un cambio en las relaciones de poder. Del mundo bipolar anterior a la caída del muro de Berlín se abría ahora un mundo multipolar con líderes regionales como Brasil, China, India, Rusia (naciones BRIC) o también Turquía e Irán, sin olvidar la presión islámica como movimiento religioso y cultural de gran influencia.

El mundo poscrisis será diferente al anterior, aunque todavía es pronto para determinar su evolución. Sin embargo, en lo económico, la situación será distinta de lo que se ha vivido hasta ahora. La geoeconomía se ha hecho presente de manera patente: la confluencia de los intereses políticos y el dominio de los mercados es lo que marca la situación actual. Las antiguas acciones militares han dado paso a otras iniciativas más sofisticadas: inversiones estratégicas de capital, innovación en productos o tecnologías de interés para el Estado, posición de dominio sobre los mercados en lugar de invadir los territorios, tarifas arancelarias, medidas regulatorias, devaluaciones de divisas y otras acciones similares son las que marcan las estrategias actuales.

Un nuevo contexto donde los elementos anteriores han quedado obsoletos y donde el valor de la información por sí sola no es ya un elemento diferencial de ventaja competitiva. Ahora es preciso tener conocimiento, adelantarse a los movimientos de países y empresas. En los tiempos actuales, una de las claves es la inteligencia, es decir, el conocimiento estructurado para la toma de decisiones. La inteligencia económica resulta, por tanto, el elemento imprescindible para empresas e instituciones en el contexto geoeconómico. Inteligencia que ha de ser capaz de:

- Describir el entorno competitivo, es decir, determinar los factores y elementos que lo constituyen: competidores, productos, condiciones regulatorias, etc., así como la estructura de precios, tecnologías, etc. que existen en ese entorno como alternativas.
- Establecer la evolución previsible de tales factores competitivos, incluyendo tecnologías disruptivas, nuevos competidores, etc.
- Verificar si los elementos que soportan la estrategia son consistentes en el tiempo; si están bien establecidos respecto del entorno actual y el previsible.
- La inteligencia debe dar respuesta a las preguntas que cuestionen la estrategia. En este contexto, será preciso disponer de las tecnologías de análisis y vigilancia que provean de la información necesaria.
- Identificar exhaustivamente las amenazas y debilidades, así como las fortalezas y oportunidades según el clásico diagrama DAFO.
- Determinar el momento en que la estrategia establecida no es sostenible, una decisión que ha de ser dinámica para ser consecuente con las nuevas acciones a poner en marcha.

Inteligencia estratégica y económica

El término inteligencia, normalmente, induce a confusión, y cuando se le añaden adjetivos la confusión aumenta; cada especialista o grupo involucrado en estas materias lo entiende de una manera distinta. Trataremos por nuestra parte de estructurarlo en sus diferentes categorías.

Aparte de los servicios de inteligencia, que son perfectamente conocidos e identificables, existen otros dominios y conceptos que se entremezclan unos con otros. Básicamente, la inteligencia se podría encuadrar en cinco categorías, cuya jerarquía se muestra en la figura 1.1 que sitúa de arriba abajo las especialidades más tecnológicas:

- Inteligencia artificial.
- Gestión del conocimiento.
- Inteligencia económica.
- Inteligencia competitiva.
- Inteligencia estratégica.

Figura 1.1. Jerarquía de los sistemas de inteligencia

Las dos primeras son muy soportadas por tecnologías de uso ya muy común. Así, el campo de la inteligencia artificial ha estado desarrollándose desde los años cincuenta del siglo pasado y va dirigido en lo fundamental a comprender la manera en que el ser humano piensa, aprende y razona para desarrollar técnicas y programas informáticos que traten de emular el comportamiento humano. De ahí nacieron la robótica, los sistemas expertos y los sistemas de ayuda a la decisión, todos ellos apoyados en tecnologías que tienen la capacidad de aprender.

Un paso más se dio con los sistemas de gestión del conocimiento que, básicamente, tienen que ver con los sistemas expertos. Son sistemas que dieron origen a una rama de la ingeniería que hoy se conoce como *ingeniería*

del conocimiento, cuyas técnicas se apoyan en varios elementos: adquisición del conocimiento, codificación del conocimiento, evaluación y pruebas del sistema codificado e implementación del sistema. La codificación se basa normalmente en reglas que, a medida que se complican debido a múltiples cadenas, se pueden transformar en *redes neuronales*; otra forma de tratar de simular la manera en que trabaja el cerebro humano. Y de ahí se puede llegar a otras funciones como son los sistemas de comprensión del lenguaje natural, visión computerizada, etc., técnicas todas ellas que no representan lo que realmente se entiende por inteligencia económica, competitiva o estratégica, pero que a veces ayudan en su desarrollo.

La inteligencia económica se ha definido de mil maneras. Depende de quien lo interprete y así serán sus aplicaciones. También depende del país: en Estados Unidos y otros países anglosajones, el término *business intelligence* se aproxima a las actividades relacionadas con la gestión del conocimiento. En concreto, son metodologías y modelos que tratan de descubrir la información «escondida» dentro de las bases de datos a fin de proporcionar herramientas para la toma de decisiones. Una derivada de ello sería el *marketing intelligence,* que se dirige a los aspectos comerciales y de *marketing* de las empresas en su entorno competitivo. De esta manera se «modelizan» los comportamientos de los clientes actuales o potenciales con el objetivo de aumentar las ventas o, simplemente, evitar que se vayan a la competencia.

De manera diferente, los franceses definen[8] la inteligencia económica —*intelligence économique*— como *el conjunto de acciones coordinadas de investigación, tratamiento y distribución con vistas a su explotación, de la información útil a los actores económicos*. Una definición que para sus autores tiene una doble consecuencia: por un lado, la inteligencia científica, que se dirige a «no inventar la rueda», es decir, a investigar en las fuentes científicas accesibles la aparición de nuevos dominios científicos que aporten ventajas económicas diferenciales, y por otro, la inteligencia competitiva que, en la misma línea, se dirige a seguir la actividad de laboratorios o fábricas de países o empresas competidoras con el objetivo de conocer sus avances y mejorar la propia competitividad. Un ejemplo serían los laboratorios farmacéuticos en otros países.

Siguiendo con estos conceptos, otros países no anglosajones entienden la inteligencia económica como las actividades del Estado para defender sus intereses económicos en el marco internacional. De ahí que sean los servicios de inteligencia los que lideren estas actividades en dichos países. Este sería el caso de España.

La inteligencia competitiva se dirige, como su propio nombre indica, a mejorar la posición competitiva en los mercados, ya sea de las propias nacio-

[8] MARTRE, Henri. *Intelligence économique et stratégie des entreprises*. La Documentation Française, febrero de 1994.

nes o de las empresas, aunque es en estas donde se ha desarrollado con más profundidad. Y, en realidad, se concentra en tener conocimiento de lo que sucede para mejorar la posición, pues si el conocimiento proporciona un valor diferencial, la inteligencia aporta poder, tal como aseguran Helen Rothberg y Scott Erickson[9]. O dicho de otra manera: la inteligencia competitiva busca lo que se necesita a partir de lo que se conoce.

Sin embargo, estos autores pierden otras perspectivas que, a nuestro parecer, se deberían incluir como elementos esenciales de la inteligencia competitiva o, incluso, estratégica, ya que, para una eficaz toma de decisiones, es indispensable establecer los cuatro elementos del *rombo de inteligencia* mostrados en la figura 1.2: asunciones condicionantes (lo que sabemos que conocemos); conocimiento latente (lo que no sabemos que conocemos); vacíos de información (lo que sabemos que no conocemos), y los puntos ciegos (lo que no sabemos que no conocemos). Así, se puede concluir que las actividades de inteligencia, independientemente del adjetivo que se les dé, han de servir para aportar conocimiento en todos los vértices de lo que nosotros definimos como *rombo de inteligencia* –as-

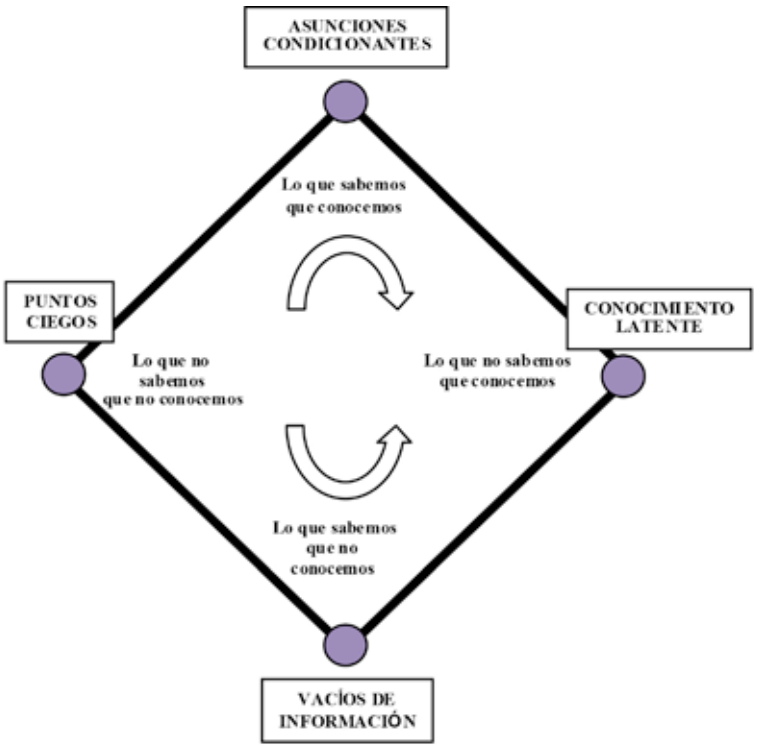

Figura 1.2. Rombo de inteligencia

[9] ROTHBERG, H. y ERICKSON, S. *From knowledge to intelligence: Creating competitive advantage in the next economy.* Butterworth-Heinemann/Elsevier, 2005.

pectos del conocimiento que interactúan y que se interrelacionan unos con otros–; con la circunstancia añadida de que si se unen los puntos verticales, es decir, «lo que sabemos», nos moveríamos en el entorno estratégico de la organización, mientras que horizontalmente, es decir, considerando «lo que no sabemos», tendríamos en esencia el eje de inteligencia. Y trabajando en ambas direcciones daríamos a la inteligencia su carácter estratégico que, en realidad, es lo que marca la diferencia competitiva.

La inteligencia estratégica, por tanto, será la agregación de las anteriores con el objetivo de proporcionar información y conocimiento a fin de facilitar una toma de decisiones de corte estratégico. Teniendo en cuenta que la información puede conducir, en lugar de al conocimiento, a elementos no deseados como son el rumor o el desconcierto, tal como muestra la figura 1.3[10].

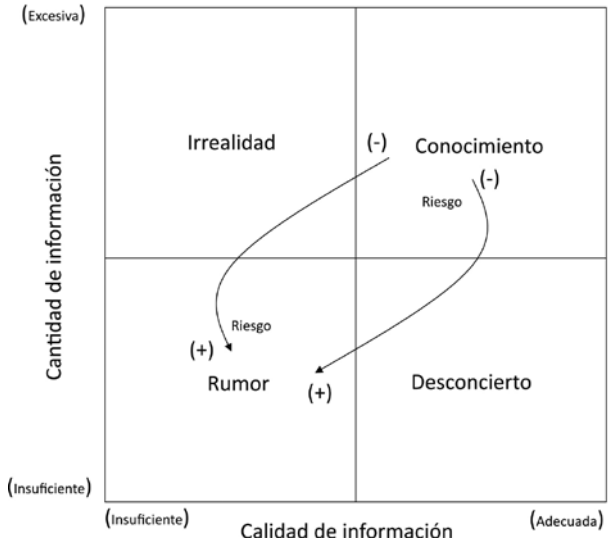

Figura 1.3. Información, rumor y conocimiento

Modelos de inteligencia económica

En lo que sigue utilizaremos indistintamente el concepto de inteligencia económica e inteligencia estratégica, si bien asimilándolos al concepto francés, es decir, a *las estrategias de inteligencia para la toma de decisiones en defensa de los intereses económicos del Estado o de las empresas*. Y es en este contexto donde podemos hacer una somera incursión en la situación en que se encuentran ciertos países de nuestro entorno.

[10] OLIER, E. «La inteligencia estratégica al servicio de la competitividad». *Revista Seguridad Global.* Instituto Choiseul España, verano de 2011.

En todos ellos se podría analizar su situación de acuerdo al posicionamiento que tendrían según el esquema que mostramos en la figura 1.4, que muestra los diferentes niveles de inteligencia de acuerdo con los objetivos a alcanzar y el nivel estratégico de los mismos, estando la inteligencia estratégica en las zonas donde realmente se promueve esta visión. Vayamos, sin embargo, a realizar una somera descripción de los diferentes sistemas considerando los países que están más avanzados: Estados Unidos, Japón, Suecia, Alemania, Francia y China.

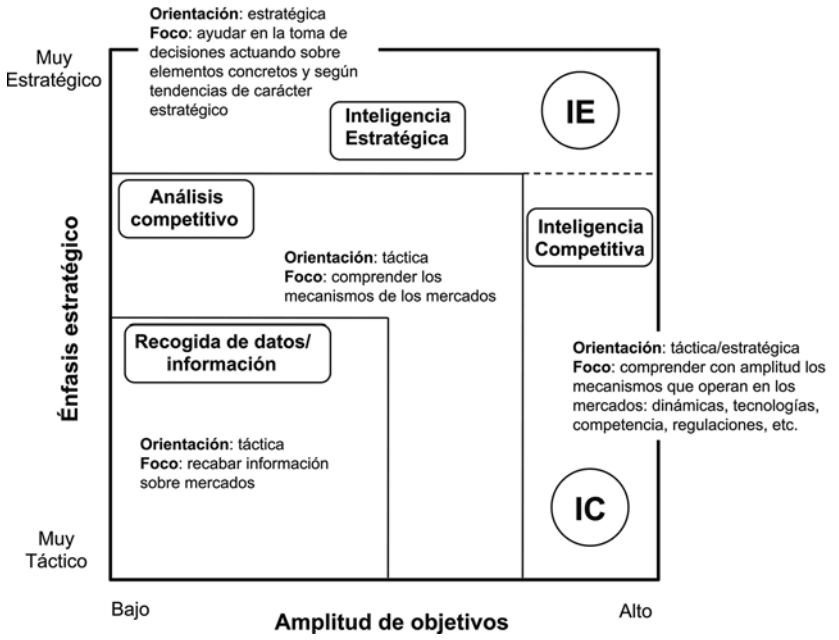

Figura 1.4. Estrategia vs. objetivos de inteligencia económica

En su expansión económica global, Estados Unidos desarrolló una estrategia de dominio basada en cuatro ejes: militar, tecnológica, económica y cultural, estando las dos primeras conectadas de alguna manera, al igual que las dos últimas entre sí. El dominio económico ha sido en lo esencial monetario: con la desaparición de la libra como divisa de referencia en los albores de la Segunda Guerra Mundial, el dólar se impuso de manera determinante en los mercados. Primero con su referencia con el oro, de manera que oro y dólar eran intercambiables pagando 35 dólares por una onza, y después por la primacía de Estados Unidos en los acuerdos de Bretton Woods y en especial en el recién nacido Fondo Monetario Internacional. Y respecto del dominio cultural, tanto el cine de Hollywood como incluso la música rock han sido fuertes instrumentos de *soft power* bien usados por los estadounidenses. Todo ello con un perfecto entramado de inteligencia económica que entrelazaba el Pentágono con otros múltiples actores: las agencias federales que,

aparte de las tradicionales, involucraba, por ejemplo, a la National Sciences Foundation o la Office of Naval Research; potentes *think tanks* e incluso universidades tan prestigiosas como el MIT; empresas de seguridad e inteligencia como Kroll o SRI International; empresas transnacionales, e incluso despachos jurídicos y de influencia (*lobbies*). Todo ello bajo la fórmula de que la «seguridad nacional» se identifica con la «seguridad económica».

Los japoneses, por su parte, como ya hemos indicado, desarrollaron toda la estrategia de inteligencia económica alrededor del Ministerio de Comercio Internacional e Industria (MITI), enmarcado en un concepto de «glocalización» que daba a entender la necesidad de proteger su mercado interno a la vez que se favorecía la expansión comercial internacional, de manera que, como es tradicional, el mercado japonés resultaba muy difícil para los extranjeros a la vez que grandes compañías niponas dominaban los mercados internacionales de la electrónica o del automóvil. Un sistema de inteligencia económica desarrollado en siete líneas estratégicas perfectamente coordinadas de «arriba a abajo» que involucra a empresas y a los servicios gubernamentales:

- Aproximación global y local a los mercados.
- Penetración comercial adaptada al contexto económico y modo de vida de cada país.
- Política de información muy selectiva, en la que participan también las empresas, con un sistema de *reporting* diario.
- Estrategia económica a largo plazo.
- Enfoque integrado y coordinación entre los grandes conglomerados industriales.
- Divulgación selectiva de la información según niveles.
- Programas de formación de jóvenes profesionales en empresas, con especializaciones por países, incluso dominando lenguas extranjeras y entendiendo los hechos culturales locales.

En cuanto a Suecia, es un pequeño país europeo que, sin embargo, comprendió la necesidad de desarrollar un sistema de protección económica para impulsar la creación de grandes empresas multinacionales y, a la vez, desarrollar un sistema educativo muy internacional basado en el conocimiento de, al menos, tres lenguas por alumno –una forma de compensar sus dificultades geoeconómicas–. De esta manera, en 2010 Suecia tenía 30 empresas en el *ranking* de la lista Forbes 2000: Astra Zeneca en biotecnología, Telia Sonera en telecomunicaciones, Ericsson y Nokia en tecnología, Ikea en muebles y otros complementos para el hogar, ABB en energía y bienes de equipo, etc. Algo que no habría sido posible de no haber existido una política y unos sistemas de inteligencia económica capaces de solventar muchas dificultades. Un esquema de «abajo a arriba» contrario al japonés, ya que, en lugar de ser el Estado quien impulsa los criterios y el sistema, son en el caso sueco las empresas y sus sistemas de información los dirigidos a mejorar su posición competitiva.

El sistema alemán responde a las características de su Estado, con la estructura federal del mismo, existiendo una coordinación a tres niveles que se entrelazan: administraciones, entidades financieras e industrias. Es un esquema que ha dado origen a unas alianzas naturales entre las industrias y las entidades financieras, en las que participan los sindicatos como agentes activos en la marcha económica; agentes que son participativos y no reivindicativos ya que encuentran su poder no en los antiguos postulados de la lucha de clases sino siendo interlocutores esenciales en la definición de las políticas económicas. De este modo, al igual que son posibles las alianzas de gobierno entre los partidos que compiten desde posiciones socialdemócratas o cristianodemócratas, también lo son entre sindicatos de diferente signo con empresarios y también con los gobiernos federales, en los que también participan sociedades de consultoría, así como fundaciones de carácter político o cultural. Este esquema lleva a:

- Una concertación permanente entre comunidades económicas diferentes: bancos, grupos industriales, etc.
- Una flexibilidad y aproximación coordinada a diferentes mercados.
- Utilización coordinada de emigrantes alemanes en el extranjero.
- Un principio de búsqueda de los intereses comunes alemanes por encima de las discrepancias, lo que potencia las actividades de inteligencia.

En Francia, la inteligencia económica es una cuestión de Estado. El conocido Informe Carayon, presentado en 2004 por el diputado M. Bernard Carayon ante la Comisión de Finanzas de la Asamblea Nacional bajo el título *Estrategia de Seguridad Económica Nacional*, es una clara muestra de la importancia que para las fuerzas políticas francesas tienen estas técnicas y servicios.

No era la primera vez que el Estado francés se tomaba en serio la puesta en marcha de un sistema nacional de inteligencia económica. Sin embargo, este informe del diputado Carayon tenía alguna diferencia; ya en su inicio, hacía mención de una nueva situación:

Los atentados del 11 de marzo de Madrid —decía— *nos lo han recordado dolorosamente: Europa es un objetivo privilegiado de los terroristas. Si las bombas representan en nuestro subconsciente colectivo una amenaza esencial, el alcance de las amenazas que pesan sobre nuestras sociedades es aún mayor. Después de veinte años, nuestro país ha entrado —sin haber necesariamente tomado conciencia— en la era de la sociedad de la información. Además de la calidad de las personas, la producción de la riqueza nacional reposa hoy en día en la masa de informaciones jurídicas, financieras, comerciales, científicas, técnicas, económicas o industriales. Las amenazas que pesan sobre nuestro entramado productivo también han evolucionado. Son ahora más difusas.*

Y continuaba:

La exacerbación de la competencia internacional transforma las informaciones estratégicas de las empresas en una verdadera cuestión de «guerra económica».

El sistema francés, desde hace muchos años, es un sistema perfectamente diseñado que se adapta según los tiempos y las necesidades, en el que, aparte de las agencias estatales, participan empresas líderes de inteligencia estratégica, así como todo el entramado económico de las Cámaras de Comercio que tratan de defender los intereses comerciales franceses dentro y fuera del país. Es una estructura de «arriba a abajo», si bien más simple que la japonesa; estructura de inteligencia bien imbricada en un contexto de *soft power*, muy potente, desarrollado en toda la geografía de la francofonía: un contexto de 58 estados miembros a los que se suman otros 20 estados observadores. Es una potencia comercial evidente a la que apoyan con un potente esquema de *hard power* proveniente de la capacidad militar francesa.

Terminamos esta reseña con un apunte sobre China, nuevo jugador económico de primera magnitud. Un país, sin embargo, siempre en conflictos internacionales, con denuncias ante la OMC por sus supuestas prácticas ilegales que sistemáticamente denuncian los Estados Unidos e Inglaterra.

Independientemente de estos hechos, China cuenta con un sofisticado y potente esquema de inteligencia económica, estructurado de acuerdo a los ejes siguientes:

- Está enfocado a la búsqueda de información de propiedades intangibles: propiedad intelectual, patentes, etc.
- Está estructurado según redes de ejecutivos de empresas multinacionales chinas que trabajan con grandes corporaciones vendiéndoles tecnologías y servicios.
- Cuenta con una red de funcionarios altamente preparados en ciberseguridad, tanto de defensa como de ataque, en estrecha coordinación con universidades.
- Es un esquema descentralizado, si bien con jerarquías de control perfectamente definidas, con difusas separaciones entre servicios de inteligencia, empresas y estructura de defensa militar.
- Tiene servicios específicos de protección de industrias estratégicas.

Inteligencia estratégica y seguridad económica

Los sistemas de inteligencia y, en especial, de inteligencia estratégica son esenciales en el complejo mundo actual. Sin embargo, en muchos casos, estos sistemas –y las organizaciones que los implementan– suelen poner el foco en la seguridad. Así, se orientan en la mayoría de los

casos al espionaje defensivo o a la protección de instalaciones o servicios que se consideran esenciales, ya sea para el Estado o para las empresas u otras organizaciones. Para ello, se basan en seguir el modelo del ciclo de inteligencia y hacen énfasis en las actividades de análisis como medio para explicitar la información y el conocimiento para la toma de decisiones. De esta manera, se sigue el esquema que se muestra en la figura 1.5, apoyándose en los datos disponibles para alcanzar el conocimiento que facilite las decisiones, todo ello según el ciclo de inteligencia como hemos indicado (figura 1.6).

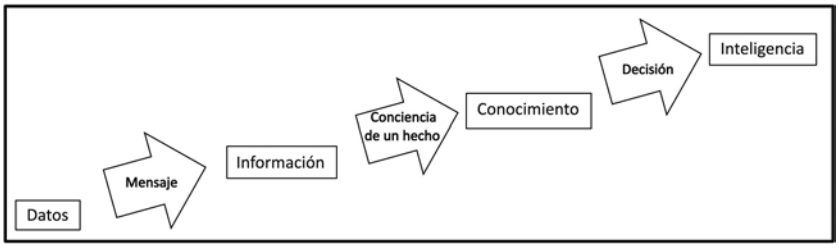

Figura 1.5. Proceso de los datos al conocimiento

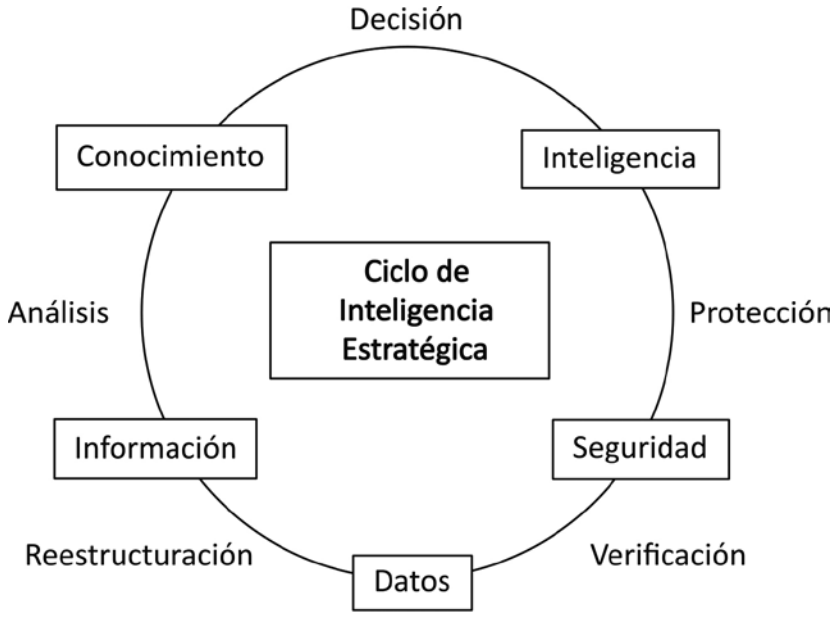

Figura 1.6. El ciclo de inteligencia

Sin embargo, lo que siempre se obvia es que la inteligencia nace de un proceso estratégico: sin estrategia no se puede implantar un modelo de inteligencia económica, ya que, si la inteligencia es entendida como *la capacidad para comprender e interactuar con el entorno a fin de tomar ac-*

ciones que permitan ventajas competitivas, no sería posible abordar este presupuesto sin que exista una estrategia definida y flexible para adaptarse a las variaciones del entorno. Es un proceso que debería tener en cuenta, al menos, los siguientes capítulos:

- Definir la estrategia, incluida la visión y misión de la organización en cuestión.
- Incorporar una capacidad para el razonamiento abstracto y comprensión de las múltiples interacciones que se dan en los entornos complejos, incluida una capacidad de juicio y desarrollo de conocimiento original.
- Tener capacidades para detectar productos sustitutivos o tecnologías disruptivas y comprender los cambios culturales o demográficos.
- Desarrollar una habilidad para anticipar cambios de las condiciones regulatorias o económicas de los operadores del mercado a fin de implantar acciones ofensivas o defensivas.

La inteligencia ha de ser, primero, estratégica y, posteriormente, económica. Luego será competitiva o simplemente reducida al análisis para la adquisición del conocimiento con las técnicas y tecnologías que proceda. Técnicas que, a nivel estatal, tendrán diferentes modos según las terminologías al uso: SIGINT (inteligencia de señales), proceso según el cual se interceptan las comunicaciones transmitidas electrónicamente a través de radares, señales de radio o sistemas de control de armas; HUMINT, conocida como inteligencia humana, que se concreta en obtener información a partir de personas; MASINT, es decir, el uso de la inteligencia para establecer informes respecto de objetivos; GEOINT, recolección de imágenes, incluidas las que se obtienen desde satélites; OSINT, inteligencia que obtiene información desde fuentes abiertas al público en general, muy especialmente desde los medios de información e Internet, y, finalmente, IMINT, o creación de imágenes a través de sistemas electrónicos tales como radares o sistemas basados en óptica electrónica, etc.

La inteligencia estratégica, por tanto, se dirigirá a establecer los intereses estratégicos que se hayan definido, así como a definir los objetivos que se pretenden conseguir. Objetivos que en un contexto geoeconómico irían dirigidos a[11]:

- Realizar análisis de previsiones económicas en entornos competitivos complejos, así como entender los escenarios políticos y geoestratégicos que intervienen.
- Conocer con exactitud las situaciones legales y regulatorias, y hacer valoraciones sobre los intereses de política exterior y de las relaciones internacionales que las puedan condicionar.

[11] OLIER, Eduardo. *Geoeconomía: las claves de la economía global*. Pearson-FT-Prentice Hall, 2011.

- Desarrollar programas estratégicos y hacer el seguimiento y control sobre el cumplimiento de objetivos.
- Hacer detallados análisis sobre predicciones económicas y comerciales en momentos de cambios de mercado o situaciones políticas nuevas.
- Hacer valoraciones sobre amenazas y riesgos, así como establecer los oportunos criterios y sistemas de seguridad, tanto desde el punto de vista físico como desde la Red.

Es un esquema que en su conjunto no puede separarse del análisis del entorno, lo que ha de considerar todos los elementos en juego en un análisis STEEP: las consideraciones políticas y geoestratégicas, el entorno regional, los retos estratégicos, etc., tal como muestra la metodología de la figura 1.7[12].

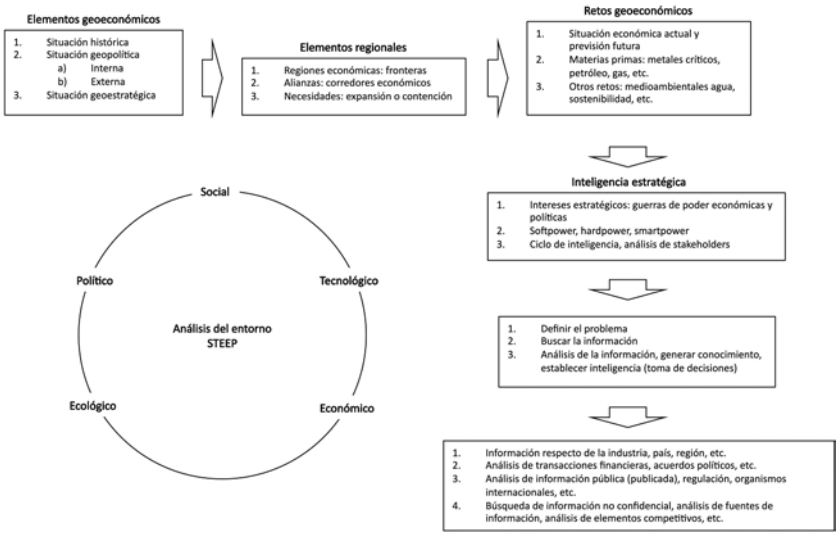

Figura 1.7. Metodología de inteligencia estratégica

Y es en este contexto donde se entroncan las actividades de inteligencia con la seguridad, en este caso económica. Este sería, por ejemplo, el caso de Suecia. Un pequeño país como hemos indicado, si bien líder en sus prácticas de inteligencia estratégica y competitiva, ya que Suecia no considera la inteligencia económica como un servicio de categoría militar sino como el medio para asegurar la paz y la prosperidad económica. Por ello, son las empresas multinacionales suecas, juntamente con los bancos y el Gobierno (y los servicios diplomáticos en el exterior), quienes comparten la información y establecen las estrategias para fortalecer la posición competitiva del país. Al tiempo que las universidades, como por

[12] OLIER, Eduardo. *Ibíd.*

ejemplo la Universidad de Lund, desarrollan programas de doctorado en este tipo de disciplinas y algunas pequeñas y medianas empresas desarrollan tecnologías disruptivas, siempre compartiendo la información como estrategia de seguridad y competitividad económica. Es una metodología que demuestra el éxito de combinar inteligencia y seguridad económica.

Influencia como un elemento esencial de la inteligencia económica

Lo anterior, sin embargo, no es suficiente para desarrollar un eficaz programa de inteligencia económica o estratégica. Hoy en día, todos los grandes países y las corporaciones más importantes ponen en juego sus capacidades de influencia, que van mucho más allá de lo que se entiende por *lobby.* En este sentido, la influencia enmarcada en el contexto de la inteligencia estratégica tiene en lo esencial tres componentes que nunca han de implantarse por separado.

La influencia estratégica, por tanto, independientemente de los objetivos que pretenda, se basa en definir una estrategia y se concreta en la puesta en marcha de acciones coordinadas según un programa basado en el logro de unos objetivos; objetivos que nunca han de verse, si el caso a tratar es complejo, como una serie de acciones a corto plazo, ya que la estrategia no lo es. De ahí la diferencia entre *lobby,* diplomacia corporativa e influencia estratégica, que se puede expresar de la siguiente forma:

- *Lobby,* que se concreta en acciones puntuales a muy corto plazo, y que nunca debe usarse.
- Diplomacia corporativa, que se concreta en acciones para llevar a cabo un programa de influencia concreto y utiliza el *lobby* y la comunicación interesada con el objetivo de desinformar.
- Influencia estratégica, que se explicita con un programa estratégico de largo plazo y que se implementa mediante acciones coordinadas de *lobbying* (si fuera preciso), *social learning* (acciones de influencia socio-cultural), *advocacy* (acciones de influencia público-política), desarrollo de redes de influencia, alianzas, políticas de comunicación (y de contracomunicación o contrainteligencia) y uso masivo de las redes sociales (bajo una estrategia definida).

De esta manera debería, entenderse la influencia como *la combinación de un conjunto de modos de actuación, ejercidos de manera directa o indirecta, abierta o cerrada, en relación con personas, colectivos, organizaciones, y/o estados a fin de obtener un mayor crédito, lograr ascendiente y, finalmente, orientar las decisiones en el sentido deseado*[13].

[13] REVEL, Claude. *Francia, ¿un país bajo influencia?* Vuiver, 2012.

La influencia es, por tanto, una *estrategia de poder* que utiliza diversos mecanismos entre los cuales es primordial una estrategia de comunicación, ya que la comunicación ayuda a transmitir mensajes siempre basados en la argumentación, muy lejos por tanto del simple «dar noticias». Esto es porque la influencia es antes que nada una cuestión de contenido: para influenciar hay que tener un mensaje, y sobre todo un mensaje coherente.

Y es aquí donde entran las diferentes técnicas y procedimientos. Influenciar es parte de la estrategia de inteligencia; no es una actividad fuera del método. Así, por ejemplo, se deberán poner en marcha mecanismos tales como la diplomacia económica; es decir, ese conjunto de actividades encaminadas a lograr posiciones favorables en el mundo económico internacional, donde aparecen los complejos entramados de inversiones, mercados, instituciones, protección y seguridad económica, y todo el complejo contexto de la economía global actual. Un entorno que no se puede dejar a la improvisación, sino que precisa de acciones estructuradas, constantes y con objetivos de medio y largo plazo. También resultan imprescindibles las técnicas de *social learning,* que se dirigen a lograr una influencia socio-cultural y desarrollar todo un programa de *soft power* que encuentra, por ejemplo, en el campo universitario, las ONG e incluso las redes sociales un campo evidente de aplicación. *Social learning* que no solo está pensada como método para los estados, ya que importantes compañías como Microsoft, Google, Twitter, etc., los utilizan profusamente, en especial con técnicas enfocadas al *marketing,* lo que ha dado origen a un nuevo concepto como es el *social marketing* y la aparición de los comunicadores de la red: los *community managers*.

Se trata, como decimos, de una estrategia de poder. Es decir, de una capacidad para «dominar» a otros mediante la habilidad para influir sobre sus conductas y sentimientos, lo que se traduce, en el campo de la inteligencia económica, en una manera «blanda» de imponer una estrategia dirigida a la consecución de unos objetivos de dominio comercial o económico, y en la capacidad también de defenderse ante los «ataques» de otros competidores. Es, en definitiva, una sofisticada aplicación del *soft power* y, dado el caso, del *smart power* o del *hard power*, según el criterio de Joseph Nye[14] que conecta liderazgo con poder según estas tres acepciones. A continuación lo desglosamos:

- Liderazgo basado en *soft power*; que transmite valores en tres niveles:
  - Visón política: atractiva a los seguidores y efectiva respecto a ideales y capacidades.
  - Comunicación: persuasiva, tanto para los cercanos como para los distantes, en símbolos y mensajes.

[14] http://www.hks.harvard.edu/netgov/files/talks/docs/11_06_06_seminar_Nye_HP_SP_Leadership.pdf.

  - Emocional: desde el punto de vista personal, autoconfianza y autocontrol, y respecto de otros gestionando con carisma las relaciones.
- Liderazgo basado en *hard power*, que se orienta a un liderazgo transaccional con:
  - Capacidad organizativa: gestionando las recompensas, sistemas de información y círculos de influencia externos e internos, tanto burocráticos como institucionales.
  - Destreza política: intimidación, pactos, compra y habilidad.
- Liderazgo basado en *smart power*, que será una combinación de los anteriores, muy fundamentado en inteligencia emocional para comprender la evolución del entorno (que requerirá amplias capacidades políticas) y sacar partido anticipándose a las tendencias previsibles, a la vez que se ajusta el estilo al contexto y las necesidades de los seguidores.

Inteligencia económica y ciberseguridad

El mundo económico actual no se entiende sin las tecnologías y el desarrollo de Internet. Es el entorno donde se da una verdadera y real globalización económica o, por decirlo mejor, financiera. Es aquí donde los movimientos de capitales o las operaciones financieras se realizan en tiempo real, moviendo divisas y operaciones financieras de todo tipo de un lugar a otro del planeta.

Sin embargo, la Red no es solo el entorno virtual de lo económico; es también el entorno virtual de lo delictivo, donde se pueden dar ataques contra infraestructuras críticas o donde se pueden sustraer patentes o simplemente robar en cuentas bancarias poco o nada protegidas.

Por dar alguna referencia, baste indicar que un estudio realizado en 2011 sobre la situación en el Reino Unido[15] reflejaba que las pérdidas económicas ocasionadas por el cibercrimen habían alcanzado el año anterior la enorme cifra de 27.000 millones de libras. Los casos iban desde el espionaje industrial al robo de patentes, sustracción de ofertas comerciales en concursos internacionales, operaciones de adquisición o venta de empresas, robo de diseños industriales, campañas de *marketing* y un largo etcétera de información empresarialmente valiosa. Según este estudio, las empresas de servicios informáticos fueron las más atacadas, con pérdidas que llegaban a los 2.500 millones de libras, a las que se-

[15] *The Cost of Cybercrime. A Detica Report in partnership with the Office of Cyber Security and Information Assurance in the Cabinet Office*. Febrero de 2011. http://www.detica.com/uploads/press_releases/THE_COST_OF_CYBER_CRIME_SUMMARY_FINAL_14_February_2011.pdf.

guían los servicios financieros, con 2.300 millones, y las empresas electrónicas, con 1.700 millones.

La realidad es que no se conoce con exactitud el coste económico de las pérdidas ocasionadas por el espionaje desde la Red. Un antiguo estudio preparado para el Congreso estadounidense en 2003[16] elevaba la cifra entonces a los 226.000 millones de dólares en todo el mundo, y añadía que las pérdidas por ataques desde la Red a empresas cotizadas podrían llegar al 5% de su valor en los siguientes días de realizada la intrusión. Se trata de todo un despliegue que se concreta en variadas prácticas, todas ellas punibles, como por ejemplo:

- Ataques cibernéticos a información sensible de países. Como fue el caso del virus *Stuxnet* que impidió la puesta en marcha de la central nuclear iraní en su día.
- Robo de información por parte de empleados. Como pudo ser el del soldado Bradley Manning y la filtración de datos a la página *Wikileaks*.
- Ataques contra navegadores como medio para acceder a los sistemas de sus usuarios.
- Robo de archivos y de bases de datos, incluidos los sistemas de *phishing*, *carding* o *skimming* bancarios y otras técnicas similares.
- Seguridad en la nube. A la preocupación por la seguridad del ciberespacio «clásico» se añaden todos los sistemas que se sitúan en los servicios de *cloud computing.*
- Riesgos en teléfonos inteligentes y tabletas.
- Ataques a redes corporativas.

Más recientemente, en enero de 2012, la prestigiosa revista Wired[17] publicaba una asombrosa noticia respecto de la dimensión de lo que allí se llamaba «cibercrimen». La noticia hacía referencia a una conferencia impartida en julio de 2011 en el American Enterprise Institute en Washington por el general Keith Alexander, director de la Agencia de Seguridad Nacional y para el extranjero de la U. S. Cyber Command, que se encarga de proteger al país de ataques informáticos. El general alertaba de que los ataques informáticos causaban «la mayor transferencia de riqueza de la historia», y daba números de estadísticas de compañías de seguridad informática como Symantec Corp., que aseguraba que el robo de propiedad intelectual en compañías norteamericanas tenía un perjuicio económico de 250.000 millones de dólares anuales y estimaba que, a nivel global, ese coste podría alcanzar el billón de dólares, casi el tamaño del PIB español, por lo que urgía al Congreso norteamericano a que Estados Unidos desarrollara una estrategia activa y con suficientes

[16] CASHELL, B., JACKSON, W. D., JICKLING, M. y WEBEL, B. *The economic impact of cyber-attacks*. *CRS Report for Congress.* Government and Finance Division, abril de 2004. http://www.cisco.com/warp/public/779/govtaffairs/images/CRS_Cyber_Attacks.pdf.

[17] http://www.wired.com/threatlevel/2012/08/cybercrime-trillion/all/.

medios para asegurar un programa de defensa digital en Estados Unidos. También se aludía a otro informe de la firma de seguridad digital McAfee Inc.[18], informe que, desde luego, pone en evidencia los peligros que para la economía tienen las actividades delictivas desde la Red.

De nuevo, se apuntaba a China como uno de los orígenes más temidos de estos ataques, llegándose a hablar de un Pearl Harbor digital que podría paralizar el país entero, y se citaba a la agencia Bloomberg que afirmaba que un grupo de *hackers* chinos, conocidos como *Byzantine Candor*, había presuntamente robado información clasificada de una veintena de organizaciones, incluida la reputada firma Halliburton Inc.

Esta circunstancia movió al Ministerio de Defensa español recientemente a crear por iniciativa del ministro el Mando Conjunto de Ciberdefensa de las Fuerzas Armadas, MCCD, amenaza que otros países menos desarrollados, como por ejemplo Colombia, llevan tiempo tomándose en serio, y que hoy son muy reales. Fue en este país donde se tomó la decisión de darle al Ministerio de Defensa el liderazgo de todas las actividades relacionadas con la defensa del ciberespacio, creando bajo su mando el COLCERT (Equipo de Respuesta a Emergencias Informáticas de Colombia) en 2009[19].

Es un escenario que afecta a los intereses económicos de cualquier país o incluso empresa y que ha de tenerse en cuenta en cualquier contexto que pretenda desarrollar una estrategia coherente de inteligencia económica.

El objetivo del presente Cuaderno

Por primera vez, el Instituto Español de Estudios Estratégicos aborda la problemática de la inteligencia económica. El título de este Cuaderno, además, no deja dudas sobre su propósito: *La inteligencia económica en un mundo globalizado*. Son la globalización y los problemas geoeconómicos que ahí se dan los que reclaman una atención especial sobre este asunto; un tema, por otra parte, que no es ajeno a las necesidades de la defensa nacional de cualquier Estado. La inteligencia económica no es solo un tema de los servicios de inteligencia, ni tampoco de los servicios diplomáticos desplazados fuera de las fronteras; es un asunto que, como referimos al inicio de este artículo, se entronca en la estrategia geoeconómica de cualquier país y, por tanto, establece un nuevo escenario

[18] *Unsecured economies: Protecting vital information. http://www.mcafee.com/us/resources/reports/rp-unsecured-economies-report.pdf.*

[19] http://www.mindefensa.gov.co/irj/go/km/docs/Mindefensa/Documentos/descargas/estudios%20sectoriales/Notas%20de%20Investigacion/Ciberseguridad%20y%20ciberdefensa.pdf.

de conflictos donde la economía se posiciona como el escenario de la confrontación.

Sin embargo, y aunque el tema de la inteligencia económica es muy amplio, en este primer Cuaderno se pone en perspectiva toda la problemática, contando, como podrá encontrar el lector, autores de gran cualificación profesional en el tema que nos ocupa.

Se abre por tanto este Cuaderno con una visión general del problema, enfocándolo hacia el elemento más complejo, que es la inteligencia estratégica. El profesor Díaz Fernández pone en perspectiva la evolución histórica de la inteligencia estratégica, haciendo hincapié en la situación actual, muy especialmente en el nuevo contexto surgido después de los ataques del 11-S a las Torres Gemelas en Nueva York.

El profesor Harbulot, ya citado en estas páginas, director de l'École de Guerre Économique y reconocido experto internacional en inteligencia económica, certifica de manera muy completa los conflictos económicos, sus porqués y su contexto. En un capítulo denominado *Estudio de la guerra económica y las problemáticas relacionadas,* esclarece con maestría esta imbricación; circunstancia que no deja únicamente en el espacio económico, sino que la enmarca también en el ideológico, aspecto geoeconómico clave ya que lo cultural y lo ideológico son piezas esenciales en los movimientos de dominio e influencia. Se trata de un estudio profundo y muy completo de todo el contexto de guerra económica que da la justificación autorizada para que las Fuerzas Armadas se tomen muy en serio esta nueva dimensión de los conflictos, no armados pero determinantes, que se dan en la globalización.

Con estas perspectivas, enmarcando la inteligencia económica, se tratan a continuación tres aspectos esenciales. El primero, quizás olvidado en muchas ocasiones, se refiere al papel que el derecho ha de jugar en estos nuevos escenarios. Es imprescindible que, al igual que sucede en los conflictos armados, la guerra económica tenga sus reglas. El profesor González Cussac pone el derecho en «valor» en el contexto de la inteligencia económica. Lo que implica —según sus palabras— *desarrollar normas de autoprotección y cooperación, además de una normativa susceptible de ofrecer una mayor capacidad de competir en igualdad de condiciones con los demás países*, atendiendo a lo que González Cussac define como una *guerra de cuarta generación*. Interesante y novedoso concepto muy a tener en cuenta.

Con este panorama, más enfocado en lo jurídico, se aborda la problemática de la inteligencia competitiva. *La inteligencia para competir: nuevo paradigma en la dirección estratégica de las organizaciones en un mundo globalizado* es el título del capítulo del profesor Fernando Palop. Dando un repaso al estado del arte, su significación y lo que se hace en otros entornos, el profesor Palop aborda también el tema de la influencia, ya

referido anteriormente en esta introducción como un instrumento esencial en la práctica de la inteligencia económica. Influencia que entronca con la seguridad, ya que como bien plantea el profesor Palop, influir no solo es una actividad de corte ofensivo sino muy esencialmente de actitud defensiva en múltiples ocasiones.

Se cierra este Cuaderno con la contribución del embajador Henning Wegener. Su conocimiento de las problemáticas que se dan en el *cuarto espacio*, pone en contexto la ciberseguridad y también el nuevo concepto de «ciberpaz».

Creemos que este número que el lector tiene a la vista, siendo un primer paso en la dirección de mejor comprender el contexto de la inteligencia económica, cumple los objetivos marcados: dar una perspectiva global sobre esta problemática esencial en el mundo actual.

Capítulo I

EL PAPEL DE LA INTELIGENCIA ESTRATÉGICA EN EL MUNDO ACTUAL

Antonio M. Díaz Fernández

Resumen

El objetivo de este capítulo es reflexionar sobre qué debemos entender por inteligencia estratégica a principios del siglo xxi. Creadas durante la Guerra Fría, las estructuras de inteligencia deben ir más allá de evitar sorpresas estratégicas y proporcionar un producto diferente a los decisores políticos. Generar un verdadero conocimiento del entorno e, incluso, intentar su modificación son tareas que requieren ahora de los servicios de inteligencia. Deben monitorizar el entorno sin caer en la falacia de que la tecnología puede hacerlo sin decirle adónde y qué debe mirar; esto supondría un error esencial en la construcción de un nuevo modelo de inteligencia que tendrá a la inteligencia económica como uno de los elementos centrales que simbolizan cómo será la lucha entre naciones y corporaciones globales a inicios del siglo xxi.

Palabras clave

Inteligencia, estrategia, planificación, sorpresa estratégica.

Abstract

The aim of this chapter is to explore about what is meant by strategic intelligence in the early twenty-first century. Created during the Cold War, decision-makers intelligence needs were faced by intelligence structures focused on avoiding strategic surprises. Generate a real knowledge of the global scenario and even try its modification is a task that is now required to the intelligence agencies. Monitoring the environment without falling into the fallacy that technology can do by itself without the assistance of the policy maker who must tell them where and what to look would be a fundamental error in the construction of a new model of intelligence. This new model will have the economic intelligence as one of its key elements and it will represent the struggle between nations and global corporations at the beginning of this century.

Key words

Intelligence, strategy, planning, strategic surprise.

Introducción

Espero que el lector que se inicia en la lectura de este apartado del *Cuaderno de Estrategia* venga pertrechado previamente de una definición propia de inteligencia estratégica. Si la inteligencia se basa en la alerta previa, esta creo que honestamente debe ser la primera de ellas. Como reflexiona Heidenrich[1], si bien todos usamos el término 'inteligencia estratégica' con gran prodigalidad, nos veríamos en un no menor apuro si tuviéramos que dar una definición más o menos afinada de la misma. Probablemente, tras una breve reflexión diríamos que tiene que ver con la toma de decisiones y con la estrategia, para pasar a definirla por su opuesto, esto es, no es la inteligencia que se dirige a resolver los problemas del ahora, no es la inteligencia táctica, sino que es la que va más allá, la que se centra en dar soporte a la estrategia nacional de un país.

Me permitirá también el lector que no entre en la habitual relación acumulativa de definiciones de la voz inteligencia que tan bien han realizado ya otros autores en el pasado[2], porque el reto de este capítulo es doble: por una parte, definir qué es inteligencia estratégica, para posteriormente reflexionar sobre cuál será su futuro y, en este sentido, qué lugar ha de ocupar la inteligencia económica. Por esto, simplemente asumamos grosso modo, a manera de basamento, que información es equivalente a dato y que inteligencia es un producto elaborado que permite tomar decisiones con la menor incertidumbre posible. A partir de aquí, se iniciará esta reflexión sobre la inteligencia estratégica.

No obstante, sí creo necesario partir de alguna reflexión previa sobre qué son la estrategia, la planificación y la gestión. Los Estados son organizaciones complejas que gestionan innumerables recursos con un propósito y un destino, el más básico de todos ellos, el de garantizar la seguridad y el suministro de alimentos a sus ciudadanos. Pero incluso para garantizar estas funciones básicas hay que contar con una estrategia, puesto que los recursos son limitados y nos encontraremos a otras organizaciones (Estados o no) en continua competencia por los mismos.

Parafraseando al soluble gato Cheshire en su diálogo con Alicia, si no sabemos adónde queremos llevar nuestra organización da igual qué camino (estrategia) emprendamos. Por eso entiendo que la estrategia habrá de reflejar la reflexión y la acción de una organización sobre su entorno. Dicho esto, una organización o un país puede planificar su futuro sin te-

[1] HEIDENRICH, John G. *The state of strategic intelligence The intelligence community's neglect of strategic intelligence*. 2007. https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/vol51no2/the-state-of-strategic-intelligence.html.

[2] RICHELSON, Jeffrey. *A century of spies*. Oxford: Oxford University Press, 1997; LOWENTHAL, Mark. *Intelligence: From secrets to policy*, Washington DC: CQ Press, 2006.

ner necesariamente que comprometerse con una planificación formal; incluso aunque se generen planes no tienen por qué activarse y convertirse en el camino a seguir.

Pero una vez asumida una estrategia, la gestión de la misma –que es lo que hace un Estado– no habría de ser más que poner a la organización al servicio de la estrategia; por tanto, la gestión en sí misma no constituye una estrategia. Lesourne[3] sostenía que «la decisión estratégica es bien aquella que crea una irreversibilidad para el conjunto de la organización, bien aquella que anticipa una evolución de su entorno susceptible de provocar tal irreversibilidad». Si bien no creo que esta asimilación sea inmediata, como recoge la teoría de las organizaciones, sí es cierto que el abanico de opciones disponibles tras una elección se limita sucesivamente. De ahí que la idea de la «gestión estratégica» sea casi un pleonasmo y la de «estrategia prospectiva», si no un oxímoron, al menos un término contradictorio aunque compatible ya que algunas prospectivas serán estratégicas y otras no. Pero no estoy hablando de decisiones estratégicas sino de decisiones adoptadas considerando que disponemos de inteligencia estratégica porque, sin inteligencia, la estrategia es un mero juego abstracto de equipos azules y equipos rojos en un tablero más o menos extenso.

Estamos tan prestos a etiquetar con un nuevo nombre un concepto o fenómeno – como si al encontrarle un nombre tuviera adherida todas sus cualidades para comprenderlo – que no prestamos la necesaria atención a su definición, interactuación y funcionamiento. Por eso considero abusivo el empleo del término «estratégico» como adjetivo para calificar cualquier concepto, idea, proceso, relación o producto que sea relativamente importante. Si bien esto es casi imposible de soslayar, lo que sí podemos hacer es evitar su asociación inmediata con decisiones de carácter irreversible que una organización adopte. En el fondo de esta suspicacia lo que subyace es un cierto recelo motivado por la dificultad que me produce el cualificar la voz «inteligencia» con aditamentos que ya le son propios, que son inherentes a ella; porque, si no es proactiva, ¿qué es si no la inteligencia? El problema con «estratégico», como indica Heidenrich[4], es que es difícil abandonar décadas de rutina durante la Guerra Fría empleando abusivamente el concepto estratégico, y qué decir de su directa asimilación con «largo plazo».

Los siempre socorridos documentos oficiales tampoco nos arrojan luz sobre qué es la inteligencia estratégica. De las pocas definiciones oficiales que podemos encontrar, la del Pentágono nos dice que sería «la inteligencia que se necesita para la formulación de la estrategia, polí-

[3] LESOURNE, Jacques. «Plaidoyer pour une recherche en prospective», *Futuribles*, n.º 137, noviembre de 1989.

[4] HEIDENRICH, *opus cit*.

tica y planes y operaciones militares a nivel nacional y sobre el campo de batalla»[5]. Sin embargo, esta definición vive huérfana en el panorama gubernamental estadounidense ya que ni tan siquiera los documentos básicos para los consumidores de inteligencia norteamericanos incluyen una definición de este concepto[6]. Además, alberga en sí una esencia muy cercana a la que nos pudiéramos haber encontrado durante la Guerra Fría, una etapa con unos actores y unas necesidades muy diferentes a las de inicios del siglo xxi.

Tampoco un texto que, a priori, debería recogerla, *ONCIX: Foreign spies stealing US economic secrets in cyberspace: Report to Congress on foreign economic collection and industrial espionage (2009-2011),* de octubre de 2011, encuentra un hueco para definirla[7]. Incluso, un académico como Jan Goldman[8], que dedicó una de sus obras a precisar la terminología empleada en el estudio de la inteligencia, no aporta claridad en su diccionario *Words of intelligence*. Su voz *strategic intelligence* nos dice que es la inteligencia que se necesita para la formulación de planes políticos y nacionales a nivel nacional e internacional y que sus componentes incluirían aspectos tales como datos biográficos, económicos, sociológicos, de transporte, telecomunicaciones, geografía, política e inteligencia científica y técnica; pero no aporta un valor añadido que pueda ser relevante para el debate que pretendo establecer.

Un caso representativo de los cambios en la última década lo representa el, en su momento, celebérrimo *Libro blanco de la defensa* de 2000 de España[9], que nos incorporó al grupo de países que desarrollaba este tipo de reflexiones. En nuestro bautizo en la planificación publicitada de la defensa, podemos ver cómo se hace referencia 217 veces a las voces «estratégico», «estratégica» y «estrategia». De aquí se colegiría que encontraríamos una intensa y extensa referencia a la inteligencia como herramienta imprescindible para hacer frente al desarrollo de aquella; sin embargo, la voz «inteligencia» no aparece en todo el texto y tenemos que conformarnos con las 66 veces en las que aparece el vocablo «información». Sin duda, el uso de la voz «inteligencia» no era habitual hace más de una década, aún muy marcada por el halo de secretismo de la guerra

5 Voz «tactical intelligence». Joint Publication 1-02 (JP 1-02), *Dictionary of military and associated terms,* Washington: Departmento de Defensa, 12 de abril de 2001, pp. 526. http://www.dtic.mil/doctrine/new_pubs/jp2_01.pdf.

6 Ni *U. S. national intelligence: An overview,* 2011, http://www.dni.gov/files/documents/IC_Consumers_Guide_2011.pdf, ni la más antigua *CIA: A consumer´s guide to intelligence*, de 1999, la recogen.

7 http://www.dni.gov/files/documents/Newsroom/Reports%20and%20Pubs/20111103_report_fecie.pdf.

8 GOLDMAN, Jan. *Words of intelligence: A dictionary*. Oxford: The Scarecrow Press, 2006.

9 *Libro blanco de la defensa.* *http://www.defensa.gob.es/politica/seguridad-defensa/marcolegal/*.

fía, pero no deja de ser llamativa su inexistencia y, por ende, cómo pensaban nuestros *policy makers* que debía llevarse a cabo la estrategia.

Quizá una pista nos la aporta la *National Intelligence Strategy* de la Casa Blanca de 2010[10], en cuya única referencia, de forma indirecta, nos sugiere que «la inteligencia estratégica [...] informa a las decisiones ejecutivas ya que esta es un apoyo de las decisiones en seguridad interior, estatal, local y gobiernos tribales, nuestras tropas y misiones nacionales esenciales. Estamos trabajando para mejorar la integración de la comunidad de inteligencia, al tiempo que fortalecemos las capacidades de los miembros de nuestra comunidad de inteligencia. Estamos fortaleciendo nuestra colaboración con servicios de inteligencia extranjeros y manteniendo fuertes lazos con nuestros aliados más próximos». Pero sobre todo porque incluye un elemento importante cuando sostiene que «la seguridad y la prosperidad de nuestro país dependen de la calidad de la inteligencia que recopilamos y el análisis que producimos, nuestra habilidad para evaluar y compartir a tiempo esta información y nuestra habilidad para contrarrestar las amenazas».

Incluye dos aspectos como la seguridad y la prosperidad. Sobre el primero, podríamos asumir un cierto impacto del carácter preventivo atribuido desde hace décadas a la inteligencia, esto es, evitar la sorpresa estratégica que bien ha analizado Posner[11], pero el segundo siempre ha tenido un peso menor, bastante menor. No obstante, podemos encontrar documentos oficiales de la década de los setenta en los cuales se asume que «nuestra política exterior se puede beneficiar si se realiza un examen más cuidadoso y analítico de la realidad de otros estados»[12]. Y es precisamente en inteligencia económica donde la evolución tiene más sentido, si bien no de forma pacífica como veremos más adelante. Este documento desclasificado de 1976 sobre inteligencia económica al que me refiero expresa que es necesaria una revisión sistemática y periódica de las necesidades de los consumidores de alto nivel lo que muestra que, a nivel estratégico y de inteligencia económica, estamos hablando de necesidades de los consumidores «civiles» de alto nivel, esto es, del Gobierno.

Ya anticipo que para mí, la clave del presente y futuro de la inteligencia estratégica está en el debate que mantenían Kent y Kendall a finales de

[10] *National intelligence strategy.* White House, 2010, p. 15. http://www.whitehouse.gov/sites/default/files/rss_viewer/national_security_strategy.pdf.

[11] POSNER, Richard A. *Preventing surprise attacks: Intelligence in the wake of 9/11*. Nueva York: Rowman & Littlefield, 2005.

[12] «E. Richardson a W. Simon». Referencia: «Intelligence support for economic policy-making» (5 páginas; localización: *Frank Zarb personal papers*; fecha: 12/20/76; material desclasificado). http://www.whitehouse.gov/sites/default/files/rss_viewer/national_security_strategy.pdf.

los años cuarenta del siglo pasado. Kendall[13] sostenía que la inteligencia estratégica consistía en «ayudar a los líderes políticamente responsables a alcanzar sus objetivos en política exterior identificando los elementos susceptibles de influencia norteamericana». Al mismo tiempo, Sherman Kent era acusado por Willmoore Kendall de tener una «preocupación compulsiva con la predicción, con la eliminación de la sorpresa de los asuntos exteriores». Y bajo esta y otras acusaciones, lo que residía eran diferentes visiones de ese nuevo elemento de la política como era la inteligencia.

En esencia, Kendall veía la inteligencia como un apoyo a los decisores políticos para conseguir influir en el devenir de los acontecimientos, ayudándoles a comprender los factores operativos en los cuales Estados Unidos podía tener un cierto impacto. Y de esto es de lo que hablamos a principios del siglo xxi si queremos hablar de algo que sea inteligencia estratégica: no de evitar sorpresas estratégicas sino de comprender el entorno para anticiparnos a él y, en alguna medida, configurarlo para que nuestra política exterior –y su dimensión económica– puedan desarrollarse y generar prosperidad para nuestro país.

El otro gran teórico de la época, Washington Platt[14], se centró en un modelo de inteligencia militar de nivel estratégico, no de carácter táctico, por lo que no nos ayuda en nuestra disquisición actual, a pesar de haber sido su pensamiento muy relevante. Por su parte, Harry Ransom[15] se preguntaba en 1980 si era precisamente la inteligencia estratégica la que guiaba la política exterior de los Estados Unidos, una pregunta que solo recientemente podría comenzar a tener respuesta positiva.

Un haz de luz en el papel de la inteligencia estratégica se encontró en la *National performance review* de 1993[16], coordinada por el vicepresidente Al Gore, donde el por entonces director de la CIA, John Deutch, afirmó que «los esfuerzos en inteligencia de los Estados Unidos deben proporcionar a los decisores la información necesaria sobre la cual basar sus decisiones respecto al desarrollo de la defensa exterior, política económica y protección de los intereses nacionales de los Estados Unidos frente a agresiones extranjeras». Coincido con Swenson y Lemozy[17] en que la

[13] KENDALL, Willmoore. «The function of intelligence», *World politics*, vol. 1, n.º 4, julio de 1949, pp. 542-552.

[14] PLATT, Washington. *Strategic intelligence production: Basic principles*, Nueva York: Praeger, 1957.

[15] RANSOM, Harry Howe. «Being intelligent about secret intelligence agencies», *The American Political Science Review,* vol. 74, n.º 1 (marzo de 1980), pp. 141-148.

[16] *National Performance Review*, 1993, http://www.fas.org/irp/offdocs/npr_sep93/index.html.

[17] SWENSON, Russell G. y LEMOZY, Susana C. «Democratización de la función de inteligencia. El nexo de la cultura nacional y la inteligencia estratégica», *National Defense Intelligence College*, Washington DC, 2009.

cualificación «estratégica» anexada a «inteligencia» disuelve el concepto más comprehensivo –por amplio y difuso– de «inteligencia para la política extranjera», pero no puedo compartir con ellos que la inteligencia estratégica excluya o suprima la contribución del cuerpo diplomático en este proceso, si bien su rol y estructuración habrían, evidentemente, de modificarse como ya hacía el informe del embajador Melitón Cardona al que me referiré más adelante.

Si asumimos que la inteligencia estratégica ayuda a proveer de contexto, desarrolla los intereses nacionales y delimita nuestros problemas y objetivos; el hecho es que los actuales y veloces ciclos de los acontecimientos políticos provocan que el consumidor político requiera de un producto de inteligencia que no es propio de la inteligencia estratégica, esto es, productos de largo recorrido y profundidad más que alertas puntuales ante potenciales sorpresas estratégicas. Esto es, los recurrentes ciclos provocan que no haya espacio para el pensamiento estratégico y que analistas y consumidores estén abocados a la cuantificación de un producto con poco espacio para la reflexión. Así, en mi opinión, a la inteligencia estratégica se le habría de pedir una presencia mucho más intensa en el inicio de las políticas, en la fijación de la agenda y en la priorización de objetivos, es decir, en la fase de diseño, pero no restringirla a la de implementación porque entonces la emplearemos principalmente como una alerta temprana ante sorpresas estratégicas.

Esta queja se recoge en el *Informe de la Comisión sobre las Armas de Destrucción Masiva* en Irak de 2005, que indicaba que «los gestores y analistas de la comunidad de inteligencia han expresado en reiteradas ocasiones su frustración por su incapacidad para disponer de tiempo para la investigación y el pensamiento a largo plazo. Este problema se refuerza con el actual sistema de incentivos para los analistas, en el cual estos son, a menudo, recompensados por el número de informes que producen más que por el sustancial conocimiento o profundidad de su producción»[18]. Un episodio más reciente lo tenemos con la denominada «primavera árabe», cuyo desconcierto creado a las cancillerías solo es comprensible por la ausencia de una inteligencia estratégica de calidad, de un verdadero conocimiento sobre sus raíces y sus condicionantes, no sobre el mañana, ni siquiera sobre el pasado mañana sino sobre la esencia de un fenómeno que nos ayudase a comprender su aparición y su probable evolución.

En consecuencia, cuando hablamos del estado, y por ende, del futuro de la inteligencia estratégica no tiene razón alguna el centrarnos en la de carácter económico ni en la militar; la inteligencia estratégica permanece

[18] Commission on the Intelligence. *Capabilities of the United States regarding weapons of mass destruction, Report to the President,* cap. 8: «Analysis». Washington DC: Government Printing Office, 2005, pp. 175. http://www.gpo.gov/fdsys/pkg/GPO-WMD/pdf/GPO-WMD.pdf.

por encima de estas dimensiones porque más que un tipo de inteligencia como la de señales, de fuentes abiertas, o técnica, entiendo que es una evolución de la misma. Quizá mejor será pasar a comprender cómo ha evolucionado y cuáles son sus elementos para comprender su posible futuro; y entender a qué nos estamos refiriendo e intentar conceptualizar la inteligencia estratégica y proponerle un futuro sigue pasando por reflexionar sobre la «Trinidad de Kent»: la inteligencia como organización, producto y proceso, pero antes es importante comentar, aunque sea someramente, el escenario en el que la inteligencia estratégica y su dimensión económica deberán producirse.

Ya no hay damas azules ni rojas en el nuevo tablero de juego

No se puede dudar de cuáles son las amenazas actuales, pero tampoco de que no lo eran hace una década y tampoco de que quizá ya no lo sean en la próxima, aunque fuera de forma mitigada. Y el hecho cierto es que los mercados –en esa etérea denominación– sí lo son ahora. En las democracias modernas, como vio Barry Buzan[19], los conflictos militares carecen de lógica por lo que las poliarquías no plantean enfrentarse militarmente entre ellas. Sin embargo, sí tiene toda la racionalidad el presionar sobre tus socios comerciales, suministradores de materias primas, apostar contra tu deuda pública y conseguir que tus empresas estén a precio de saldo en la Bolsa y puedan ser compradas por capital extranjero; lo que sin duda, a buen seguro, Clausewitz consideraría una suerte de «guerra por otros medios».

La Estrategia Europea de Seguridad (EES)[20] adoptada por el Consejo Europeo en diciembre de 2003 hacía de la responsabilidad del proyecto europeo, en relación a la seguridad global, el eje de una estrategia de seguridad para Europa. Señalaba que «el contexto de seguridad a que ha dado lugar el fin de la Guerra Fría se caracteriza por una apertura cada vez mayor de las fronteras que vincula indisolublemente los aspectos internos y externos de la seguridad». La EES aboga por el compromiso preventivo, por una estrategia de multilateralismo eficaz y por la extensión del imperio de la ley internacional. Esta Estrategia –que es más un *policy paper*– versa sobre cómo hacer más capaz a la Unión Europea apostando por un enfoque «ascendente», es decir, el interés lo fija en cómo aumentar la seguridad de los seres humanos individualmente considerados en diferentes partes del mundo. En el informe se desarrollan tanto un conjunto de principios, sobre los cuales debería basarse la política de seguridad de Europa, como las capacidades que necesitará para realizar una

[19] BUZAN, Barry. *Security: A new framework for analysis*. Boulder, London: Lynne Rienner Publishers, 1998.

[20] *Una Europa segura en un mundo mejor. Estrategia europea de seguridad*, 12 de diciembre de 2003. http://www.consilium.europa.eu/uedocs/cmsUpload/031208ESSIIES.pdf.

contribución creíble a la seguridad global, de la cual depende su propia seguridad, pero poco espacio se dedica a los instrumentos para hacer efectiva esa contribución.

La Unión Europea saca al terreno de juego el concepto de «seguridad humana» –a la que apela en esta EES– y que no deja de ser otro concepto de seguridad; una narrativa que encapsula los objetivos y métodos de una política exterior y de seguridad altamente diversificada y que se centra en diferentes actores y va dirigida a variadas audiencias que, en definitiva, sería un concepto demasiado difuso y débil. Sin embargo, quienes desde mediados de los años noventa defienden la seguridad humana sostienen que no es posible la unilateralidad, y entienden la necesidad de desarrollar nuevos instrumentos, así como la persistencia de las dimensiones interior y exterior. Con este concepto de seguridad, si la Unión Europea quiere proseguir por él, será muy necesario realizar reflexiones intensas sobre cómo emplear la inteligencia, ya no solo o ni siquiera la estratégica sin otras como la policial-criminal, en pleno desarrollo.

Pero, en definitiva, a nivel europeo no contamos con un concepto operativo como el de *homeland security* que los estadounidenses están consolidando; por esto, desde Europa se siguen empleando otros como seguridad interna, seguridad pública o seguridad doméstica. El profundizar en este concepto no debe llevarnos a cerrarlo sin entenderlo de una forma comprensiva; de ahí que algunos hablen de un «espacio de protección» de forma amplia. Así es como se percibe en la Unión Europea y cuál es su enfoque de seguridad y el escenario sobre el cual proteger a los ciudadanos europeos.

Estaríamos por tanto abordando una seguridad de carácter integral, definible como una lógica de acción proactiva y defensiva, que trasciende ampliamente la clásica dimensión de la seguridad nacional, destacando la necesidad de incidir –para garantizar dicha seguridad– sobre los sistemas energéticos, sanitarios, alimentarios, medioambientales, de infraestructuras, tecnológicos, militares y de la seguridad interior, y debiendo ser promovida coordinadamente desde los instrumentos de gestión pública en el ámbito político-institucional, técnico, diplomático y de inteligencia para el desarrollo de estrategias preventivas, así como de respuestas ejecutivas de variado alcance, con el objetivo último de garantizar la satisfacción de las necesidades básicas de las personas y la seguridad de los consumidores, amparar el respeto de los derechos humanos y proteger el ejercicio de los derechos democráticos.

Por tanto, no estamos únicamente en un enfoque nacional sino global. La mayoría de amenazas que afrontan las potencias son globales en sus orígenes y en sus consecuencias. Por este motivo, la cooperación global se ha claramente regionalizado. El informe *A human security doctrine for*

Europe de 2004[21] sostiene que la seguridad de los ciudadanos europeos no puede separarse de la seguridad humana de cualquier lugar del mundo, y que la Unión Europea tiene por tanto un interés crucial en el desarrollo de capacidades que contribuyan a la seguridad humana mundial. Sostienen que los europeos no pueden estar seguros mientras que millones de personas viven en una inseguridad intolerable. Donde la gente vive con anarquía, pobreza, ideologías exclusivistas y violencia cotidiana, existe un terreno fértil para las redes criminales y el terrorismo y desde estas regiones en conflicto se exportan o transportan drogas y armas a la Unión Europea.

No es, por tanto, difícil concluir que abordamos necesidades de seguridad mucho más amplias que a las que debía informar la inteligencia de apenas hace dos décadas. A través de los diferentes libros blancos e informes sobre escenarios de seguridad, varios estados, al igual que la Unión Europea, han venido reflexionando sobre su futuro. En una suerte de autoanálisis, estos documentos nos permiten ver cómo son percibidas las amenazas desde la Unión y los estados miembros. Por ejemplo, en marzo de 2008, el Reino Unido hace pública la nueva Estrategia de Seguridad Nacional[22], en la que, con un carácter integral, integra una versión revisada de informes e iniciativas anteriores. Considera esta nueva iniciativa como novedosa y bienvenida en el enfoque británico hacia la seguridad internacional, pero duda de si efectivamente supera las visiones tradicionales de determinados aspectos de la seguridad internacional y sus consecuencias para la seguridad interior del país.

Esta Estrategia de Seguridad Nacional del Reino Unido, con el sugerente título de *Security in an interdependent world,* establece que la amenaza de la Guerra Fría ha sido sustituida por una serie de diversos pero interconectados riesgos y amenazas, a la sazón: el terrorismo internacional, armas de destrucción masiva, conflictos en estados fallidos, pandemias y crimen organizado transnacional. Estos estarían interconectados por una serie de factores subyacentes, incluidos el cambio climático, la lucha por las fuentes de energía, pobreza y débil gobernanza de algunos estados, cambios demográficos y globalización, lo que no se separa de otros informes nacionales.

La gran mayoría de las potencias han desarrollado sus escenarios estratégicos de seguridad, que alcanzan una media de 20-25 años. Un repaso a los mismos indica que todos parten de la seguridad integral pero

[21] *A human security doctrine for Europe: The Barcelona report of the Study Group on Europe's security capabilities*, 15 de septiembre de 2004, http://www2.lse.ac.uk/internationalDevelopment/research/CSHS/humanSecurity/barcelonaReport.pdf.

[22] *A strong Britain in an age of uncertainty: The national security strategy*, 2008. http://www.direct.gov.uk/prod_consum_dg/groups/dg_digitalassets/@dg/@en/documents/digitalasset/dg_191639.pdf.

les cuesta apartarse en el diseño y en los mecanismos de la tradicional amenaza militar, si bien está comenzando a realizarse. La Directiva de Defensa Nacional de 2012 se redacta de forma autista como bien analiza Arteaga[23], quien continúa reflexionando sobre la evolución que se ha producido en los últimos años cuando el escaso planeamiento se centraba en los esfuerzos de defensa, entendidos como puramente militares. Esto cambia ya que, eliminada la pura amenaza militar, aparece una plétora de ellas.

La Estrategia Española de Seguridad de 2011 se une a esta visión de riesgos específicos pero también de objetivos generales cuando indica que «tenemos también intereses estratégicos que atañen a la consecución de un entorno pacífico y seguro: la consolidación y el buen funcionamiento de la Unión Europea, la instauración de un orden internacional estable y justo, de paz, seguridad y respeto a los derechos humanos, la preservación de la libertad de intercambios y comunicaciones y unas relaciones constructivas con nuestra vecindad»[24].

Esta Estrategia Española de Seguridad habla de unos potenciadores del riesgo (disfunciones de la globalización, desequilibrios demográficos, pobreza y desigualdad, cambio climático, peligros tecnológicos y las ideologías radicales y no democráticas) que coinciden con otros informes como *La seguridad interior: España 2020,* publicado tiempo antes[25]. A su vez, desarrolla las amenazas a las que ha de hacer frente España, tales como: conflictos armados, terrorismo, crimen organizado, inseguridad económica y financiera, vulnerabilidad energética, proliferación de armas de destrucción masiva, ciberamenazas, flujos migratorios no controlados, emergencias y catástrofes en infraestructuras, suministros y servicios críticos. Pero estos objetivos «nacionales» coinciden con los internacionales, como el del Reflexion Group for the Future of the European Union, presidido por Felipe González en 2010, por lo que no estamos ante una miríada de nuevas amenazas sino, en algún caso, un ascenso o descenso de las mismas en las agendas de seguridad estatales, en caso de que existieran como tal.

Más allá de los relevantes casos de las grandes potencias, que cuentan con un plus de énfasis por los intereses globales con los que cuen-

[23] ARTEAGA, Félix. «La Directiva de Defensa Nacional 1/2012: tiempos de cambio para cambiar a tiempo», ARI 58/2012, del Real Instituto Elcano. http://www.realinstitutoelcano.org/wps/portal/rielcano/contenido?WCM_GLOBAL_CONTEXT=/elcano/elcano_es/zonas_es/ari58-2012.

[24] *Estrategia española de seguridad: una responsabilidad de todos*, Gobierno de España, pp. 16. http://www.lamoncloa.gob.es/nr/rdonlyres/d0d9a8eb-17d0-45a5-adff-46a8af4c2931/0/estrategiaespanoladeseguridad.pdf.

[25] JAIME JIMÉNEZ, Óscar y DÍAZ FERNÁNDEZ, Antonio M. *La seguridad interior: España 2020*. Madrid: Fundación Alternativas, 2009, http://www.falternativas.org/la-fundacion/documentos/libros-e-informes/la-seguridad-integral-espana-2020.

tan, un necesario repaso a los libros blancos y doctrinas nacionales de seguridad desde 2001 nos muestra una coincidencia en cuatro grandes amenazas: i) terrorismo, ii) crimen organizado, iii) proliferación de armas de destrucción masiva y iv) problemas energéticos-climáticos. Es cierto que, en buena medida, todos ellos intentan evitar el enfoque basado en términos exclusivamente defensivomilitares y casi enteramente en relación a las amenazas directas al Estado. En esta dirección, como indica López Espinosa[26], está emergiendo un nuevo concepto de seguridad nacional como un concepto superior que desplazaría del centro de atención a otros como el de defensa nacional o seguridad interior. No se crea una nueva política ni se amplían otras de carácter sectorial, sino que –como rasgo principal– todas las existentes se adaptan a las orientaciones de la nueva estrategia en un proceso de ajuste de instrumentos, competencias y recursos estatales y, entre ellas, estaría el elemento económico.

Pero en este evidente cambio de escenario nacional, internacional y, por lo cercano, el europeo, el tenor de los últimos documentos de la Unión Europea no parece que asigne un nuevo papel a la inteligencia. Así, en el Programa de Estocolmo[27], vemos cómo el Consejo Europeo insta al Consejo y a la Comisión a «la reflexión sobre un planteamiento anticipatorio y basado en inteligencia»; sin duda es positivo, pero es esencialmente la misma aproximación. El *Proyecto de estrategia de seguridad interior* de la Unión Europea de 2010[28] indicaba que «nuestra Estrategia, pues, debe subrayar la prevención y la anticipación, sobre la base de un enfoque proactivo y de inteligencia, así como tendente a la obtención de pruebas para proceder a encausar judicialmente. Solo es posible llevar a cabo una acción legal con éxito si se dispone de toda la información necesaria».

A esta reflexión, que amplía el escenario de la seguridad a nivel global, se le une la del National Intelligence Council, que ha actualizado sus anteriores previsiones generando las que tienen como horizonte el 2030[29]. Las tres diferencias con respecto al informe anterior serían la aparición con fuerza de tres variables clave: i) la economía globalizada, ii) la demografía y iii) los nuevos actores (China e India). Plantea además el informe cuatro posibles escenarios que serían más relevantes para la potencia mundial que para el resto de países, a la sazón:

---

[26] LÓPEZ ESPINOSA, María de los Ángeles. «Inteligencia y terrorismo internacional. Un panorama de cambios», *La inteligencia, factor clave frente al terrorismo internacional. Cuadernos de Estrategia,* n.º 141, Instituto Español de Estudios Estratégicos, Ministerio de Defensa, 2009, pp. 197-239.

[27] *Programa de Estocolmo: una Europa abierta y segura que sirva y proteja al ciudadano*, 2010. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2010:115:0001:0038:es:PDF.

[28] *Proyecto de Estrategia de Seguridad Interior de la Unión Europea: hacia un modelo europeo de seguridad*, 8 de marzo de 2010, http://register.consilium.europa.eu/pdf/es/10/st07/st07120.es10.pdf.

[29] *Global trends 2030: Alternative worlds,* http://www.dni.gov/index.php/about/organization/national-intelligence-council-global-trends.

Escenario I: Supone un mundo en el cual los nuevos poderes suplantan a Occidente como líderes mundiales (escasez en la abundancia, era pospetróleo, geopolítica de la energía, agua y alimentos y cambio climático).

Escenario II: «Sorpresa» o el impacto de la falta de atención al cambio climático mundial (conflictos en potencia, disminución de la inestabilidad, armas nucleares, nuevos conflictos sobre recursos, terrorismo, Afganistán, Pakistán e Irak, etc.).

Escenario III: Auge intenso de las potencias emergentes (BRICS), entrándose en una disputa por los recursos vitales como fuente de conflicto (preparación a los cambios, multipolaridad sin multilateralismo, mundo de redes, etc.).

Escenario IV: Ampliación de la política, que ya no será siempre de ámbito local; así, el establecimiento del medio ambiente en la agenda internacional eclipsa a los Gobiernos.

Y lo más adecuado sería finalizar este esbozo del escenario en el que debería moverse la inteligencia estratégica con el informe francés de 2008. Pocas bagatelas conceptuales tiene este documento que es, en mi opinión, el más agudo en sus planteamientos «estratégicos» de los de su clase. En el *Défense et Sécurité Nationale: Le Livre Blanc*[30], se indica que «el desarrollo del conocimiento y la capacidad de anticipación es nuestra primera línea de defensa. [...] Las batallas del siglo xxi tendrán lugar en el campo de la información, el conocimiento y las personas y las sociedades. [...] Los políticos deben tener acceso a todos los datos que servirán de base a sus decisiones y evaluar las situaciones con plena soberanía. [Debe asumirse que] los poderes públicos están haciendo todo lo posible para el análisis de los riesgos para un futuro y tratar de evitarlos preparando los medios para hacerles frente». Se aproxima por tanto más al papel que entiendo debe asignársele a la inteligencia estratégica a principios de siglo.

La Trinidad de Kent rediseñada

Organización: Matrix ya ha nacido

Las organizaciones de inteligencia han debido sufrir un proceso de evolución desde el primer sistema de inteligencia con el que ha contado el mundo: el modelo de la Guerra Fría que, por otra parte, fue muy similar en ambos lados del Muro. A partir de entonces, y hasta el momento ac-

[30] *Défense et Sécurité nationale: Le livre blanc 2008*, p. 66. http://www.ladocumentationfrancaise.fr/var/storage/rapports-publics/084000341/0000.pdf.

tual, todos los modelos de inteligencia se han basado en la conjugación, con diferentes papeles y cometidos, de las Fuerzas Armadas, la Policía y los servicios de inteligencia si bien, como es obvio, con un papel central de estos últimos como estructura más especializada. Más en concreto, las principales características que, en mi opinión[31], han dibujado el modelo de inteligencia que nace durante la Guerra Fría –y su específico entendimiento de «estratégico»– han sido: i) práctica de la desinformación, ii) gran uso de la tecnología para el control de los ciudadanos, iii) primacía de la efectividad frente a los derechos y libertades ciudadanas, iv) presencia de los servicios de inteligencia en todos los ámbitos de la vida, y v) realización de acciones encubiertas.

Este no era claramente un modelo estructural para los retos que vendrían tras el final de la Guerra Fría. La caída del Muro supuso una modificación objetiva en las necesidades de inteligencia y la volatilización del bloque del Este generó dos dinámicas diferentes. Una de ellas quería entender que era tiempo de recoger los «dividendos de la paz» y destinar los fondos invertidos en seguridad e inteligencia a otros cometidos, propugnando incluso la desaparición de los Ejércitos. La otra aglutinaba a aquellos que vieron la necesidad de adaptar los sistemas existentes a una nueva realidad llena de amenazas que obligatoriamente debían reemplazar a las que expiraban. Diversas comisiones y grupos de trabajo, esencialmente en los Estados Unidos, se constituyeron para discutir y abordar la naciente situación. En el resto de países no se reflexionó sobre el tema más allá de unas mínimas aportaciones de algunos centros de pensamiento y la voluntariosa firma de limitados acuerdos de cooperación entre servicios de inteligencia de diferentes países para controlar la proliferación de armas de destrucción masiva y los maletines nucleares que podían salir de la antigua Unión Soviética.

Durante la década que va de 1989 a 1999, los servicios de inteligencia fueron sobrecargados con una multitud de nuevos e incipientes cometidos: verificación de tratados de reducción de armamento, investigación de genocidios, protección de redes de comunicación, blanqueo de dinero, crimen organizado, terrorismo... Esta atribución tan desmesurada de objetivos a los servicios de inteligencia no fue premeditada sino que se produjo residualmente por necesidad ante la falta de estructuras alternativas a las que asignárselos. Estructuralmente, no se había producido la reflexión necesaria para que los servicios pudieran acometer estas misiones con las garantías necesarias, llevándolas a una asombrosa saturación de cometidos al tiempo que malgastaban la oportunidad de ir ajustándose al escenario en ciernes. Esto les comportó a los servicios de inteligencia un retraso de diez años en su adaptación para la lucha

[31] Para una análisis más extenso, véase DÍAZ FERNÁNDEZ, Antonio M. «La adaptación de los servicios de inteligencia al terrorismo internacional», ARI 52/2006, Real Instituto Elcano, 2006.

antiterrorista: esta década fue el momento clave para que la inteligencia se hubiera podido adaptar a las necesidades del siglo xxi. Pero tras esta tardanza ya no había posibilidad de reflexionar sobre si era más adecuado emprender un proceso evolutivo o revolucionario de la inteligencia; ahora el tiempo de reacción era demasiado exiguo como para plantearse revoluciones cuyo coste de transición solo puede ser aceptable cuando hay un escenario de cierta tranquilidad por delante y no había, como en este caso, individuos dispuestos a inmolarse en cualquier momento en pleno corazón de nuestras ciudades.

Esta falta de un modelo actualizado de inteligencia condujo al 11 de septiembre de 2001, que representa trágicamente el final del breve y aparente período de estabilidad nacido con la caída del Muro. El nuevo modelo de inteligencia que debía haber reemplazado al de la guerra fría y lidiar con las amenazas correspondientes a su época aún no estaba listo, ni tampoco se había abierto la ventana de oportunidad para que se pudiera implementar alguno de los diseñados por congresistas y las propias agencias. En gran medida, la ausencia se debía a que se había trabajado en él de forma tan parsimoniosa que el Estado acabó por ser incapaz de anticiparse al nuevo tipo de amenazas.

Pero todo esto componía –y compone– un lamento sobre el cual la urgencia del momento ya no permitía detenerse. Lo cierto y evidente es que, ante la ausencia de un modelo finalizado, los estados tuvieron que acudir a un modelo refugio, aquel que conocían de la Guerra Fría, y aplicarle un elemento incrementalista con la esperanza de que eso sirviera para adaptarlo a la nueva situación. Tanto el mayor número de recursos como de capacidades tecnológicas aparecidas desde que este modelo estaba plenamente en vigor durante las décadas anteriores habrían de ser ese elemento incrementalista que algunos consideraron suficiente para actualizar el modelo. En resumidas cuentas, esto significaba que volvían a aparecer, pero con mayor intensidad, todas las características del modelo de la Guerra Fría; un modelo que escasamente sirvió para las necesidades de los políticos de aquellos años y que a duras penas, por no decir por mera casualidad, podría afrontar el combate antiterrorista en ciernes.

Este modelo de urgencia aplicado tras los ataques contra los Estados Unidos estaría caracterizado, en mi opinión, por los siguientes elementos: i) práctica de la desinformación, ii) amplio uso de la tecnología para el control de los ciudadanos, iii) primacía de la efectividad frente a los derechos y libertades ciudadanas, iv) presencia de los servicios de inteligencia en todos los ámbitos de la vida, y v) realización de acciones encubiertas. Reformas estructurales dirigidas a que mejorase el *connecting the dots,* que el informe del 11-S señalaba como uno de los errores de la comunidad de inteligencia; esto es, los datos los tenía el Estado pero guerras internas y falta de coordinación impidieron su adecuado tratamiento

y, en consecuencia, produjeron los fallos que condujeron a los atentados. Pero, de nuevo, la idea subyacente es mejorar la inteligencia para que evite sorpresas, un Pearl Harbor físico o un Pearl Harbor cibernético como será el próximo que vivamos dentro de algunos años.

Es cierto que algunas reflexiones, incluidas las del informe del 11-S, avanzaron la importancia de comprender mejor el mundo de inicios de siglo para poder organizar la inteligencia de una manera más adecuada. También es cierto que en el inmediato período tras los atentados del 11-S se produjeron algunas reformas en países como Austria, Holanda, España y también estados latinoamericanos y del bloque del Este; sin embargo, sus dinámicas y motivaciones son diferentes a las generadas por aquellos atentados, correspondiendo a contingencias nacionales propias. En unos casos, como Holanda, se volvió atrás sobre decisiones tomadas años atrás y se llevó a desmantelar la inteligencia exterior; en España había que ajustar y regular con rango de ley un sistema generado durante la transición a la democracia sin un modelo previo y por el ajuste mutuo de burocracias; los estados latinoamericanos buscan coordinar las agencias de seguridad interior y exterior bajo la cobertura de un sistema que habitualmente tiene el nombre de Sistema Nacional de Inteligencia, una estructura que ya estableció Portugal en 1986 pero con similar y escaso resultado.

En la Europa del Este se modernizaban y profesionalizaban sus estructuras de inteligencia tras la culminación de sus procesos de democratización y reproducen también esta estructura de Sistema Nacional de Inteligencia; pero tienen una particularidad ya que conservan poderes policiales al igual que sucedió en Colombia hasta 2012, y como se planteó establecer la República Dominicana. Además, algunos estados aprovecharon que tenían que hacer sus propias reformas para introducir algunos elementos novedosos en sus organigramas, como flexibilizar sus unidades y reducir la amplitud vertical de la estructura del servicio para así afrontar entornos más mutables.

Es esta falta de adaptación la que explica los fallos del 11-S y que en cadena desembocan en los atentados de Bali, Madrid y Londres, poniendo de relieve la falta de modelo alternativo y la imperiosa necesidad de reformular los sistemas de inteligencia. Las estrategias de prevención se convierten así en la base de la seguridad en el siglo xxi, en el campo abonado para los servicios de inteligencia y, sin duda alguna, en la base de los sistemas de seguridad en el futuro. Es, por lo tanto, un hecho que los servicios de inteligencia debían salir de sus inercias y convertirse en estructuras más adaptadas a las mutables necesidades de seguridad que trae el siglo xxi, digamos, ¿más estratégicas?

Reorganizar la comunidad de inteligencia para que pueda adaptarse más rápidamente requiere no solo de cambios en los organigramas. En los Estados Unidos, desde el establecimiento en 1947 del sistema de inteli-

gencia, diecinueve comisiones, comités y paneles habían intentado modificar el papel de la autoridad centralizada del director de la comunidad de inteligencia, e incluso se propuso la creación de un director de inteligencia. La propuesta Turner de 1985 ya planteaba la creación de un director de la comunidad de inteligencia; desde entonces, lo sucedido han sido las apuestas más o menos tímidas por esta opción. De hecho, las reformas propuestas por Boren-McCurdy en 1992 no consiguieron que fueran aprobadas por el rechazo del Departamento de Defensa; esto es algo que aprendieron los miembros de la posterior comisión Aspin-Brown, quienes evitaron proponerlo con tanta contundencia y así suavizaron este aspecto proponiendo la creación de dos vicedirectores que auxiliaran al director de la comunidad de inteligencia en su tarea. Finalmente, la Comisión del 11-S recomendó la creación de una nueva autoridad que coordinase a todas las agencias, creándose la figura del director nacional de inteligencia. En definitiva, muchos de los debates que están teniendo lugar en la actualidad son un golpe de péndulo más de propuestas que llevaban más de treinta años produciéndose.

Aun consiguiendo introducir importantes avances en la construcción de la comunidad de inteligencia, el problema es que tanto la Comisión del 11-S como las reflexiones y estudios llevados a cabo en diferentes países han basado la adopción de medidas en evitar otro atentado similar al del 11-S pero no en adaptar las estructuras al nuevo tipo de amenazas como, por ejemplo, el crimen organizado. Sin duda, esta focalización de la inteligencia en el contraterrorismo ha distraído atención y esfuerzos de otras amenazas no menos graves y sí de largo plazo como el crimen organizado. Hay que comprender que las reformas de la inteligencia tienen como acicate la lucha contraterrorista pero no pueden tenerlo como único objetivo[32].

Una potencial pérdida de presupuesto y de influencia al abrir la labor de la inteligencia a otras agencias de una más amplia comunidad de inteligencia explica en gran medida este veto del Departamento de Defensa a cualquier cambio. Lo que es muy llamativo es que los grandes fallos en inteligencia militar durante la primera guerra del golfo llevaran a políticos y militares norteamericanos a querer transferir los recursos de la inteligencia estratégica a la táctica aplicada al combate; esto es, no reorientar sino más inteligencia táctica. Hay que comprender que en esos años, el Pentágono se había hecho con el grueso del presupuesto total en inteligencia, algo a lo que no quería renunciar y que condicionaría posteriormente la concepción, por ejemplo, del contraterrorismo como un problema militar. La influencia del Departamento de Defensa en las modificaciones del sistema de inteligencia que pudieran emprenderse no deben dudarse.

[32] DÍAZ FERNÁNDEZ, Antonio M., REVENGA, Miguel y JAIME, Óscar. *Cooperación europea en inteligencia: nuevas preguntas, nuevas respuestas*. Pamplona: Aranzadi, 2009.

La principal reflexión sobre la necesaria evolución de la comunidad de inteligencia se produjo en el seno de la Comisión Aspin-Brown (1994-96); un trabajo muy ambicioso y de gran interés que abarcó todas aquellas dimensiones que debían modificarse o adaptarse en los sistemas de inteligencia. Sin embargo, la falta de liderazgo político y sobre todo de nuevo una gran oposición del Departamento de Defensa impidieron su aplicación. No obstante, Holshek[33] realiza una interpretación voluntarista de la evolución de la comunidad de inteligencia norteamericana cuando afirma:

> *El sistema de seguridad nacional de los Estados Unidos adoptado finalmente ha sido más previsor, colaborativo, ágil e innovador. Es más capaz de combinar todos los elementos del poder nacional y la integración de la inteligencia, la toma de decisiones adecuadas y bien fundamentadas, y tomar una acción decisiva yendo más allá de nivel de todo el Gobierno, llegando a nivel de todo el país. Los líderes norteamericanos habían aprendido a pensar globalmente y actuar localmente – estratégica más que operativamente–. Priorizaron las inversiones en oportunidades y fortalezas por encima de las amenazas al tiempo que reducían los costes y riesgos. Situaron el desarrollo económico y la diplomacia por delante de los aspectos de la defensa. Se hicieron eco de los cambios en la comunidad económica, las agencias aprendieron y se hicieron más reducidas, menos redundantes, más adaptables y más dispuestas a trabajar en grupo y en red. Los recursos estaban en primer lugar dirigidos por los objetivos estratégicos, desechando la mentalidad despilfarradora. El sistema se hizo más inclusivo debido a la cooperación de los sectores público y privado y fortaleciendo el soft power de Estados Unidos.*

Las organizaciones tienen que mirar hacia fuera para ser más competitivas[34], y esta lógica supone que el escenario ha de ser una parte de nuestra actividad que está más allá de nuestra organización pero que debemos conocer e intentar modelar. Como sostiene Baumard[35], la inteligencia empresarial está más estructurada en los países occidentales mientras que, por ejemplo, en Japón se encuentra más a nivel de cultura organizativa.

---

33 HOLSHEK, Christopher. *America's first quarter millennium: Envisioning a transformed national security system in 2026*, Project on National Security Reform (PNSR), 2009, http://0183896.netsolhost.com/site/wp-content/uploads/2011/12/pnsr_americas_first_quarter_millennium.pdf.

34 ARROYO VARELA, Silvia. *Inteligencia competitiva: una herramienta en la estrategia empresarial*, Madrid: Ediciones Pirámide, 2005, p. 106.

35 BAUMARD, Philippe. «From noticing to 'sense-making': The use of intelligence in strategizing», *The International Journal of Intelligence and Counterintelligence*, vol. 7, n.º 1, 1994, pp. 29-73.

No podemos concebir en la actualidad a las organizaciones –ni las comunidades de inteligencia– sin su dimensión tecnológica, un peso que ya Mintzberg[36] advirtió que se iría incrementando. Tecnología es, no obstante, un vocablo erróneamente empleado ya que entendemos por tecnología lo que no es más que parte de ella y, en nuestro caso, Internet y el *software* de proceso de datos en sus más variadas dimensiones. El ser humano siempre ha sido tecnológico y esto es lo que le ha permitido dar solución a los problemas a los que se ha enfrentado; tecnología lo fue tanto el fuego o la rueda como un misil balístico intercontinental. Además, tengamos en cuenta que la tecnología siempre ha sido elemento esencial en la inteligencia. Así, durante las guerras mundiales, conocer qué buques cruzaban el Estrecho y su posible cargamento era un elemento de seguridad esencial, del mismo modo que fueron un éxito los análisis de Sherman Kent que impresionaron a los mandos militares al diseñar unos escenarios espectaculares fruto de los textos disponibles en la Biblioteca del Congreso y que había sabido buscar y procesar, como recoge Davis[37].

Algunos autores[38] sostienen que la estrategia ha estado muy centrada en el proceso mecánico y que debe evolucionar a un modelo más centrado en la persona. Sin dejar de ser cierto, las tecnologías han incrementado las posibilidades de evitar ser sorprendidos «estratégicamente», pero también suponen un incremento del potencial de las amenazas sobre nosotros y nuestros intereses. Avanzar hacia una inteligencia estratégica pasa, además de por comprender los escenarios, por tener claro cómo realizar el procesamiento y la fusión de los datos disponibles de las múltiples e ingentes fuentes de información. La necesaria fusión de información que genera se referiría, por tanto, a los medios, no al fin, y ha de incluir toda una serie de técnicas como redes de sensores para la gestión de datos, recopilación de datos con la interactuación máquina-persona, optimización organizativa o el análisis de datos a gran volumen.

Esta fusión de información a alto nivel es en gran parte intuitiva para los seres humanos pero es un formidable reto para los sistemas informáticos. No entraré en aspectos como los análisis *bayesianos,* los metadatos o el uso de ontologías, pues ni es un área donde pueda aportar valor

[36] MINTZBERG, Henry. *La estructuración de las organizaciones*, Madrid: Ariel, 1979.

[37] DAVIS, Jack. «The Kent-Kendall Debate of 1949», *Studies in Intelligence*. 1991, n.º 2, p. 35.

[38] MARTÍN BARBERO, Isaac. «Inteligencia económica: Tan lejos, tan cerca», *Inteligencia y Seguridad: Revista de análisis y prospectiva*, n.º 2, 2007, pp. 107-120; SERVICE, Robert W. «the development of strategic intelligence: A managerial perspective», *International Journal of Management*, vol. 23, n.º 1, 2006, pp. 61; SOLBERG SØILEN, Klaus. «Management implementation of business intelligence systems», *Inteligencia y Seguridad: Revista de análisis y prospectiva*, n.º 9, 2010, pp. 41-65; PORTER, Michael y MILLAR, Victor E. «How information gives you competitive advantage», *Harvard Business Review*, julio de 1985, pp. 1-13.

añadido ni sería el lugar para lo mismo. Sí centro la atención en que la inteligencia estratégica requiere saber qué estamos buscando para poder encontrar patrones de funcionamiento, si no, la emergente ciencia del razonamiento analítico que facilitará a analistas y decisores los interfaces interactivos[39] les hará caer en un ensueño estilo *Minority report*. Prestos a poner recursos y modificar legislaciones relativas a derechos y libertades, los decisores políticos delegarían en el conocimiento autómata de poderosos sistemas informáticos que rastrearían la Red para desactivar las amenazas antes de materializarse.

Combinando técnicas de análisis automatizados con la visualización interactiva específicamente diseñada para dar apoyo a analistas y a decisores políticos, se debería conseguir una interacción entre los objetivos del decisor político con datos reales para una efectiva comprensión, razonamiento y toma de decisiones sobre la base de enormes y complejas bases de datos[40]. Esta reflexión no es tan clara para, por ejemplo, el combate contraterrorista que parece dominado por una obsesión por la masiva recopilación de datos y su explotación a través de plataformas integradas, algunas en desarrollo por grandes empresas de informática. De nuevo, el debate vuelve a recaer sobre uno previo y de carácter más básico como es la diatriba entre qué peso han de tener en el cóctel HUMINT contra SIGINT u OSINT, pero no es el lugar para hablar de esto y su influencia en la inteligencia estratégica si no queremos caer en lugares comunes y en sobre lo que Rosales[41] ya avanzó hace tiempo.

Un nuevo producto de verdad estratégico

La inteligencia económica existió ya en el pasado[42], por lo que no es bajo ningún concepto un elemento nuevo. Empezando por el popular Marco Polo, el interés por ampliar mercados y obtener información comercial, industrial o económica está largamente documentado. Durante algún tiempo, como publicaba Rousseau en 1925[43], se entendía la inteligencia económica como un complemento a la inteligencia militar que permitía

39 COOK, K., EARNSHAW, R. y STASKO, J. «Discovering the unexpected», *IEEE computer graphics and applications*, septiembre/octubre de 2007, pp. 15-19.

40 KEIM, D., KOHLHAMMER, J., ELLIS, G y MANSMANN, F. (eds.), *Mastering the information age: Solving problems with visual analytics*. Constanza: 2011. www.vismaster.eur/book/.

41 ROSALES, Ignacio. «La inteligencia en los procesos de toma de decisiones en la seguridad y defensa», *El papel de la inteligencia ante los retos de la seguridad y la defensa internacional*, *Cuadernos de Estrategia,* n.º 130. Instituto Español de Estudios Estratégicos, Ministerio de Defensa, 2005, pp. 35-59.

42 DÍAZ FERNÁNDEZ, Antonio M. *Los servicios de inteligencia españoles*. Madrid: Alianza Editorial, 2005.

43 ROUSSEAU, «Economic intelligence». *Journal Royal United Service Institution*, vol. 70, 1925, pp. 701-709.

conocer las capacidades del enemigo pero no como una herramienta de conocimiento de las potencialidades del otro fuera de la esfera bélica; pero esa aproximación ya no es la predominante.

Según la CIA, el 40% de la información obtenida y los análisis realizados a mediados de los años noventa ya tenía que ver con temas económicos. El final de la Guerra Fría hace que mucha información económica y comercial esté disponible y, en la actualidad, un 95% de ella provenga nada menos que de fuentes abiertas. En teoría, las agencias de inteligencia norteamericanas no están envueltas en el espionaje para el beneficio de sus industrias nacionales, sin embargo, cada vez están más involucradas en situaciones que implican la identificación de escenarios en el exterior donde las marcas norteamericanas se sitúan en una situación de desventaja debido a acciones escrupulosas como sobornos de competidores extranjeros.

Pocos dudarán de que los servicios de inteligencia se han centrado habitualmente en amenazas de carácter militar, político o, más recientemente, en la actividad terrorista. Que los servicios de inteligencia pueden suministrar un producto de carácter económico más allá del que les interese para conocer la capacidad bélica del enemigo también es indudable, de hecho, lo han venido haciendo desde hace años como recopilan Zelikov o Levet[44]. Lo que, en mi opinión, con toda lógica y sinceridad, Brander se plantea es si el Estado debe implicarse en estas tareas y, para sostener sus interrogantes, da tres argumentos a favor del sí[45]: por una parte, los fallos del mercado hacen que el Estado deba intervenir; en segundo lugar, la inteligencia es un bien público que solo puede ser prestado por él, y, en tercer lugar, tiene una labor de protección al igual que otras instituciones del Estado.

Sherman Kent definía la inteligencia estratégica como «el tipo de conocimiento que un Estado debe poseer para garantizarse que sus intereses no sufrirán ni sus iniciativas fracasarán debido a que sus decisores políticos o sus soldados planifican y actúan bajo la ignorancia»[46]. Esta definición es igualmente aplicable al mundo de la empresa pero precisamente aquí recae una de las diferencias más esenciales en mi opinión: las empresas no solo evitan que otros competidores les arrebaten cuota de mercado sino que se adentran y adelantan e intentan lograrla ellos, algo sobre lo que teorizó Rodenberg[47].

---

[44] ZELIKOV, Philip (1997). «American economic intelligence: Past practice and future principles», *Intelligence and national security*, vol. 12, n.º 1, pp. 164-177; LEVET, Jean-Louis (2001). *L'intelligence économique: Mode de pensée, mode d'action,* Ed. Económica.

[45] BRANDER, James A. «The economics of economic intelligence», *Commentary, Canadian Secret Intelligence Service*. Reimpreso por Evan Potter, ed. Economic Intelligence and National Security, Carleton University Press, Ottawa, 1998, pp. 197-217.

[46] KENT, *opus cit.*

[47] J. H. A. M. Rodenberg. *Competitive intelligence and senior management*, Eburon Publishers, Delft, 2008.

El potencial de las agencias de inteligencia que han adaptado sus instrumentos y medios a esta nueva tarea es impresionante. Esto se debe, como recoge Fraumann[48], a que el actual espionaje económico realizado por potencias extranjeras va más allá del espionaje industrial clásico. Porque «no podemos espiar políticamente a un aliado», podrían justificar inocentemente algunos, pero, y ¿económicamente? Tanto una como otra parcela son objeto de la acción de la inteligencia, pero, en el caso del espionaje económico, asumir que espiamos la economía de otros supone dividir esta inteligencia en dos grandes dimensiones, la público-privada y la ofensiva-defensiva, que paso a desarrollar.

Por una parte, la globalización ha cambiado el concepto de «nuestro» y «suyo», de nacional e internacional. Los mercados ya no son estrictamente locales, nacionales o internacionales sino globalizados, pero los Gobiernos y sus instrumentos continúan siendo nacionales. Así, la distinción entre público y privado, que ya es de por sí más compleja, se une a unos Estados que han perdido parte de su poder de regulación y policial tanto a nivel estatal como fuera de sus fronteras. Es en este entorno en el que se movería la inteligencia económica, como un instrumento para la estrategia y la gestión de las compañías y el Estado en un mundo global si, claro está, este último acepta que debe tener un rol preeminente en el mismo.

La segunda línea de discusión recae, por tanto, no en si el Estado puede sino en si debe implicarse en un espionaje económico directo o bien desarrollar sus capacidades exclusivamente de forma defensiva[49]. Pero tampoco debemos dedicar mucho tiempo a la reflexión ya que realmente el tema es la conjugación y equilibrio entre ambos. Si el espionaje existe es por necesidad y por reciprocidad, por tanto, si estamos desarrollando una capacidad de protección frente a amenazas es porque partimos de que otros países lo realizan activamente, y no es solo una presunción: los informes anuales de control y de gestión de comités de control parlamentario y de servicios de inteligencia, respectivamente, señalan sin empacho a China y Rusia como agentes muy activos en el espionaje económico, incluyendo el de tipo industrial. Quizá por esto, no deja de ser interesante que los dos países con un mayor interés en el espionaje económico no hagan referencia a la importancia de la inteligencia económica en sus libros blancos de defensa ni en textos similares.

Por tanto, en mi opinión, si bien la justificación teórica para que el Estado se adentre y afinque en este área no es discutible, sí lo es si debe adoptar un rol ofensivo-defensivo; si bien no estaría de más reflexionar sobre el hecho de que si los servicios de inteligencia de todo el mundo

[48] FRAUMANN, Edwin (1997). «Economic espionage: Security missions redefined», *Public Administration Review*, 5 (4), pp. 303-308.

[49] BRANDER, *opus cit*. 1998, 205.

fueran tan exitosos robando secretos comerciales, el I+D caería vertiginosamente puesto que los actores privados no podrían amortizar sus inversiones. Por otra parte, estaríamos hablando de la información como un bien público –como habla Seiglie[50]– en el sentido de un producto que por su esencia solo puede ser proveído por el Estado y que, si este falla, el mundo privado no puede generar ya que no es producido por el sector privado. Pero la información no es un bien en sentido puro, aunque está muy cerca, como se ve por la existencia de empresas privadas de inteligencia y su increíble expansión en el último lustro.

Claude Revel[51] sí apuesta por una opción ofensiva de la inteligencia económica. Dice esta experta francesa que la seguridad económica consiste en la prevención y evitación de todas las situaciones que pueden interrumpir la vida tanto de empresas como del Estado. Sin duda es una forma peculiar de entender «ofensivo». El contraespionaje económico está bien visto pero no el de carácter ofensivo. La estrategia canadiense, que se recoge en su *Securing an open society: Canada's national security policy* de 2004[52], relaciona la inteligencia con el espionaje exterior, esto es, como la amenaza de otras potencias de las que deben protegerse.

Sin duda, una de las reflexiones más clarividentes sobre cómo mantener el equilibrio la realiza mark Lowenthal –aunque extensible a todos los participantes– ante el Congreso estadounidense[53] sobre lo que profundiza Claude Revel[54] en el último informe *Développer une influence normative internationale stratégique pour la France.* Allí, Revel apuesta por «la necesidad de una estructura de una inteligencia económica nacional que sea un centro neuronal de alerta, de impulso, de acompañamiento y que haga un seguimiento de las estrategias de información, de seguridad y de influencia, que deben estar inextricablemente enlazadas». Continúa la autora francesa indicando que «deberá contarse con una coordinación interministerial e inevitablemente mantenida a nivel de Estado, pudiendo contar con todas las informaciones útiles de todos los servicios del Estado, de los actores privados. La estructura debe centralizar la información, orientar la estrategia, la táctica y la acción en los entornos internacionales y realizar

50 SEIGLIE, Carlos, COISSARD, Steven y ÉCHINARD, Yann. «Economic intelligence and national security», *War, peace and security. Contributions to conflict management, peace economics and development*, vol. 6, 2008, pp. 235-248.

51 REVEL, Claude. *Economic intelligence: An operational concept for a globalised world,* ARI de Real Instituto Elcano, n.º 134/2010.

52 *Securing an open society: Canada's national security policy*, abril de 2004, http://publications.gc.ca/collections/Collection/CP22-77-2004E.pdf.

53 *Hearing before the Select Committee on Intelligence of the United States Senate One Hundred Third Congress*, First Session on Economic Intelligence, Thursday, August 5, 1993 http://www.intelligence.senate.gov/pdfs103rd/103650.pdf.

54 REVEL, Claude. *Développer une influence normative internationale stratégique pour la France*, 2013, http://proxy-pubminefi.diffusion.finances.gouv.fr/pub/document/18/14133.pdf.

el seguimiento de la evaluación.» Indica que todo esto debe realizarse en plena coordinación con todos los centros del Estado de forma que permita anticiparse y tomar las decisiones sobre materias complejas.

Volviendo al debate entre Kent y Kendall, aquí encontraríamos una diferencia esencial: o bien queremos una organización que quiere anticiparse a las amenazas –esencialmente los ataques– o bien quiere modular el entorno, algo perfectamente asumible en gestión –estratégica, claro está–. Y el Informe Carayón muestra, en mi opinión, la evolución decidida de este debate. En su página 37, indica que una verdadera política de seguridad económica debe imponer al Estado una anticipación de las amenazas y un tratamiento activo de las agresiones que sufran sus empresas. Es tiempo de pasar de una postura estática y reactiva (la Defensa) a una de carácter activo (la seguridad económica) implicando a todos los servicios del Estado y en primer lugar a los servicios de inteligencia y seguridad.

Proceso estratégico: la nueva planificación

Russel Ackoff afirmaba que la planificación era «concebir un futuro deseado así como los medios necesarios para alcanzarlo»[55]. Los análisis estratégicos compartidos permiten producir la síntesis del compromiso colectivo, contrariamente a lo que postulaba Henry Mintzberg[56]. Lo más difícil no sería realizar una buena elección, sino la de estar seguros de que se ha acertado en la formulación de las preguntas adecuadas. Un problema que está bien planteado, y colectivamente compartido por aquellos a quienes dicho problema concierne, podemos decir que es un problema casi resuelto. Podemos, por tanto, decir que planificamos para resolver los problemas, en nuestro caso, del Estado en sus diferentes dimensiones, incluida la económica.

Pero el tiempo es y será una variable clave. Ni los analistas pueden emplear todo aquel que quisieran para obtener un conocimiento profundo ni el decisor político lo tiene para comprender los complejos asuntos de los que diariamente es responsable. El proceso de planificación parte de la clara asignación de cometidos por lo que el liderazgo –en nuestro caso político– es esencial para la planificación. Los decisores políticos quieren información que les ayude a evitar desagradables sorpresas por lo que, aunque no pidan inteligencia estratégica, la necesitan. Pero el hecho cierto es que nuestro futuro se planea por personas que quieren sentirse cómodas con sus decisiones pero que no favorecen la recepción de inteligencia estratégica que les prevé de acontecimientos duros que no encajan en sus políticas, esto es, quieren evitar sorpresas estratégicas

55 ACKOFF, Russel L. *Méthodes de planification dans l'entreprise*. Paris : Les Editions d'Organisation, 1973.

56 MINTZBERG, *opus cit*, 1979.

pero raramente desarrollar actuaciones «estratégicas» que van más allá del período en el que permanecerán en el puesto.

El flujo informativo de arriba a abajo suele ser la fórmula tradicional empleada por el Estado, que coordina, estimula y financia estas estructuras; sin embargo, el pasado nos muestra que la aproximación de abajo a arriba proviene de experiencias exitosas que favorecen la retroalimentación en la cual la participación del Estado es pragmática y en respuesta a iniciativas que surgen desde el terreno[57]. Estos elementos previos indican, en mi opinión, que el papel que hayan de jugar los altos funcionarios que dan permanencia a las políticas de un país es clave, si bien no es el espacio para desarrollarlo.

Quizá por eso haya que recuperar un documento relevante que pasó desapercibido como fue el *Informe de la Comisión para la Reforma Integral del Servicio Exterior del Ministerio de la Presidencia* dirigido por el embajador Melitón Cardona en 2005[58]. Interesante por el enfoque comprehensivo, por la fecha y por el erial que España es para este tipo de documentos. En él ya se establecía que el Servicio Exterior tenía problemas de carácter organizativo que se reflejan en problemas de planificación, de coordinación y de delimitación de competencias, y problemas en el ámbito consular. Entre los de planificación figuraban la escasa capacidad de planificación y formulación estratégica de la acción exterior del Estado español. El informe refería que «este problema, que viene sufriendo la política exterior española desde hace décadas, hace que la acción exterior de nuestro país se mueva dentro del nuevo contexto internacional con un enfoque cortoplacista. Por otro lado, la inadecuación del diseño de la red de misiones españolas en el extranjero. Este problema obedece tanto a la escasa planificación de la política exterior española como a la falta de agilidad para abrir y cerrar misiones diplomáticas, consecuencia de los complejos procedimientos administrativos existentes».

Añadía también el informe:

> *La falta de concreción de los objetivos de las misiones diplomáticas. La escasa planificación conjunta de nuestra política exterior hace que las misiones diplomáticas españolas no dispongan de objetivos que permitan orientar y controlar su actuación. Esto conduce a que se trabaje de manera reactiva y a que sea difícil evaluar objetivamente sus acciones. La carencia de Consejerías Sectoriales en determinadas áreas se traduce en una falta de seguimiento puntual de esos temas, dado que el consejero de la Misión Diplomática a quien se le encargan esas*

[57] MARCO, Christian y MOINET, Nicolas. *L´intelligence économique,* París: Dunod, 2006, p. 120.

[58] *Comisión para la Reforma Integral del Servicio Exterior.* Ministerio de la Presidencia, 2005, presidida por el embajador Melitón Cardona, http://www.maec.es/SiteCollectionDocuments/Documentos/informe_CRISEX.pdf.

> *cuestiones tiene que estar a su vez ocupándose de otros muchos asuntos. La inexistencia de determinadas Consejerías Sectoriales acarrea también la necesidad de desplazamientos continuados de los funcionarios de los Ministerios con competencia en dichos asuntos, y como consecuencia, un gasto elevado en comisiones de servicio.*

Pero el embajador Cardona también hablaba de problemas de coordinación. En concreto,

> *...de falta de suficiente coordinación interministerial, debida en parte a la inoperancia de los órganos colegiados con responsabilidades a tal efecto, como el Consejo de Política Exterior, que es el ámbito en que deberían hacerse compatibles la política general del Gobierno con las prioridades de cada uno de los Ministerios con acción exterior. También de la falta de flujos de información sistemáticos, lo que provoca gran parte de los problemas de coordinación tanto en los servicios centrales como en las misiones diplomáticas. La información no se transmite de arriba hacia abajo ni horizontalmente porque no se han fijado pautas para que la información circule en todos los sentidos. Falta de coordinación entre los distintos departamentos de la misión, tanto por la mala circulación de la información como por la errática regularidad de las reuniones de coordinación. Falta de una adecuada coordinación de los demás actores nacionales con acción exterior.*

En Francia, el Informe Carayon[59], sucesor del Informe Martre[60] elaborado una década antes, marcó un punto de inicio en el desarrollo de la inteligencia estratégica que se necesitará en el siglo XXI. En Carayon, se explicaba que la competitividad necesitaba de políticas de inteligencia económica y que estas tienen que estar coordinadas con vistas a ser eficientes. No obstante, si bien en ninguno de ambos informes se establece una definición única de inteligencia económica, en el primero sí se indica que esta debe basarse en cuatro pilares: i) animar a esta práctica a nivel de empresa, ii) optimizar la transferencia de información entre los sectores públicos y privados, iii) construir las bases de datos a la luz de las necesidades de los usuarios y iv) movilizar al mundo de la formación y la educación. Una serie de retos que muy lentamente se están desarrollando en la mayoría de los países, inclusive en aquellos en los cuales hay una clara voluntad de desarrollar este tipo de inteligencia.

En España la inteligencia económica se encuentra recogida en la Estrategia Española de Seguridad. Pero con anterioridad, la ley de 11/2002, de 6 de mayo, reguladora del Centro Nacional de Inteligencia, incluye un verbo clave para el desarrollo de la potencialidad de la inteligencia estratégica

[59] *Intelligence économique, compétitivité et cohésion sociale*, julio de 2003. http://www.ladocumentationfrancaise.fr/var/storage/rapports-publics/034000484/0000.pdf.

[60] *Intelligence économique et stratégie des entreprises*, febrero de 1994. http://www.ladocumentationfrancaise.fr/var/storage/rapports-publics/074000410/0000.pdf.

y, claro está, de la inteligencia económica. En su artículo 4, indica que «para el cumplimiento de sus objetivos, el Centro Nacional de Inteligencia llevará a cabo las siguientes funciones: a) 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.» El verbo «promover» es clave puesto que implica que el Centro puede salir de un funcionamiento centrado en evitar amenazas para pasar a ser un instrumento de desarrollo, entre ellas, de la inteligencia económica, sin duda una evolución en el desarrollo de nuestra inteligencia estratégica.

Conclusiones

El uso abusivo del calificativo «estratégico» está ampliamente asumido y no solo en el mundo de la inteligencia sino en el del *marketing,* la gestión de personal o las decisiones empresariales, entre muchos otros. El final de la Guerra Fría, en el campo de la inteligencia, genera la necesidad de reorientar la función de unas estructuras creadas ex profeso para luchar en los fríos campos de la segunda posguerra mundial. Y esto debe quedar meridianamente claro. La forzada evolución de las agencias de inteligencia es motivo de estar concebidas y desarrolladas para luchar básicamente contra la sorpresa estratégica; por mucho que la palabra estratégico llenara informes y declaraciones e incluso llegase a hablarse de armas nucleares «estratégicas», de estratégico podíamos encontrar poco. De la noche a la mañana, un mundo divisible casi quirúrgicamente en dos se ha mostrado plural, poliédrico, complejo, extraño... En este escenario es donde la verdadera inteligencia estratégica tiene su hueco; una inteligencia que ayuda a comprender, en su sentido etimológico, a hacer entender al decisor político cuáles son los retos a medio y largo plazo, asumiendo la inevitable existencia de sorpresas estratégicas que, por propia definición, siempre existirán porque la incertidumbre es consustancial a la vida en la Tierra.

Comprender el mundo significa evolucionar la Trinidad de Kent en sus tres dimensiones. Las organizaciones deben ser más adaptables, contar con analistas a quienes se les permita un pensamiento dilatado y extendido en el tiempo, alejado de la gestión por objetivos que mata este tipo de capital humano basado en el saber aquilatado durante años de experiencia y lectura. También el producto debe cambiar. Más allá de continuas actualizaciones, se requiere de un mayor conocimiento del decisor político y de cuáles son sus necesidades, lo que implica una mayor planificación y seguimiento por órganos de coordinación interministeriales, algo casi ignoto, al menos, en el panorama español. Por último, los procesos deben modificarse, en gran medida por la nueva relación que ha de establecerse entre consumidores y productores de inteligencia, pero sobre todo para aprovechar las potencialidades de la tecnología y huir de

una continua monitorización del entorno que nos dará mucha información siempre y cuando sepamos qué estamos mirando y, eso, es algo que no existe sin una verdadera aproximación estratégica a la inteligencia.

El Estado tiene un papel pionero en muchas ocasiones debido a que abarca actividades que son caras o complejas pero que habitualmente abandona cuando entra en juego el sector privado. En el caso de la inteligencia económica, este planteamiento es algo más discutible ya que la inteligencia de tipo económico fue importante siglos antes de que la Guerra Fría generase los primeros servicios de inteligencia. Podríamos decir que el Estado –antes el príncipe de Maquiavelo– está volviendo a uno de sus primigenios objetivos: la información económica. El rol que vaya a adoptar, bien ofensivo bien de contraespionaje para evitar que otras potencias o empresas beban de sus secretos económicos, será un debate que cada Estado deberá mantener en profundo diálogo con sus empresarios, puesto que no podemos hablar en puridad de empresas nacionales ya que la globalización ha quebrado esta dialéctica nosotros-ellos que durante tantos siglos funcionó. No obstante, el deber de ayudar a las empresas a protegerse frente al espionaje económico alberga pocas dudas.

Por esto, sin llegar a una privatización de la inteligencia, retórica muy acusada durante los últimos años de los noventa, es necesario no duplicar recursos y dejar que organismos como universidades, centros de pensamiento y centros de análisis, de cálculo y fuentes abiertas se ocupen de parte del proceso de reflexión sobre las nuevas amenazas. No olvidemos que, aunque las necesidades de inteligencia sean ahora de muy corto plazo, el verdadero papel de los servicios de inteligencia es el apoyo estratégico a largo plazo y ahí deben concentrar el grueso de sus esfuerzos; olvidar este aspecto en aras de la eficacia diaria puede llevar a ulteriores sorpresas estratégicas dentro de una década.

Si bien es cierto que no podemos asociar el futuro de la inteligencia estratégica con la económica, tampoco podemos identificar el atraso actual en algunas facetas por haber sobredimensionado el aparato de inteligencia para centrarlo en el terrorismo y, del mismo modo, que no estamos mirando al crimen organizado como gran amenaza como alertaba el comité parlamentario de control de los servicios de inteligencia 2001-2002. Pero, en definitiva, y por ir concluyendo, los factores claves para el éxito de las políticas de inteligencia económica, tanto para el Estado como para las empresas, habrán de ser su habilidad para: i) anticipar y no solo extrapolar escenarios antiguos, ii) adaptar estructuras y leyes a procesos cada vez más rápidos, y iii) establecer redes de cooperación principalmente entre los sectores público y privado, sobre todo entre países que comparten los mismos intereses generales.

La visita al oráculo de Delfos en el centro de Grecia es una experiencia ilustrativa para comprender la inteligencia. Las pitonisas solo daban sus

augurios una vez al mes y su preocupación por el día a día se diluía ya que su visión era sobre la vida, sobre los elementos esenciales, y a eso había que dedicarle reflexión. En Delfos, diferentes ciudades tenían su propia sede donde además guardaban tesoros y ofrendas, una suerte de reunión de todos aquellos con interés en conocer el futuro y que acudían a conocer el augurio. Y, por último, los augurios no eran designios ciertos, indicaban cómo podían evolucionar los acontecimientos o la vida de la persona y, a partir de ahí, de la integración entre ese «pensamiento estratégico» y una lectura acertada del día a día, el peregrino a Delfos podía tener un mapa para funcionar durante, quizá, años en su vida. Esto supone que había una «realidad» que podría ser conocida por anticipado. Y durante años esta fue la creencia del político, la de que con más medios tendría una inteligencia que redujese casi a cero la incertidumbre, y la de las comunidades de inteligencia, que ponían el énfasis en los recursos como argumento para lograr mejores análisis sin reconocer que lo que no querían era emitir informes entre los cuales, indefectiblemente, se podría colar la siguiente sorpresa estratégica. También es cierto que en Delfos había pasadizos y humos que emanaban del subsuelo y que permitían apariciones y desapariciones mágicas pero la retórica de lo oculto siempre tendrá su pequeño elemento de misterio más allá del elemento estratégico.

Bibliografía

ACKOFF, Russel L. *Méthodes de planification dans l'entreprise*. París: Les Editions d'Organisation, 1973.

ARROYO VARELA, Silvia. *Inteligencia competitiva: una herramienta en la estrategia empresarial*. Madrid: Ediciones Pirámide, 2005.

BAUMARD, Philippe. «From noticing to 'sense-making': The use of intelligence in strategizing». *The International Journal of Intelligence and Counterintelligence*, vol. 7, n.º 1, 1994, pp. 29-73.

BRANDER, James A. «The economics of economic intelligence», en *Commentary.* Canadian Secret Intelligence Service. Reimpreso en Evan Potter, ed. Economic Intelligence and National Security, Carleton University Press, Ottawa, 1998, pp. 197-217.

BUZAN, Barry. *Security: A new framework for analysis*. Boulder, London: Lynne Rienner Publishers, 1998.

COLBY, William E. «Reorganizing western intelligence», en Carl Pete Runde y Gregg Voss (eds.): *Intelligence and the new world order: Former Cold War adversaries look toward the 21th Century*. Butstehude: International Freedom Foundation, 1992.

COOK, K., EARNSHAW, R. y STASKO, J. «Discovering the unexpected». *IEEE computer graphics and applications*, septiembre-octubre de 2007, pp. 15-19.

DAVIS, Jack. «The Kent-Kendall debate of 1949». *Studies in Intelligence*, n.º 2, p. 35, 1991.

DÍAZ FERNÁNDEZ, Antonio M. *Los servicios de inteligencia españoles*. Madrid: Alianza Editorial, 2005.

— «La adaptación de los servicios de inteligencia al terrorismo internacional». *ARI 52/2006,* Real Instituto Elcano, 2006.

DÍAZ FERNÁNDEZ, ANTONIO M., REVENGA, Miguel y JAIME, Óscar. *Cooperación europea en inteligencia: Nuevas preguntas, nuevas respuestas*. Pamplona: Aranzadi, 2009.

FERRER, Juan. *Seguridad económica e inteligencia estratégica en España*. *Documento Opinión*, n.º 85. Instituto Español de Estudios Estratégicos, 2011.

FRAUMANN, Edwin. «Economic espionage: Security missions redefined», *Public Administration Review*, 5 (4), 1997, pp. 303-308.

GOLDMAN, Jan. *Words of intelligence: A dictionary*. Oxford: The Scarecrow Press, 2006.

HOLSHEK, Christopher. *America's first quarter millennium: Envisioning a transformed national security system in 2026*. Project on National Security Reform (PNSR), 2009.

JAIME JIMÉNEZ, Óscar y DÍAZ FERNÁNDEZ, Antonio M. *La seguridad interior: España 2020*. Madrid: Fundación Alternativas, 2009.

KEIM, D.; KOHLHAMMER, J.; ELLIS, G. y MANSMANN, F. (eds.). *Mastering the information age: Solving problems with visual analytics*. Constanza, 2011. www.vismaster.eur/book/

KENDALL, Willmoore. «The function of intelligence». *World Politics*, vol. 1, n.º 4, julio de 1949, pp. 542-552.

KENT, Sherman. *Strategic intelligence for American world policy*. Princeton: Princeton University Press, 1949.

LESOURNE, Jacques. «Plaidoyer pour une recherche en prospective». *Futuribles*, n° 137, noviembre de 1989.

LEVET, Jean-Louis. *L'intelligence économique : Mode de pensée, mode d'action.* París: Economica, 2001.

LÓPEZ ESPINOSA, María de los Ángeles. «Inteligencia y terrorismo internacional. Un panorama de cambios». *La inteligencia, factor clave frente al terrorismo internacional*, *Cuadernos de Estrategia,* n.º 141, Instituto Español de Estudios Estratégicos, Ministerio de Defensa, 2009, pp. 197-239.

MARCO, Christian y MOINET, Nicolas. *L´intelligence économique*. París: Dunod, 2006.

MARTÍN BARBERO, Isaac. «Inteligencia económica: Tan lejos, tan cerca». *Inteligencia y Seguridad: Revista de análisis y prospectiva*, n.º 2, 2007, pp. 107-120.

MINTZBERG, Henry. *La estructuración de las organizaciones*. Madrid: Ariel, 1979.

PLATT, Washington. *Strategic intelligence production: Basic principles*. Nueva York: Praeger, 1957.

PORTER, Michael y MILLAR, Victor E. «How information gives you competitive advantage». *Harvard Business Review*, julio de 1985, pp. 1-13.

POSNER, Richard A. *Preventing surprise attacks: Intelligence in the wake of 9/11*. Nueva York: Rowman & Littlefield, 2005.

REVEL, Claude. *Développer une influence normative internationale stratégique pour la France*, 2013. http://proxy-pubminefi.diffusion.finances.gouv.fr/pub/document/18/14133.pdf.

— «Economic intelligence: An operational concept for a globalised world», *ARI* de Real Instituto Elcano, 2010, n.º 134/2010.

RODENBERG, J. H. A. M. *Competitive intelligence and senior management*. Delft: Eburon Publishers, 2008.

ROSALES, Ignacio. «La inteligencia en los procesos de toma de decisiones en la seguridad y defensa». *El papel de la inteligencia ante los retos de la seguridad y la defensa internacional*, *Cuadernos de Estrategia* n.º 130, Instituto Español de Estudios Estratégicos, Ministerio de Defensa, 2005, pp. 35-59.

ROUSSEAU. «Economic intelligence». *Journal of Royal United Service Institution*, vol. 70, 1925, pp. 701-709.

SEIGLIE, Carlos, COISSARD, Steven y ÉCHINARD, Yann. «Economic intelligence and national security». *War, peace and security. Contributions to conflict management, peace economics and development*, vol. 6, 2008, pp. 235-248.

SERVICE, Robert W. «The development of strategic intelligence: A managerial perspective». *International Journal of Management*, vol. 23, 2006, n.º 1, pp. 61-77.

SOLBERG SØILEN, Klaus. «Management implementation of business intelligence systems». *Inteligencia y Seguridad: Revista de análisis y prospectiva*, n.º 9, 2010, pp. 41-65.

SWENSON, Russell G. y LEMOZY, Susana C. *Democratización de la función de inteligencia. El nexo de la cultura nacional y la inteligencia estratégica.* Washington DC: National Defense Intelligence College, 2009.

WHITNEY, Merill E. y GAISFORD, James D. «Economic espionage as strategic trade policy». *Canadian Journal of Economics*, XXIX special issue, 1996, pp. 627-632.

ZELIKOV, Philip. «American economic intelligence: Past practice and future principles». *Intelligence and National Security*, vol. 12, 1997, n.º 1, pp. 164-177.

Capítulo II

ESTUDIO DE LA GUERRA ECONÓMICA Y DE LAS PROBLEMÁTICAS RELACIONADAS

Christian Harbulot

Resumen

La historia de la humanidad está caracterizada por relaciones de fuerza de naturaleza económica identificables en las distintas etapas de su desarrollo: la lucha por la supervivencia, la colonización y la esclavitud, la conquista territorial y comercial, la rivalidad económica, los enfrentamientos geoeconómicos y competitivos. Pero no existe literatura alguna sobre guerra económica reconocida por el mundo académico. Esta laguna se explica por la falta de legitimidad de este concepto debido a la voluntad de ocultar la finalidad de los enfrentamientos de naturaleza económica. Las expresiones más visibles e irrefutables de la guerra económica, tales como las fases más conflictivas de la colonización o las dos guerras del Opio, no han servido de impulso para unas lecturas obligadas. El fin de este artículo es el de acabar con este déficit de reflexión sobre una realidad que se hace cada vez más evidente. Al contrario que en otros países como Estados Unidos, Corea del Sur o China, Europa está muy desprovista a la hora de abordar esta problemática.

Palabras clave

Guerra económica, supervivencia, colonización, conquista, lecturas obligadas, ocultamiento, estrategia, aumento de poder.

Abstract

The history of mankind is dominated by power relationship of economic nature identifiable at the different stages of progression: the struggle for survival, colonization and slavery, territorial conquest and trade, economic competition, the geo-economic and competitive fighting. But there is no recognized written culture on economic warfare in the academic world. This gap can be explained by the lack of legitimacy of the concept due to the desire to conceal the purpose of fighting economic. The most visible expressions and irrefutable economic warfare as the most contentious phases of colonization or the two opium wars have not led to the beginnings of a reading grid. This article aims to fill this gap in thinking about a reality that everyday becomes more demonstrative. Unlike other countries such as the United States, South Korea and China, Europe is powerless to address this problem.

Keywords

Economic war, survival, colonization, conquest, read gate/obliged readings, concealment, strategy, increase in power.

Introducción

La guerra económica se está convirtiendo en una realidad incuestionable en las relaciones internacionales, aunque fue considerada durante mucho tiempo como algo exótico por parte del medio universitario. Los intelectuales que critican las relaciones de fuerza entre potencias[1] se han visto obligados a doblegarse ante la evidente evolución de las relaciones internacionales. A los actos de alcance geopolítico (como el gas utilizado por Rusia como arma para reforzar su estatus de potencia o el cuestionamiento de la supremacía monetaria del dólar por Irán), se han añadido hechos de naturaleza geoeconómica tales como las tensiones diplomáticas entre China y Japón por los recursos o la política proteccionista defendida por los Estados Unidos frente a China en lo referente a la industria solar. Esta diversidad de situaciones hace destacar el interés por una lectura más profunda de los enfrentamientos ligados a la guerra económica.

El principio del siglo xx está marcado por el cuestionamiento de la visión positiva del desarrollo heredado de las revoluciones industriales y de la relativa pacificación derivada de la globalización de los intercambios, tal y como lo han dado a entender la mayor parte de los economistas liberales. En este mismo orden de ideas, la *pax americana* oficializada por la desaparición de la URSS, principio del mito del fin de la historia[2], deja sitio a riesgos de enfrentamiento multipolarizados debido a la limitación progresiva de los recursos, a las tensiones crecientes en cuestión de energía, a las crisis estructurales del mundo occidental provocadas por la desindustrialización y a la voluntad de conquista comercial de nuevos actores. De facto, iniciamos un largo periodo de tensiones diversas cuyo seguimiento no se podrá limitar a un mero discurso paliativo sobre la búsqueda de crecimiento.

Analizar la guerra económica[3] implica pasar de lo implícito a lo explícito, difícil ejercicio si se tiene en cuenta la voluntad casi universal de los beligerantes de disimular la naturaleza de sus enfrentamientos no militares. Los trabajos realizados en los últimos dieciséis años bajo mi dirección en la Escuela de Guerra Económica de París nos ha permitido poner los cimientos de unas lecturas obligadas para descifrar las estrategias de incremento de poder mediante la economía y las relaciones de fuerza que generan.

1 BADIE, Bertrand. *L'impuissance de la puissance*. París: Fayard, 2004.

2 FUKUYAMA, Francis. *La fin de l'histoire et le dernier homme*. París: Flammarion, 1992.

3 HARBULOT, Christian. *Comment travailler sur l'absence d'histoire*, crónica de 7 de noviembre de 2012, www.lesinfluences.fr.

La emergencia de los principios fundacionales de la guerra económica

La historia de la humanidad está marcada desde sus orígenes por dos etapas esenciales: la prioridad dada a la supervivencia y la oposición entre sedentarización y nomadismo. La situación de supervivencia ha sido una situación predominante para la mayor parte de la población mundial hasta el principio de las revoluciones industriales. Ha dado lugar al recurso, a menudo sistemático, de la violencia.

La violencia y la supervivencia

La supervivencia es una de las etapas estructurantes de la naturaleza de los enfrentamientos económicos –no se puede hacer referencia a la guerra económica dado el nivel de enfrentamiento principalmente individual, y por tanto, limitado en el plano colectivo–. La oposición entre pueblos sedentarios y pueblos nómadas ha conllevado enfrentamientos regulares tal y como lo demuestra la génesis de la vieja Rusia[4]:

La estepa rusa es la prolongación de las estepas de Asia y se funde en la estepa húngara. Este continente de estepas –del mar Amarillo al lago Balatón– está poblado de nómadas que, desde la Prehistoria, recorren enormes distancias en busca de pastos. Llegados de las profundidades de Asia, los nómadas llegan por oleadas a la estepa. Echan a los habitantes que, a su vez, ocupan los pastos de pueblos más débiles.

Este *ballet* guerrero entre los «bárbaros» del este y las poblaciones de ciudades del oeste surgidas del comercio fluvial y terrestre entre el mar Báltico y el mar Negro durará varios siglos y tendrá un papel determinante en la construcción del espacio geopolítico ruso. En este mismo orden de ideas, la historia de la antigua China está marcada por las invasiones repetitivas de pueblos nómadas turco-mongoles. La primera versión de la guerra económica deriva de este nexo dialéctico entre la acumulación de riqueza del sedentario y la rápida incursión del nómada en territorio extranjero para llevar a cabo pillajes.

Recursos y territorios

La cuestión de los recursos está en el centro de la problemática del desarrollo de las civilizaciones. En el siglo xv a. C., los faraones del nuevo imperio[5] necesitaban tres recursos naturales: madera para la construcción

[4] HELLER, Michel. *Histoire de la Russie et de son empire*. Colección *Histoire*, p. 55. París: Champs, 1999.

[5] GRANDET, Pierre. *Les pharaons du Nouvel Empire: une pensée stratégique (1550-1069 av JC).* París: Rocher, 2008.

de monumentos y de barcos, cobre y estaño, cuya aleación en forma de bronce se utilizaba en aquella época para fabricar herramientas y armas. Las rutas comerciales marítimas (el Mediterráneo, la Mancha, el Báltico) y terrestres (las rutas de la seda, del estaño) se volvieron fuentes de enfrentamiento recurrentes.

El progreso de la humanidad entre la Antigüedad y la Edad Moderna amplía el campo espacial del proceso de enfrentamiento económico; así es como la piratería se convirtió en una palanca de poder real. Atraídos por las ganancias del comercio triangular[6], los piratas ingleses fueron los precursores de la futura Marina Real británica. Tanto en el mar como sobre tierra, los beligerantes integraron la dimensión económica a su estrategia militar y diplomática. Al final de la Edad Media, algunos monarcas recurrieron al arma económica[7] para apoyar la acción militar. En su prolongada lucha contra Carlos el Temerario, Luis XI movilizó su flota para perturbar el aprovisionamiento de granos y arenques de Flandes, perteneciente a la casa de Borgoña. El rey de Francia presionó también a los banqueros para disuadirlos de financiar el coste de la guerra de su rival e impulsó la creación de ferias en Lyon para disminuir las entradas de dinero de las ferias de Ginebra, punto de intercambio de las rutas comerciales entre Alemania, Italia y Borgoña.

La seguridad del territorio y de su patrimonio urbano y rural se percibe en el siglo xvii como una prioridad estratégica para ciertos estados en proceso de constitución. Las siete Provincias Unidas del Norte[8] contra España elaboran el primer modelo de santuario formado sobre una red de baluartes, reforzado por la utilización de arroyos y ríos como defensa natural. La Francia de Vauban hizo lo propio creando fortificaciones a lo largo de las nuevas fronteras surgidas tras la conquista de territorios al norte del reino. Esta barrera defensiva desembocó en el concepto de *pré carré*[9], que tiene un significado moderno al incluir la zona de influencia exterior (diplomática, militar y económica).

La seguridad del territorio se hizo también de forma indirecta mediante concesiones económicas dadas a un estado aliado aprovechando su supremacía militar. En 1373, Portugal firmó un tratado con el reino de Inglaterra[10] para beneficiarse de su protección. Mediante este acto diplomático,

6 El comercio triangular fluye en las primeras fases de la colonización de las Américas. Cubrió el comercio de esclavos entre África y el continente americano, así como los intercambios comerciales entre las colonias y Europa.

7 FAVIER, Jean. *Louis XI*. París: Fayard, 2001. Página 754.

8 CORNETTE, Joël. *Le roi de guerre, essai sur la souveraineté de la France du Grand Siècle*. París: Petite Bibliothèque Payot, 2010. Página 42.

9 BITTERLING, David. *L'invention du pré carré. Construction de l'espace français sous l'Ancien Régime*. París: Albin Michel, 2009.

10 LACOYE, Mateus Alice y HARBULOT, Christian. «La complexité des rapports de force économiques». *Revue Française de Géoéconomie*. París: abril de 2008.

Portugal buscaba huir de la voluntad anexionista de Castilla. Esta alianza ratificada en igualdad de condiciones se transformó poco a poco en un protectorado inglés ya que los ingleses dieron su apoyo militar a cambio de un dominio financiero y comercial sobre Portugal que duró varios siglos.

Las dinámicas conflictivas ligadas a la colonización

La constitución de los imperios es indisociable de los procesos de colonización que jalonan la historia de la humanidad. Los enfrentamientos militares que se derivan están fuertemente relacionados con los desafíos económicos. La colonización es la base de la creación de imperios que sirven, en particular, para asegurar el dominio sobre las riquezas del subsuelo y los recursos así como sobre las rutas comerciales. La captura y la explotación de seres humanos es una de las manifestaciones más evidentes de las relaciones de fuerza generadas por el afán de lucro. Tal y como afirman los profesores de la Universidad de Nueva York Jane Burbank y Frederik Cooper[11]: «En Gran Bretaña, en Francia y en ciertas regiones de los imperios portugués y español, la esclavitud hizo lucrativo el imperio y el imperio hizo posible la esclavitud». La guerra económica está presente en todas las fases de desarrollo de la colonización, independientemente de que se tratara de la dinámica de expansión del Imperio romano o de las fases de construcción de los imperios marítimos europeos a partir del siglo XVI. El elemento más paradójico, a mi modo de ver, de la formación de este principio es que no se ha reconocido como uno de los elementos recurrentes de los enfrentamientos ligados a la globalización de los intercambios.

La colonización de América del Norte ilustra de manera muy didáctica la superposición de lógicas conflictivas creadas por los desafíos económicos. Las Trece Colonias, implantadas a lo largo del litoral atlántico entre el Canadá francés y la Florida española, se establecieron firmemente a partir de 1733. Los colonos habían empezado a plantar algodón en el siglo XVII. Esta política de plantación se desarrolló a gran escala al final del siglo XVIII, engendrando lo que se llamaría después «el comercio triangular». Los barcos británicos cargaban los productos manufacturados y los licores en África occidental para cambiarlos por esclavos que desembarcaban en las Indias occidentales y en el sur de las Trece Colonias. Los barcos volvían después a Gran Bretaña con cargamento de algodón, ron, azúcar y tabaco, resultado del trabajo de los esclavos.

Los colonos americanos se consideraron perjudicados en sus relaciones con Inglaterra por la presión fiscal y las restricciones comerciales con el

[11] BURBANK, Jane y COOPER, Frederik. *Empires, de la Chine ancienne à nos jours*. París: Payot, 2011. Página 246.

resto del mundo impuestas por la Corona. Gran Bretaña llevaba ventaja en todos los casos ya que una proporción sustanciosa de las mercancías importadas del Nuevo Mundo era reexportada al continente europeo por las sociedades de comercio insulares. Los beneficios obtenidos de estas operaciones comerciales transatlánticas contribuyeron al desarrollo del comercio asiático del Imperio británico.

La riqueza acumulada agudizó las ansias que se transformaron poco a poco en tensiones, en relaciones de fuerza y en enfrentamientos armados entre Inglaterra y sus colonos, entre estos y los indios y entre los dos reinos rivales de la época, Inglaterra y Francia.

El control de las rutas comerciales

El reino de Inglaterra construyó su poderío a través del mar y el comercio. En un principio, la Inglaterra del siglo XVI era un país pobre y sin una capacidad militar real de proyección al exterior; su poder era muy inferior al de los reinos de España y de Portugal, que en ese momento dominaban los mares gracias a sus técnicas de navegación, a las primeras representaciones de cartografía marina y a su superioridad naval. A diferencia de los españoles y portugueses, los ingleses no eran ni misioneros ni colonos. Cuando los ingleses decidieron utilizar el mar como medio de expansión, tuvieron que buscar beneficios inmediatos, por lo que su situación de inferioridad con respecto a las flotas de guerra adversarias los llevó a recurrir a la piratería. Los corsarios y bucaneros ingleses robaban los metales preciosos transportados por los navíos españoles y portugueses procedentes de América del Sur. Durante el reinado de Isabel I, las redes comerciales británicas se extendieron hacia Turquía y Rusia. Si la demanda de azúcar atrajo a los mercaderes ingleses hasta el Caribe, la demanda de especias, de té y de tejidos les incitó a proyectarse hacia Asia. La incorporación del reino de Escocia al reino de Inglaterra, que dio lugar al nacimiento de Gran Bretaña en 1707, llevó a la creación del mayor sector de libre comercio de la época y también a la aparición del primer modelo de consumo de masas del mundo para los productos importados, tales como el té, el café, el tabaco y el azúcar.

Durante el siglo XVII, los ingleses aprovecharon el enorme potencial comercial de las adquisiciones en ultramar. La creación de la British East India Company (BEIC) abrió la vía de la colonización hacia la India. La agresividad comercial de la Compañía Británica de las Indias Orientales la llevó a adoptar progresivamente una postura político-militar sobre el subcontinente indio, y tuvo que reclutar tropas locales para poder realizar operaciones armadas contra soberanos regionales que protestaban contra su hegemonía. El aumento del marco militar de la colonización fue resultado también de la rivalidad entre los diferentes imperios europeos.

El desarrollo de intercambios entre los continentes gracias al comercio triangular incitó a los ingleses a tomar el control de las principales rutas marítimas más allá de Europa occidental, no solo hacia las Indias orientales sino también hacia el Báltico, América del Norte, el Mediterráneo y África occidental. En el origen de los desafíos económicos de las guerras anglo-holandesas entre 1684 y 1784 se encuentran en:

- El control de las principales rutas comerciales.
- La confiscación del tráfico comercial con las colonias británicas.
- El cuestionamiento de la posición dominante adquirida por la Compañía Holandesa de las Indias Orientales (Vereennigde Oost-Indische, VOC[12]).

Los holandeses habían sentado las bases de un imperio comercial a partir de una dinámica privada. La VOC era una sociedad mercantil surgida de las alianzas matrimoniales de grupos familiares y provinciales que erigió en dos siglos un auténtico imperio comercial[13] que la convirtió en la compañía más influyente entre las compañías europeas fundadas en el siglo XVII para explotar las riquezas de Asia. Pero la vocación privada de la VOC no le permitió hacer frente a la versatilidad guerrera de los imperios español y portugués, que buscaban acaparar el control del comercio de especias procedentes del archipiélago indonesio. Tuvo que incorporar al desarrollo comercial los mecanismos de conquista armada inspirados en el modelo portugués. En 1699, la VOC era la mayor fuerza económica privada del mundo y disponía de una fuerza militar en consonancia de cuarenta navíos de guerra y diez mil soldados. Gran Bretaña entró en conflicto con ella para romper su estrategia de monopolio sobre el comercio entre América y Asia.

La protección de las rutas comerciales de Gran Bretaña, y con ello de su prosperidad económica, guió la política exterior británica y trajo consigo intervenciones militares durante el período del Imperio. Numerosos ejemplos de luchas armadas ilustran estos hechos:

- Desde el momento en que Gran Bretaña sintió amenazados sus intereses en India por la expansión meridional y oriental de los rusos, la protección de la India contra estos por vía terrestre y marítima se convirtió en el eje principal de la política exterior victoriana. De ahí el enfrentamiento militar con la Rusia zarista en Asia central, que era todavía un «punto débil» alejado de las expansiones coloniales europeas. Las dos guerras anglo-afganas, la primera (1839-1842) y la segunda (1878-1880), muestran esta estrategia.

[12] BURBANK, Jane y COOPER, Frederik. *Empires, de la Chine ancienne à nos jours*. París: Payot, 2011. Página 219

[13] La VOC era un auténtico Estado dentro del Estado. Aseguraba las principales funciones reguladoras (policía, defensa, justicia) en sus despachos comerciales de las Indias orientales y decidía sobre la guerra y la paz con los príncipes autóctonos, disponiendo de esta forma de una diplomacia autónoma.

- Las guerras del Opio[14] (1839-1842 y 1856-1860) entre el Reino Unido y el Imperio quing tenían una finalidad económica. Gran Bretaña quería forzar al Imperio chino a abrirse al comercio internacional. Uno de los objetivos del Imperio británico era obtener la cesión del territorio de la ciudad de Hong Kong por parte de China con el fin de almacenar el opio y comerciar con él en China. Se trata de un ejemplo claro de acto militar al servicio de un objetivo económico.
- La decisión del primer ministro Disraeli de adquirir una parte de los títulos del canal de Suez en 1875 intentaba impedir que Francia tomara el control de una ruta comercial esencial.
- La ocupación de Egipto aseguró al Imperio británico el mantenimiento del control de la plataforma estratégica de El Cairo.
- La guerra declarada por el Imperio británico contra los Boers estaba justificada por el control del punto estratégico que representaba Ciudad del Cabo. Los británicos prepararon esta base en el extremo de África con el fin de acondicionar una ruta marítima de emergencia en caso de cierre del canal de Suez. En segundo lugar, una parte del territorio gobernada por los Boers se reveló como una de las mayores reservas de oro del mundo.

El ejemplo británico ha demostrado cómo el predominio de una potencia en el control de rutas comerciales se convierte en una baza determinante en los enfrentamientos de naturaleza geoestratégica.

La imbricación de la guerra y de la economía

Las guerras revolucionarias y napoleónicas, escalonadas entre 1792 y 1815, acentuaron el peso de la economía en la evolución de las relaciones de fuerza entre los países implicados en esta sucesión de conflictos sometidos a alianzas. A este respecto, las repercusiones económicas de los bloqueos tuvieron un gran peso en los cambios estratégicos de Francia y Rusia.

La influencia de los enfrentamientos económicos en la conducción de la guerra

El primer ministro William Pitt, cuya fortuna familiar provenía del comercio angloindio, se fijó como línea de acción preservar la posición de Gran

[14] A mediados del siglo xix, los occidentales vendían en China varias decenas de miles de cajas de opio al año. Los británicos se hacían pagar en lingotes de plata para recuperar una parte de los fondos que pagaban a los chinos en el comercio del té. Este tráfico de opio permitió al Imperio británico invertir a su favor el desequilibrio de los intercambios con este país. La guerra del Opio surgió de una relación desigual que generó una corrupción cada vez mayor entre los funcionarios chinos y provocó estragos entre la población.

Bretaña en su dominio del comercio mundial a través del control de los mares. Su estrategia era apostar por la Royal Navy, que representaba la única fuerza superior comparada con la capacidad militar de la Francia revolucionaria y posteriormente napoleónica. Mientras que el aliado prusiano de Gran Bretaña combatía a los franceses y sus aliados en Europa, la Royal Navy debilitaba el potencial económico del enemigo común impidiendo a Francia comerciar por mar. El punto clave de la política seguida por Pitt fue establecer una ventaja marítima indiscutible, pues obtuvo el apoyo del Parlamento de Londres para aumentar la flota de combate británica hasta los 105 navíos. Esta carrera armamentista naval dio a Inglaterra una ventaja decisiva ya que la flota francesa solo disponía de 70 navíos.

Por primera vez en la historia, la guerra económica se convirtió en global con la aparición de dos sistemas de bloqueo utilizados por los beligerantes: el bloqueo marítimo de Inglaterra contra Francia y el bloqueo continental[15] de Francia para cortar las exportaciones británicas hacia Europa. Anteriormente, las acciones de bloqueo solo habían afectado a ciudades portuarias. La originalidad de los dos bloqueos era la voluntad recíproca de franceses e ingleses de utilizar las medidas de represalia económica a nivel estratégico para alcanzar una salida favorable al conflicto. Es lo que, por otra parte, sucedió, pero no forzosamente tal y como esperaba Napoleón I ya que la retirada de Rusia del «sistema continental» buscado por Francia desencadenó la campaña de Rusia, tan funesta para el Imperio napoleónico.

Esta imbricación de la guerra y la economía dio lugar al nacimiento de los primeros mecanismos de guerra económica que se prolongaron en tiempos de paz. A finales del siglo XVIII, Francia estaba muy debilitada en el plano industrial por el esfuerzo bélico realizado durante las guerras revolucionarias contra la Europa de las monarquías. Napoleón confió a un científico, Jean-Antoine Chaptal[16], la misión de encontrar los medios de dinamizar la industria francesa y protegerla de las amenazas comerciales británicas. Esta voluntad de resurgimiento productivo demandaba una recuperación en términos de innovación. Napoleón quería saberlo todo sobre los puntos fuertes y las debilidades de la economía británica y confió esta misión a la creada Sociedad de Estímulo de la Industria Nacional (SEIN), que orquestó el dispositivo de observación de los descubrimientos al otro lado del canal de la Mancha. Con un retraso de entre quince y veinte años en conocimientos técnicos, las manufacturas francesas debieron cubrir imperativamente esa desventaja por todos los medios, incluyendo el recurso a prácticas ilegales de contrabando de máquinas compradas clandestinamente o robadas en suelo británico.

[15] El bloqueo fue efectivo en los países aliados a Francia y en países ocupados por sus tropas (Italia, España, Holanda, Baja Alemania y Dinamarca).

[16] Chaptal ocupó a la vez las funciones de ministro del Interior y de Industria.

En un contexto de prohibición de importación de productos ingleses iniciado en 1793, Napoleón consolidó este sistema de defensa económica con la militarización de las aduanas[17]. Su ministro Chaptal consideraba esta administración como la «garante de la independencia industrial de Francia»: las aduanas representaban el 20% del total del personal de la administración en 1815 (excluido el Ejército). Esta política de restricción comercial con respecto a Gran Bretaña se prolongó con la Restauración bajo la gestión del director general de aduanas Saint Cricq, que se mantuvo en funciones hasta 1824, año en el que pasó a ocupar la cartera del Ministerio de Comercio con Carlos X.

Lucha ideológica y relaciones económicas de fuerza entre potencias

A pesar del enorme coste económico de las guerras contra Francia, Gran Bretaña se mantenía en una posición de fuerza. La revolución industrial, iniciada mucho antes que en el continente, situaba sus productos manufacturados en una posición de competencia muy ventajosa. Sus colonias le garantizaban un abastecimiento importante en materias primas y su supremacía naval le permitía bloquear las principales rutas comerciales marítimas. Consecuentemente, a Londres le interesaba promover la desaparición de las barreras aduaneras con el fin de vender sus productos en otros países, especialmente en Europa.

Para romper con las barreras proteccionistas mantenidas por Francia, el Gobierno británico le otorgó una mayor dimensión estratégica a las técnicas incipientes de guerra económica en tiempos de paz. La prensa[18] jugaría un papel determinante en esa relación de fuerzas: Londres envió a París, presidiendo la comisión británica encargada de las negociaciones con las autoridades galas sobre libre comercio (*free trade*), al economista político John Bowring[19]; las razones que llevan a David Todd[20] a presentar a John Bowning como un agente influyente al servicio de la Corona son sus métodos de trabajo cuyos objetivos principales son, en primer lugar, crear en Francia grupos de presión favorables a las tesis británicas, y en segundo, utilizar a la prensa local para hacer llegar sus ideas a los círculos de poder económico y político. Así resume su gestión:

> *En 1834, a través de una serie de misivas enviadas a Lord Auckland, presidente del Board of Trade, Bowring le explica en detalles la es-*

[17] TODD, David. *L'identité économique de la France. Libre échange et protectionnisme (1814-1851*). París: Grasset, 2008. Página 64.

[18] En 1834, en París, se imprimieron 6.500 ejemplares de tratados y manuales de economía liberal.

[19] También intervendría en Suiza, Italia y Alemania.

[20] Véase p. 183.

trategia que desarrolla en Francia en sus desplazamientos. En cada ciudad que visita, intenta congregar y formar un grupo de partidarios del libre comercio. A continuación, mantiene una correspondencia intensa con dichos partidarios para dirigirlos hacia el objetivo común: el derrocamiento de los monopolios. Los grupos se encargan de divulgar en prensa las ideas liberales y de formular declaraciones solemnes a favor de la libertad de mercado. Así consiguen influir favorablemente en la opinión pública: «La opinión, la opinión ilustrada, es el mejor instrumento para la consecución de nuestro objetivo: sin ella no haríamos el menor progreso; con ella los alcanzaremos todos».

John Bowring la emprendió con las tesis de Saint Cricq, a quien consideraba un enemigo de Inglaterra[21]. Centra su acción en las regiones exportadoras (sedas en Lyon, vinos en Burdeos). Sus numerosas intervenciones en los círculos de poder franceses tenían como objetivo incitarles a que denunciasen el sistema prohibitivo francés, y así busca apoyos en regiones arrebatadas a los ingleses en la guerra de los Cien Años, como Aquitania, donde muchos productores de vinos se oponen a las tasas aduaneras[22]. Otra forma de acercamiento empleada por Bowring fue el diálogo que establece con los liberales franceses, como con Benjamin Constant y Jean Baptiste Say, con quienes mantenía contactos como político. Bowring sabe aprovecharse de las contradicciones internas del mundo de la política gala, apoyándose en los órganos de la prensa republicana antigubernamental que va desde el centro izquierda a la extrema izquierda. También supo recoger los frutos de su trabajo sobre el terreno e incitó a sus partidarios a que formulen peticiones colectivas reclamando la eliminación de las barreras proteccionistas impuestas por Francia.

Creación de estructuras dedicadas a la guerra económica

La Primera Guerra Mundial[23] asentó las bases del arma económica como forma de alcanzar un objetivo. A partir de 1914, conscientes de que el conflicto será largo, las potencias implicadas conciben una estrategia de guerra económica, como lo atestigua la siguiente nota[24] dirigida al agregado militar norteamericano en París.

Tras la batalla del Marne, frente a la nueva deriva de la guerra, el alto mando entendió que sería larga y que no bastaría con combatir al ene-

21 Véase p. 199.

22 Los viticultores franceses eran muy poderosos en aquella época al representar la décima parte de la población activa implicada en actividades vitícolas principales o secundarias, es decir, dos millones de personas.

23 SOUTOU, Georges-Henri. *L'or et le sang, les buts de guerre économiques de la Première Guerre Mondiale*. París: Fayard, 1989. Página 566.

24 *Revue Historique des Armées*, n.º 4. París: 2001.
BOURLET, Michaël. *Guerres mondiales et conflits contemporains, Jean Tannery (1878-1939) à l'origine de la guerre économique*. París: PUF, 2004.

migo en el campo de batalla sino que había que combatirlo en su propia casa. Impedir que los ejércitos enemigos dispusieran de material, minar moralmente y físicamente al conjunto de la población, cortarle el suministro de materias primas necesarias para su industria, colapsar el comercio, bloquear las finanzas, alcanzando incluso el abastecimiento alimentario. Estas son las ideas básicas sobre las que se asienta la guerra económica.

El ministro de la Guerra francés organizó, en 1915, un sistema dedicado a la información económica. Se creó una Sección de Control, dirigida por el civil Jean Tannery[25], magistrado del Tribunal de Cuentas. Dicha sección organizó la recogida de información que se requería para la puesta en práctica de acciones de guerra económica:

- Identificación de los ejes de abastecimiento alemanes y estudio de las disposiciones que habrían de tomarse para impedir dicho abastecimiento.
- Seguimiento de la organización y desarrollo de la industria de guerra alemana.
- Preparación de planes de destrucción de los centros industriales.
- Establecimiento de las listas de empresas relacionadas con el enemigo.
- Aplicación de restricciones y trabas.
- Control de los flujos económicos con el fin de impedir las relaciones económicas de Alemania con el exterior.

Gran Bretaña se organizó de manera diferente usando un organismo independiente, el War Trade Department Intelligence, que gravitaba en torno al Foreign Office. Los italianos crearon por su lado, en 1916, el Ufficio di Raccolta e Controllo di Notizie Economiche, vinculado a su Ministerio de la Guerra. Estas estructuras estaban coordinadas por una Oficina Interaliada con sede en París.

A lo largo del conflicto, las acciones de guerra económica fueron centrándose, ya fuera sobre objetivos internacionales como el racionamiento de los países del norte de Europa, con el fin de obligarles a renunciar a sus exportaciones con Alemania, o con operaciones militares llevadas a cabo gracias al desarrollo de la aviación, como el bombardeo de las estaciones de selección de una Lorena, que, ocupada, proporcionaba las tres cuartas partes del hierro que necesitaba la industria siderúrgica alemana.

En 1918, hubo disparidad de criterios entre franceses, británicos y estadounidenses sobre los objetivos que había que alcanzar. Para París, el arma económica no solamente era un arma de guerra para forzar a Alemania a firmar la paz, sino también la posibilidad de preservar las

[25] BOURLET, Michaël. *Guerres mondiales et conflits contemporains, Jean Tannery (1878-1939) à l'origine de la guerre économique*. París: PUF, 2004.

ventajas conquistadas en caso de victoria. Francia deseaba llegar al entendimiento entre los aliados sobre la manera de mantener a Alemania en una situación de debilidad económica, controlando conjuntamente las materias primas. Para Washington, el arma económica podía desempeñar el papel de palanca estratégica y política que forzara a Alemania a firmar una paz aceptable y que acabase con su expansión económica[26].

Enarbolando los principios del liberalismo económico, Estados Unidos buscaba hacerse un sitio dentro del mercado mundial mientras que Londres seguía la línea de Washington aunque preservando sus propios intereses (protección de las principales industrias, relaciones de privilegio con los *dominions* sobre la cuestión del control de las materias primas).

Tras el final del conflicto, las estructuras de la guerra económica desaparecieron. Al inicio de la Segunda Guerra Mundial, el primer ministro británico, Neville Chamberlain, creó, en septiembre de 1939, un Ministerio de la Guerra Económica con atribuciones similares a las estructuras elaboradas durante la Primera Guerra Mundial. En julio de 1940, Winston Churchill le otorga a ese ministerio un papel muy ofensivo al adjudicarle un nuevo servicio, el Special Operations Executive, que se encargaría de las operaciones de sabotaje en el continente y de la incitación a la rebeldía y a la resistencia en los territorios ocupados por los ejércitos alemanes. La notoriedad de ese nuevo organismo hizo que pasaran a un segundo plano los aspectos específicos de la guerra económica. Ese ministerio cesó su actividad tras la derrota de la Alemania nazi.

Si la imbricación de la economía y de la guerra hizo visible, durante algunas décadas, la problemática de la guerra económica, en la segunda parte del siglo xx se volvió invisible por las siguientes razones:

- La Guerra Fría obligó a los estados del bloque occidental a acallar o a enmascarar sus desacuerdos económicos, primando la imagen de unidad ideológica frente al bloque comunista.
- Los Estados Unidos, nueva superpotencia mundial, hizo suya la estrategia británica de presión aplicada para acabar con las barreras proteccionistas en Europa continental. Los textos sobre el libre comercio y la libre competencia se han convertido en lectura obligada de la realidad económica del mundo político occidental. Las relaciones económicas de fuerza entre potencias se silencian o se consideran dentro del mundo universitario, en particular por la mayoría de los economistas liberales, anomalías poco representativas de la relación de competencia entre empresas.

[26] HAUSER, Henri. Les *méthodes allemandes d'expansion économique*. París: A. Colin, 1919.

Las justificaciones geopolíticas de la conquista

La búsqueda de lecturas obligadas sobre la guerra económica implica analizar simultáneamente la evolución de los mecanismos de conquista (territorial y comercial) y los métodos de desarrollo de poder de los Estados.

Las conquistas comerciales comenzaron a sustituir a las conquistas territoriales durante el siglo XIX. Contrariamente a la conquista territorial, a menudo llevada a cabo recurriendo a la guerra tradicional, la conquista comercial tiende al incremento de la supremacía de un Estado por la ampliación de sus círculos de poder sobre los mercados exteriores.

Históricamente, algunas potencias no han dudado en debatir casi públicamente sobre su expansión, necesaria para su supervivencia. Es en particular el caso de Japón y de Alemania, que se han preguntado en varias ocasiones sobre el tema de su espacio vital en términos de conquista territorial o de conquista comercial.

La conquista contra el imperialismo mercantil

A partir de 1853[27], Japón fue sometido a la conveniencia de los países occidentales. En un primer momento, los japoneses cedieron a las primeras presiones occidentales firmando el tratado de 31 marzo de 1854 en Kanagawa que consagraba la apertura de los puertos de Shimoda y Hakodate a los navíos comerciales con bandera estadounidense; en los años siguientes, el Reino Unido y las principales potencias europeas obtienen privilegios equivalentes. La subida al trono en 1867 del joven emperador Mutsuhito (cuyo reinado se denominaría *Meiji Tenno)* modificará los términos de la relación de fuerza: escuchando a los reformistas, el joven soberano quiso evitar caer bajo la dominación de Occidente (como fue el caso de China durante el mismo período con los « tratados desiguales»[28]).

La estrategia aplicada por Japón se apropió de un eslogan muy significativo: país rico, ejército fuerte. El *Naimusho*, fundado en 1873, es el ministerio encargado de planificar el desarrollo industrial. Hizo construir fábricas estatales inspiradas en modelos de las manufacturas europeas y luchó

[27] Es el año durante el cual la escuadra estadounidense, compuesta por cuatro navíos de guerra mandados por el comodoro Perry, se presenta en la bahía de Tokio. Era portador de una carta «amistosa» del presidente de los Estados Unidos para el *shôgun* de la familia Tokugawa. Después de una segunda escala en 1854, el comodoro Perry exige al *shôgun* la apertura de los puertos japoneses a los navíos comerciales y a los balleneros norteamericanos.

[28] Resultado de las derrotas militares chinas frente a las tropas occidentales, los tratados desiguales firmados en el siglo XX entre China y las potencias occidentales y el que Rusia trataba de imponer a China una apertura de su mercado interior.

discretamente para impedir que el capital extranjero tomara posesión de los puntos estratégicos de una economía de mercado nipona emergente (infraestructuras portuarias, astilleros navales, industria de armamento). La modernización de Japón se realiza en el marco de una política de adquisición de conocimientos de toda índole adquiridos fuera de las fronteras, siguiendo el ejemplo de los países más experimentados en su ámbito.

Al inicio del siglo xx, el expansionismo japonés (anexión de Corea, reivindicación de una tutela sobre China) provoca un antagonismo con los Estados Unidos, que querían dejar una puerta abierta en China. Benoit Meschin[29] resume así el informe de fuerzas entre los dos países tras la conferencia naval de Washington[30] en 1921:

> *Ligado por los acuerdos de Washington, excluido por los Estados Unidos con su nueva ley de inmigración, dificultado en su desarrollo económico por las restricciones cada vez más severas impuestas por el servicio de aduanas americano a la importación de productos japoneses a los Estados Unidos, ¿qué puede hacer Japón para no quedar recluido en sus islas y resolver los problemas dramáticos derivados del aumento cada vez más rápido de su población?*

Después de haber buscado en un principio romper con el aislamiento recurriendo a una especie de colonización en Corea, Japón consideró que le sería vital construir una zona de prosperidad compartida a nivel regional[31] que reagruparía a todos los países ocupados por el Ejército Imperial japonés durante las fases de expansión del Imperio. La ocupación de Manchuria en 1931 se inscribe en esta perspectiva.

La fundación del Estado de Manchukuo, un año más tarde, es un ejemplo de reproducción de sistemas militarizados de conquistas inventados por los portugueses e imitados por los holandeses e ingleses al inicio de los procesos de colonización de la Historia Moderna.

Los japoneses han copiado el modelo de la antigua Compañía de las Indias pero se han inspirado también en la dinámica del desarrollo producido por las compañías de ferrocarril americanas, que construyeron un imperio industrial al unir la costa este al Pacífico. Al final de los años 30, Manchukuo estaba bajo administración de la Compañía de Ferrocarriles Manchúes[32], que gobernaba este territorio de manera relativamente au-

[29] MESCHIN, Benoit. *Histoire de l'armée allemande*, tomo 1. París: Robert Laffont, colección Bouquins. Página 847.

[30] Los Estados Unidos rechazan la igualdad marítima con Japón y le obligan a desarmar parte de su flota de guerra.

[31] El proyecto de área compartida de prosperidad de la Gran Asia oriental fue propuesto por el general Hachirō Arita, ministro de Asuntos Exteriores de 1936 a 1940.

[32] Más del 75% de los ingresos de la compañía procedían de las explotaciones de soja a Japón y a Europa. En 1927, la mitad de la oferta mundial de soja procedía de Manchuria.

tónoma con respecto a Tokio. Dirigía las tropas japonesas de ocupación, gestionaba su propia Policía, estaba a la cabeza de una Administración local de más de 200.000 empleados y poseía su propio banco de emisión así como su flota mercante. El Estado de Manchukuo servía de laboratorio de experiencias a un nuevo concepto de supremacía del poder mediante la economía.

La conquista del espacio vital

La historia de Alemania está marcada por la búsqueda de nuevos territorios para ser conquistados ya sea de forma pacífica o mediante el uso de la fuerza. Desde el principio de la Antigüedad, los escritos de los romanos dan cuenta de las condiciones de vida particularmente difíciles de los pueblos germanos. Cubiertos de bosques y poco propicios a la agricultura, los territorios del norte de Europa no permitían la subsistencia de sus poblaciones. Para sobrevivir, los pueblos germanos debían conquistar territorios más prósperos en cuanto a subsistencias. Esta estrategia de conquista fue llevada a cabo sobre el frente terrestre y el marítimo: al final de la Edad Media, los colonos alemanes habían comenzado a establecerse al este de Baviera y banqueros como la familia Fugger de Augsburgo habían financiado la explotación de las minas y bosques checos. Este intercambio comercial les había permitido conquistar pacíficamente los antiguos mercados de los príncipes eslavos, estando en el origen del urbanismo de los territorios de Bohemia y Moravia. Pero esta colonización no ha sido siempre pacífica: los polacos la habían rechazado y se habían opuesto a los Caballeros Teutones.

La fundación de la Liga Hanseática[33] abriría la vía a la conquista marítima. La expansión de los puertos del Báltico le brindó a Alemania, así como a las ciudades del norte de Europa, los medios para establecerse pacíficamente en las costas polacas entre los siglos XVI y XVII. Las campañas militares llevadas a cabo por la familia prusiana de los Hohenzollern consumaron la creación de una esfera de influencia al este de Alemania. Esta búsqueda permanente de un espacio vital en el exterior de las fronteras ha forjado de manera permanente en el espíritu de las élites alemanas un sentido agudo del reparto de fuerzas.

El debate sobre la oportunidad estratégica de la conquista territorial o la conquista comercial domina la vida política del II Reich. La realización de la unidad alemana por Bismarck permitió a este país asumir un papel influyente a nivel mundial y trajo el aumento del poder de Alemania al final del siglo XIX, que no se limita al paso dado por la economía alemana a la

[33] Asociación de comerciantes alemanes y posteriormente de ciudades de Alemania del Norte y de Europa septentrional que dominó el comercio báltico entre el siglo XII y el XVII.

era industrial pues la movilización de los actores económicos alemanes es indisociable de las posturas geoestratégicas del II Reich, que estaba fuertemente determinado por la actitud de los imperios coloniales británico y francés. El corazón estratégico alemán (Konzern[34], bancos, sociedades de seguros) forjado en aquella época quería dominar a las demás potencias europeas.

Esta dimensión del debate no se les escapó a adversarios de Alemania como Georges Clémenceau quien, desde 1915, estimaba que el peligro alemán era mayor en la paz que en la guerra, por la manera en la cual Alemania había sabido desarrollar una economía competitiva hasta el punto de rivalizar en el plano mundial con la economía del Imperio británico.

La Primera Guerra Mundial hizo surgir controversias sobre la manera de administrar una hipotética victoria militar en el ámbito geoeconómico una vez conquistada la paz. El resultado de esta reflexión en Alemania apareció en 1915 con una obra que puede ser considerada hoy como el esbozo de un manual de guerra económica. Fue traducido al francés adoptando el provocador título de *El plan de guerra comercial de Alemania*[35]. Desde el principio del libro, la connotación es evidente: «todo comercio es una guerra, el mundo es un campo de batalla». Calificado posteriormente por los estadounidenses como el Bernhardi[36] del comercio, Herzog definió los medios de acción económica a poner en marcha contra los enemigos del Reich. Son de dos tipos:

- Los factores que pueden influenciar o controlar las exportaciones en la guerra comercial.
- Los factores que permitirán a Alemania vencer la resistencia pasiva de los países vencidos.

En caso de victoria contra los aliados, Alemania sabe que tiene que afrontar el «odio mundial». Deberá entonces hacer frente a todo tipo de represalias de los países vencidos (cese de aprovisionamiento de ciertas materias primas, boicot a sus exportaciones, censura a sus científicos en los encuentros internacionales o plagio sistemático a su tecnología punta). Para justificar sus temores, Herzog cita una revista técnica inglesa que insiste, al principio de las hostilidades, sobre la necesidad de lanzar contra Alemania una guerra económica basada en la ciencia. Los británicos aún conservan el resentimiento de la época victoriana por el pillaje de sus técnicas por los europeos y norteamericanos.

El dominio de la innovación que conlleva el control de la ciencia es para ellos la base de toda guerra económica. Para conservar el patrimonio eco-

[34] Asociación de empresas que se desarrollan mediante concentración horizontal y vertical.

[35] HERZOG, S. *Le plan de guerre commerciale de l'Allemagne*. París: Payot, 1919.

[36] General alemán (1849-1930) teórico del pangermanismo.

nómico de su país, Herzog sugiere un control estatal que se aplicará «a las industrias que los países extranjeros no hayan despojado aún de sus capacidades». A pesar de defender esta medida, no cuestiona la economía de mercado: se debe amparar la iniciativa privada sin perjudicar los intereses económicos de la nación, ya que el afán de lucro puede incitar a los empresarios a deslocalizar las empresas a países que se apropiarán de los secretos de fabricación convirtiéndose así en competencia potencial.

En cuanto la obra de Herzog se dio a conocer, los norteamericanos la hicieron traducir y la difundieron ampliamente. Herbert Hoover, ministro americano de Abastecimiento, futuro presidente de los Estados Unidos, indicó en un prefacio de la versión americana del libro que la amenaza de enfrentamiento económico se había percibido claramente en este inicio de siglo: «No satisfecha de la supremacía militar, vemos a Alemania intrigar por la supremacía comercial, con ese desprecio insultante hacia los derechos de los demás, y ese recurso a la mala fe que ha caracterizado toda su política desde Federico el Grande».

El encubrimiento de la guerra económica

Desde la antigüedad hasta la era de las revoluciones industriales, la supremacía de la realidad económica es una constante en la naturaleza de las relaciones de fuerza entre individuos, grupos y países. El profesor Edward Mead Earl, del Institute for Advanced Study, ha recalcado la relación dialéctica entre la dimensión política y económica del poder[37]:

> *De ser posible separar el poder económico del poder político, esto solo ocurriría en las sociedades más primitivas. En los tiempos modernos (con la emergencia del Estado nacional, la expansión de la civilización europea en el mundo entero, la revolución industrial y los progresos constantes de la tecnología militar), ha sido necesario afrontar la cuestión de la interdependencia entre la fuerza comercial, financiera e industrial por una parte, y la fuerza política y militar por otra. Esta correlación es uno de los problemas más peliagudos del arte de gobernar. Afecta a la seguridad de una nación y, en gran medida, a la determinación del grado de vida, libertad, propiedad y felicidad que puede gozar el individuo.*

Lo mismo ocurre con la teoría realista de las relaciones internacionales: a pesar de haber ignorado el aspecto económico de la búsqueda del poder, se describe el *animus dominandi* como elemento constitutivo del conjunto de asociaciones humanas y de relaciones sociales y, por tanto, de la vida política nacional e internacional. Hans Morgenthau[38] destaca

[37] Mead Earl, Edward. *Les maitres de la stratégie,* tomo 1. París: Flammarion, 1986.

[38] MORGENTHAU, Hans. *Politics among nations. The struggle for power and peace*. Nueva York: Mac Graw-Hill, 1948, p. 29.

que la política internacional es una lucha por el poder. Pero el poder no es solo militar. Sin embargo, al contrario que en la guerra militar, la guerra económica no se ha convertido en un tema de debate en los medios políticos y académicos.

¿Cómo explicar tal omisión de relaciones de fuerza en las lecturas obligadas referentes a las relaciones conflictivas entre los pueblos? Desde la alta Edad Media, se ha negado el carácter de fenómeno histórico a todo lo relativo a la guerra económica con el pretexto de que las justificaciones políticas de la guerra económica se percibían como acciones de agresión ilegítimas. El debate sobre la guerra, apenas iniciado por San Agustín y Santo Tomás de Aquino, sienta las bases de un razonamiento que identifica la guerra económica con «una visión negativa de la guerra desencadenada por la codicia y la voluntad de enriquecerse a costa de los demás[39]».

La idea de injusticia se asoció rápidamente a las guerras de conquista. Durante el descubrimiento del Nuevo Mundo, los conquistadores tuvieron que justificar el recurso a las armas contra los pueblos que se oponían a la conquista de sus territorios. El texto *De jure belli* de la Escuela de Salamanca (XVI-XVII) calificó a los indígenas rebeldes como enemigos desleales al adoptar una actitud intratable frente a los conquistadores. Así, mediante el embargo de los bienes y la cautividad de los indígenas rebeldes, el resultado de una guerra-sanción quedaba justificado a los ojos del mundo cristiano.

Los resultados de este debate ideológico, fuertemente inculcado en la historia de las ideas políticas, han incitado a los actores estatales de los enfrentamientos económicos a enmascarar su estrategia mediante pretextos diversos como la difusión de un pensamiento religioso, la modernización de los países del Tercer Mundo, y, de manera más reciente, el desarrollo de la democracia. Esta política casi sistemática de disimulación de los verdaderos objetivos de conquista ha falseado la interpretación de las relaciones de fuerza ligadas al proceso de supervivencia de un pueblo o provocados por la búsqueda, el mantenimiento y el aumento del poder de un país. Quizás habría que encontrar una relación con el hecho de que, en la actualidad, no existe ninguna doctrina sobre guerra económica en el seno de las organizaciones internacionales de vocación militar tales como la OTAN (Organización del Tratado del Atlántico Norte). En el enfoque global definido por la nueva doctrina (OTAN) 2010[40], el recurso al

[39] «Où en est la notion de guerre juste?» Texto de François Rigaux, profesor emérito de derecho internacional de la Universidad Católica de Lovaina, publicado en la obra *Colère, courage, création politique*, vol. 1, p. 163-177. París: L'Harmattan, 2011.

[40] *Concept et doctrine*, OTAN, sitio oficial.
http://.www.nato.int/nato_static/assets/pdf/pdf_publications/20120203_strategic-concept-2010-fr.pdf.

arma económica no aparece nunca como una opción ofensiva sino como un factor de comprensión del entorno. Este tipo de omisión se entiende por la divergencia de los desafíos económicos nacionales en el seno de la comunidad de los estados miembros[41].

El encubrimiento de la guerra económica se aplica tanto a las estrategias de dominación puestas en marcha por los imperios coloniales como a las estrategias de recuperación de los países que querían evitar la colonización o que persiguieron posteriormente el poder.

Las estrategias de dominación

La cuestión religiosa contribuyó a enmascarar la finalidad de los enfrentamientos, que implicaba beneficios económicos nada desdeñables. Una bula papal de 1452 daba carta blanca a los portugueses para atacar, conquistar y someter a los sarracenos, paganos y demás infieles. Una segunda bula papal de 1454 reconocía los actos de conquista portugueses en África al contemplar las posibilidades de conversión al cristianismo de las poblaciones locales y validando el monopolio comercial de los portugueses en una zona territorial de la costa de Guinea, así como en todos los territorios situados presuntamente en la ruta de la seda.

En 1494 se negoció el Tratado de Tordesillas[42] bajo la autoridad de la Iglesia Católica con Alejandro VI, papa de origen español. Buscaba la resolución de los conflictos originados a raíz de los descubrimientos de Cristóbal Colón y estableció el reparto de las tierras del Nuevo Mundo entre España y Portugal, que eran las dos potencias coloniales emergentes. Además, los portugueses obtuvieron el reconocimiento papal de las conquistas de sus territorios en África y se arrogaron el derecho de inspeccionar cualquier barco que se encontrara en aguas africanas. Este tratado no fue reconocido por ningún otro reino europeo, pero tradujo ante todo la realidad de las relaciones de fuerza entre las dos potencias marítimas dominantes en esa época.

Tras haber sido durante mucho tiempo enmascarada con el pretexto de la evangelización de los pueblos considerados primitivos, el encubrimiento de la guerra económica es la consecuencia de una nueva fase de desarrollo del poder en los albores de las revoluciones industriales. Si la guerra militar había evolucionado gracias a las invenciones técnicas, la noción de poder había sido objeto de una auténtica

41 Mazzucchi, Nicolas. «Alliance militaire et guerre économique», *Revue de la Défense Nationale,* n° 752, pp. 1-3. Paris: 2012.

42 Casi todas las Américas pertenecían a España, excepto Brasil. Los portugueses se aseguraban el control de varios territorios costeros de África, Oriente Medio (Eritrea, Somalia) y del sudeste asiático (Goa, Colombo, Malacca, Timor), excepto las islas Filipinas, reivindicadas por España junto con las Canarias (Atlántico).

metamorfosis bajo el impacto de la creación de imperios económicos. El nacimiento del liberalismo destaca una nueva manera de incremento de poder mediante la conquista comercial, que se convierte a su vez en una alternativa a la conquista territorial tradicional. El Imperio victoriano integra la dinámica de la guerra económica, legitimando su razón de ser y enmascarando su finalidad mediante un discurso sobre la apertura de los mercados defendida por la teoría del libre comercio. La dinámica imperialista del Imperio británico contempla un deslizamiento decisivo de la lógica de la conquista territorial, necesariamente politizada, a la lógica de conquista comercial, es decir, de control por los mercados. El libre comercio se transforma así en norma para todo el Imperio[43]:

> *En definitiva, a través de la creación de una economía-mundo bajo la influencia británica, se dibujan las primeras estrategias económicas de incremento de poder. Gran Bretaña, al multiplicar las relaciones económicas –basadas en el* leit motiv *de Adam Smith «dejar hacer, dejar pasar»– con las unidades estatales gravitando en el interior y exterior de su economía-mundo, crea una zona de libre comercio en la que el liberalismo se propaga y el mercado se institucionaliza llegando incluso a sacralizarse como un medio de pacificación en las relaciones internacionales y de desarrollo de las naciones participantes. Por consiguiente, el Imperio británico obtenía grandes beneficios de este sistema que era su gran centro de poder al permitirle influenciar la circulación de capitales, de mercancías y de hombres. Consciente de su hegemonía, el centro de la economía-mundo (Londres) podía por tanto definir o incluso imponer la política comercial según sus intereses. De esta manera, entre 1840 y 1860, el volumen comercial entre Inglaterra y el resto del mundo se triplicó: los industriales ingleses exportaban sus bienes al resto del mundo en navíos ingleses con el apoyo de aseguradoras y bancos ingleses. Además, la balanza comercial es aproximadamente del 10% a favor de Inglaterra entre los años 1870 y 1914. Este crecimiento permite a Inglaterra estar en cabeza de los países en vías de industrialización, ser la primera potencia marítima y, sobre todo, controlar casi el 25% del mundo en 1901. Este cambio en el modo de conquista tiene su aplicación teórica en el desplazamiento de la lógica imperialista –militar y vertical– a la de la hegemonía económica, siendo esta última la capacidad de una unidad política de ejercer su soberanía efectiva en unas sociedades políticas extranjeras sin controlarlas formalmente*[44]*. Transformación*

[43] BLANOT, Harold; BOYER, Adrien; KÛHL, David y SPIESS, Margo. *La guerre économique comme explication structurante de la construction d'un pays*. EGE. París: Éditions de la Bourdonnaye, 2013.

[44] BATTISTELLA, Darion. «La notion d'empire en théorie des relations internationales», *Questions Internationales*, n° 26, julio-agosto de 2007, pp. 27-32, p. 30.

del poder que hará que Benjamín Constant afirme que la guerra no es más que una pulsión salvaje mientras que el comercio es cálculo civilizado. Los imperios coloniales conllevan un reparto de la tierra en distintas esferas de influencia.

La conquista comercial puede desembocar en guerra comercial al convertirse en un medio de coerción cuando los países codiciados por los comerciantes británicos se oponen a la voluntad de penetración en sus mercados internos. Para imponer sus productos en los mercados de Oriente Medio y de Asia oriental, los británicos instauraron la práctica de la «política de la cañonera», que tuvo su apogeo durante el bloqueo del puerto de Alejandría por la Royal Navy en 1840-1841 y, con posterioridad, en las dos guerras del Opio que, sucesivamente, enfrentaron a China contra Gran Bretaña y a China contra una coalición de países occidentales. Fue entonces cuando el mundo occidental impuso el comercio de la droga por medios militares a un país teóricamente independiente. William Jardine, que dirigía la firma de opio Jardine&Matheson en Hong Kong, legitimó esta acción haciéndose el valedor de la «libertad de empresa, independiente y sin restricciones»[45]. Conviene recordar que el pretexto utilizado para recurrir a la fuerza por parte de la potencia británica fue el embargo y la destrucción por las autoridades chinas de 20.282 cajas de opio desembarcadas en Cantón en 1839. El emperador chino Daoguang decidió suspender el comercio con los ingleses y condenar a la pena de muerte a los comerciantes extranjeros dedicados al comercio del opio. Los británicos consideraron las represalias chinas como un crimen de «leso comercio»[46] e iniciaron hostilidades que desembocaron en la adopción de tratados desiguales que «eran inicuos y cuya conclusión dejó, en las conciencias chinas, el germen de una voluntad de venganza que no haría más que ir en aumento a través de las generaciones sucesivas y tomaría su fuerza del resentimiento que suscitaba el recuerdo de una humillación»[47].

Las guerras del Opio dan gran visibilidad a la agresividad económica y llevan a países como Japón[48] a moldear la identidad nacional con una política de poder basada en la expansión económica simbolizada en el eslogan «un país rico, un Ejército fuerte».

La llegada al poder del emperador Mutsuhito en 1868 es el comienzo de una serie de reformas cuyo objetivo es recuperar el atraso respecto a

45 BRIZAY, Bernard. *Le sac du palais d'Eté. Seconde guerre de l'opium.* París: Rocher, 2011.

46 BRIZAY. *Ibíd.,* p 35.

47 LEGER François. *Les influences occidentales dans la révolution de l'Orient. Inde, Malaisie, Chine. 1850-1950.* París: Plon, 1955.

48 SOUYRI, Pierre-François. *La nouvelle histoire du Japon.* París: Perrin, 2010.

Occidente. Japón tardó más de un siglo en elaborar los fundamentos de una economía al servicio del poder. Al final de los años 80, la Central Intelligence Agency (CIA) publicó el informe *Japan 2000*[49] redactado por un grupo de trabajo compuesto por personalidades del mundo civil y militar. Este documento es una de las contadas muestras escritas contemporáneas de un texto de alcance gubernamental sobre las relaciones económicas de fuerza entre dos potencias. La parte más explicativa del texto denuncia la «propaganda japonesa» de enmascaramiento de medidas proteccionistas que el país aplica a las demás economías de mercado y su falta de respeto al liberalismo económico. Algunos pasajes del informe estigmatizan en estos términos la estrategia japonesa de poder: «Los miembros del Club del Crisantemo (que reúne a la élite de los medios políticos e industriales de Japón) consideran que el sistema occidental está condenado a desaparecer y actúan, en la medida de sus posibilidades, de manera a adelantar su final». La estrategia de recuperación japonesa llevada a cabo desde la era Meiji le permitió alcanzar el segundo puesto en la economía mundial en poco más de un siglo de esfuerzo. Al final de los años 80, se oyeron voces de denuncia del expansionismo nipón y del recurso a las técnicas de guerra económica en medios políticos y económicos de Estados Unidos y Europa.

La agresividad comercial del antiguo Imperio del Sol Naciente con respecto a Occidente se detuvo con la adopción de distintas medidas por parte de las autoridades norteamericanas (ataques repetidos para romper el proteccionismo nipón, desestabilización de su sistema bancario por la negativa a conceder una serpiente monetaria durante la crisis financiera asiática, bloqueo de su estrategia de tecnoglobalismo[50] y limitación de juegos de influencia japoneses en el sistema político administrativo norteamericano). La caída del muro de Berlín privó a Japón de su chantaje implícito a los Estados Unidos: las autoridades gubernamentales norteamericanas ya no tenían nada que temer de la inestabilidad de este aliado/antiguo adversario en la esfera de influencia soviética en el caso de que los Estados Unidos no otorgasen a Tokio el suficiente margen de maniobra para la construcción de su potencia económica. A pesar de ello, el estancamiento brutal de la potencia económica japonesa no invalidó las oportunas estrategias de recuperación.

[49] El informe *Japan 2000,* rápidamente retirado de la circulación por las protestas de las autoridades japonesas, anunciaba una tensión en las negociaciones entre Estados Unidos y Japón sobre la apertura de su mercado interior y el acceso al accionariado de sus grandes empresas.

[50] Elaborado en 1987 por el Ministerio de Industria y Comercio japonés (MITI), el tecnoglobalismo buscaba evitar un parasitismo de la investigación debida a las prácticas competitivas y poder así colmar la separación entre el norte y el sur, creando un patrimonio común de la humanidad. Tuvo lugar tras el endurecimiento norteamericano en el campo de las patentes y los intercambios científicos con Japón.

Las estrategias de recuperación

Las estrategias de recuperación se articulan en torno a objetivos elementales fuertemente dependientes del contexto geográfico y cultural. En el caso de Japón, su insularidad le ha empujado a dotarse prioritariamente de una infraestructura de vocación marítima (astilleros, puertos) y, en segundo término, a fundar las bases de una economía industrializada. Varios países, como Corea del Sur, India, Brasil o China, siguieron la estela japonesa privilegiando la construcción naval y la formación de grandes conglomerados industriales privados, los *chaeboles*, equivalentes coreanos de los *keiretsu* japoneses o antiguos *zaibatsu* disueltos por las autoridades de ocupación estadounidenses tras la derrota japonesa de 1945.

India siguió otros derroteros para posicionarse como actor dominante en la industria informática mundial. Las autoridades de Nueva Delhi llevaron a cabo una reforma escolar entre 1993 y 2004 para crear un yacimiento de recursos humanos necesario para el desarrollo de este campo de actividades de tecnologías de la información. El Gobierno federal decidió retirar momentáneamente del programa de enseñanza secundaria las materias literarias para reforzar el número de horas dedicadas a las matemáticas; el objetivo era favorecer la orientación de un máximo de estudiantes hacia las profesiones técnicas y de ingeniería informática. A partir de 2004 y de manera progresiva, las materias literarias fueron introducidas de nuevo por las autoridades al estimar que el objetivo había sido alcanzado. Esta política se basó igualmente en la transformación de la ciudad de Bangalore en capital de la alta tecnología. Las razones de su elección fueron sus condiciones climáticas al tratarse de uno de los escasos lugares de la India en el que la amplitud del monzón es débil. Se crea de esta manera un marco adaptado al regreso de los ingenieros indios y se facilita la vida de los expatriados occidentales.

Brasil desarrolló estrategias de recuperación apostando por el sector energético (el petróleo no convencional gracias a los yacimientos *offshore* y sus reservas amazónicas, el agua por sus presas hidráulicas, las energías renovables). El Estado brasileño[51] hizo de la firma Petrobras la avanzadilla de su estrategia de influencia geoeconómica. Este país busca adquirir una superioridad regional en el sector energético, principalmente por la adopción de numerosos acuerdos bilaterales firmados con los estados vecinos que le confieren un peso predominante en el aprovisionamiento energético del continente latinoamericano. En materia de *soft power*[52], Brasil está perfeccionando también su imagen de potencia

[51] MAZZUCCHI, Nicolas. «L'énergie, source de la nouvelle puissance brésilienne», número tres de la *Nouvelle Revue Géopolitique*. París: 2012.

[52] Acción indirecta que busca colocar a una potencia en una relación de fuerza que le resulte favorable en referencia a un tema de debate de interés internacional. Las estrategias de *soft power* delimitan también las estrategias de influencia destinadas a que

emergente en materia de desarrollo sostenible así como reivindicando el ser uno de los países más limpios del mundo gracias a su producción eléctrica.

China ha construido su estrategia de recuperación apostando por la apertura (creación de zonas económicas especiales y fuertes políticas de atracción de inversiones extranjeras), al contrario que Japón que buscó captar el conocimiento cerrando el acceso a su mercado interior. El nexo de unión entre los dos países consiste en la prioridad dada durante sus fases de desarrollo mutuo a la conquista de los mercados exteriores. En ambos casos, esta forma de agresividad comercial ha desembocado en reacciones hostiles por parte de Estados Unidos y debates mediáticos sobre la problemática de la guerra económica[53] en el mundo occidental. Se acusa a China de llevar a cabo una estrategia de infiltración en los organismos de normalización con el fin de imponer sus normas[54]: tiene miembros activos en el 82% de los comités técnicos de la Organización Internacional de Normalización (ISO), cuya sede se encuentra en Ginebra. Esta participación es superior a la de Francia (80%), Japón (79%) y Estados Unidos (75%). La desconfianza hacia China genera distintos tipos de reacción difíciles de no asimilar a formas de enfrentamiento económico. Tomemos como ejemplo las medidas proteccionistas de la Administración Obama referentes a las tecnologías fotovoltaicas y el rechazo a la participación en grupos industriales occidentales, como la negativa a la solicitud de participación de la compañía china Minmetal en la empresa australiana Oz Metal por parte del Gobierno australiano en Camberra.

El cambio de paradigma de guerra económica

Los métodos de control y dominación económica elaborados por los imperios coloniales sufrieron una mutación bajo el efecto de la supremacía geopolítica, militar y comercial que Estados Unidos asumiría en los albores de la Segunda Guerra Mundial. Contrariamente a los métodos coercitivos aplicados por los imperios coloniales en sus posesiones territoriales, Estados Unidos instauró un nuevo modelo de expresión del poder económico en la base del siguiente principio: una superpotencia que busca dominar un país aliado en una cuestión económica o cultural debe buscar el mejor posicionamiento en el vértice de una jerarquía de valores, regulaciones y arbitrajes de la economía de mercado. Esta maniobra de monopolio desde la cúspide implica un nuevo método de desciframiento de los enfrentamientos económicos. Estados Unidos ha

determinados países se alineen con las mismas posturas de una potencia conforme a sus intereses.

53 «Dossier 2013, l'année de la guerre économique». Revista *l'Expansion,* n.º 780. París: diciembre de 2012.

54 *Ibídem*, página 44.

impuesto esta práctica de guerra económica silenciosa en tiempos de paz a los países industrializados del bloque occidental, pero un factor geopolítico y otro de índole geoeconómico van a modificar este período de estabilidad de enfrentamientos económicos:

– La apertura de los nuevos espacios de mercado surgidos a raíz de la desaparición del bloque del Este.
– La agresividad comercial generada por las estrategias de recuperación de las economías emergentes.

La intensidad de la competitividad mundial derivada de la unión de estos dos factores hace que los Estados Unidos tomen en consideración los enfrentamientos económicos de manera casi oficial.

Las políticas de seguridad económica

El auge de Asia y la construcción de un espacio económico europeo afectan a la predominancia geoeconómica mundial de Estados Unidos desde el fin de la Segunda Guerra Mundial. Esta redefinición de las relaciones de fuerza ha relanzado la problemática de la guerra económica desde un nuevo paradigma: la relación aliado/adversario sustituye el enfrentamiento directo o indirecto entre dos enemigos. La guerra económica practicada desde la Antigüedad había puesto en evidencia el enfrentamiento directo: la potencia que se hacía con territorios se oponía frontalmente al país que intentaba resistirse a esta conquista. Los siglos de colonización fueron su más viva expresión.

La globalización de los intercambios modifica el marco económico conflictual tanto en los países industrializados como en las economías emergentes. La competición se codea con la *coopetición.* Los intereses estratégicos de las potencias se diversifican y se hacen más complejos, y un interés militar o geopolítico puede chocar con un interés económico o viceversa. Con otras palabras, un país puede aliarse con otro desde un punto de vista militar y enfrentarse a él en términos económicos. De esta manera, surge el nuevo tipo de relación de fuerza aliado/adversario. En los hechos, se traduce en una atenuación de las relaciones económicas de fuerza tal y como se habían manifestado en el pasado. Pero esta atenuación formal no borra la intensidad de las rivalidades entre potencias, en particular en los espacios geográficos en los cuales se organizan nuevos mercados, y en los territorios ricos en recursos.

La primera potencia económica mundial se siente legitimada para oficializar durante los años 90 una política de seguridad económica ya iniciada en los años 70 con la instauración de la sección 301[55] del *Trade Act* de

[55] La sección 301 permite a los Estados Unidos oponerse a las barreras comerciales que penalizan las exportaciones norteamericanas.

1974 y la súper[56] y especial 301[57] del *Omnibus Trade and Competitiveness Act* de 1988. Las autoridades americanas tomaron el pretexto de luchar contra la competencia desleal sufrida por las empresas norteamericanas en algunas partes del mundo. Si la expresión «guerra económica» no se cita en los textos oficiales, los comentarios de algunos representantes oficiales del poder ejecutivo norteamericano subrayaban un endurecimiento de las posturas en sus análisis sobre los intercambios comerciales. Carla Hills[58], representante para el comercio de 1980 a 1993, lo expresó a su manera mediante la expresión inversa de la zanahoria y el palo: «abriremos los mercados extranjeros con un palo si es necesario, pero con un apretón de manos siempre que sea posible».

A pesar de las protestas de numerosos estados, esta regulación unilateral no fue abolida. Estados Unidos la utiliza desde entonces como un medio de presión hacia el órgano de solución de diferencias de la OMC. El representante del Departamento de Estado[59] fue igual de explícito al comentar el informe sobre el gasoducto entre Tailandia y Birmania: «La compañía Total ha sustituido prácticamente a Conoco y ha conseguido un contrato que habría sido muy beneficioso para Conoco. Queremos castigar a aquellas empresas que tengan esa actitud en el futuro».

Las leyes Torricelli (1992), Helms-Burton (1996) y D'Amato (2001) completan estas medidas de represalia comercial impidiendo el acceso a países hostiles a Estados Unidos con el fin de impedir que empresas puedan ganar mercados en esas regiones haciendo la competencia a las compañías norteamericanas. Con excepción de Cuba, objeto de embargo norteamericano desde 1962, los países a los que afectaban estas leyes, como Irak, Libia, Irán y Nigeria, tenían importantes recursos petrolíferos.

La Administración Clinton completó este dispositivo legislativo mediante la creación, en 1993, del Consejo Económico Nacional[60], que trabaja estrechamente con el Consejo Nacional de Seguridad. El secretario de Estado norteamericano Warren Christopher resaltó la importancia del asunto: «La seguridad económica norteamericana debe ser la primera prioridad en política exterior».

---

[56] La súper 301 lucha contra el conjunto de las prácticas desleales registradas por la Oficina del Representante de Comercio de los Estados Unidos *(Office of United States Trade Representative).*

[57] La especial 301 fue concebida para proteger a las empresas norteamericanas frente a la violación de su propiedad intelectual por parte de la competencia extranjera.

[58] JACOB, Evon y GUILLON, Serge. *En finir avec la mondialisation déloyale*. París: La Documentation Française, enero de 2012.

[59] REVEL, Claude y PEDRON LIOU, Isabelle. *La diplomatie exportatrice des Etats-Unis*. París: Observatoire du Marché International de la Construction, 1997.

[60] Inicialmente se tendría que haber llamado Consejo Nacional para la Seguridad Económica pero esta denominación les pareció demasiado agresiva a los países europeos.

Varios países siguieron el ejemplo norteamericano con distintos resultados. En primer lugar, Francia creó en 1995 un Comité para la Competitividad y la Seguridad Económica presidido por el primer ministro Edouard Balladur. La duración de este comité fue efímera, sin embargo, las medidas de seguridad económica adoptadas se hicieron permanentes bajo la dirección del Ministerio del Interior. Desde la primera presidencia de Vladimir Putin, el Kremlin reforzó el papel de ciertos organismos estatales para la protección del patrimonio económico y sensibilizó a los gobernadores de los estados de la Federación Rusa en lo referente a esta nueva misión. China también siguió esta vía en la década pasada.

El impacto de las estrategias económicas de incremento de poder

¿Puede ser cuestionada la mutación en las relaciones económicas de fuerza del tipo de confrontación aliado/adversario por las estrategias económicas de incremento de poder de nuevos actores del mundo occidental en el mercado mundial? El debilitamiento económico del mundo occidental puede acentuar, si se confirma a medio/largo plazo, las tensiones entre las nuevas potencias conquistadoras y los países industrializados que dominaron la economía mundial del pasado siglo. Varios factores pueden hacer resurgir las problemáticas de enfrentamiento y dominación:

- La adquisición de recursos energéticos y mineros.
- Los desafíos territoriales ligados a su localización geográfica.
- Los problemas de dependencia económica.
- Las nuevas formas de colonización cultural por la sociedad de la información.
- Las posibilidades de inversión de alianzas.

A partir de ahora, existe un desequilibrio entre las dinámicas de poder de los nuevos actores y la manera en la cual el mundo occidental se ha acostumbrado a gestionar su poder económico sin rivales reales. Los nuevos actores tienen como prioridad la conquista de mercados externos para financiar su política de incremento de poder mientras que los países del mundo occidental han separado la problemática del poder (principalmente militar y diplomática) de las lógicas de guerra económica silenciadas a partir de la segunda mitad del siglo XIX. La política de desregulación iniciada en el mundo occidental acentúa esta paradoja. Los líderes nacionales están desmantelándose en Europa mientras que los nuevos actores construyen su competitividad centrándose en el potencial de los consorcios financiados por los bancos controlados directa o indirectamente por el poder político del país. Este tipo de funcionamiento es incompatible con el sistema competitivo del mundo occidental. De ello se deriva un desequilibrio competitivo que debilita a los países industrializados que han separado la cuestión del incremento de poder de la pro-

blemática de la competición económica. Tal desequilibrio está reforzado por la importancia de las finanzas en el funcionamiento de la economía de mercado occidental. Los mercados financieros influyen en la definición de los desafíos estratégicos en la medida en que las políticas prefieren el corto plazo en los criterios de temporalidad en la construcción y preservación del poder.

Los dirigentes chinos, que han conseguido a su vez adaptar una dictadura comunista a las reglas de la economía de mercado, tienen unos objetivos más ambiciosos que el simple afán de lucro. Conscientes de las reacciones hostiles que puede generar el auge de China, oficiales del Ejército Popular de Liberación chino han inventado el término de *guerra irrestricta*[61]. El balance del fracaso de la URSS en su carrera armamentística contra el mundo occidental les incita a anteponer modos de enfrentamiento que se salen del marco estrictamente militar y que, en parte, son consecuencia de la guerra económica. El concepto de *guerra irrestricta* aplicada al ámbito geoeconómico es una manera de desviar la retórica elaborada por el ámbito empresarial anglosajón, abre la vía a otra forma de percepción de los enfrentamientos económicos. Durante un seminario francoamericano en abril de 2012 en Estados Unidos, representantes del Pentágono recordaron ante sus interlocutores franceses el delicado informe sobre el saqueo tecnológico de origen chino. Teniendo en cuenta la amplitud del fenómeno, se preguntaban si sería oportuno calificar este tipo de agresión como acto de guerra en lugar de acto de espionaje industrial. Este cambio de vocabulario reabre el debate sobre la cuestión de la negación o de la oficialización de la guerra económica. Los Estados Unidos han conseguido orientar el debate en el sentido de la negación de los enfrentamientos económicos entre potencias (véase el discurso dominante de los economistas), discurso de pacificación de los intercambios en la *aldea global* de la globalización que se justifica por los beneficios obtenidos de su estatus de superpotencia a partir de 1945.

Los límites del etnocentrismo occidental

Occidente ha dominado el mundo gracias a los imperios coloniales y, posteriormente, a la superpotencia norteamericana. El cuestionamiento de la colonización (máxima expresión de la guerra económica a lo largo de la historia) ha abierto una brecha geopolítica[62] que quedó enmascarada por la victoria del bloque occidental sobre el bloque del Este a raíz del desmoronamiento de la URSS. El impulso de las economías emergentes ha abierto una brecha geopolítica materializada por el proceso de desin-

[61] Qiao Liang, Wang Xiangsui, *La Guerre hors limites*, Paris, Payot et Rivages, 2003.

[62] La pérdida de las colonias ha tenido repercusiones políticas en algunos países. En Bélgica, el conflicto lingüístico entre flamencos y valones se convierte en un problema nacional a partir de 1962.

dustrialización y el debilitamiento de algunas economías de mercado occidentales. Estas dos brechas resaltan los límites de un etnocentrismo occidental que incitaba a analizar las relaciones de fuerza partiendo del principio de que el fuerte solo podía estar del lado occidental.

Las contradicciones entre los Estados Unidos y Europa

En este reparto de naipes, el mundo occidental se encuentra debilitado por numerosas contradicciones. La primera recuerda la fábula del regador regado: Gran Bretaña y, posteriormente, Estados Unidos han utilizado el liberalismo para legitimar el desmantelamiento de los sistemas proteccionistas de los países-clientes con el fin de favorecer la venta de sus productos y su dominación sobre los mecanismos financieros internacionales; hoy en día resulta difícil recular porque supondría asestar un golpe mortal a la validez del discurso. La segunda contradicción es estadounidense: importantes intereses privados del otro lado del Atlántico, tanto industriales como financieros, intentan aprovecharse, a corto plazo, de las oportunidades que les ofrece la globalización de los intercambios; la flexibilidad del discurso liberal les permite legitimar las deslocalizaciones y los efectos de la desindustrialización, y los debates en el Congreso de Estados Unidos reflejan la lucha a menudo desigual entre los grupos de poder a favor de la apertura de los mercados y las fuerzas que anteponen la salvaguarda de los intereses de la población residente en territorio americano. La tercera contradicción es la incapacidad de la Unión Europea de afirmarse como potencia consciente de la importancia de los desafíos de la guerra económica: desde la misma posguerra, las negociaciones de las contrapartidas de los beneficiarios del Plan Marshall abren fuertes debates en Francia sobre algunas de las condiciones económicas estadounidenses, como el gravamen de la soja americana destinada a la alimentación animal o la distribución del cine de Hollywood en su mercado cinematográfico; con ocasión de su vuelta al poder en 1958, el general de Gaulle definió los criterios de una política de independencia nacional que se opone a los intereses norteamericanos:

- Creación del consorcio petrolero Elf Aquitaine para reducir la dependencia de Francia frente a las siete compañías petroleras anglosajonas.
- Fijación de cuotas para limitar la implantación de firmas multinacionales estadounidenses.
- Desenlace de una polémica sobre el papel predominante del dólar como moneda de referencia mundial.

La visión gaullista de independencia nacional no resistió el alegato liberal referente a la apertura de mercados. La doctrina liberal eliminó toda posibilidad de discurso estructurante sobre la naturaleza de los enfrentamientos económicos, a pesar de que hubo diferencias comerciales entre

los Estados Unidos y Europa que perturbaron de forma esporádica las negociaciones del GATT y de la Organización Mundial del Comercio. La construcción del mercado europeo sirvió de pretexto incluso para marginar la reflexión intelectual sobre el papel de la economía en la construcción del poder.

En 1976, Giscard d'Estaing y Raymond Barre desmantelaron los instrumentos concebidos para dotar a la industria francesa de una capacidad de respuesta en términos de poder económico. Fue así como se suprimió la Comisión Permanente de la Electrónica del plan. Esta comisión era un lugar de intercambio entre los directores generales de las grandes empresas del sector, de representantes de organizaciones profesionales, de pymes y de ministerios. Los temas sometidos a debate trataban de la estrategia francesa en sectores estratégicos como la informática, las telecomunicaciones, la aeronáutica y la electrónica. Esta comisión fue el origen de una toma de conciencia en los años 60 sobre la necesidad esencial de dotar a nuestro país de una industria electrónica lo suficientemente poderosa como para emanciparse de la dominación norteamericana. El comisariado del plan había creado incluso un sistema informático llamado Marte que era una base de datos creada a partir de flujos de información generados por 250 empresas, 30 servicios administrativos y 23 sindicatos profesionales. La información circulaba en ambos sentidos ya que los industriales podían acceder a ella bajo ciertas condiciones y de esta manera podían mejorar su aportación a la innovación y su enfoque al mercado mundial. Del lado estatal, el sistema Marte permitía medir la eficacia de los créditos inyectados al sector electrónico; incluso se pensó extenderlo al conjunto de la industria francesa. El periódico *Le Monde* destacó en aquella ocasión que multinacionales de origen francés jamás habrían aceptado jugar el papel de una estrategia de poder centrada en Francia y preferían cooperar con las empresas norteamericanas. De esta manera surgía una línea de fractura entre los que estaban a favor de un mercado globalizado y los defensores de un territorio económico. Esta contradicción, a pesar de ser fundamental, no fue tenida en cuenta cuando el primer ministro Dominique de Villepin reabrió el debate sobre el patriotismo económico a principios del siglo XXI.

Lejos de ser un debate artificial u obsoleto, el tema del patriotismo económico se alimenta de los efectos negativos de las políticas de recuperación de las economías emergentes. Su atractivo, representado por una mano de obra barata, no sirve de explicación para todo. Ciertos países emergentes se han transformado en *economías de combate* para estar al mismo nivel que las economías occidentales; no han hecho más que reproducir las técnicas iniciadas desde hace siglos en el mundo occidental. Solo hay que volver a leer la historia: después de las guerras revolucionarias, Francia hizo todo lo posible por intentar subsanar su retraso técnico con respecto al Reino Unido recurriendo al tráfico de maquinaria

importada clandestinamente desde Gran Bretaña y al espionaje industrial en manufacturas británicas. Las estrategias ofensivas de las economías emergentes han completado esta panoplia de técnicas agresivas mediante una ingeniería de acopio de información amplificada gracias a Internet, al robo de patentes, a la práctica del *dumping* y a la industrialización de las imitaciones, sin olvidar el tráfico ilícito de metales como el cobre derivado del incremento de la demanda mundial. Estas acciones desleales contribuyen a la degradación de la hegemonía económica en el mundo occidental y se está convirtiendo en un tema de preocupación en Estados Unidos. En Europa quedan relegadas a la categoría de excepciones que confirman la regla, o lo que es lo mismo, se sigue creyendo ciegamente en la supremacía del modelo liberal.

Los efectos perversos de la ejemplaridad liberal

Los Estados Unidos no dudan en dotarse de un sistema coercitivo de sanción de actos de depredación o de aislamiento económico de los países hostiles. Bruselas imita a veces el comportamiento de Washington pero no suele pasar a los hechos. En 1984, la Unión Europea se dotó de un instrumento de represalia comercial[63] inspirándose en la sección 301 del *Trade Act* estadounidense. Dotada de este arma contra las prácticas ilícitas de terceros estados en sectores no regulados en los acuerdos del GATT, la Unión Europea recurrió solo de manera excepcional[64] a este tipo de presión que puede asimilarse a una medida de guerra económica en tiempos de paz.

La imposibilidad de que surgiese en un país como Francia una idea unificada acerca de las prioridades geoeconómicas del país no es una consecuencia de un bloqueo cultural. La Unión Europea se limita a acordar las disposiciones preventivas que pueden tomar los estados miembros frente a los riesgos de depredación económica y de competencia desleal. La protección del perímetro de la defensa nacional y del orden público es el único margen de maniobra soberano reconocido por la Comisión de Bruselas. En 2006, el ejecutivo europeo resolvió algunos procedimientos de infracción sancionando actitudes contrarias a las reglas del mercado interior, copiando el decreto anti-OPA francés que obligaba a solicitar una autorización previa ante las autoridades francesas por parte de los inversionistas extranjeros que quisiesen tomar el control o una minoría de bloqueo del 33,33% en sociedades de 11 sectores de actividad considerados estratégicos.

[63] Este tipo de herramienta permitía luchar contra países que practicaban la competencia desleal con medidas sancionadoras en los intercambios con países de la Unión Europea: restricciones cuantitativas a la exportación o incrementos de los derechos aduaneros.

[64] Utilizada en seis ocasiones en un periodo de diez años.

Al contrario que en Gran Bretaña, Países Bajos o Alemania, que integraron el encubrimiento de la guerra económica en sus modus operandi, Francia busca la validación de sus márgenes de maniobra mediante textos oficiales reconocidos a nivel europeo. Durante los primeros años de su mandato[65], Alain Juillet, alto responsable para la Inteligencia Económica, tardó meses en intentar convencer a sus interlocutores de la Comisión Europea de que aceptasen los sectores industriales energéticos que Francia hubiese querido proteger mejor. Para justificar su negativa, la Unión Europea reivindicó la aplicación ejemplar de las normas del liberalismo como elemento pacificador en los intercambios.

Esta actitud está lejos de ser unánime en el continente euroasiático. En diciembre de 2008, el Gobierno ruso estableció una lista de 295 empresas consideradas estratégicas, sin omitir las del sector energético[66]. Vladimir Putin añadió 1.500 sociedades vitales para la economía nacional y susceptibles de recibir ayudas estatales, amnistías fiscales y privilegios aduaneros. La advertencia del jefe de Estado ruso a sus homólogos europeos sobre el riesgo de un corte en el suministro de gas demostró la fragilidad estratégica de Europa en aprovisionamiento energético durante este periodo. Sobre este tema concreto, la doctrina liberal que centraba el pensamiento europeo sobre la desregulación de un mercado abierto a la competencia no parecía adaptada a la situación. Sin embargo, este defecto no impulsó la búsqueda de una posición unificada entre los socios europeos[67].

Conclusiones

La globalización hace mucho tiempo que justamente se considera como portadora de elementos positivos como la mejora del nivel de vida de la población de los países industrializados, el proceso de negociación de conflictos comerciales, la regulación gradual del comercio y el fortalecimiento de los mecanismos de protección para el reconocimiento de patentes internacionales. Pero este mundo «mixto» producto de la globalización no ha pacificado la economía. El tablero de relaciones de fuerza geoeconómicas es en la actualidad profundamente más multipolar que el mercado global. Las rivalidades crecientes entre el mundo occidental y los nuevos actores debilitan la dinámica de pacificación impulsada por un mundo occidental dominante.

Cabe preguntarse si Europa ha aprendido la lección de las guerras mundiales que le hicieron perder su supremacía o si ha conseguido medir

[65] Su misión referente a la puesta en marcha de la inteligencia económica en el SGDN (Secretaría General de la Defensa Nacional) tendrá una duración de 2003 a 2009.

[66] El grupo gasístico Gazprom y las compañías petroleras Lukoïl y Rosneft.

[67] Alemania había firmado en 2000 un acuerdo bilateral con Rusia.

correctamente la importancia de las amenazas que se ciernen sobre su futuro geopolítico y geoeconómico. Desprovista de análisis sobre enfrentamientos económicos e incapaz de sacar conclusiones de su evolución estratégica a través de los siglos, Europa sigue atrasada en la actualidad con respecto a Estados Unidos. A pesar de las apariencias, está más dividida que nunca por una cohabitación que no se quiere nombrar. El norte de Europa está capitaneada por Alemania, que juega un doble juego al favorecer discretamente el renacimiento de su poder mientras aparenta una imagen de país profundamente pacifista por sus errores militaristas pasados; el sur de Europa intenta sobreponerse a sus crisis infraestructurales, y la Europa de los antiguos países socialistas intenta encontrar un camino todavía muy marcado por las estrategias de influencia estadounidense, alemana y rusa.

Para salir de este callejón sin salida estratégico, es importante pensar en nuevas lecturas obligadas sobre guerra económica. Parece lógico pensar en una nueva economía política basada en una conveniente articulación entre construcción de poder de un Estado, dominio en la conquista de los mercados y desarrollo de los territorios. Estas tres dimensiones estratégicas no son compatibles de manera natural. El poder político debe dotarse de los medios para definir una gradación de los desafíos y de las prioridades a corto, medio y largo plazo. En la actualidad, la Unión Europea es incapaz de hacerlo. Sin embargo, es una prioridad absoluta.

Bibliografía

ESAMBERT, Bernard. *La guerre économique mondiale*. París: Olivier Orban, 1991.

CARAYON, Bernard. *A armes égales*, informe al primer ministro. París: Assemblée Nationale, 2006.

CROUZET, François. *La guerre économique franco-anglaise au XVIIIe siècle*. París: Fayard, 2008.

DELBECQUE, Eric y HARBULOT, Christian. *La guerre économique*. París: Que sais-je, PUF, 2010.

DENÉCÉ, Eric y REVEL, Claude. *L'autre guerre des États-Unis, économie: les secrets d'une machine de conquête*. París: Robert Laffont, 2005.

FONVIELLE, Dominique. *De la guerre économique. Défense et défis nouveaux.* París: Presses Universitaires de France, 2002.

FOURQUET, François. *Richesse et puissance, une généalogie de la valeur*, París: La Découverte, 1989.

GAUCHON, Pascal. *Le Monde, manuel de géopolitique et de géoéconomie*, París: PUF, 2008.

HARBULOT, Christian. *Techniques offensives et guerre économique* (reedición). París: La Bourdonnaye, 2012.

— *La main invisible des puissances*. París: Ellipses, 2007.

— *Manuel de l'intelligence économique*, obra colectiva. París: PUF, 2012.

HUISSOUD, Jean-Marc y MUNIER, Frédéric. *La guerre économique, Rapport Anteios*. París: Puf, 2010.

LAÏDI, Ali. *Aux sources de la guerre économique, fondements historiques et philosophiques*. París: Armand Colin, 2012.

LAÏDI, Ali y LANVEAUX, Denis. *Les etats en guerre économique*. París: Le Seuil, 2006.

LEONETTI, Xavier. *La France est-elle armée pour la guerre économique?* París: Armand Colin, 2011.

LUCAS, Didier y TIFFREAU, Alain. *Guerre économique et information*. París: Ellipse 2001.

LUTTWAK, Edward. *Le rêve américain en danger*. París: Odile Jacob, 1995.

NADOULEK, Bernard., *L'intelligence stratégique: philosophie de l'action face à la mondialisation cultures, économies et rapports de puissance*, París: Centre de Prospective et d'évaluation, Ministère de la Recherche, 1990.

NORA, Dominique. *L'étreinte du samouraï, le défi japonais*. París: Calman-Levy, 1991.

QIAO LIANG, Wang Xiangsui. *La Guerre hors limites*. París: Payot et Rivages, 2003.

SOUTOU, Georges-Henri, *L'or et le sang.* París: Fayard, 1989.

Capítulo III

INTELIGENCIA JURÍDICA: EL VALOR ESTRATÉGICO DEL DERECHO EN LA SEGURIDAD ECONÓMICA

José L. González Cussac

Resumen

Dentro del contexto actual de globalización y protagonismo de las nuevas tecnologías, con un tránsito desde la idea de geopolítica al de geoeconomía, y la pujanza de una noción de «guerra económica» o «guerra de cuarta generación», se desarrolla la idea de *inteligencia jurídica*. Para ello se parte de la premisa de que toda actividad humana está sometida a reglas, lo que alcanza inexorablemente a la economía y a la inteligencia. Desde aquí se analiza el derecho como objeto de la inteligencia y el derecho como herramienta de la inteligencia. La conclusión es el valor estratégico del derecho. El sujeto capaz de crear e imponer las reglas posee una ventaja decisiva, y los competidores que no conocen su significado y pautas de aplicación no pueden competir en igualdad de condiciones.

Palabras clave

Inteligencia jurídica, troyanos normativos, seguridad económica, seguridad jurídica, seguridad nacional, inteligencia económica y competitiva, reglas y derecho.

Abstract

In the present context of globalization where new technologies have taken on prime importance, the idea of *legal intelligence* is developed. In addition, in this area there has been a development in the idea of geopolitics towards the idea of geoeconomics and there has been a rise of the notion of «economic warfare» or «fourth generation warfare». The basic premise is that all human activity is subject to regulations that influence the economy and intelligence. On this basis, the paper examines the law as a matter of intelligence and the law as a tool of intelligence. The conclusion is that the law is strategically valuable. The one who is capable of creating and impose rules commands a decisive advantage, and the competitors who do not know the meaning of those rules are not in a position to compete on equal terms.

Key words

Legal intelligence, normative trojans, economic security, legal security, national security, economic and competitive intelligence, rules and law.

Planteamiento

La política, el derecho y la economía muestran distintos modelos de maridaje a lo largo de la historia. En realidad, son diferentes formas de ejercer el poder. El poder es dominación dentro de un escenario de enfrentamiento o competencia y en el marco de unas reglas de juego. En el siglo pasado asistimos a un modelo de dominación colonial, y luego a otro de dominación poscolonial durante la Guerra Fría; pero en la actualidad asistimos a un nuevo escenario geopolítico en el que la dominación se ejerce por otros mecanismos. La globalización es la clave y, en palabras de Juillet, reúne dos clases de economía que están lejos de ser coincidentes: la del mercado y la de los estados. Sin embargo, el final de la confrontación «este-oeste» ha conducido el enfrentamiento a la competición económica, de suerte que ha situado la «economía de mercado» en la *geoeconomía* de las grandes potencias. Esta competencia universal en la que participan potencias clásicas, potencias emergentes, hasta llegar a más de doscientos países, requiere nuevas reglas –nacionales, regionales e internacionales– que arbitren el juego entre intereses múltiples y que determinen el reparto entre países dominadores y países subalternos. Y en este gran juego de poder, intereses y reglas, las nuevas tecnologías desempeñan un papel fundamental[1].

En este contexto, varios autores –siguiendo a Clausewitz– hablan ahora de la economía como continuación de la guerra, de modo que nos hallaríamos ante una «guerra económica encubierta» (Harbulot)[2]. Así, habríamos transitado desde la geopolítica a la *geoeconomía*[3]; los países se juegan su soberanía y los ciudadanos su bienestar. En este nuevo tablero intervienen también factores y agentes no estatales con motivaciones exclusivamente económicas (mercados financieros), pero también acciones de influencia y desestabilización dirigidas por agencias gubernamentales, y, estrechamente vinculado a este punto de partida, está la idea de que la «nueva guerra» se desarrolla, fundamentalmente, en la red (*ciberguerra*)[4] y, en gran parte, dentro de lo que clásicamente denominaríamos espionaje económico (Clarke y Knake)[5].

---

1 JUILLET, Alain (2006). «Principios de aplicación de la inteligencia económica». *Inteligencia y Seguridad: Revista de análisis y prospectiva*, n.º 1, diciembre de 2006, pp. 123.

2 HARBULOT, Christian (1992). *La machine de guerre économique: États-Unis d'Amérique, Japon, Europe*, París: Economica. También CARAYON, Bernard (2006). *Patriotisme économique: De la guerre à la paix économique*. Mónaco: Editions du Rocher.

3 Un excelente desarrollo y exposición en OLIER ARENAS, Eduardo (2011): *Geoeconomía,* Pearson Prentice Hall.

4 OLCOTT, Anthony. «Revisiting the legacy: Sherman Kent, Willmoore Kendall and George Pettee. Strategic intelligence in the digital age», *Studies in Intelligence*, vol. 53, n.º 2 (extractos, junio de 2009, pp. 21-32.

5 Extensamente en CLARKE, Richard A. y KNAKE, Robert K.: «*Guerra en la red: los nuevos campos de batalla*», Barcelona: Ariel, 2011.

La economía, y su derivada la inteligencia económica y competitiva, son hoy algo más que un componente esencial de la seguridad nacional según la clásica formulación (Potter)[6]; como advirtiera Juillet, la globalización y la falta de regulación han configurado de forma esencial el espacio de la geopolítica, añadiendo a los tradicionales agentes públicos las empresas y otros sujetos de la sociedad civil[7].

Quizás por compartir este análisis, aunque desde otros ángulos, autores como Joseph Stiglitz, Paul Krugman o Alain Touraine, entre otros, consideran que la inicial crisis financiera de 2008 se ha convertido no solo en una crisis económica global, sino en una auténtica crisis política y social. En cierta forma, asistimos a un auténtico y completo cambio de paradigma mundial: la geoeconomía ha entrado en escena, y con ella el desarrollo de variados modelos de «seguridad económica» (Buzan, Waever, Wilde)[8]. La seguridad nacional ya no se puede reducir a sus contenidos clásicos, ni tampoco la seguridad económica sin una dimensión humana. Así pues, la seguridad económica, como componente de la seguridad nacional, no solo se mide por criterios económicos tradicionales de riqueza (también la disponibilidad de bienes y servicios, estabilidad, niveles de protección, etc.) y traslada el centro de gravedad desde la idea de seguridad de los estados hasta el de la seguridad de las personas.

Sin embargo, la liberación del comercio y las inversiones, esto es, determinados efectos de la globalización, comporta una pérdida progresiva de la capacidad de los Estados-nación para regular estas actividades y a su vez para proporcionar bienes y servicios a sus ciudadanos. De suerte que los Estados, con todo su entramado legislativo nacional, a la vez que han perdido capacidad de decisión siguen soportando las demandas de seguridad de sus ciudadanos.

A todo este panorama de profundos cambios hay que sumar la actual crisis económica mundial a la que ya he hecho referencia, que ha desvelado, cuando no ocasionado, una seria inestabilidad e inseguridad a todo el sistema internacional, y no solo en el plano económico. La disponibilidad de recursos estratégicos y materias primas, los flujos de capital, el peso del Estado de bienestar o el funcionamiento institucional son factores determinantes en mayor o menor peso en regiones y países que ahora se hallan en la encrucijada. Y como toda gran crisis económica, provoca

[6] POTTER, Evan H., editor. «*Economic intelligence and national security*», Carleton University Press, 1998. Cfr. ARNETT, Dennis, MENON, Anil y WILCOX, James B. «Using competitive intelligence: Antecedents and Consequences». *Competitive Intelligence Review, vol.* 11, issue 3, 2000, pp. 16-27.

[7] VENEGAS GONZÁLEZ, Álvaro. (2008). «Inteligencia económica: un componente estratégico por desarrollar», en *AA Inteligencia,* año 1, número 2, pp. 10-19. Chile: 2008.

[8] BUZAN, Barry, WEAVER, Ole y DE WILDE, Jaap. (1998): *Security. A new framework for analysis.* Londres: Lynne Rienner Publishers, 1998, pp. 95 y ss.

una profunda expansión con efectos –con diferentes grados de impacto– en todos los espacios y actores, y en consecuencia conlleva un riesgo adicional de primera magnitud para la estabilidad política. Sabido es que la evolución de las mismas acentúa las diferencias sociales, y por tanto representa un escenario idóneo para los estallidos sociales, el auge de los movimientos populistas y el brote de los radicalismos. Todo lo cual, sumado y agitado, constituye el mayor de los peligros para los sistemas democráticos y el Estado de derecho[9].

De todo lo anterior se deriva la necesidad de modificar, actualizar y revisar los modelos normativos con el objetivo de reforzar el sistema institucional propio del Estado democrático de derecho, único capaz de brindar la seguridad jurídica mínima para garantizar una convivencia civilizada.

Esta tarea implica el desarrollo de normas y prácticas interpretativas de autoprotección y cooperación, además de una legislación susceptible de ofrecer una mayor capacidad de competir en igualdad de condiciones con los demás países de su esfera. El derecho se visualiza desde esta perspectiva como un arma estratégica de primera magnitud para hacer frente a una guerra de «cuarta generación», donde agentes asimétricos solos o en alianza con otros estados pueden coordinar ataques a países, compañías o sistemas financieros con graves perjuicios a la seguridad nacional, en la que los derechos económicos de los ciudadanos son un componente esencial.

En este dibujo, la inteligencia económica, como parte de la política económica global y componente básico de la seguridad nacional, debe articular su estrategia en un desarrollo normativo que permita el logro de sus objetivos. Estos objetivos concretos se centran en los siguientes aspectos básicos: a) asegurar la vigilancia estratégica para facilitar la toma de decisiones públicas y privadas; b) sostener la competitividad de las empresas y la capacidad de transferencia de tecnología de los centros de investigación, y c) garantizar la seguridad económica de empresas y centros de investigación.

Por consiguiente, un sistema de inteligencia económica debe hoy apoyarse en un adecuado desarrollo normativo, tanto a escala nacional como internacional[10]. Es por ello que podemos hablar de la necesidad de desarrollar una *inteligencia jurídica* con valor y proyección estratégica.

---

9 GONZÁLEZ CUSSAC, José Luis y LARRIBA HINOJAR, Beatriz. *Inteligencia económica y competitiva: Estrategias legales en las nuevas agendas de seguridad nacional*. Valencia: Tirant, 2011, pp. 13 y 14.

10 POOLEY, James y HALLIGAN, R. Mark. «Intelligence and the Law», en MILLER, Jerry (ed.): *Millennium intelligence: Understanding and conducting competitive intelligence in the digital age*. Medford, NJ: CyberAge Books, 2000, pp.171-187.

El derecho como conjunto de normas

Wittgenstein protagonizó una auténtica revolución en el pensamiento filosófico del siglo xx, en particular hacia una «clarificación conceptual». Este pensamiento ha traído un giro decisivo en la filosofía, en las ciencias sociales y en el derecho[11]. Pues bien, a los efectos de este trabajo, deseo subrayar que tomo como punto de partida una de sus ideas centrales: que toda actividad está sometida a reglas –comenzando por el propio lenguaje–, o mejor aún, que solo poseen sentido y significado desde su comprensión a través de reglas. Pues bien, el derecho, la economía, la seguridad económica y la inteligencia económica no son una excepción: sin reglas ni siquiera es posible hablar de las mismas[12].

El derecho es un conjunto de normas positivas, esto es, impuestas por la autoridad que tiene la potestad para ello. Por tanto, el derecho también regula la economía y la inteligencia: todas las actividades humanas están reguladas, sometidas al «imperio de la ley»; esta es la esencia del Estado de derecho. Consecuentemente, la constante tendencia en las últimas décadas de las políticas de desregulación, autorregulación y «códigos de buen gobierno» en ciertas áreas económicas cuando menos plantean, ya de inicio, una espinosa cuestión.

Un segundo aspecto capital descansa en la emergencia de un nuevo orden jurídico mundial, con unas condiciones espaciales y temporales distintas a las tradicionales, enmarcado en el proceso de globalización. Las categorías centrales del derecho, como soberanía, Estado-nación y ley fundamental se enfrentan a nuevos retos y reestructuraciones (Jáuregui)[13]. En concreto, destaca la necesidad de estructurar el tiempo, teniendo en cuenta no solo el presente sino también el futuro, un reto mayúsculo para el derecho que implicará la formulación de un nuevo «contrato social», y, en segundo término, el tránsito de un escenario de Estados-naciones a otro de instancias *supraestatales* en el que a su vez se opera un cambio conceptual desde la idea de «gobierno» al de «gobernanza», más amplio y menos formalizado. De este modo, se enfatiza la imposibilidad, en la era de la globalización, de Estados no sujetos a restricciones de

[11] Un magistral desarrollo y aplicación del derecho penal desde el pensamiento de Wittgenstein puede verse en VIVES ANTÓN, Tomás Salvador: *Fundamentos del sistema penal*, 2.ª edición. Valencia: Tirant lo Blanch, 2010.

[12] Sobre los equívocos y dificultades del lenguaje, y en particular aplicados al ámbito jurídico del secreto industrial, del espionaje y de la inteligencia competitiva, puede verse la magnífica exposición de HOROWITZ, Richard. *Competitive Intelligence, law and ethics: The Economic Espionage Act revisited again (and hopefully for the last time).* SCIP, vol. 14, n.º 3, julio-septiembre de 2011, pp. 45-46.

[13] JÁUREGUI, Gurutz. «La emergencia de un nuevo orden jurídico-institucional: el Estado y la Constitución de la era de la globalización», en INNERARITY, Daniel y SOLANA, Javier, editores*: La humanidad amenazada: gobernar los riesgos globales.* Barcelona: Paidós, 2011, pp. 237 y ss.

carácter externo. A ello hay que sumar una falta de orden internacional, una insoportable asimetría en las relaciones internacionales y, con ello, un proceso de deslegitimación constante de todas las instituciones existentes. En definitiva, nos hallamos ante la necesidad de transformar las instituciones jurídicas para adaptarlas a los nuevos parámetros sociales, culturales, políticos y económicos.

Pues bien, en este nuevo contexto, la *inteligencia económica* tampoco puede quedar lastrada en el análisis macroeconómico de regiones, sectores y países, ni dirigirse exclusivamente al escrutinio del crimen organizado en sus múltiples facetas, ni ofrecer solo la protección de la industria y tecnología de doble uso; ni siquiera basta con tratar de estabilizar el sistema financiero[14]. Al hablar de inteligencia económica, normalmente se pone el acento en los riesgos asociados a la rentabilidad de una inversión, pero se suelen obviar tanto el examen de los riesgos políticos aparejados a la propia inversión –si bien estos son tenidos cada vez más en cuenta– como el de los riesgos asociados a la inseguridad jurídica de la misma. Riesgos ambos que, tal y como demuestran los últimos acontecimientos mundiales, son mucho más importantes que los financieros.

Por consiguiente, al trasladar este planteamiento al derecho, la inteligencia no puede tampoco detenerse en proporcionar herramientas jurídicas en todas estas áreas, ni siquiera añadiendo las necesarias para desarrollar labores de contrainteligencia. También debe favorecer, por ejemplo, normas que dificulten o amortigüen acciones externas dirigidas a alterar el normal funcionamiento de los mercados y desde luego tiene que posibilitar el despliegue de acciones de influencia dentro y fuera de las fronteras nacionales.

En este sentido, la experiencia contrastada de la legislación sobre la industria de defensa y la regulación de las tecnologías de «doble uso», que explicitan una fuerte vinculación entre materias aparentemente distantes como son la militar y la comercial, constituyen un excelente ejemplo del camino a seguir. Pero son simplemente buenas pautas o indicadores necesitados de un sofisticado desarrollo normativo.

En todo caso, el derecho es el único instrumento que aporta un valor esencial en la convivencia y relaciones humanas de toda índole: la *seguridad jurídica*. La medición de este concepto esencial, con su complejo entramado de derechos y garantías, tiempos, dilaciones, procedimientos, de un poder judicial independiente, de la calidad de la legislación, de prácticas aplicativas estables y, en definitiva, de orden y funcionamiento institucional formalizado seguro, condicionan decisivamente el juego de los diversos intereses económicos, políticos y sociales. La inseguridad

[14] BÉGIN, Lucie, DESCHAMPS, Jacqueline y MADINIER, Héléne. «Une approche interdisciplinaire de l´intelligence économique». *Cahier de Reserche,* n° HES-SO/HEG-GE/C--07/4/1-CH, Haute École de Gestion de Genève, 2007.

jurídica tiene un alto coste económico, y este coste igualmente conecta con el grado de corrupción de un país y de su asociación con organizaciones y grupos criminales transnacionales[15]. Y, desde luego, no debe olvidarse el coste de la exclusión social, con sus niveles de conflictividad y consiguiente riesgo de inestabilidad[16]. Es decir, es un riesgo político mayúsculo.

Así pues, el derecho, como conjunto de reglas de cumplimiento imperativo, es determinante en cualquier actividad humana, y especialmente en los siguientes ámbitos propios de esta problemática.

En primer término, al conjunto de normas aplicables al ciclo de inteligencia, en particular, a la inteligencia y contrainteligencia económica y competitiva[17], y muy significativamente a las acciones encubiertas y de influencia[18]. Aquí cobra un protagonismo singular el grave problema del espionaje industrial, comercial y tecnológico[19], y toda la novedosa problemática asociada al ciberespacio y su regulación[20].

---

15 Todos los indicadores muestran un significativo aumento de prosperidad en los países iberoamericanos y la consolidación de una emergente clase media; sin embargo, lastra este progreso la desigualdad social y la inseguridad ciudadana. SERRANO MONTEAVARO, Miguel Ángel: «La nueva clase media Americana. Hacia una mayor seguridad económica y social», *Documento Informativo,* IEEE 02/2013, diciembre de 2012.

16 Imprescindible la exposición de STIGLITZ, Joseph E. *El precio de la desigualdad.* Madrid: Taurus, 2012.

17 BRADFORD, William. *The three faces of competitive intelligence: defection, collusion and regulation*, en University of Florida, Warrintong College of Business, 19 de febrero de 2007.

18 Ampliamente en GONZÁLEZ CUSSAC, José Luis y LARRIBA HINOJAR, Beatriz (2011), *cit.,* pp. 89 y ss.

19 HOROWITZ, Richard. *Competitive Intelligence, law and ethics: The Economic Espionage Act revisited again (and hopefully for the last time).* SCIP, vol. 14, n.º 3, julio-septiembre de 2011, p. 43. Horowitz afirma que uno de los mayores problemas en este ámbito se encuentra en que, aunque teóricamente existe la diferencia entre espionaje y obtención lícita de información, en la práctica jurídica es muy difícil trazar la diferencia entre métodos legales e ilegales.

20 LARRIBA HINOJAR, Beatriz (2013). «Ciberespionaje económico: Una amenaza real para la seguridad nacional», en *Nuevas amenazas a la seguridad nacional. Terrorismo, criminalidad organizada y tecnologías de la información y la comunicación* (directores: GONZÁLEZ CUSSAC, José L. y CUERDA ARNAU, María Luisa; coordinador: FERNÁNDEZ HERNÁNDEZ, Antonio). Valencia: Tirant, 2013. Esta autora subraya que el ciberespionaje económico constituye una de las más serias amenazas para la seguridad nacional en el siglo XXI. Sobre esta inquietante temática puede verse también GONZÁLEZ CUSSAC, José Luis: «Estrategias legales frente a las ciberamenazas», en *Ciberseguridad. Retos y amenazas a la seguridad nacional en el ciberespacio*, *Cuadernos de Estrategia*, n.º 149. Madrid: Instituto Español de Estudios Estratégicos. Ministerio de Defensa, 2010, pp. 85-127. Y del mismo autor: «Tecnocrimen», *en Nuevas amenazas a la seguridad nacional. Terrorismo, criminalidad organizada y tecnologías de la información y la comunicación* (directores: GONZÁLEZ CUSSAC, José L. y CUERDA ARNAU, María Luisa; coordinador: FERNÁNDEZ HERNÁNDEZ, Antonio). Valencia: Tirant, 2013.

En segundo lugar, el derecho debe ofrecer una suficiente y eficaz protección a las empresas y a los centros de investigación, preservando su seguridad y competitividad. Esto comporta una normativa coordinada desde diversos organismos públicos con competencias en áreas tan diversas como exteriores, relaciones internacionales y cooperación; seguridad y justicia; hacienda, industria, turismo, agricultura, pesca, fomento e infraestructuras; educación, cultura, ciencia, investigación, tecnología, entretenimiento, y medio ambiente. Pero junto a una normativa protectora de todos estos campos, el Estado debe implementar otra capaz de aumentar la capacidad de transferencia de los centros de investigación públicos y privados a las empresas, y también ofrecer estímulos reglados a las empresas.

En definitiva, la política económica ha de traducirse en leyes eficaces y favorables al desarrollo económico sostenible, que no incumbe únicamente a instituciones y empresas sino también a los individuos. Y la inteligencia debe aplicarse también a esta tarea, y para ello dispone de diferentes modelos de articulación[21]. Esto es, a la comprensión de las normas que regulan cualquier actividad humana. Lo que comporta una labor de análisis no solo cuantitativo o descriptivo de las leyes, sino esencialmente a un conocimiento cualitativo o de interpretación de su significado y de sus efectos y consecuencias.

El derecho como objeto de la inteligencia

En el apartado anterior hemos sentado que toda actividad, como si se tratara de un juego, incluida la económica y las actividades de inteligencia correlativas, está sometida a reglas: mejores o peores, definidas o vaporosas, suficientes o insuficientes. Incluso la ausencia de reglas expresa la aplicación de una regla: la del más fuerte, pero al fin y al cabo siempre existen reglas. Entonces, es obvio que el jugador que produce, crea e impone las reglas tiene más ventajas. Y en cualquier caso, el jugador que no conoce adecuadamente las reglas del juego es un temerario y un más que probable perdedor.

Ambos aspectos, creación y conocimiento de las normas, deben tenerse presentes y los abordaré separadamente.

Cualquiera que sea el objetivo a alcanzar, el *jugador* o competidor debe tratar de imponer sus reglas. En la teoría jurídica se distingue al efecto entre las fuentes materiales y las fuentes formales de creación de normas. Las primeras, las materiales, hacen referencia a los diferentes poderes sociales con capacidad para impulsar, influir o condicionar la legislación. Las segundas, las fuentes formales, designan los diferentes

[21] UGARTE, José Manuel (2005). *La relación entre inteligencia y política, y sus consecuencias en las estructuras y normas de los sistemas de inteligencia*. Brasilia.

procedimientos formalizados de creación y manifestación del derecho. En este plano, opera tanto el Estado como los agentes no estatales, y el campo de juego básicamente se limita a dos ámbitos espaciales: el *territorio* donde un Estado tiene soberanía (legislación nacional) y más allá de sus fronteras, en el escenario internacional.

En principio, dentro de su territorio el Estado es soberano para producir la legislación que considere oportuna y necesaria, conciliando los diferentes intereses en conflicto. En este plano el Estado posee *potestas y autoritas* para decidir, al menos teóricamente, la legislación pertinente de acuerdo a sus intereses nacionales y conforme a sus procedimientos materiales y formales de producción legislativa. Desde el exterior, formalmente solo le atan y condicionan sus compromisos internacionales trasladados e incorporados en normas internas (tratados, convenios, acuerdos, asociaciones, etc.). Naturalmente, el grado de soberanía real dependerá de múltiples factores internos y externos, lo que no excluye la necesidad de vigilarlos y controlarlos suficientemente con el fin de no sufrir una influencia normativa externa desencadenante de una dependencia y subordinación a intereses ajenos.

En el circuito internacional, el Estado y los agentes no estatales también desempeñan un papel esencial en la producción material y formal de normas jurídicas; de ahí la necesidad de presencia de cualquier Estado en todas las instituciones internacionales de decisión o de deliberación. Igualmente imprescindible resulta poseer una normativa que permita ejercer la influencia en actores extranjeros, dentro de la legislación internacional. Así pues, los Estados deben favorecer legislativamente la acción proactiva sobre cualquier organización o agente capaz de generar impacto sobre la actividad económica, ya sea a través de la comunicación, las relaciones públicas, la influencia o el *lobby.* Para muchos autores, la economía global está determinada por el poder de no más de 120 grandes corporaciones multinacionales. La combinación de este poder material con el desplegado por los Estados constituye hoy el gran reto en este terreno.

El segundo aspecto a desarrollar descansa en la necesidad de utilizar los recursos de la inteligencia jurídica para conocer lo mejor posible las leyes y prácticas jurídicas de un país o de la normativa internacional, pues sin conocimiento de las reglas de juego es imposible competir en condiciones de igualdad y menos aún de ventaja.

El conocimiento de la legislación, de la jurisprudencia y otras prácticas y costumbres es esencial para asegurar una inversión en un país extranjero. No basta con conocer o dominar las leyes laborales, mercantiles, penales o tributarias. Una labor fundamental de la inteligencia económica, desarrollada tanto por servicios públicos como privados, es detectar los entornos altamente inestables y dependientes de la discrecionalidad total de los Gobiernos o aquellos manejados por grupos de presión o incluso

por grupos corruptos. No se trata solo de ofrecer información meramente descriptiva, sino de auténtica inteligencia jurídica, esto es, cualitativa. Por ello, también implica el conocimiento de los sujetos intervinientes.

La inteligencia jurídica podríamos definirla con carácter general como el tipo de inteligencia que se ocupa de la obtención, procesamiento y protección de información estratégica útil para todos los actores jurídico-económicos. Es un proceso que tiene entre sus objetivos clave el de dar un significado estratégico y jurídico a la información ambiental, de modo que el valor añadido a la información viene, precisamente, de la captación de su significado, interpretado desde una perspectiva estratégica. Conlleva pues la «búsqueda, tratamiento y transformación de la información de uso normativo en conocimiento jurídico», con los fines, a título orientativo, de:

- Preservar a los individuos y a las empresas de litigios, o cuando menos, abordarlos en las mejores condiciones posibles. Ello exige un conocimiento preciso de normas y prácticas aplicativas, y en todo caso requiere desplegar estrategias preventivas o defensivas mediante la anticipación de la búsqueda y consolidación de pruebas.
- Garantizar el reconocimiento y protección jurídica de los derechos sociales o corporativos e inmateriales de las empresas y de los ciudadanos. La protección de la información sensible de una empresa se logra, en primer lugar, mediante el conocimiento profundo y exacto de la normativa y prácticas sobre propiedad industrial e intelectual, y en segundo lugar, el reconocimiento y adecuada protección jurídica de una corporación se obtiene mediante el *lobby*: concienciación de todos los agentes intervinientes (legislativos, administrativos, económicos, mediáticos, etc.) de las necesidades de una empresa. Esta clase de acciones de influencia no se pueden confundir con comportamientos de tráfico de influencias o corrupción, pues se circunscriben a manifestar la opinión de la empresa acerca de la clase de normas y sus aplicaciones que le favorecen[22].
- Defensa de la imagen corporativa, comunicación reactiva y campañas exponiendo el acomodo a prácticas siempre legales y deontológicas.

[22] En los últimos meses asistimos a un fuerte debate y a diversas iniciativas legales de países como Reino Unido, España, Francia, Alemania e Italia, con el fin de reducir la «competencia tributaria» entre diversos países europeos. En efecto, pues varias multinacionales, como por ejemplo Amazon, Microsoft, Apple, Facebook, Inditex, Samsung o Starbucks, entre otras, imitando al gigante Google, aprovechaban las oportunidades brindadas por las diferentes legislaciones fiscales nacionales para eludir o reducir el pago de impuestos. Así, imputaban los beneficios a filiales que, actuando como intermediarias, declaraban en estados de baja tasa fiscal como Irlanda, Luxemburgo, Holanda o incluso las Bermudas. Ahora, para evitar esta fuga de ingresos, los citados países tratan de homogeneizar sus legislaciones internas con la intención de fijar la obligación de contribuir en el lugar de desarrollo de la actividad y generación de beneficios, y no en el lugar de residencia social.

Aquí la clave reside en protocolos de actuación interna orientados a evitar o atenuar acciones de desestabilización mediante diversos mecanismos de instrumentalización de la justicia. La necesidad de dotarse de órganos especializados con sus protocolos internos de estrategias jurídicas reactivas, inmediatas, frente a campañas mediáticas orquestadas por un competidor mediante iniciación de procesos jurídicos que, aunque temerarios, permiten denigrar o disminuir el valor de la empresa («riesgos informacionales»), por ejemplo, ante una salida a cotización bursátil. O que busquen en el procedimiento judicial la obtención de información sensible de la empresa o del individuo. No hay que olvidar que, también en el ámbito jurídico, la ventaja siempre es del que ataca, del que demanda o denuncia. De aquí la necesidad de reducir las posibilidades de sorpresa[23].

- La vigilancia jurídica ofrecida por asesores competentes y fiables para salvaguardar el patrimonio tangible e intangible; reglas contractuales de confidencialidad; política de patentes, esto es, decidir si se patenta o se explota antes la invención pero con un adecuado sistema de protección; enfrentar prácticas fraudulentas como las «patentes cebo» o la inundación de patentes del mercado para confundir respecto a la auténticamente útil, etc[24].
- Ante procesos de negociación con otras sociedades, y adelantando posibles intentos de adquisición por empresas competidoras mayores, deben articularse pactos entre accionistas que blinden estas entradas foráneas de nuevos socios que en ocasiones persiguen el control y hundimiento de la marca, o cuando menos el dominio social.

Así pues, la misión fundamental del derecho es «garantizar la seguridad económica», identificando los riesgos de injerencia en empresas nacionales y centros de investigación. En este sentido, debe desarrollarse una normativa que ofrezca una protección suficiente y disuasoria. La legislación debe afrontar la competencia en una economía global abierta, que enfrenta ventajas de crecimiento pero también la confrontación con poderosos agentes consolidados con los emergentes.

De modo que es fundamental desarrollar un concepto de seguridad económica vinculado a la categoría más amplia de seguridad, y en particular de seguridad nacional, detectando las amenazas y así impulsando una normativa a la vez preventiva y sancionadora de su incumplimiento. Esta

[23] Un buen ejemplo reciente de ataque jurídico sorpresa es el sufrido por la fragata argentina Libertad en Ghana, originado por una demanda de embargo presentada ante un tribunal de Nueva York por el fondo de inversión NML Capital, que logró que el Tribunal del Mar, con sede en Hamburgo (Alemania), ordenara a los tribunales del país africano la confiscación del Buque Escuela de la Armada Argentina con motivo de una deuda de 300 millones de dólares impagada desde 2002.

[24] Cfr. LARRIBA HINOJAR, Beatriz. *La tutela penal del diseño industrial*. Valencia: Tirant lo Blanch, 2006.

categoría incluiría la seguridad económica en sentido estricto (liberalización del comercio, aranceles, proteccionismo, inflación, inestabilidad financiera, volatilidad de los mercados, falta de transparencia en las inversiones); seguridad del comercio (criminalidad internacional, terrorismo, espionaje, ataques cibernéticos, corrupción); seguridad alimentaria (reservas de alimentos, subvenciones de agricultura y pesca, transgénicos, biocombustibles); seguridad energética (reservas y continuidad de suministros, escalada de precios); seguridad medioambiental (calentamiento global, reservas naturales, prevención de emergencias por desastres naturales); seguridad del consumo y salud (enfermedades contagiosas, transgénicos, biotecnología), y seguridad social (laboral, coberturas y asistencia, pensiones).

En realidad, la categoría de *seguridad económica* integraría una más amplia junto a otras más consolidadas como la citada seguridad nacional, seguridad colectiva, seguridad común, seguridad humana, seguridad cooperativa y seguridad sostenible[25].

La *inteligencia jurídica* debe orientarse tanto al mercado interior como al exterior, y para ello debe favorecer una normativa que permita una fluida coordinación entre administraciones central, regional y local con diferentes clases de empresas. Aquí surge la conveniencia de creación o fortalecimiento de empresas públicas en sectores estratégicos, así como el impulso de foros estables de cooperación entre el sector público y el privado.

Las nuevas tecnologías de la información permiten también en este campo un trabajo fácil, rápido y en tiempo real, abriendo el camino a un conocimiento de la legislación y de las prácticas aplicativas igualmente ágil y preciso. Su combinación con el uso de fuentes humanas altamente formadas permite reunir capacidades técnicas ilimitadas que proporcionen análisis detallados para la toma de decisiones y a la vez posibiliten el despliegue de múltiples acciones de influencia a través de redes sociales, medios de comunicación, publicaciones especializadas y foros profesionales, y desde luego también acceso a los circuitos de toma de decisión.

La *inteligencia jurídica* tiene que posibilitar el conocimiento de contratos, oportunidades, proyectos, necesidades y hasta de perfiles de la competencia, acompañando las ofertas nacionales en el interior y en el exterior. Esta labor implica el estudio e impulso de normativas que favorezcan la investigación y revalorización de la investigación pública cuya prioridad sea beneficiar a empresas nacionales, ofreciendo ventajas jurídicas a las invenciones tecnológicas para abrir o consolidar mercados y favorecer la

[25] BALLESTEROS MARTÍN, Miguel Ángel y JOYANES AGUILAR, Luis (2011). «Los efectos de la globalización en el ámbito de la seguridad y defensa», en *Inteligencia y Seguridad: Revista de Análisis y prospectiva,* n.º 10, pp. 14 y ss.

exportación. Del mismo modo, deben articularse modelos contractuales que aseguren el retorno de la inversión.

Las patentes, la notoriedad de las marcas, las bases contractuales (condiciones, legislación aplicable y jurisdicción) son elementos indispensables. Hoy la cuestión clave en economía reside, más que el proceso productivo como simple fabricación, en el diseño, en el valor añadido. De aquí la importancia de la inversión en tecnología, en innovación y en la normativa e instrumentos para su protección (antiespionaje)[26] y explotación en condiciones seguras.

La preferencia son contratos estratégicos: atraer «inversiones directas», favorecer inversiones en el extranjero y singularmente la exportación en sectores prioritarios. La creación, conocimiento y manejo legal de estas esferas es en la actualidad absolutamente decisivo.

Y en este contexto de competencia internacional, debe partirse de que las leyes nacionales no son idénticas, como es obvio entre las europeas, las americanas y las asiáticas, por lo que el trato jurídico a las empresas es muy distinto en uno u otro lugar[27]. Tampoco es recíproco el grado de cumplimiento de los tratados internacionales, baste por ejemplo saber que el convenio anticorrupción de la OCDE, firmado por todos los países europeos le resta competitividad frente a otros estados que no lo han suscrito ni por tanto lo aplican a sus empresas.

En consecuencia, en las estrategias nacionales de seguridad deben contenerse los desarrollos normativos nacionales e internacionales favorables para su crecimiento y estabilidad, así como los mecanismos de influencia exterior[28].

El derecho como herramienta de la inteligencia

En la actualidad, la inteligencia económica se extiende a cualquier información que pueda tener una influencia sobre los resultados de una

[26] Un ejemplo significativo puede verse en *«The Economic Espionage Act of 1996: A brief guide». National Counterintelligence Center. Estados Unidos: 1997, Cfr.* SZOTT MOOHR, Geraldine. «The problematic role of criminal law in regulating use of information: The case of the Economic Espionage Act», *Public law and legal theory series*, 2009-A-5. Houston: Universidad de Houston, Law Center, 2009.

[27] Ilustra estas diferencias el enconado debate actual en el seno de la Unión Europea sobre la implantación de un impuesto sobre las transacciones financieras. Cfr. MONTOYA CERIO, Fernando, SAMBEAT VICIÉN, Andrés y FABRA RODRÍGUEZ, Óscar: «La tasa Tobin europea. Un impuesto sobre las transacciones financieras», *Documento de Opinión*, IEEE, 06/2013. 16 de enero de 2013.

[28] En materia de alianzas comerciales internacionales, el desarrollo de la Asociación Pacífico (TPP) sin duda representa un cambio mundial de primera magnitud, al reunir ya a EE. UU., Canadá, México, Perú, Chile, Australia, Nueva Zelanda, Malasia y Singapur, y la probable incorporación este año de Japón y Corea del Sur.

actividad empresarial, y desde ahí puede trascender al bienestar común (seguridad nacional). Y el conocimiento sobre leyes y prácticas jurídicas es parte sustancial de esos datos con potencial afectación al objeto social, pues forma parte del entorno competitivo de un sector económico. La normativa es uno de los elementos claves para la toma de decisión.

El uso del derecho como herramienta de inteligencia se manifiesta abiertamente en el marco de las acciones encubiertas y de las acciones de influencia.

El modelo norteamericano de la OSI (Office of Strategic Influence)[29], que desde 2001 pasa por la creación de *lobbies* normativos, constituye uno de los mejores exponentes al respecto.

Como ejemplo paradigmático, ahí está la normativa sobre las empresas de «colecta de información», en particular Google. Estas corporaciones atesoran múltiples posibilidades de obtener informaciones y datos de los consumidores y agentes económicos de cualquier parte del mundo. Una vez adquiridos también se plantea su hipotética comunicación, dentro de una estrategia de inteligencia económica estadounidense, a empresas competidoras de esta nacionalidad –aunque solo sea una recolecta de datos diversos con el objetivo de crear perfiles de internautas–. El conocimiento es poder[30]. Pero no solo en el sentido de adquirir información masiva procedente de todo el planeta; también desde la óptica de hacerlo además mediante una cobertura legislativa. Semejan-

[29] Hay que precisar que la existencia de la OSI como tal es hoy una incógnita. Parece ser que fue una sección creada por el Departamento de Defensa de los Estados Unidos, en octubre de 2001, para apoyar la guerra contra el terrorismo a través de «operaciones psicológicas» en países-objetivo, incluidos los Estados Unidos. Aunque en un principio su cierre fue anunciado en 2002 por el entonces secretario de Defensa Donald Rumsfeld –una vez que se hizo de conocimiento público su existencia–, diversas fuentes aseguran que la OSI continúa operando –con otra denominación secreta– y que únicamente se eliminó su nombre, pasando la mayoría de sus competencias «públicas» a la Information Operation Task Force. Pero, obviamente, al tratarse de actividades secretas, nadie sabe realmente si ahora siguen llevándose a cabo y en su caso qué organismo es el competente. La OSI originalmente fue autorizada para emplear lo que se denomina engaño militar (*military deception*) de la opinión pública, presentando informaciones, imágenes o declaraciones falsas con el objetivo de engañar a los ejércitos o agentes enemigos y a poblaciones civiles mediante la desinformación.

[30] SOLOVE, Daniel, J. «A brief history of Information Privacy Law», *Public Law Research Paper*, n.º 215. George Washington University Law School, 2006. Del mismo autor: «A taxonomy of privacy» en *University of Pennsylvania Law Review,* vol. 154, n.º 3, enero de 2006, pp. 484-486; p. 478. Sin duda, la obtención de información posee un valor estratégico, pero igualmente constituye una intromisión en el derecho fundamental a la intimidad de los ciudadanos, por lo que estas actividades deben llevarse a cabo con estricto sometimiento a la legalidad, incluso en situaciones relativas a la seguridad económica nacional. GONZÁLEZ CUSSAC, José Luis y LARRIBA HINOJAR, Beatriz (2011). *Inteligencia económica y competitiva: Estrategias legales en las nuevas agendas de seguridad nacional*. Valencia: Tirant lo Blanch, pp. 89 y ss.

te capacidad de creación e imposición de las normas aplicables a estas grandes empresas de la información expresa un poder inteligente[31]. Aquí podríamos lanzar un elocuente excurso sobre la aplicación territorial y extraterritorial de la legislación nacional de los Estados Unidos de América, así como sobre la nebulosa y diferente normativa sobre computación en la nube[32].

En realidad estamos hablando de lo que Nye bautizó como «poder blando»[33]. En este caso: la exportación de sistemas jurídicos, la capacidad para aplicar la legislación nacional fuera de sus fronteras (extraterritorialidad), la potestad para crear normas proteccionistas en su mercado interior, su posición dominante en organismos internacionales o la influencia en el proceso de creación de legislaciones de otros estados[34]. Estas capacidades normativas permiten unas ventajas reales y en numerosas ocasiones absolutas, y han sido calificadas con ingenio como auténticos «troyanos normativos». Algunos ejemplos claros son los siguientes:

– Promoción desde EE. UU. de las IFRS (*international financial reporting standard)* o NIIF (Normas Internacionales de Información Financiera). Algunos analistas entienden que estas normas son aplicadas con gran flexibilidad en los EE. UU. mientras que en Europa rigen con mayor rigor en cuanto a contabilidad[35].

[31] GERADIN, Damien y SIDAK, J. Gregory (2008). *European and American approaches to antitrust remedies and the institutional design of regulation in telecommunications*. Liége: Howrey LLP and Criterion Economics, L. L. C., Working paper series, abril de 2008.

[32] GONZÁLEZ CUSSAC, José Luis (2012). «La verificación de los ordenamientos internos en los países de localización como garantía de la seguridad y la confidencialidad de la información», en *Derecho y cloud computing* (Ricard Martínez Martínez, editor). Madrid: Civitas, 2012, pp. 289 a 307.

[33] NYE, Joseph S. Jr. *The future of power*. Nueva York: New York Public Affairs, 2011.

[34] La capacidad de influir jurídicamente en otros países guarda una estrecha vinculación con las clásicamente llamadas «normas de cultura», y de ahí la relevancia del término «geocultura». Cfr. MEJÍA VELÁSQUEZ, Hernán: «La geopolítica de la geoeconomía», revista *Pensamiento Humanista*, n.º 4. Medellín: 1998.

[35] Desde que se promulgó la plataforma estable de las normas internacionales de información financiera (NIIF) en el año 2005 –posteriormente revisadas y modificadas–, un gran número de empresas y países de todo el mundo han adoptado estas normas (anteriormente denominadas NIC) como base para sus informes financieros. Este conjunto de normas contables de carácter mundial –aprobadas por el Consejo de Normas Internacionales de Contabilidad–, tiene como objetivo el exigir información comparable, transparente y de alta calidad en los estados financieros y en otros tipos de información financiera con el fin de ayudar a los participantes en los mercados de capitales de todo el mundo, y a otros usuarios, a tomar decisiones económicas. Hoy por hoy, uno de los principales retos que se plantean en este ámbito es el desarrollo del compromiso de convergencia establecido entre las NIIF y los principios contables generalmente aceptados en los Estados Unidos de América (US GAAP por sus siglas en inglés). Vid., en detalle: PEÑALVA ACEDO, Fernando. «NIFF versus US GAAP: resumen de las principales diferencias», en *Revista de Contabilidad y Dirección,* vol. 4, 2007, pp.55-69.

- Sin embargo, no podemos perder de vista el objetivo final: la continuación del proceso de convergencia entre los GAAP estadounidenses y las normas internacionales de contabilidad. Ciertamente, en la actualidad se está realizando un proyecto de convergencia para equiparar en mayor medida las normas incluidas en las *Normas internacionales de información financiera* (IFRS) y los *Principios de contabilidad generalmente aceptados* (USGAAP).
- El SOX, abreviatura de *Sarbanes Oxley Act*[36], es una ley norteamericana promulgada en el año 2002 como respuesta a los escándalos financieros que, como el caso ENRON, minaron la confianza de los inversionistas y del propio Estado norteamericano en los datos contenidos en los informes financieros/contables de las corporaciones. El nombre de la ley se deriva de los apellidos de sus dos principales patrocinadores, el diputado Michael G. Oxley y el senador Paul S. Sarbanes.
- El principal objetivo de esta ley es favorecer una mayor transparencia y fiabilidad en relación a los datos de los informes que emiten tanto las empresas públicas de Estados Unidos y sus subsidiarias en todo el mundo como las empresas extranjeras que coticen en cualquier bolsa de valores en los Estados Unidos. En concreto, y entre otras, establece un nuevo consejo de vigilancia, supervisado por la Comisión de Valores de Estados Unidos (SEC o *Security Exchange Commision*, por sus siglas en inglés) e incluye nuevos requerimientos de información y sanciones más graves para las conductas de fraude corporativo.
- En realidad, se trata de un agregado normativo estadounidense (Ley Sarbanes-Oxley) del IFRS que permite al PCAOB (*Public Company Accounting Oversight Board*) extender las investigaciones sobre las empresas en términos de datos financieros y estratégicos más allá de sus fronteras[37].
- La Ley Patriótica (*Patriot Act*), que obliga a las instituciones financieras, como la PCAOB, a transmitir los informes financieros a los servicios de inteligencia (CIA, NSA…) sin necesidad del permiso de las empresas y sin que estas lo sepan[38]. Tras lo cual, el CFIUS (Committee of Foreign Investment in United States) evalúa el carácter sensible de la empresa para los intereses norteamericanos según su elástica Ley de Seguridad Nacional[39].

---

[36] Sarbanes-Oxley Act de 2002. Pub. L. n.º 107-204, 116 Stat. 745, 30 de julio de 2002.

[37] Para un análisis más detallado de esta norma, vid.: ROMANO, Roberta. «The Sarbanes-Oxley Act and the making of quack corporate governance», 2004, en NYU, *Law and Econ Research Paper 04-032*; *Yale Law & Econ Research Paper 297*; *Yale ICF Working Paper 04-37*; ECGI - *Finance Working Paper 52/2004*.

[38] PHILLIPS, Heather A. *Libraries and National Security Law: An examination of the USA Patriot Act*. Progressive Librarian, vol. 25, verano de 2005.

[39] Un complemento de esta legislación, en el sentido de atribuir jurisdicción federal a EE. UU. para investigar y perseguir cualquier negocio, lo encontramos en la Economic

Como agudamente resume Zunzarren, «si el CFIUS estima que los datos que posee Google son sensibles para los intereses norteamericanos, por la Ley Sarbanes-Oxley y por la Patriot Act pueden obtenerlos sin el acuerdo de Google y sin el conocimiento de la empresa investigada aunque no sea estadounidense. Y no nos olvidemos de que la empresa Concileo es uno de los gigantes en cuanto a la moderación del contenido de la web, algo que algunos tachan de censura; y es estadounidense. Son quienes pueden cortar por lo sano los contenidos de la web, pero ¿bajo qué criterios?»[40].

Juillet ya destacó la importancia del derecho y su uso, al decir que «los americanos, inspirándose en el mundo de los negocios, han elegido modificar el entorno conduciendo al sistema hacia una nueva configuración recurriendo a la innovación tecnológica. La finalidad es cambiar el juego, dictar nuevas normas, después de ponerse a la cabeza en una competición actualmente asimétrica. La potencia tecnológica unida a la definición del campo de batalla hacen que el adversario solo tenga la elección del modo de derrota y de su velocidad de realización»[41]. Este es el modelo que tratan de imitar los demás países principales, particularmente los occidentales.

En efecto, pues como sigue subrayando el citado autor, las bases de la soberanía de un Estado ya no son solo el nivel de vida, el producto interior bruto o la capacidad exportadora. Ni siquiera su capacidad nuclear. El escenario mundial ha cambiado y son un pequeño grupo de tecnologías estratégicas las que aseguran la independencia real de las naciones. Pero la experiencia científica requerida para trabajar en estos campos y el volumen de las inversiones necesarias impedirán a muchos países permanecer en la carrera tecnológica. Por ello, el lanzamiento de programas comunes a nivel europeo resulta indispensable, puesto que «desde hace más de quince años, los americanos tienen una estrategia clara y perfectamente identificada. Invierten sin descanso en las tecnologías de la información, así como en el desarrollo del conocimiento y del saber, elementos que están en el núcleo de la potencia y de la independencia modernas. Animados por su Estado, los industriales americanos no dudan en establecer alianzas y en comprar empresas, en el mundo entero, cuando quieren adquirir una tecnología, completar su experiencia o neutralizar a un competidor»[42].

Espionage Act. En este sentido, amplia y críticamente, ver: HOROWITZ, Richard. *Competitive Intelligence, law and ethics: The Economic Espionage Act revisited again (and hopefully for the last time).* SCIP, vol. 14, n.º 3, julio-septiembre de 2011, pp. 41 y ss.

40 ZUNZARREN, Hugo, en http://idinteligencia.wordpress.com/archivos-2/posts-precedentes/inteligencia-juridica-en-los-eeuu/.

41 JUILLET, Alain. «Principios de aplicación de la inteligencia económica». *Inteligencia y Seguridad: Revista de análisis y prospectiva*, n.º 1, diciembre de 2006, pp. 123-132.

42 Este texto es el resumen de la intervención de Alain Julliet en el Coloquio Independencia de Europa y Soberanía Tecnológica, celebrado en abril de 2012 en París y

En el plano internacional son innumerables los ejemplos[43], baste aquí traer a colación el actual conflicto en Nigeria, donde se debate la aprobación de una legislación que habilitaría la imposición de cuantiosas sanciones a las petroleras por los daños ocasionados en el delta del Níger en sus actividades de extracción de crudo. Pero como es natural, los poderosos *lobbies* de estas multinacionales, supuestamente apoyados por las instituciones y servicios de sus países de origen, tratan de influir para paralizar esta propuesta, retrasarla o, cuando menos, limitar su aplicación.

La reciente intervención militar francesa en Mali también es analizada no solo como un decidido freno al terrorismo, sino también con una finalidad geoeconómica: proteger sus inversiones en el vecino Níger (produce el 8% del uranio mundial), donde su multinacional AREVA, con el 80% de titularidad pública, extrae uranio que importa a Francia y que representa alrededor del 40% de su consumo. La *seguridad energética* sin duda también ha pesado para que China no se opusiese a esta intervención, ya que protege igualmente a sus gigantescas empresas CNIUC y CNPC, con intereses en uranio y petróleo.

La importancia de las reglas en la economía global tiene hoy un exponente extraordinario en la regulación de los llamados «fondos soberanos». Su importancia estratégica no hace falta destacarla desde el momento en que se trata de fondos públicos, esto es, manejados por los Gobiernos, pero invertidos en el sector privado. Pero justamente una de las mayores críticas a estos instrumentos financieros es su falta de transparencia, junto a ciertos indicios de proteccionismo, la cesión de control estratégico a determinados sectores (bancario y tecnológico) y su posible utilización por algunos estados como instrumento de presión política y económica frente a otros países.

Toda esta controversia dio lugar a la creación en abril de 2008 del Grupo Internacional de Trabajo sobre Fondos Soberanos de Inversión (GITFSI), que culminó en octubre de 2008 en Chile con la aprobación de un código deontológico. Este acuerdo fue denominado *Principios y prácticas generalmente aceptadas* (PPGA) o Principios de Santiago. Pues bien, pese a su importancia decisiva en la economía mundial del siglo XXI, siguen siendo un modelo de autorregulación y no auténticas normas jurídicas vinculantes. Por tanto, aunque su finalidad se diga que es exclusivamente económica y financiera, no se excluye expresamente que su utilización

titulado *Cambian las bases de la soberanía mundial. Se desplazan factores económicos y de seguridad a algunas tecnologías clave que Europa no ha cultivado*. Se reproduce con autorización del autor. Traducción del francés: Eduardo Martínez. http://www.tendencias21.net/Cambian-las-bases-de-la-soberania-mundial_a337.html.

43 GONZÁLEZ CUSSAC, José Luis y LARRIBA HINOJAR, Beatriz. *Inteligencia económica y competitiva: Estrategias legales en las nuevas agendas de seguridad nacional*. Valencia: Tirant, 2011, pp. 72 y ss.

esté sujeta a «otras consideraciones»[44]. He aquí un arma geoeconómica de gran calibre a considerar central en cualquier análisis de inteligencia jurídica y económica.

En esta panorámica conviene también subrayar los llamados Acuerdos de Basilea, así como la Organización Mundial del Comercio (OMC, en inglés WTO).

En 1974, el Comité de Basilea, integrado por los gobernadores de los bancos centrales de los países del G-10, aprobaron el primero de los Acuerdos de Basilea, un conjunto de recomendaciones dirigidas básicamente a establecer el capital mínimo que debía poseer una entidad bancaria en consideración a los riesgos que afrontaba. Se trataba de una simple recomendación, de modo que los estados signatarios no quedaban obligados a incorporarlos a sus legislaciones, o podían hacerlo con modificaciones. Lo suscribieron más de cien países. Sin embargo, se detectaron dos grandes inconvenientes: su insensibilidad a las variaciones de riesgo y la ausencia de valoración sobre la calidad crediticia.

Para superar estas críticas se adoptó en 2004 el Acuerdo de Basilea II, creando un subgrupo encargado de impulsar su implantación internacional (Accord Implementation Group, AIG). Hoy rige en toda la Unión Europea –impuesto obligatoriamente a través de directivas–, en Japón, en Australia y en más de 95 países diferentes a los integrantes del Comité. Pues bien, al margen de su incuestionable avance hacia una práctica internacional homogénea y de sus posibles deficiencias técnicas, llama otra vez la atención su naturaleza jurídica, que permite un diverso grado de cumplimiento a nivel mundial. Y ello a pesar de su transcendencia en la génesis de la actual crisis financiera y de su valor extraordinario en un mercado estratégico como es el financiero. De nuevo nos hallamos ante una falta de normativa obligatoria y una carencia notable de transparencia.

La Organización Mundial del Comercio (World Trade Organization*)*, aunque no forma parte de la ONU ni de los organismos de «Bretton Woods» (FMI, Banco Mundial), integra a más de 158 países y a 26 en calidad de observadores. Su objetivo es la regulación multilateral del comercio internacional, y en la actualidad administra alrededor de 60 acuerdos. Las disposiciones originales, denominadas *GATT 1947,* fueron ampliadas desde la célebre Ronda Uruguay, conocidas como *GATT 1994,* es decir, Acuerdo General sobre Aranceles Aduaneros y Comercio. Sabido es que su impulso inicial fue fruto del acuerdo entre los países más desarrollados, especialmente EE. UU. y la Comunidad Europea, con el propósito de liberalizar el comercio internacional, reduciendo los aranceles de aduanas, subvenciones y otros instrumentos de «distorsión del comercio». Sin

[44] CORONAS VALLE, Daniel y LÓPEZ JIMÉNEZ, José M.ª: «Crisis y fondos soberanos: ¿El abrazo del oso?», *Documento de Opinión, IEEE 14/2013,* de 5 febrero de 2013.

embargo, se objetó que solo lo hacían en los sectores que convenía a sus intereses, pero exceptuaba los que necesitaban mantener medidas proteccionistas (textil y agricultura). A partir de la Ronda Uruguay, esta situación comenzó a cambiar. No obstante, las medidas de flexibilización fueron insuficientes a juicio de los países menos desarrollados, y además, en contrapartida, se introdujeron nuevos sectores, como el comercio de servicios y, particularmente, el referente a la propiedad intelectual, por exigencia norteamericana[45].

La OMC exige la adhesión a todos sus acuerdos, sin excepción. De modo que las reglas de comercio rigen para todos exactamente igual y con independencia del nivel de desarrollo humano, tecnológico y social. Este contraste suscita la crítica esencial, demandando tratos especiales y diferenciados acordes con el grado de desarrollo de cada país. La llamada Ronda de Doha de 2001 (Programa Doha para el Desarrollo) persiguió este objetivo, todavía muy lejano y abandonado con el estallido de la gran crisis de 2008. Por consiguiente, en la actualidad, los países más desarrollados, afectados por la crisis, mantienen unos acuerdos que les favorecen claramente en el comercio internacional y no parecen muy dispuestos a hacer concesiones ni a los países emergentes ni a los poco desarrollados. De nuevo el valor del derecho, la ventaja de quien tiene la capacidad de crear las reglas y su valor estratégico[46].

En el caso español, entre otros recientes, podríamos citar la disputa de Repsol-YPF en Argentina, altamente significativa de lo que venimos hablando. Muy controvertida fue también la reforma del art. 135 de la Constitución, el 27 septiembre de 2011. Para unos constituye una manifestación de pérdida de soberanía económica, influida por los intereses de los acreedores internacionales y garantizada al máximo nivel normativo; para otros, sin embargo, resultaba una necesidad la corrección del déficit presupuestario público (estructuralmente del 5% del PIB y disparado tras la gran crisis actual) con la introducción de un límite de gasto y endeudamiento o principio de estabilidad presupuestaria[47]. En efecto, pues determinados a imponer estrictas reglas sobre el déficit presupuestario, también deberían extenderse a los desequilibrios de las balanzas comerciales; reformar la normativa fiscal hacia una comprensión flexible y adaptable a periodos de expansión o de recesión de la economía[48].

---

45 Al respecto puede verse ARCOS MARTÍN, Rubén (2010): «*La lógica de la excepción cultural*». Madrid: Cátedra, 2010.

46 REYNAUD, Julien P. M. y VAUDAY, Julien. «IMF lending and geopolitics», *ECB working paper* n.º 965. International Monetary Found, 14 de noviembre de 2008.

47 Merece una reflexión la tesis que propugna una clasificación entre países que acumulan riqueza (balanza comercial favorable, tecnología y ahorro) y países que acumulan deuda.

48 Para una visión más completa acerca de la geopolítica del petróleo en la actualidad, vid.: MAUGERI, Leonardo. «Oil: The next revolution», *Discussion paper 2012-10*. Belfer Center for Science and International Affairs, Harvard Kennedy School, junio de 2012.

La transcendencia estratégica de una sólida alianza entre innovación tecnológica y acompañamiento normativo se expresa en la actualidad de forma paradigmática en la industria energética[49]. Según el informe de 12 de noviembre de 2012 de la Organización de Energía Atómica (AIE en inglés, Energy Information Administration), los EE. UU. de América serán en 2017 el mayor productor de petróleo y en el 2030 el mayor exportador. Ello gracias a que se ha permitido legalmente –a pesar de los obstáculos y advertencias de riesgo medioambiental– el desarrollo de una tecnología innovadora de perforaciones horizontales y de «fachada hidráulica» que permite la extracción de crudo y gas por medio de presión de agua (*fracking)*. Este cambio ya está teniendo efectos geopolíticos determinantes y consecuencias múltiples sobre otros países tan dispares como Arabia Saudí (y otros países del golfo pérsico), Rusia, China, Venezuela, Ecuador o Bolivia[50].

Estos «troyanos normativos» expresan la alegórica construcción de BENTHAM del *panóptico,* magistral descripción de la forma de poder bajo la que vivimos, y muy particularmente en la era digital. Es más, las nuevas tecnologías hasta pueden prescindir de la torre central de vigilancia y de cualquier otra herramienta material, pues con estas infraestructuras ejercen un control completo. Las grandes compañías financieras, energéticas, de servicios de Internet y telefónicas constituyen algo más que buenos ejemplos; su alianza o colaboración con los Gobiernos aumenta las competencias y extensión de lo vigilado y de los vigilados. Sin embargo, Internet presenta un inconveniente para los vigilantes, puesto que al vigilar dejan rastro de su observación y pueden ser a su vez vigilados, aunque para hacer posible esta posibilidad de doble dirección, es preciso desarrollar normas que lo posibiliten: en el ámbito internacional tratados que limiten y regulen la vigilancia global, y en el plano interno, leyes de libertad de información y especialmente de transparencia, donde los ciudadanos puedan controlar a los vigilantes.

En definitiva, se hace indispensable poseer una legislación nacional e internacional que posibilite una organización con una potente actividad que disuada las acciones hostiles exteriores. De esta forma se actualiza la doctrina de la disuasión, pues se hace patente que las consecuencias negativas para quien lo intente serán mayores que cualquier beneficio. Necesitamos normas especiales y excepcionales para tiempos de profundo cambio en las relaciones sociales, o si se prefiere llamar así, para tiempos de «guerra económica». Las normas deben contribuir a dismi-

[49] YOUNGS, Richard. «Europe's external energy policy: Between geopolitics and the market». *Centre for European Policy Studies working documents,* n.º 278. 20 de noviembre de 2007.

[50] NYE, Joseph S. Jr. «American and Chinese power after the financial crisis», *The Washington Quarterly*, 33:4. Center for Strategic and International Studies, Octubre de 2010, pp. 143-153.

nuir o anular las vulnerabilidades y a generar bienestar común. Podría enunciarse como la necesidad de un nuevo derecho económico para un nuevo contexto mundial.

Para lograrlo resulta básico fortalecer las instituciones, dotándoles de capacidad real para aplicar una normativa protectora y sancionadora de los ataques al patrimonio económico, científico, tecnológico, histórico, artístico, cultural y medioambiental, y de una especial tutela frente al espionaje de datos sensibles frente a intrusiones, así como articular mecanismos públicos de control sobre capital de empresas estratégicas y vigilancia sobre los inversores, especialmente sobre los *no deseados*.

Este complejo normativo debe extenderse especialmente a las pymes, permitiendo el desarrollo de redes que permitan defender sus derechos en todo el mundo, contribuyendo a la reducción de oligopolios y a las imposiciones de las grandes corporaciones multinacionales y, en resumen, posibilitando esa vieja aspiración liberal de la libre competencia. Junto a ello es preciso brindar normas premiales para impulsar el despliegue exterior y la consolidación interna e implementar mecanismos formalizados de asesoramiento para paliar las trabas burocráticas, la falta de datos o las acciones de desinformación.

Conclusiones

La primera conclusión es reivindicar el valor del derecho, tanto del poder de crear normas como de su conocimiento y aplicación, para la inteligencia económica. Para ello es imprescindible la interrelación entre los tres planos anteriormente expuestos, de suerte que si hoy es una obviedad la dependencia entre seguridad nacional y prosperidad económica, también lo es que ambas son vicarias de las reglas vigentes.

La segunda, señalar la hasta ahora insuficiente atención que, para la seguridad económica como parte integrante de la seguridad nacional, se ha venido prestando al fenómeno del crimen organizado, su estrecha vinculación con la corrupción y su tremendo impacto institucional. En fechas muy recientes esta actitud está siendo corregida, como muestra, por ejemplo, la atención prestada por diferentes estrategias de seguridad nacional y regional o la del Parlamento Europeo con su informe de 2011 sobre crimen organizado internacional en la Unión Europea.

La tercera, y de todo punto esencial, se refiere a las causas profundas de la actual gran crisis internacional. En este panorama destaca justamente el predominio de las políticas de «no-derecho», eufemísticamente catalogadas de desregulación, autorregulación o antiintervencionismo estatal. Obviamente, estas políticas responden a una ideología tras la cual se esconden notorios intereses económicos, y de ningún modo expresan ninguna clase de «ley natural de los mercados». Provocada por los gran-

des oligopolios financieros, energéticos y de las nuevas tecnologías de la comunicación y de la información, permiten imponer sus intereses particulares por encima de los intereses generales, ya sea en connivencia con algunos países o bien a pesar de otros más débiles[51]. El resultado es la generación de un empobrecimiento constante de estos y de sus ciudadanos, y también ocasionan una erosión de las instituciones y su constante pérdida de legitimación –mejor para ellos, pues cuanto más débiles sean las instituciones públicas más poder acumulan–.

Este estado de cosas, junto a los daños directos en la calidad de vida de millones de personas, alimenta el discurso de los radicales y de las ideologías extremistas, y también resucita el históricamente fracasado discurso del proteccionismo económico. Así, se alzan propuestas a favor de la *desglobalización*. En concreto, algunos se muestran partidarios de un retorno a normativas estatales proteccionistas[52].

Ciertamente, el capitalismo ejerció su control económico permitiendo que los Gobiernos, a través del derecho, dieran satisfacción a concretas demandas sociales. Sin embargo, con la caída del contrapeso representado por los estados comunistas, este equilibrio se rompió. La ideología neoliberal del capitalismo moderno se ha levantado sobre un doble argumento: el intervencionismo estatal reduce las libertades individuales y frena la iniciativa de la sociedad civil. Desde este presupuesto se desencadenó un proceso constante y sistemático de reduccionismo de la esfera pública hacia el «Estado mínimo». El mensaje explícito ha sido simple: todo intervencionismo estatal es sinónimo de dominación, de restricción de las libertades; por consiguiente, todo producto del Estado es negativo. Así, la regulación legal, con sus formalidades y exigencias de control y publicidad, se presenta como inútil burocracia; la política es siempre equivalente a corrupción, y la justicia, con sus procedimientos garantistas, una rémora del pasado, lenta e ineficaz. El mensaje subliminal esconde la interesada identificación de sociedad civil con mercados libres, es decir, con los monopolios del poder financiero, y consecuentemente el progreso requiere la agilidad y flexibilidad de la desregulación, la *autorregulación*, el arbitraje, la mediación y cualquier mecanismo no formalizado.

En definitiva, el descrédito del Estado y su permanente deslegitimación reclama menos reglas, menos derecho, menos *res publica*. Pero como advirtiera Epicureo, «si se suprimieran las leyes, los hombres necesita-

[51] De gran interés el conocimiento del funcionamiento del mercado financiero mundial, especialmente de la denominada «permuta de incumplimiento crediticio» (*credit default swap)*: Cfr. ÁLVAREZ RUBIAL, Gregorio Pablo. «El *credit default swap* como agente transformador del paradigma financiero internacional», *Documento de Opinión, IEEE, 04/2013*, 9 de enero.

[52] TODD, Emmanuel. *Después de la democracia.* Madrid: Akal, 2010; MONTEBOURG, Arnaud. *¡Votad la desglobalización!* Barcelona: Paidós, 2011.

rían las garras de los lobos, los dientes de los leones». Solo el derecho proporciona reglas, valores, razones, intereses, imperativos capaces de transitar desde una sociedad donde rige el poder del más fuerte –históricamente la fuerza militar, hoy el oligopolio financiero– a una convivencia ordenada, plural y transparente: el Estado del derecho. Solo con seguridad jurídica puede existir una auténtica economía libre, y la inteligencia económica y competitiva debe primero conocer esas reglas, y luego propiciar su correcta aplicación y reforma conforme a los intereses generales. Esa es la dimensión de la economía como integrante de la seguridad nacional.

En esta dirección, algunas propuestas parecen imprescindibles para lograr el objetivo de una mayor seguridad económica. En primer lugar, hay que subrayar que la comunidad internacional ya posee normas útiles y eficaces que, en gran medida, pueden resolver muchas de las cuestiones aquí planteadas. Su reconocimiento, aplicación y control de cumplimiento son esenciales para la actividad económica.

En segundo lugar, impulsar leyes sobre competencia más estrictas y posibilitar su efectiva aplicación, en especial sobre las entidades financieras, energéticas y de nuevas tecnologías de la información y comunicación. Ello comporta acabar con bonificaciones desproporcionadas, subvenciones fiscales y ayudas públicas, y más transparencia y el fin de los paraísos fiscales; pero también reformas tributarias que corrijan las grandes desigualdades actuales, modificar la normativa sobre quiebras y, en definitiva, una nueva legislación que, en palabras de Stiglitz, «suavice la globalización»[53].

Esta gran crisis debe superarse con más democracia (mayor participación ciudadana) y más derecho (una regulación actualizada y precisa). Es fundamental el incremento de la transparencia, vía esencial de control de la ciudadanía sobre los representantes públicos, que no pueden continuar reservando información pública y así pretender conservar exclusivamente la capacidad de decisión sobre los asuntos generales, amparados en el falaz presupuesto de que son los únicos conocedores y por tanto los únicos cualificados. Ya lo ha expresado categóricamente Hobsbawm:

> *Los estados con una economía boyante y estable y una distribución de la riqueza relativamente equitativa son menos susceptibles de sufrir un seísmo social y político que aquellos pobres, donde las desigualdades están a la orden del día y cuya economía es todo menos estable. Del mismo modo, la posibilidad de la paz se vería afectada por un aumento drástico de las desigualdades económicas y sociales, tanto en el seno de los países como entre unos y otros*[54].

[53] STIGLITZ, Joseph E. (2012). *El precio de la desigualdad.* Madrid: Taurus, 2012, p. 343.
[54] HOBSBAWM, Eric (2006). *Guerra y paz en el siglo xxi.* Barcelona: Crítica, 2006, p. 16.

La experiencia histórica nos muestra la consecuencia que para el Estado democrático de derecho tiene la inestabilidad económica y social, manifestada constantemente por periodos de inflación demoledores de las clases medias. Y ya sabemos que sin ellas no es posible un régimen de libertades. El riesgo de la inflación acecha hoy a muchos países desarrollados y, por consiguiente, su control debe constituir una de las prioridades de nuestros Gobiernos[55].

Así mismo, los Estados jurídicamente desarrollados –lo que comporta un importante grado de implantación de derechos civiles, individuales y sociales (especialmente laborales)– favorecen el crecimiento sostenible y consecuentemente atraen las inversiones económicas. Esta premisa es una constante histórica, y en la actualidad comienza a vislumbrarse con el incipiente final de la tendencia hacia la deslocalización y externalización de grandes empresas. En efecto, pues muchas de ellas han comenzado el regreso «a casa» como reacción a los ingentes problemas de inseguridad jurídica, corrupción e inestabilidad política e insuficiente desarrollo tecnológico y de infraestructuras de muchos de los países que inicialmente atrajeron su residencia debido a sus bajos costes.

Con Berlin, podemos rechazar análisis y respuestas monistas: ni hay una sola crisis –sino varias entrelazadas– ni la respuesta es única –solo financiera y económica–, sino también institucional, con una demanda y necesidad acuciante de desarrollo de normas construidas sobre valores compartidos. En efecto, porque como también recuerdan los economistas, esta crisis financiera y económica es sobre todo una crisis de valores, esto es, una crisis moral y consecuentemente una crisis de derechos, de inseguridad y de falta de confianza[56].

Voy concluyendo con una idea expresada con gran claridad por Juillet:

> *Frente a la presión ejercida por todos los que quieren aumentar su participación en el mercado mundial, la única verdadera respuesta consiste en crear reglas del juego claras y aplicables en todos los países. Es un caso raro ahora porque muchos tienen la tendencia a buscar privilegios o a escabullirse. Frente a la dificultad de hacer cumplir los acuerdos internacionales, hace falta llegar a convencer de que la ausencia de reglas, el incumplimiento de las normas y el pirateo de patentes son ruinosos para las empresas y para las economías. El reconocimiento y la supervisión de las normas, así como el control del cumplimiento de*

[55] TOURAINE, Alaine (2011). *Después de la crisis*. Madrid: Paidós, 2011.

[56] STIGLITZ, Joseph E. *Caída libre: el libre mercado y el hundimiento de la economía mundial*, Madrid: Taurus, 2010, pp. 324 y ss. En este punto, cobra un valor fundamental una educación integral, esto es, humanista, porque sin ella no hay ciudadanos verdaderamente libres (críticos), y sin ellos la democracia queda en una idea hueca.

las reglas aplicables para todos, están pues en el corazón de la actividad de inteligencia económica[57].

En resumen, si, como he tratado de subrayar en estas líneas, toda actividad humana está sometida a reglas, su conocimiento, manejo, aplicación y, especialmente, su creación son un valor estratégico esencial (*auctoritas, non veritas, facit legem)*. Como ya advirtiera Aristóteles, la inteligencia consiste no solo en el conocimiento, sino también en la destreza de aplicar los conocimientos en la práctica.

Normas, valores, intereses, imperativos, todo esto es derecho. Sin leyes fiables no puede existir una economía verdaderamente libre, o lo que es lo mismo, sin seguridad jurídica tampoco puede haber seguridad económica. Y sin una economía libre y segura para todos es imposible la convivencia pacífica y ordenada (*salus populi suprema lex)*. Por eso, solo el derecho es el futuro de la democracia.

Bibliografía

ÁLVAREZ RUBIAL, Gregorio Pablo. «El credit default swap como agente transformador del paradigma financiero internacional», *Documento de Opinión, 04/2013,* IEEE, 9 de enero de 2013.

ARCOS MARTÍN, Rubén. *La lógica de la excepción cultural*. Madrid: Cátedra, 2010.

— «Hacia un sistema español de inteligencia para la seguridad económica y la competitividad», en *Inteligencia y Seguridad: Revista de análisis y prospectiva,* n.º 11, 2012, pp. 103 y ss.

ARNETT, Dennis, MENON, Anil y WILCOX, James B. «Using competitive intelligence: Antecedents and consequences». *Competitive Intelligence Review,* vol. 11, issue 3, 2000, pp. 16-27.

ARMENTA DEU, Teresa. «*Exclusionary rule:* Convergencias y divergencias entre Europa y América», *Revista de Estudios de la Justicia,* n.º 11, 2009.

AA. VV. *Modelos de reflexión estratégica europea e inteligencia económica*. Universidad rey Juan Carlos, Instituto Juan Velásquez de Velasco y Cátedra de Servicios de Inteligencia y de Sistemas Democráticos, 2012.

BALLESTEROS MARTÍN, Miguel Ángel y JOYANES AGUILAR, Luis. (2011): «Los efectos de la globalización en el ámbito de la seguridad y defensa», en *Inteligencia y Seguridad: Revista de análisis y prospectiva,* n.º 10, pp. 14 y ss.

[57] JUILLET, Alain (2006). «Principios de aplicación de la inteligencia económica». *Inteligencia y Seguridad: Revista de análisis y prospectiva*, n.º 1, diciembre de 2006, pp. 123-132.

BUZAN, Barry; WEAVER, Ole y DE WILDE, Jaap. (1998): *Security. A new framework for analysis.* Londres: Lynne Rienner Publishers, 1998, pp. 95 y ss.

BÉGIN, Lucie, DESCHAMPS, Jacqueline y MADINIER, Héléne. «Une approche interdisciplinaire de l´intelligence économique». *Cahier de Reserche,* n° HES-SO/HEG-GE/C--07/4/1-CH, Haute École de Gestion de Genève, 2007.

BRADFORD, William. *The three faces of competitive intelligence: defection, collusion and regulation*. Universidad de Florida, Warrintong College of Business, febrero de 2007.

CARAYON, Bernard. *Patriotisme économique: De la guerre à la paix économique*. Mónaco: Editions du Rocher, 2006.

CLARKE, Richard A. y KNAKE, Robert K.: *Guerra en la red: los nuevos campos de batalla.* Barcelona: Ariel, 2011.

COMAI, Alessandro (2009). «El sistema de inteligencia económica de Francia: Una política pública», en *Puzzle* (*Revista de Inteligencia Competitiva)*, año 8, edición n.º 30, julio-septiembre de 2009.

CORONAS VALLE, Daniel y LÓPEZ JIMÉNEZ, José M.ª: «Crisis y fondos soberanos: ¿El abrazo del oso?»*. Documento de Opinión, 14/2013,* IEEE, 5 de febrero de 2013.

DE NARDIS, Laura. *Governance at the Internet's core: The geopolitics of interconnection and Internet exchange points (IXPs) in emerging markets.* 2012.

ESTEBAN NAVARRO, Miguel Ángel (coordinador). *Glosario de inteligencia*. Madrid: Ministerio de Defensa, 2007.

— Equipo de Inteligencia Económica del CNI. «Aproximación a la inteligencia competitiva», en *Inteligencia y Seguridad: Revista de análisis y prospectiva*, n.º 9, 2011**,** pp.19-40.

FERRER RODRÍGUEZ, Juan.: «Seguridad económica e inteligencia estratégica en España», *Documento de Opinión 85/2011*. Instituto Español de Estudios Estratégicos, 5 de diciembre de 2011.

GERADIN, Damien y SIDAK, J. Gregory. (2008). «European and American approaches to antitrust remedies and the institutional design of regulation in telecommunications». *Working Paper Series,* Liége: Howrey LLP and Criterion Economics, LLC, abril de 2008.

GONZÁLEZ CUSSAC, José Luis. (2010): «Estrategias legales frente a las ciberamenazas», en *Ciberseguridad. Retos y amenazas a la seguridad nacional en el ciberespacio, Cuadernos de Estrategia,* n.º 149. Madrid: Instituto Español de Estudios Estratégicos, Ministerio de Defensa, 2010, pp. 85 a 127.

GONZÁLEZ CUSSAC, José Luis y LARRIBA HINOJAR, Beatriz. «Un nuevo enfoque legal de la inteligencia competitiva», en *Inteligencia y Seguridad: Revista de análisis y prospectiva*, n.º 8, 2010, pp. 39-73.

— *Inteligencia económica y competitiva: Estrategias legales en las nuevas agendas de seguridad nacional*. Valencia: Tirant lo Blanch, 2011.

GONZÁLEZ CUSSAC, José Luis (coordinador). *Inteligencia.* Valencia: Tirant lo Blanch, 2012.

— «La verificación de los ordenamientos internos en los países de localización como garantía de la seguridad y la confidencialidad de la información», en *Derecho y cloud computing* (Ricard Martínez Martínez, editor). Madrid: Civitas, 2012, pp. 289 a 307.

— «Tecnocrimen», *en Nuevas amenazas a la seguridad nacional. Terrorismo, criminalidad organizada y tecnologías de la información y la comunicación* (directores: GONZÁLEZ CUSSAC, José L. y CUERDA ARNAU, María Luisa; coordinador: FERNÁNDEZ HERNÁNDEZ, Antonio). Valencia: Tirant lo Blanch, 2013.

GUIORA, Amos N. «Anticipatory self-defence and international law. A re-evaluation», *Journal of Conflict and Security Law*, U of Utah Legal Studies Paper, n.º 057-08-10, 2008.

HARBULOT, Christian. *La machine de guerre economique: Etats-Units, Japon, Europe.* París: Economica, 1992.

HIDALGO SCHNUR, Diego. *Europa, globalización y unión monetaria.* Siddarth Mehta, 1998.

HOBSBAWM, Eric. «*Guerra y paz en el siglo XXI*». Barcelona: Crítica, 2006.

HOROWITZ, Richard. *Competitive Intelligence, law and ethics: The Economic Espionage Act revisited again (and hopefully for the last time).* SCIP, vol. 14, n.º 3, julio-septiembre de 2011, pp. 41 y ss..

JÁUREGUI, Gurutz. «La emergencia de un nuevo orden jurídico-institucional: el Estado y la Constitución de la era de la globalización», en INNERARITY, Daniel, y SOLANA, Javier (editores): *La humanidad amenazada: gobernar los riesgos globales.* Barcelona: Paidós, 2011, pp. 237 y ss.

JUILLET, Alain. «Principios de aplicación de la inteligencia económica». *Inteligencia y Seguridad: Revista de análisis y prospectiva*, n.º 1, diciembre de 2006, pp. 123-132.

— Texto el resumen de su intervención en el Coloquio Independencia de Europa y Soberanía Tecnológica, celebrado en abril de 2012 en París y titulado *Cambian las bases de la soberanía mundial. Se desplazan factores económicos y de seguridad a algunas tecnologías clave que Europa no ha cultivado*. Se reproduce con autorización del autor. Traducción del francés: Eduardo Martínez. http://www.tendencias21.net/Cambian-las-bases-de-la-soberania-mundial_a337.html.

LARRIBA HINOJAR, Beatriz. «Ciberespionaje económico: Una amenaza real para la seguridad nacional», en *Nuevas amenazas a la seguridad nacional. Terrorismo, criminalidad organizada y tecnologías de la*

información y la comunicación (directores: GONZÁLEZ CUSSAC, José L. y CUERDA ARNAU, María Luisa; coordinador: FERNÁNDEZ HERNÁNDEZ, Antonio). Valencia: Tirant, 2013.

— *La tutela penal del diseño industrial*. Valencia: Tirant lo Blanch, 2006.

LODEIRO, Andrea. «Ámbito de la inteligencia económica: significación, teoría y práctica», en *AA Inteligencia*, versión digital, diciembre de 2006.

MAUGERI, Leonardo. «Oil: The next revolution», *Discussion paper 2012-10*. Belfer Center for Science and International Affairs, Harvard Kennedy School, junio de 2012.

MEJÍA VELÁSQUEZ, Hernán. *«La geopolítica de la geoeconomía».* Revista *Pensamiento Humanista*, n.º 4. Medellín, 1998.

MONTEBOURG, Arnaud. *¡Votad la desglobalización!* Barcelona: Paidós, 2011.

MONTERO GÓMEZ, Andrés y MARTÍN RAMÍREZ, José. «Inteligencia económica como vector internacional de seguridad», *Documento de Trabajo 18/2008.* Real Instituto Elcano, 2008.

The Economic Espionage Act of 1996: A brief guide. Estados Unidos: National Counterintelligence Center, 1997.

MONTOYA CERIO, Fernando, SAMBEAT VICIÉN, Andrés, y FABRA RODRÍGUEZ, Óscar. «La tasa Tobin europea. Un impuesto sobre las transacciones financieras». *Documento de Opinión 06/2013*, IEEE, 16 de enero de 2013.

NYE, Joshep S. Jr. «*The future of power»*. Nueva york: New York Public Affairs, 2011.

— «American and Chinese Power after the financial crisis», *The Washington Quarterly*, 33:4. Center for Strategic and International Studies, octubre de 2010, pp. 143-153.

OLCOTT, Anthony. «Revisiting the legacy: Sherman Kent, Willmoore Kendall and George Pettee. Strategic intelligence in the digital age», *Studies in Intelligence,* vol. 53, n.º 2 (extractos), junio de 2009, pp. 21-32.

OLIER ARENAS, Eduardo. *Geoeconomía.* Pearson Prentice Hall, 2011.

PEÑALVA ACEDO, Fernando. «NIFF *versus* US GAAP: resumen de las principales diferencias», en *Revista de Contabilidad y Dirección,* vol. 4, año 2007, pp. 55-69.

PHILLIPS, Heather A. «*Libraries and national security law: An examination of the USA Patriot Act»*. Progressive Librarian, vol. 25, verano de 2005.

POOLEY, James and HALLIGAN, R. Mark. «Intelligence and the law» en MILLER, Jerry (ed.): *Millennium intelligence: Understanding and conducting competitive intelligence in the digital age.* Medford, NJ: CyberAge Books, 2000, pp.171-187.

POTTER, E. *Economic intelligence and national security.* Ottawa: Carleton University Press and the Centre for Trade Policy and Law, 1998.

REYNAUD, Julien P. M. y VAUDAY, Julien. *IMF lending and geopolitics*. *ECB working paper n.º 965*, International Monetary Found, 14 de noviembre de 2008.

ROMANO Roberta. «The Sarbanes-Oxley Act and the making of quack corporate governance», en NYU, *Law and Econ research paper 04-032*; *Yale Law & Econ research paper 297*; *Yale ICF working paper 04-37*; *ECGI - finance working paper 52/2004.* 2004.

SANZ ROLDÁN, Félix. «El Centro Nacional de Inteligencia ante el reto de la seguridad económica», en *Inteligencia y Seguridad: Revista de análisis y prospectiva*, n.º 9, 2011**,** pp. 11-18.

SERRANO MONTEAVARO, Miguel Ángel. (2012): *La nueva clase media americana. Hacia una mayor seguridad económica y social.* Documento informativo 02/2013. IEEE, 2012.

SOLOVE, Daniel J. «A brief history of Information Privacy Law». *Public law Research Paper,* n.º 215. George Washington University Law School, 2006.

— «A taxonomy of privacy» en *University of Pennsylvania Law Review,* vol. 154, n.º 3, enero de 2006, pp. 484-486; p. 478.

STIGLITZ, Joseph E. *Caída libre El libre mercado y el hundimiento de la economía mundial*. Madrid: Taurus, 2010.

— *El precio de la desigualdad.* Madrid: Taurus, 2012.

SZOTT MOOHR, Geraldine. «The problematic role of criminal law in regulating use of information: The case of the Economic Espionage Act», *Public Law and Legal Theory Series*, 2009-A-5. University of Houston Law Center, 2009.

TODD, Emmanuel. *Después de la democracia.* Madrid: Akal, 2010.

TOURAINE, Alaine. *Después de la crisis.* Madrid: Paidós, 2011.

UGARTE, José Manuel. *La relación entre inteligencia y política, y sus consecuencias en las estructuras y normas de los sistemas de inteligencia*. Brasilia: 2005.

VENEGAS GONZÁLEZ, Álvaro. «Inteligencia económica: un componente estratégico por desarrollar», en *AA Inteligencia*, año 1, número 2, pp. 10-19. Chile: 2008.

VIVES ANTÓN, Tomás Salvador. (2010): *Fundamentos del sistema penal*, 2.ª edición. Valencia: Tirant, 2010.

YOUNGS, Richard. (2007). «Europe's external energy policy: Between geopolitics and the market». *Centre for European Policy Studies Working Documents,* n.º 278, 20 de noviembre de 2007.

ZUNZARREN, Hugo. En http://idinteligencia.wordpress.com/archivos-2/posts-precedentes/inteligencia-juridica-en-los-eeuu/.

Capítulo IV

LA INTELIGENCIA PARA COMPETIR: NUEVO PARADIGMA EN LA DIRECCIÓN ESTRATÉGICA DE LAS ORGANIZACIONES EN UN MUNDO GLOBALIZADO

Fernando Palop Marro

Resumen

El autor parte de los retos a los que las organizaciones tienen que hacer frente en el mundo global del siglo xxi ante una dinámica de cambios en sus mercados, tecnologías y contexto socioeconómico. Los mismos comportan con frecuencia un carácter disruptivo de lo establecido tanto por su contenido como por su complejidad e incertidumbre derivada en parte de la velocidad con la que se producen. Esa dinámica requiere de un nuevo paradigma a tomar en consideración, tanto en lo que atañe a la cultura y procesos de aprendizaje de la organización en relación a los cambios que acontecen a su alrededor como en la forma en que se construyen y toman las decisiones. Es decir, cómo la organización y su esfera de influencia detecta, anticipa y «lee» el significado e implicaciones de dichos cambios, pero también cómo integra y transforma los resultados de esa capacidad de aprendizaje en acciones, en decisiones.

Esa necesidad de integración se acentúa en el ámbito de las decisiones que afectan a la dirección y rumbo estratégico de los negocios. Ese nuevo paradigma, que exige de inteligencia para competir, es recogido por la propuesta que formula la inteligencia competitiva como entre otras denominaciones también es conocido. La inteligencia competitiva no es como tal una propuesta «nueva», lleva ya más de medio siglo de práctica en muchas empresas y organizaciones tal como hoy

la entendemos[1], y tiene antecedentes desde muchos siglos atrás; pero todavía es desconocida y parcial o totalmente desaprovechada por un amplio número de las mismas. Por eso, cabe decir que no aprovechar hoy el potencial que plantea la IC en las organizaciones supone una desventaja competitiva. El artículo revisa el término, sus fundamentos y los procesos que conlleva. Se presentan los principales beneficios y algunos ejemplos de aplicación, y se trata la relación entre la inteligencia competitiva, IC, la seguridad en la actividad empresarial y la importancia del concepto de influencia. Centrado en el mundo de la empresa, también se abordan otras aplicaciones del mismo concepto, tal es el caso de la inteligencia del territorio. Finalmente, se aportan algunas tendencias de evolución en este campo.

Palabras clave

Inteligencia competitiva, planificación estratégica, toma de decisiones, aprendizaje organizativo, gestión del conocimiento, inteligencia organizativa.

[1] MASSON, J. L., 2005.

Abstract

The author starts from the challenges that organizations cope in the global world of the twenty-first century with a dynamic of changes in their markets, technologies and socio-economic context. Those changes often behave disruptive character of the prevailing by both its content and its complexity and uncertainty derived in part from the speed with which they occur. This dynamic requires a new paradigm to be taken into consideration. First in terms of culture and learning processes of the organization in relation to the changes taking place around them but as well in the way decisions are built and made. That is how the organization and its sphere of influence detects, anticipates and «reads» the meaning and stakes of those changes. But also how integrates and transforms the results of that learning capability into actions, decisions.

This integration need is stressed in the decisions field, affecting the management and strategic direction of the business. This new paradigm that requires intelligence to compete is collected by the proposal formulated as competitive intelligence and other denominations also known. Competitive intelligence is not as such a «new» proposal, it takes more than half a century of practice in many companies and organizations as we understand it today, and precedents from many centuries ago. But it is still unknown and partially or completely unexploited by a large number of them. So it can be said that not exploit today the potential posed by CI in organizations is a competitive disadvantage. The article reviews the term, its foundations and the processes involved. Main benefits and some application examples are brought forward. The relationship between competitive intelligence, CI, business security and the importance of the influence concept are reviewed. Focused on the business world this paper also addresses other applications of the same concept, as in the case of territorial intelligence. Finally some evolutionary trends in this field are provided.

Keywords

Competitive intelligence, strategic planning, decision process, organizational learning, knowledge management, organizational intelligence.

Resumen ejecutivo

La IC forma parte de las respuestas desarrolladas por las organizaciones (de toda índole y sector) para proporcionar a la dirección de las organizaciones las claves para conducir la estrategia y muchos de los temas tácticos en un mundo como el actual, de elevado grado de incertidumbre y velocidad de cambio. Ese grado de incertidumbre y velocidad de cambio ha llevado a la obsolescencia a una parte de las prácticas tradicionales que afrontan la recogida de información y el análisis en la toma de decisiones no estructuradas.

La IC no elimina la incertidumbre pero sí puede reducirla en la medida en que el carácter sistemático de su práctica posibilita identificar un mayor porcentaje de información pertinente, porcentaje que varía de forma importante en función del contexto del tema a decidir. Por otro lado, tampoco suprime el riesgo pero contribuye a gestionarlo.

La *inteligencia para competir* plantea un cambio de paradigma en el modo tradicional de abordar el proceso de maduración y toma de decisiones por los directivos. Tradicionalmente, la generación de inteligencia para decidir es asumida casi en exclusiva por los decisores; dentro del nuevo paradigma, la organización no se limita por lo general a aportar al decisor datos e información, comienza por implicarlo en el proceso de IC y colabora con este generando inteligencia (implicaciones y significados de los hechos, tendencias, alternativas, propuestas de acción...) para decidir.

La IC forma parte de las características de las organizaciones actuales contempladas como aprendices. Desde la IC, la organización participa activamente con distintos roles y dedicaciones en las tareas de observación y recogida de información, organización y análisis y, finalmente, en su comunicación. En la IC existe una amplia implicación y participación de la organización en el proceso, no reducida a unas pocas personas del *staff* de dirección. Incluso desde el concepto de red, se gestiona la implicación de personas externas a la organización pero en su esfera de influencia.

La IC es ante todo un proceso de carácter transversal a las funciones tradicionales verticales de la organización, de desempeño continuado en el tiempo (por la dimensión de alerta y anticipación), focalizado en cuanto a sus prioridades de atención y orientado a futuro.

La IC como proceso permite ser gestionada dentro del conjunto de procesos de la empresa y medida en sus resultados mediante indicadores, y cuenta con referencias normativas desde la innovación y calidad, como la AENOR UNE 166.006.

La IC toma una buena parte de sus herramientas de otras áreas del conocimiento (como planificación estratégica, *marketing,* análisis financiero, gestión del conocimiento o prospectiva), pero también, además del

proceso, ha generado, en especial en la etapa de análisis, un importante acervo de experiencia práctica –en parte originado en su aplicación en el área de la defensa, seguridad y la geopolítica– con aportaciones y propuestas en el campo de los sesgos cognitivos, en el empleo de analogías, inducciones, deducciones, inferencias, etc.

La IC supone una ventaja competitiva para aquellas organizaciones que saben aprovechar el potencial no gestionado en sus organizaciones. La IC, según se ha contrastado empíricamente mediante encuestas, aumenta el grado de cohesión del grupo en torno a los objetivos y prioridades estratégicas y a su consecución.

Posiblemente, una de las características más propias y singulares de la IC hoy es su capacidad de detección y anticipación de riesgos. Frente a otras funciones en la organización, que también reúnen datos e información del ambiente exterior, la IC se centra en aportar el contexto de los hechos, su significado e implicaciones para la organización y su posible evolución. Esos hechos aparecerán solamente desde la IC como evidencias de sustentación de los razonamientos que conduzcan a la inteligencia aportada. En ese sentido, B. Gilad sostiene que la IC plantea una perspectiva específica de los riesgos y oportunidades externas para el desempeño global de la empresa, y así es parte de la actividad de gestión del riesgo de la organización.

Introducción

La confluencia en las últimas décadas de un conjunto de cambios en el entorno socioeconómico y tecnológico de las organizaciones viene sometiendo a estas a importantes retos en su adaptación a dichos cambios. Detrás de esa necesidad de adaptación se encuentra su capacidad de aprendizaje sobre los mismos y la integración de dicha capacidad en el proceso de decisiones en el plano organizativo y estratégico. El que esa adaptación sea eficaz está ligada, como se expondrá, a la forma en que se produce dicho aprendizaje y al modo en que se construyen y adoptan las decisiones.

En ese conjunto de cambios antes aludido sobresalen los desafíos que plantea un mundo global; el acelerado cambio técnico que modifica no solo productos y servicios sino los hábitos de consumo y apropiación de los mismos. También figura la obligada presencia internacional que tienen hoy muchísimas empresas, no solo las grandes corporaciones, para alcanzar el óptimo beneficio en sus modelos de negocio. Tampoco se puede ignorar la realidad de un mundo con menor seguridad económica donde aparecen nuevas dimensiones de la competencia a considerar, como la influencia. Todo ello ha contribuido a que las organizaciones afronten un aumento del riesgo e incertidumbre de elevada complejidad en su gestión.

Es en este contexto donde las organizaciones se encuentran ante la necesidad, hoy ineludible, de gestionar una dimensión, la del seguimiento y aprendizaje de los cambios que suceden a su alrededor, particularmente los que trascienden un ámbito funcional o divisional. Hasta hace no mucho tiempo se consideraba dicha dimensión una obligación de propósito general para cualquier puesto directivo, no requería ser asignada a ninguna definición de puesto en particular ni parecía necesitar de unas tareas o proceso específico; todos la reconocían pero no era responsabilidad de nadie. No se medía y como consecuencia no se administraba, salvo excepciones como es el caso de la función de *marketing*[2] pero quedando restringida al ámbito de la misma. Sin embargo, la historia ha venido mostrando múltiples casos de organizaciones, y en particular de empresas, que han sobrepasado la primera generación empresarial cuando sus directivos han sido capaces de conectar la reflexión estratégica con esa capacidad transmitida a sus organizaciones de vivir al tanto de los acontecimientos que condicionan el rumbo para entenderlos, actuar y decidir en consecuencia. Esto ha sido mucho más frecuente en sectores dependientes de la ciencia, caso por ejemplo del biofarmacéutico habituado a trabajar a muchos años vista.

Este panorama viene penalizando a todas aquellas organizaciones que no son capaces de detectar a tiempo las señales que generan dichos cambios o que detectándolas no toman decisiones en consecuencia. Dicha carencia termina convirtiéndose en una debilidad de esas empresas y organizaciones para competir en un mercado global. La misma ya fue resaltada por I. Ansoff en 1975 al introducir el concepto de gestión estratégica o *strategic management*. Ya en aquel año ponía énfasis –a la hora de hacer frente las empresas a las turbulencias del entorno– en la necesidad de centrarse en su capacidad para anticipar amenazas y oportunidades. Más tarde, otros autores de referencia, entre otros Michael Porter (1980) o Gary Hamel y C. K. Prahalad (1994), resaltaron la importancia del posicionamiento estratégico basado en el análisis de información del entorno. El primero, además de proponer técnicas para analizar el sector y la competencia, planteó cómo generar inteligencia sobre los competidores mediante un «sistema de inteligencia». Por su parte, los segundos resaltaron la importancia para los equipos directivos de competir por la obtención de una visión prospectiva del sector. Más tarde, Clayton M. Christensen (2004) recurre a la obtención de determinados tipos de señales de cambio como punto de partida de su proceso de análisis para predecir el cambio en el sector.

En cuanto a los beneficios de anticipar las acciones y entender las estrategias de competidores y otras fuerzas del mercado o de aquilatar las

[2] El concepto ligado a dicha función de análisis o inteligencia del entorno – *environmental scanning*–, inteligencia del mercado, aunque limitado a su ámbito, comparte planteamientos con la inteligencia competitiva.

consecuencias e implicaciones de cambios tecnológicos, no se requiere hoy mayor justificación, al igual que las negativas consecuencias de la toma de decisiones a partir de información incompleta, no fiable o no disponible a tiempo.

Pero en lo que respecta a la toma de decisiones tenemos un proceso de obtención de información (cada vez más colectivo y ligado a esa capacidad de aprendizaje) y otro complementario de análisis y decisión en consecuencia. Es aquí donde de nuevo se está generando una desventaja competitiva entre las organizaciones que continúan bajo el paradigma tradicional (el directivo asume la iniciativa y el protagonismo) frente a propuestas más participativas como las formuladas desde modelos como las organizaciones aprendices (Peter Senge, 1990). A este respecto, este autor resalta en su capítulo 1 que «hay sorprendentes ejemplos donde la inteligencia del equipo supera a la inteligencia de sus integrantes».

Es en este contexto en el que vamos a tratar la inteligencia competitiva, también conocida con otros calificativos como estratégica, corporativa o económica, y cercana a otros conceptos como el de vigilancia tecnológica o estratégica o al de inteligencia de mercado. No nos parece que la denominación sea hoy tema relevante sino más bien consecuencia de la juventud de este ámbito; por eso titulamos esta contribución como *inteligencia para competir,* en adelante IC. La misma, aunque tenga precedentes anteriores, nace propiamente en los años ochenta en el ámbito empresarial como respuesta a ese contexto comentado al inicio de esta introducción. Se trata de aprovechar la capacidad para entender el entorno en el proceso de toma de decisiones no estructuradas, estratégicas y parte de las operativas.

IC y direccionamiento estratégico

La IC supone una corriente metodológica cada vez más ligada a las necesidades del direccionamiento estratégico y de la innovación en la empresa. D. Bernhardt (1994) ya apuntó cómo la inteligencia era la savia de la estrategia e incluso llegaba a sugerir que la estrategia sin inteligencia se vería necesitada de recurrir a conjeturas. Recientemente, recordaba Roger Martin en 2013 cómo en más de una ocasión, al preguntarles a directivos de empresa sobre la estrategia de la misma, estos le contestaban que no querían o no podían desarrollarla por el elevado grado de cambio en su ambiente de funcionamiento. Según estos, particularmente en sectores de alta tecnología –pero también sería posible encontrar otros casos fuera–, no habría suficiente certidumbre para desarrollar la estrategia con eficacia. El peligro para los mismos, por supuesto, es que mientras estén usando la incertidumbre como una excusa para posponer la toma de decisiones estratégicas, la competencia puede estar haciendo algo completamente distinto, como anticiparse gracias precisamente a

su estrategia. No es por tanto casualidad que aquellos se quejen después del hecho de haber sido sorprendidos por algo inesperado. Su narrativa tiende a ser que cuando sucedió era demasiado tarde para hacer algo constructivo al respecto. El fracaso no era en absoluto su culpa, porque para ellos es el sector el que es incierto y este tipo de cosas solo ocurren de «forma natural» e imprevisible.

Como acertadamente recuerda este profesor de Administración en Toronto, cada empresa tiene una estrategia. Ya sea explícita o no, su realización, las decisiones que se adoptan a diario, dan como resultado el desempeño de la empresa en alguna parte del terreno de juego (por ejemplo, adoptar una elección sobre «dónde competir») y competir allí de alguna manera (es decir, hacer una elección sobre «cómo ganar»). Sin hacer un esfuerzo por «hacer estrategia» –y recordamos que ello requiere alimentarla con inteligencia–, una empresa corre el riesgo de que sus numerosas opciones diarias no tengan coherencia entre ellas, de ser contradictorias entre sus divisiones y niveles y de, al final, tener un impacto reducido respecto a los objetivos que se hubiera planteado.

Resumiendo, la práctica de la estrategia se ve favorecida por la existencia de un proceso de inteligencia competitiva y a su vez la IC requiere de la existencia de unas prioridades estratégicas para poder contribuir y aportar eficazmente al desempeño de la organización.

Campo de actividad de la IC

La actividad de IC centra su atención en el exterior de la organización, pero para ello debe partir de un sólido conocimiento del interior de la misma. Fleisher señala cómo, en cuanto a ese papel exterior, la IC se centra en la comprensión de:

- La estructura de la industria y su evolución: especial hincapié en el atractivo del sector.
- La macroeconomía: vista de otro modo, como aquellos aspectos sociales, tecnológicos, económicos, ecológicos y políticos/legales (STEEP)[3] del entorno asociados con la propia empresa.
- Las partes interesadas: aquellas organizaciones que pueden afectar o son afectadas por el logro de los objetivos competitivos de la organización.
- Cuestiones o problemas: estos son las brechas que existen entre las acciones de la organización y las expectativas de aquellos (por ejemplo, grupos de interés tales como clientes, proveedores, etc.) que pueden afectar a sus objetivos competitivos.

[3] También se conoce como PESTEL.

Beneficios aportados por la IC a la organización

La práctica profesional y la literatura sobre el tema señalan los beneficios más habituales:

- Reduce riesgos e incertidumbre. Gilad concreta: «plantea una perspectiva específica de los riesgos y oportunidades externas… y así es parte de la actividad de gestión del riesgo de la organización».
- Alerta sobre sorpresas tecnológicas, comerciales y del entorno. Este beneficio se deriva de su capacidad para lograr anticipación. Más adelante se trata en el apartado «Fundamentos de la IC».
- Contribuye al proceso de toma de decisiones no estructuradas de las empresas, tanto en las decisiones estratégicas como en muchas de las tácticas.
- Identifica «oportunidades, amenazas, debilidades y fortalezas».

En el caso de la planeación estratégica, hay que resaltar su capacidad para caracterizar el sector de actividad mediante la elaboración de perfiles del propio sector, de sus actores –en especial competidores– o de las tecnologías que lo condicionan satisfaciendo así necesidades específicas del decisor. Prescott señala su capacidad para aportar respuestas a preguntas que exigen la elaboración de esos perfiles, tales como:

- ¿Cuáles son las características fundamentales de mi industria y de los competidores?
- ¿Cuál es el posicionamiento actual de mis competidores?
- ¿Cuáles pueden ser son los movimientos más probables de mis competidores?
- ¿Qué movimientos puede realizar nuestra organización para lograr una ventaja competitiva?

De este modo:

- Transforma la información recopilada en inteligencia práctica orientada a la acción.
- Se da la colaboración de todos los miembros de una organización en su proceso de inteligencia como «antenas» o vigías.
- Se adapta a la dinámica del tiempo para hacer frente a la evolución de los temas críticos y facilitar así la renovación de la organización.
- Favorece el seguimiento y anticipación de cambios en la estructura del mercado y actividades competitivas tales como: surgimiento de nuevos negocios, nuevas alianzas, expansión de capacidad, fusiones y adquisiciones, etc. (Fleisher, 2001).

Analiza referentes competitivos: procesos, productos, organizaciones…

- Procede a la vigilancia o monitoreo de tecnologías y sus implicaciones: actividades de I+D, innovaciones basadas en la tecnología o tecnologías emergentes.

La IC como proceso

En términos generales, la IC es el proceso por el que las organizaciones reúnen y analizan información –evidencias que puedan traducirse en acción– sobre los competidores y el entorno competitivo, y en el supuesto ideal, la aplican a su proceso de toma de decisiones y planificación para mejorar su rendimiento. Implica la comprensión a tiempo del significado e implicaciones de los cambios y novedades en el entorno. La IC pone en relación señales informativas de cambios sin relación aparente y dispersas en distintas fuentes, acontecimientos, percepciones y datos, estableciendo pautas y tendencias relativas al ambiente del mercado.

Para la norma UNE 166.006:2011, «la inteligencia competitiva comprende [...] el análisis, interpretación y comunicación de información de valor estratégico acerca del ambiente de negocios, de los competidores y de la propia organización, que se transmite a los responsables de la toma de decisiones como elemento de apoyo para ajustar el rumbo y marcar posibles caminos de evolución de interés para la organización». Dicha norma define la IC en su apartado 3.3 como: «Proceso ético y sistemático de recolección y análisis de información acerca del ambiente de negocios, de los competidores y de la propia organización, y comunicación de sus significado e implicaciones destinada a la toma de decisiones» (AENOR, 2011).

La IC utiliza fuentes de acceso público para encontrar y desarrollar información sobre la competencia, los competidores y el ambiente de mercado (Vella y McGonagle, 1987, citado por Fleisher, 2001). La IC no es espionaje comercial; es ético, legal y legítimo, mientras que el espionaje comercial es claramente ilegal, innecesario y no forma parte de la descripción de los puestos de trabajo de IC. La información de fuentes públicas no necesariamente implica información publicada. Hay una serie de datos y evidencias a las que se puede acceder legalmente sin requerir su publicación (Fleisher, 2001).

La mayor parte de organizaciones hoy en día realizan IC en alguna forma básica, sean o no conscientes de ello. Muchos directivos practican IC en sus actividades diarias cuando tratan de comprender cómo situar mejor los productos o servicios de su organización en el mercado. No solo las grandes corporaciones, también empresas pequeñas –especialmente en sectores como bienes de equipo o más dependientes de la ciencia como biotecnología o ciencias de la salud–, que a menudo suelen ser más sensibles a la reunión de información y al uso de IC con eficacia, tal vez porque su tamaño no admite muchos niveles y todos tienen «los pies más en la tierra». No es raro que sean en estos casos empresarios motivados los que lideren esta exigencia en su organización, acostumbrados a conocer personalmente tanto como sea posible sobre el mercado que les rodea y los competidores.

Caso 1: Ejemplo de una pequeña empresa de proceso de fundición.

Tal es el reciente caso de una empresa de proceso de fundición de treinta empleados en un país de América del Sur. Durante años había funcionado holgadamente en su mercado local a partir de un proceso muy manual ejecutado con profesionalidad pero con una debilidad: un elevado porcentaje de su facturación dependía de trabajos por cuenta de una empresa exterior. El desarrollo que en los últimos años experimenta su país ha llevado a esa empresa extranjera a decidir invertir en una planta propia de fundición en el país, terminando con la relación de tanto tiempo, justo en el mismo momento en que la empresa pequeña realizaba una inversión para ampliar y modernizar sus instalaciones y proceso. La empresa pequeña, tras participar en un proceso de transferencia de habilidades en IC y realizar un análisis del mercado, ha desarrollado por vez primera un ejercicio de reflexión estratégica para reorientar su actual posición antes de que las consecuencias de los cambios se precipiten.

Fuente: elaboración propia con la colaboración de los técnicos y personal de la empresa Templamos.

La IC, sus conceptos y prácticas, muestran ser de gran valor potencial para distinto tipo de organizaciones, no solo empresas sino también entidades públicas, entes locales, organizaciones sociales, universidades y centros de investigación con necesidad de toma de decisiones fundada en evidencias buscando anticipación y reducción de riesgos. Este es el caso de una institución hospitalaria para la toma de decisiones de inversión en la ampliación de sus urgencias clínicas.

Caso 2: Ejemplo de implantación de vigilancia tecnológica e IC en un hospital de referencia.

El Hospital Pablo Tobón Uribe, HPTU, de Medellín, Colombia, concibió en 2011 un ambicioso plan de ampliación de su capacidad de asistencia que conllevaba la potenciación de los servicios de atención de urgencias clínicas para situarlos entre los referentes en su ámbito en América del Sur. En ese mismo año, la dirección del HPTU decide participar en una iniciativa[4] que coordina la agencia de innovación local, Ruta-n, para formar e implantar prácticas en IC entre empresas de la región de Antioquia. Las instituciones de salud cada vez tienen que afrontar decisiones estratégicas de inversión más dependientes de la tecnología, y a su vez, estas pueden condicionar su desempeño futuro. La dirección del HPTU seleccionó como ejercicio piloto de IC la decisión concerniente a eficiencia en el servicio de Urgencias. Como resultado, un equipo

[4] Esta iniciativa contó con la dirección del autor de este artículo desde la Universidad Politécnica de Valencia y se financió dentro de un programa denominado ERICA con fondos de ayuda a la cooperación de España a través de la AECI y de instituciones locales.

del hospital, en colaboración con una institución universitaria local, ITM, formados previamente en IC, elaboraron en doce semanas, siguiendo la metodología de IC aprendida, un informe de ámbito internacional con mejores prácticas, tendencia y procesos en la organización de las unidades de urgencias hospitalarias. Se identificaron un par de tecnologías de comunicación aplicadas a las urgencias que solo estaban implantadas hasta la fecha en EE. UU. La dirección respaldó los resultados del informe y dio continuidad a estas prácticas de VT e IC en el hospital. El responsable de calidad y el de sistemas y TIC se han integrado en el equipo de trabajo de VT e IC.

Fuente: elaboración propia con la colaboración de los técnicos y personal médico del HPTU.

Adaptando un trabajo del profesor Craig Fleisher de 2001, una manera de entender el funcionamiento de la IC es verla como una progresión desde las materias primas o insumos hasta productos terminados. Desde esta perspectiva, la IC comienza con porciones dispersas de los datos en bruto, básicos; esta materia prima se organiza por los practicantes de la IC y se convierte en información; la información se convierte en inteligencia cuando, una vez obtenidas las derivadas de la misma –significados, implicaciones, consecuencias para la organización–, se coloca en un formato útil para las necesidades clave o únicas de inteligencia de un tomador de decisiones (los llamados factores clave de inteligencia o FCI). La buena IC es impulsada por las necesidades; sin orientación al cliente de la IC, esta no tiene el menor sentido. La implicación del decisor en el proceso de IC comienza en la definición de su necesidad y culmina en la interacción con los resultados o comunicación para decidir. La inteligencia es por lo tanto la información que se analiza, interpreta y se comunica con implicaciones desarrolladas. La inteligencia competitiva es el producto de inteligencia más preciso que satisfaga las necesidades únicas de un tomador de decisiones para la comprensión de un aspecto competitivo del entorno interno y/o externo de la organización.

La IC como función organizativa o enfoque de gestión

La IC es ese proceso comentado, pero para desplegar todo su potencial también requiere el ser administrada como un enfoque de gestión o sistema que aproveche el potencial de aprendizaje del conjunto de la organización y de su área de influencia como red de atención y obtención de señales de alerta sobre aquellos cambios que pueden implicar en mayor medida a la organización. En ese sentido, se plantea como una función organizativa y por tanto procede hablar de la formalización y estructuración de un sistema.

De hecho, este es el planteamiento de la UNE 166.006 cuando, al hacer referencia en el apartado 1 al objeto del sistema de vigilancia tecnológica e inteligencia competitiva, indica:

La formalización y estructuración en la organización del proceso de escucha y observación del entorno para apoyar la toma de decisión a todos los niveles de la organización, hasta devenir en la implantación de un sistema permanente de vigilancia tecnológica e inteligencia competitiva. En ese sentido, el sistema contribuirá a asentar las bases para definir la posición competitiva que ha de tomar la organización, sus objetivos –en el caso de la norma, dado su objeto, indica especialmente en materia de I+D+i– *y el esquema organizativo adecuado a tal posición y objetivos*.

La IC puede proporcionar los fundamentos para la construcción, evaluación y modificación de las estrategias y tácticas tanto de mercado y tecnológicas como en otros ámbitos. Como función principalmente orientada a la dirección, la IC resulta transversal a otras funciones. Por eso, en la práctica coexisten organizaciones donde el planteamiento de IC se desarrolla funcionalmente desde *marketing* o planeación y en menor medida otras funciones, como I+D. Al tiempo que estas, aparecen otras prácticas, las menos, donde la IC integra en función de la necesidad abordada desde compras hasta comercial pasando por marketing, ingeniería, recursos humanos, financiero y planeación y existe una coordinación de IC para todo el proceso. Más adelante se profundiza más en el apartado cómo se organiza.

Por otro lado, la IC podrá tener en cuenta dos enfoques de trabajo posibles y complementarios en muchas ocasiones: el aportar inteligencia para la adopción de una decisión en un momento dado y el seguimiento continuado en el tiempo, vigilancia o monitoreo de un tema dado de interés. La norma UNE 166.006 lo recoge en su apartado 7.1 como:

a) La búsqueda e investigación de lo que se desconoce, y
b) la búsqueda y seguimiento sistemático de novedades en áreas que ya están previamente acotadas.

Etapas esenciales del proceso de trabajo de la IC

El proceso o ciclo de IC que muestra la figura 4.1 reúne una serie de pasos o etapas habituales en un ejercicio o proyecto de IC que, con algunas variaciones menores en la terminología y en el número de pasos, responde al modelo estándar en este ámbito de función de inteligencia (Aguilar, 1967; Porter, 1980; Bernhardt, 1994. En Equipo CNI, 2010, se realiza en español una divulgación del mismo). Madureira reivindica como más adecuado a las exigencias actuales de generación de inteligencia, primando respuestas inmediatas, el modelo OODA Loop del norteamericano John Boyd. Es importante resaltar que aunque las etapas aparecen como consecutivas dentro de un ciclo la práctica real no es así, de forma que el cliente-decisor es bueno que esté al tanto y oriente los avances de la investigación a lo largo de la misma. Tampoco la etapa de análisis empieza una vez finalizadas las anteriores. Al final, existe un alto grado de trabajo

en paralelo e interacciones que permiten acortar los tiempos de entrega que implicarían un proceso estrictamente secuencial de estas etapas.

Figura 4.1. Proceso o ciclo genérico de la Inteligencia Competitiva

Fuente: Elaboración propia a partir del ciclo/proceso de inteligencia competitiva tradicional en PALOP MARRO, F. y MARTÍNEZ, J. F. (2012).

Planificación

El proceso o ciclo de IC suele comenzar con un decisor, el cual tiene una necesidad de inteligencia específica (factor o necesidad de inteligencia clave o FCI) y de personas que colaboren para construirla. Es importante determinar lo que hay que conocer, para quién y cómo y cuándo se va a utilizar.

Autores como J. Herring hablan de tres tipos de necesidades más habituales. Estas, a su vez, constituyen la base del enfoque de estructuración del proceso de trabajo sobre los temas de VT/IC como proyectos o factores clave de inteligencia (FCI). Cada uno de esos tres grupos de necesidades requiere un tipo de resultados diferentes, y esto determina las fuentes a consultar y las técnicas de análisis a aplicar pero también la estructura/informe que contendrá la respuesta.

– Decisiones estratégicas y acciones, incluyendo el desarrollo de planes estratégicos y estrategias. Como ejemplos, aparecen decisiones

vinculadas a la inversión en una tecnología, entrada en un mercado o la alianza con una empresa.
- Temas de alerta temprana. Posibles iniciativas de la competencia, avances técnicos y tecnologías que puedan sorprender, cambios socioeconómicos y geopolíticos y sus implicaciones, modificaciones en reglamentos y normas que haya que cumplir.
- Descripciones sobre los actores de un determinado mercado. Entre otros, competidores, proveedores, clientes, posibles aliados o el regulador.

Cuando la IC se desarrolla con carácter «espontáneo», no existen formatos predefinidos de informes para organizar la inteligencia que se genere. Pero esto ya no ocurre cuando estamos en una situación de IC planificada: como consecuencia de buscar productividad en las tareas y agilidad en los plazos de entrega, se predefinen unos tipos de informes o productos de IC tales como perfiles de un competidor, alertas sobre riesgos y oportunidades, informes de estado del arte de una tecnología, comparativas o *benchmarking* de productos y servicios, servicios de monitoreo o informes tipo síntesis, etc., cuya comunicación se trata más adelante.

Cada uno de estos informes o productos se diferencian entre sí considerando variables como:

- Objeto y valor esperado en relación a la necesidad planteada y tipo de decisión.
- Cliente principal y otros destinatarios.
- Fuentes de información a utilizar.
- Modelos, métodos analíticos y herramientas de *software* en su caso a emplear.
- Formas de comunicación y tipo de plantilla para el informe.
- Coste en términos de horas de dedicación y adquisición de información.

Obtención de la información

La aparición de Internet y las redes sociales ha supuesto un nuevo paradigma en la forma en que se accede a la información publicada electrónicamente. No obstante su incontestable valor, no puede menospreciarse el papel dentro de las fuentes primarias del contacto sobre el terreno con las personas protagonistas de los temas. Lo que en el mundo anglosajón se denomina *humint* o inteligencia a partir de información y conocimiento tácitos que solo residen en personas. La necesidad de acceder a estos «expertos» o protagonistas de los temas de interés, principalmente por teléfono, correo electrónico o encuentros profesionales, se muestra imprescindible en numerosas ocasiones para contrastar y completar piezas sustanciales de ese «rompecabezas» que permite completar la inteligen-

cia. También resultan insustituibles para que dirijan a otros expertos que finalmente permitan completar la tarea. En este sentido, no hay que olvidar que la globalización también permite plantear el acceso a esos expertos desde una óptica global. Por otro lado, téngase en cuenta también que en pleno «reinado» de Internet y las fuentes electrónicas coexisten toda una serie de mercados –por ejemplo, los de la energía en países remotos– donde prima la escasez de datos en fuentes convencionales y donde es necesario hasta la comprobación in situ de la identidad de los interlocutores antes de negociar[5].

Caso 3: Ejemplo de cómo las empresas se vigilan entre sí: Microsoft y Google.

Microsoft llevaba meses en un proyecto masivo destinado a derribar a Google cuando la verdad comenzó a abrirse paso para Bill Gates. Era diciembre de 2003. Estaba hurgando en la web de la compañía Google y se encontró con una página con descripciones de todos los puestos de trabajo buscados por la empresa. ¿Por qué, se preguntó, los requisitos para muchos de dichos puestos resultaban idénticos a las especificaciones de trabajo de Microsoft? Google nació como un negocio de búsqueda en la web, sin embargo, aquí en la pantalla eran puestos para ingenieros con experiencia que no tenían nada que ver con la búsqueda y en cambio todos estaban relacionados con el negocio principal de Microsoft –personas capacitadas en cosas como el diseño del sistemas operativos, optimización del compilador y sistemas de arquitectura distribuida–. Gates se preguntaba si Microsoft podría estar enfrentándose mucho más que a una guerra en la búsqueda. En un correo electrónico que envió a un puñado de ejecutivos ese día, se decía, en efecto: «Tenemos que vigilar a estos chicos. Parece que se está construyendo algo para competir con nosotros».

Fuente: Adaptado de Fred Volgestein, 2005.

Análisis

Desde el planteamiento de la IC, los datos y la información son el punto de partida, no de llegada. Por tanto, los datos e información reunidos en la anterior etapa no son inteligencia. Para que aporten a la toma de decisiones sentido o *sense making* –como dice Jaworski–, significados y valor, es decir inteligencia, deben ser seleccionados, validados y organizados para su análisis e interpretación. Dicho de otro modo, se trata de construir a partir de fragmentos inconexos compuestos por datos, testimonios personales e información un rompecabezas o panorama que permita entender cuál es la realidad analizada e intuir probables caminos de evolución. En definitiva, construir IC es transformar esa información en elementos para decidir y actuar.

[5] Debo esta enseñanza a un técnico de una empresa de la industria del gas.

En este sentido, aunque se haya escrito mucho sobre el papel de la intuición en la IC y del carácter de «arte» que tiene la interpretación de los hechos reunidos, no ignorando su aportación, no nos parece que sea un punto de partida adecuado para abordar el aprendizaje del análisis. En consonancia con lo que luego se expone en los fundamentos de la IC, entendemos como clave la construcción de los razonamientos de IC a partir de la interpretación de las evidencias reunidas y su significado para el contexto de la empresa. Una construcción de la IC basada en evidencias y modelos analíticos permite implicar a los decisores dentro de una cadena transparente del proceso de decisión. Al mismo tiempo, la inteligencia gana en objetividad al reducir su dependencia de las personas que formulen las conclusiones e interpretaciones. Por último, favorece el aprendizaje de esta etapa clave del proceso de IC. Dicho esto, por supuesto con el tiempo la experiencia acelera la capacidad del analista para intuir consecuencias y derivadas de los hechos, pero debe tratar de justificarlas mediante evidencias para no introducir excesivos sesgos en los resultados.

Los resultados producidos por el análisis, como recuerda Fleisher[6], deben poder inducir a la acción, tener un carácter prospectivo u orientado hacia el futuro, aportar la perspectiva de los hechos al contexto del negocio, ayudar a los tomadores de decisiones a desarrollar mejores estrategias competitivas, facilitar una mejor comprensión del entorno competitivo que la que dispongan los competidores e identificar no solo a los competidores actuales y futuros, sus planes y estrategias, sino los riesgos y oportunidades clave. El objetivo final del análisis es obtener mejores resultados empresariales, no lograr resultados intermedios de mejores decisiones o análisis. Un buen análisis proporciona una respuesta a la conocida reflexión en IC: *si es así, ¿entonces qué?* (en otras palabras, la información recopilada me dice algo nuevo u original que necesito saber sobre el mercado que pueda satisfacer el tema o FCI planteado por el decisor).

El mismo Fleisher, en 2001, completa esta descripción del análisis cuando indica cómo un practicante eficaz de IC debe reconocer la interacción entre las etapas de recolección y análisis, utilizar la creatividad y el pensamiento alternativo[7], emplear el razonamiento deductivo e inductivo, comprender los modelos analíticos básicos, introducir modelos interesantes y atractivos para inducir la idea de descubrimiento desde el análisis más que un enfoque de investigación más árido, saber cuándo y por qué utilizar las distintas herramientas de análisis, reconocer la existencia inevitable de lagunas y ángulos muertos y saber cuándo hay que dejar de analizar con el fin de evitar la parálisis por exceso de análisis.

[6] Adaptado con cambios de Craig Fleisher.

[7] Nota del autor: en el sentido de fuera de la caja del pensamiento convencional.

La relación de las personas ocupadas en el análisis dentro del proceso de IC con las distintas herramientas de análisis debe ser la de conocedores de las posibilidades que ofrece cada una de ellas dentro de la «caja de herramientas» y aplicar la más adecuada en cada caso. Los profesores Fleisher y Bensoussan vienen realizado un meritorio esfuerzo de recopilación de herramientas analíticas empleadas en el ámbito empresarial, muchas de ellas ignoradas e infrautilizadas y dando pautas para su aplicación.

Por último, los analistas requieren una formación diferente a las personas de perfil informacional, más orientadas a la obtención y organización de la información, pues pertenecen a culturas diferentes. En las grandes organizaciones, desarrollan dentro de la IC una función diferente y a veces desde un lugar diferente.

Comunicación, puesta en práctica de lo aportado y evaluación

La etapa de comunicación presupone un proceso interactivo entre el decisor que va a poner en práctica la inteligencia y quienes contribuyen a crear la misma. Lo aportado no llegará a ser inteligencia directamente aplicable por el decisor si este no se implica e interactúa especialmente en esta etapa con el equipo que contribuye para que estos orienten y personalicen sus resultados, justamente como el decisor necesita. Por eso los informes enumerados anteriormente en la etapa de planificación adoptarán ante el decisor concreto distintas formas de comunicación, tales como: informes personalizados, comunicaciones personales, presentaciones programadas, notas especiales, archivos, bases de datos informatizadas, boletines, reuniones periódicas, seminarios de formación, tablones electrónicos en la intranet o retiros de trabajo.

La aplicación de los resultados también incluye por lo general ciertos subprocesos no menos importantes. Entre estos figura el control del proceso de IC, es decir, la evaluación y comunicación sobre lo aportado, su eficacia sobre las decisiones adoptadas y el resultado de estas. En definitiva, la capacidad mostrada por la IC para contribuir a generar valor. También desde la óptica de la calidad, se tendrá en consideración la experiencia adquirida y su desarrollo, recursos empleados, etc. en la retroalimentación para la mejora del proceso de IC –motor de calidad– tal y como propone la UNE 166.006:2011. Por último, los resultados también pueden influir en la necesidad de revisar o replantear algún aspecto de la estrategia de la organización.

A la hora de medir y controlar el rendimiento y valor aportado por los recursos dedicados a la IC se tiene que ir más allá de los indicadores cuantitativos de actividad al resultado; es necesario centrarse en medir su capacidad para generar valor. En este sentido, algunas preguntas del tipo de las siguientes, formuladas periódicamente, pueden ayudar a eva-

luarlo: quiénes son los clientes del proceso de IC; qué tipo de necesidades están demandando; cómo valoran la inteligencia que reciben; cómo están aplicando la inteligencia; cuáles son los costes de los recursos dedicados a IC; en qué medida ha contribuido a la facturación/beneficios y al ahorro en costes de la organización el trabajo del equipo de IC y de dicho proceso.

Cómo aparece organizada la IC

No cabe hablar de un único modelo organizativo de referencia sino de distintas realidades que dependen del grado de maduración de su experiencia en IC, el sector en que se produzca, etc. Los autores que han estudiado este aspecto (desde Rouach en 1996 a Michaeli o Singh en 2006, entre otros) coinciden esencialmente –aunque empleando distintos términos– en señalar entre tres a cinco situaciones. Una primera, ampliamente extendida, de IC reactiva, practicada espontáneamente con carácter individual como respuesta a una necesidad apremiante de reunir información y tomar decisiones ante la aparición de determinados cambios. Esas prácticas en muchas organizaciones aparecen formalizadas como proceso de trabajo en equipo con un coordinador dentro de alguna de las divisiones funcionales o de alguna unidad de negocio pero sin desarrollar sinergias entre las mismas. Finalmente, en algunas empresas se encuentra la IC organizada como proceso corporativo transversal ya consolidado con un directivo dedicado o una unidad de IC dentro del personal de dirección.

Aunque en muchos casos se comprueba un proceso de evolución entre las distintas situaciones descritas desde los espontáneos/reactivos hacia los planificados y consolidados, cada organización termina encontrando el modelo en el que encuentra más confort. Resumimos a continuación las situaciones más típicas.

Desde departamentos funcionales de forma independiente o coordinadamente mediante la figura de un coordinador o jefe de proyecto:

- R. Michaeli plantea una evolución desde su organización como «islas» en las divisiones o departamentos funcionales hasta organizarse como «centro».
- Fleisher (2001) destaca su organización a partir de un programa específico propio de la empresa.
- Cartwright, Boughton y Miller en 1995, citados por Fleisher, hablan de 1) ad hoc, 2) continuada integral, 3) continua focalizada, y/o 4) basados en proyectos. Ad hoc sería la IC más extendida, se realiza bajo demanda y produce resultados que son por su naturaleza de un solo momento y se centran en un competidor en particular, acontecimiento o producto/servicio competitivo.

Pensado para grandes corporaciones, Martín propone en 2010 un modelo de unidad de IC y manual de operaciones donde se aporta un estudio de la agenda de riesgos.

Desde la pasada década de los noventa encontramos cómo la IC contribuye a la toma de decisiones estratégicas integrada en unidades dedicadas formales, ya sea de forma independiente o muy habitualmente dentro de *marketing* o de planificación. Las actividades de inteligencia competitiva se orientan a la toma de decisiones tanto tácticas como estratégicas e incluyen análisis cualitativos y cuantitativos a partir de evidencias. La inteligencia competitiva recibe una atención moderada de la alta dirección y es a menudo un factor valioso para tomar decisiones estratégicas.

Países referentes en la práctica de la IC. La situación en España. La oferta de formación

Si elaboráramos un indicador compuesto con dicho fin a partir de variables como oferta de formación en grados y postgrados en IC desde el ámbito académico, cursos para empresas, conferencias y seminarios y empresas con procesos formalizados de IC, es probable que entre los países que presentaran una mayor puntuación se encontraran la mayor parte de países de la OCDE. Entre ellos, algunos vienen siendo citados tradicionalmente como referentes: EE. UU., Canadá, Francia, Alemania, Reino Unido, Israel, Japón, Corea del Sur, Finlandia, Suecia o Suiza. Muchas de las empresas multinacionales de dichos países es conocido que implican a sus empleados como antenas de observación de su ambiente de negocio.

En cuanto a España, se constata que la visibilidad pública de la IC aparece todavía muy por debajo de su interés empresarial y de su potencial de generación de valor en un mundo globalizado. Es cierto que desde los años noventa, impulsada por la internacionalización de muchas de sus empresas y la asunción de riesgos, más complejos ha registrado un impulso significativo. Sin embargo, su conocimiento y práctica no es equiparable a la situación que se da en países de nuestro entorno. Hay que destacar en cualquier caso el papel jugado en los últimos años en su difusión por instituciones como AENOR con su norma UNE 166.006:2011, el ICEX, el CNI o el máster interuniversitario entre las universidades Carlos III y Rey Juan Carlos de Madrid, al que recientemente se ha incorporado la Autónoma de Barcelona.

La IC impulsada desde las instituciones

Países como Francia, Alemania, Israel, Japón, Corea del Sur o Suecia mantienen distintas políticas e instrumentos de apoyo a sus empresas desde redes de información institucionales. A partir de ahí se han venido

produciendo algunas interacciones y transferencias a la esfera comercial y económica.

Resaltamos el planteamiento francés de *intelligence economique* por tratarse Francia de un país vecino y por su particular interpretación e implicación de las instituciones de aquel país en el desarrollo de la IC en el ámbito empresarial como una política.

Este concepto fue madurando en las últimas décadas impulsado a instancias del Gobierno y mediante grupos de trabajo con amplia participación del mundo empresarial. El mismo contiene una interpretación propia para los intereses de Francia y su economía de las consecuencias de la globalización. Así, se pasó de la consideración prioritaria de la vigilancia estratégica a la aparición en 1994 del Informe Martre en el que se ya se hablaba del actual concepto de *intelligence economique* y se presentaba en relación su papel relevante en la mejora de la competitividad del país y a su cohesión social[8].

Es en enero de 2003 cuando se da un nuevo paso a instancias del primer ministro del Gobierno francés y se desarrolla el conocido como Informe Carayon (2003). Fue el primer ministro Jean-Pierre Raffarin quien pidió al diputado Bernard Carayon «hacer un inventario de cómo nuestro país integra la función de inteligencia en su sistema educativo y de formación en su actuación pública y en el mundo de los negocios», y le instó a hacer recomendaciones para mejorar esta función. Dicho informe considera la política pública de la competitividad, la seguridad económica, la influencia, especialmente con las organizaciones internacionales, y la formación. Se deriva de una lectura original de la globalización que tiene en cuenta la vida diaria de los mercados, la elusión de sus reglas y los juegos de poder e influencia. La inteligencia económica es contemplada en el informe como una política pública más orientada a la identificación de sectores y tecnologías estratégicos, a la organización de la convergencia de intereses entre la esfera pública y la esfera privada.

El informe hace hincapié en la trilogía formada por la obtención de información (vigilancia del entorno, etc.), la protección y la influencia. El énfasis en la influencia se presenta como una característica de los investigadores franceses (tanto en forma de grupos de presión, de influencia política para respaldar las conquistas de mercados por las empresas, como también de capacidad para imponer normas a nivel internacional, imágenes, valores e ideas generales favorables a sus intenciones económicas).

Por todo lo cual, hoy el concepto de inteligencia económica en el país vecino está asociado sobre todo a:

[8] Martre. *Intelligence économique et stratégie des entreprises.* Commissariat Général au Plan, 1994.

- Vigilancia e inteligencia empresarial (obtención de información relevante).
- Protección del patrimonio en activos de información (no dejar revelar sus secretos).
- Apoyo a las decisiones (análisis, cartografía de la decisión, escenarios y «sala de guerra»).
- Influencia (difundir una información o formas de comportamiento y de interpretación que favorezcan la estrategia).

Como tal política ha implicado a distintos niveles institucionales y territoriales. Así, las Cámaras de Comercio francesas se han mostrado muy activas desde hace años haciendo llegar este planteamiento a las empresas medianas y pequeñas, mientras que en el territorio, en torno al concepto de agrupación o *cluster,* se han priorizado distintos «polos tecnológicos» de especialización a lo largo de la geografía jugando el concepto de inteligencia un papel relevante. Más adelante se volverá a ello al abordar el concepto de inteligencia del territorio.

Harbulot y Baumard aportan en 1997 antecedentes históricos al concepto francés de inteligencia económica y, entre otras referencias, citan a autores como el ya citado Harold Wilensky, con su visión de la inteligencia organizativa. Este autor plantea, entre otras, dos cuestiones principales que siguen vigentes:

- Las estrategias colectivas y la cooperación entre las instituciones y las empresas en la producción de un conocimiento común para la defensa de la ventaja competitiva.
- La importancia del conocimiento en la economía y la industria como un factor estratégico de desarrollo y cambio.

La oferta de formación

Hay que distinguir entre la oferta desde instituciones académicas de titulaciones de grado y posgrado y la oferta de formación no reglada.

Todavía, salvo excepciones en países como Francia, Canadá, EE.UU., Suecia o Finlandia, los estudios de IC no están presentes como tales en la oferta de grados aunque sí se reflejan en áreas de conocimiento cercanas (Ciencias de la Información, Biblioteconomía). En posgrado existe una mayor oferta en titulaciones de máster en distintos países, siendo de destacar en España el interuniversitario ya comentado de Analista de Inteligencia y algún curso de corta duración ofrecido por la UOC.

En formación no reglada, proliferan distintos cursos de contenidos y duración dispar que asumen el término IC. Recientemente, se ha incorporado a este mercado la escuela de negocios ESIC en Madrid con un curso especializado de setenta horas.

Específicamente con una oferta pensada para directivos de empresas, aparecen las ofertas en distintos países de la UE del Institute for Competitive Intelligence (ICI), con sede en Alemania, y la norteamericana Academy of Competitive Intelligence LLC (ACI). La condición de certificación de las titulaciones que imparten es uno de los elementos clave de estas ofertas.

Fundamentos de la IC. Estado del arte

El autor que suscribe el presente trabajo no conoce un modelo aceptado que integre para las organizaciones el aprendizaje del entorno y el proceso de decisiones no estructuradas. En este sentido, coincide con Day y Schoemaker cuando estos, para el concepto que denominan de «visión periférica» de la organización, particularmente necesario en lo que se refiere a la inteligencia sobre cambios emergentes, consideran que «no existe un modelo universalmente asumido y aceptado que la sustente. En este sentido, uno de los retos a cubrir por la inteligencia competitiva en su contexto actual es el análisis y la previsión de oportunidades futuras que todavía están alejadas de la propia actividad».

Por eso suscribimos como punto de partida para establecer los fundamentos de la IC las reflexiones que con dicho fin realizan esos autores para la «visión periférica»:

> *Entre nuestras muchas fuentes, hemos recurrido a los campos de toma de decisiones (ciencias de la decisión), marketing, estrategia, teoría de la organización, y economía así como a campos de ciencia aplicada como planificación de escenarios, inteligencia competitiva, investigación de mercados, escaneo del entorno y previsión tecnológica.*

Esto nos lleva a una primera conclusión: estamos ante un campo de naturaleza *interdisciplinar* y todavía, como sostienen Fleisher y Blenkhorn, en proceso de normalización. Estos aplican –partiendo de Ashley y Morrison– las fases en el tiempo del ciclo de evolución de los problemas a la resolución y regulación de algunas de las cuestiones todavía en debate dentro de la IC, entre otras su denominación.

La no existencia de un modelo de referencia de la IC o la persistencia de falta de consenso en cuanto a ciertas cuestiones ha podido dificultar la difusión de este campo todavía joven tal como lo entendemos hoy pero no en sus antecedentes, como se expone a continuación. Por contra, como ya se argumentó anteriormente, los actuales retos del mercado han contribuido a extender tanto el concepto como su puesta en práctica.

Desde una perspectiva histórica, los profesores A. Juhari y D. Stephens, de la Universidad de Loughborough en el Reino Unido, han realizado un valioso repaso a los antecedentes y desarrollo de la IC. Los mismos plantean la génesis de la inteligencia a partir de las confrontaciones militares, las necesidades de información de las empresas y las prácticas gu-

bernamentales. Este proceso de configuración del campo de la IC supone un continuo que se remonta en el tiempo a muchos siglos de antigüedad hasta llegar a la situación de la IC que conocemos hoy en día, que se sitúa al final de la década de los años setenta del pasado siglo.

Es así como se ha ido configurando en los últimos años un ámbito multidisciplinar. En este confluyen, por un lado, la gestión de un proceso de trabajo, el de la inteligencia competitiva (IC), que requiere una cultura y habilidades en la gestión del conocimiento por parte de la organización y un proceso que la integre para la toma de decisiones. En este sentido, tiene sinergias obvias con el concepto de inteligencia. Este concepto abarca la gestión del conocimiento y el aprendizaje de la organización, y tiene un propósito finalista al orientar la gestión del conocimiento hacia su adaptación estratégica al entorno y la satisfacción de los objetivos del negocio (W. E. Halal, 1998). Su precursor fue Harold Wilensky, en 1967.

Este proceso es necesariamente transversal a la organización pues implica y necesita de la contribución de personas de distintos departamentos y unidades funcionales de la misma y del empleo de un conjunto de técnicas inspiradas en la planificación estratégica y en la prospectiva. Finalmente, un referente que siempre debe presidir la dirección de este esfuerzo es el direccionamiento estratégico y de innovación de la empresa.

Palop Marro ha tratado de reflejar anteriormente ese carácter interdisciplinar, pero refiriéndose en particular al ámbito de la vigilancia e inteligencia sobre tecnologías (ver figura 4.2). Antes, entre otros, ya lo

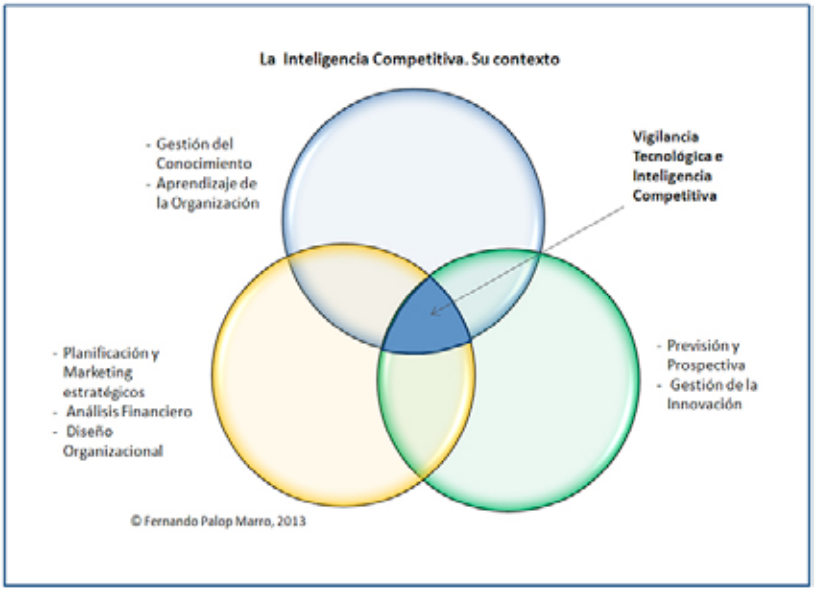

Figura 4.2. Carácter interdisciplinar de la IC

Fuente: Adaptado de Palop Marro, 2012.

hizo J. L. Masson en 2005, quien, al constatar cómo la IC resultaba de la integración de algunas áreas del conocimiento, se refería también a las tecnologías de la información, la lingüística y, dentro de la gestión del conocimiento, a la gestión de la información y documentación.

Constatado este carácter interdisciplinar, vamos a plantear a continuación en qué medida la IC conlleva una propuesta de cambio en el paradigma sobre el que se basa el actual proceso de toma de decisiones estratégicas. En particular, interesa el papel en dicho proceso del decisor y de las personas que integran la organización y el valor de las evidencias obtenidas como soporte principal e insustituible de las propuestas de IC a las decisiones. Ello se va a argumentar a continuación sobre tres ejes: el proceso de información orientado a la toma de decisiones, los mecanismos de aprendizaje de los cambios en el entorno por parte de las organizaciones y la necesidad de generar anticipación que requiere ese aprendizaje. Los dos primeros vienen a partir de la propuesta de Day y Schoemaker de 2006 y aquí añadimos el tercero.

Se constata desde una perspectiva de planeación y toma de decisiones cómo los individuos son los receptores de la organización y cómo los procedimientos internos de la misma son los que imponen en última instancia los asuntos que deben recibir atención. Existen retos importantes a nivel individual, grupal y organizativo para ocuparse de los temas apropiados en el momento oportuno (Stoner y Wankel, 1989). Para valorar dichos asuntos, Day y Schoemaker proponen incorporar:

- A nivel del individuo, diversos sesgos de criterio y de elección.
- A nivel de empresa, la dinámica organizativa y estratégica.

Implicaciones para las organizaciones. Su aprovechamiento vs. su protección

Estos son los tres ejes sobre los que situar los fundamentos de la IC en las organizaciones:

1. El proceso de información orientado a la toma de decisiones.

En el pasado, Palop sostiene que el lento ritmo de los cambios posibilitaba el que un reducido grupo de directivos con acceso a información y capacidad de visión prospectiva pudiera ir marcando con éxito la evolución de su organización. Hoy, lo que estamos viviendo es que esos mismos directivos deben plantearse modificar su paradigma tradicional de toma de decisiones y apoyarse más en su organización, en que esta participe activamente en la integración a tiempo de múltiples fuentes de información y su análisis. En un mundo donde competir significa tomar decisiones con elevado grado de incertidumbre, los razonamientos y construcción de inteligencia que exigen dichas decisiones deben estar fundados en

evidencias. El alto directivo debe descubrir, si no lo ha hecho ya, que en dicha tarea debe contar con el protagonismo de su propia organización, incluidas las redes de relaciones que esta atesora.

Alan Newell y Herbert Simon propusieron una «perspectiva del procesamiento de la información en la toma de decisiones organizativas». La naturaleza heurística del razonamiento humano tal como lo entiende la psicología cognitiva sigue sin resolver la interacción entre emoción y cognición. Cuando se aplica al problema de la visión sobre la periferia que rodea a la organización o «visión periférica», Day y Schoemaker entienden que el paradigma del procesamiento de la información indica la presencia de cuatro fases clave: percepción, juicio, acción y retroalimentación o *feedback*. Al nivel de la organización, las etapas paralelas de este proceso pueden describirse como: adquisición de información, diseminación de información, interpretación compartida, acción coordinada y aprendizaje colectivo. Nos parece relevante esta interpretación de Day y Schoemaker pues comporta los elementos que requiere en nuestra opinión el nuevo paradigma.

Tampoco hay que ignorar, como nos recuerdan dichos autores, que «en todas la etapas, el proceso está guiado por un conjunto de modelos o esquemas mentales que residen en niveles muy profundos de la organización». Es decir, no basta con generar valor con la IC, con implantar un proceso o invertir en una costosa herramienta de *software*, hace falta incidir en un nuevo tipo de liderazgo que modifique también aquellos aspectos de la cultura ligados a la gestión de la información y el conocimiento.

2. El aprendizaje de los cambios en el entorno por parte de las organizaciones y sus implicaciones en la gestión del conocimiento que requiere la IC.

Tiene muchos antecedentes, así como puntos de intersección, con el punto de vista del proceso de la información para decidir.

El libro de Peter Senge *La quinta disciplina* (1990) podría considerarse como un punto de inflexión, al trasladar a una audiencia de directivos más amplia la valoración de la importancia de una focalización en el aprendizaje[9]. Senge combina sus aportaciones con otros puntos de vista, en especial la importancia del pensamiento sistémico, para dar lugar a una perspectiva completa de la organización que aprende. El trabajo afín

[9] Además del libro de P. Senge, la importancia estratégica del aprendizaje –sobre todo acerca del futuro– es subrayada por Gary Hamel y C.K. Prahalad en su libro *Competing for the future* (Boston: Harvard Business School Press, 1994). De los obstáculos organizativos al aprendizaje y al cambio se ocupa Chris Argyris en su obra *Strategy, change and defensive routines* (Boston: Pitman Publishing, 1985). En el campo de las nuevas tecnologías, estos obstáculos se ciernen amenazantes, tal y como muestra Clayton M. Christensen en *The innovators dilemma* (Boston: Harvard Business School Press, 1997).

llevado a cabo por John Sterman[10], Chris Argyris y otros ayudó a configurar el aprendizaje organizativo como una perspectiva intelectual diferenciada. El punto de vista fundamental es que en entornos dinámicos el aprendizaje es complejo y, por tanto, no es simple ni automático. Para intentar determinar lo que sucedió y por qué, nos encontramos –siguiendo a Day y Schoemaker– con lo siguiente: *feedback* ambiguo, reacciones a destiempo, causalidad parcial múltiple, atribuciones interesadas, informaciones ausentes, efectos del tratamiento, ruido al azar y la ilusión de controlar todos los intentos de asolar la organización.

Cuando a esto le añadimos la probabilidad y la naturaleza ambigua de las señales, más baja cuanto más provenga de la periferia del negocio de la organización, el problema se agudiza mucho. Algunos autores han demostrado que la gente muestra una gran aversión a la ambigüedad cuando se enfrenta a decisiones que involucran peligros desconocidos: la gente prefiere «lo malo conocido» que lo supuestamente bueno por conocer. Por consiguiente, nunca viven ni aprenden bien en entornos de gran ambigüedad. Esta propensión puede exacerbarse a nivel organizativo, donde se espera y se desea que domine la racionalidad y la capacidad de previsión. Sin embargo, las nuevas oportunidades suelen acarrear un elevado nivel de incertidumbre y por tanto demandan un elevado grado de tolerancia a la ambigüedad. Estas reflexiones de Day y Schoemaker, procedentes del análisis de tecnologías emergentes, son perfectamente válidas para muchos mercados maduros donde las circunstancias sociopolíticas les confieren una elevada incertidumbre. Por ejemplo, las decisiones de nacionalización que se están tomando en algunos países latinoamericanos con Gobiernos populistas o la situación para las empresas en algunos países árabes salidos recientemente de largos periodos dictatoriales.

Para Day y Schoemaker, la concepción de culturas que sean capaces de aprender de entornos complejos puede requerir unos principios y valores de gestión distintos de los que son necesarios para maximizar la actividad vigente de la organización. En este caso, surge un conflicto entre la cultura del rendimiento y la del aprendizaje, y es a la alta dirección a quien corresponde determinar el equilibrio correcto entre ambas.

3. La necesidad de generar anticipación que requiere ese aprendizaje.

Distintos trabajos asocian los fallos en la administración empresarial con frecuencia a la incapacidad de anticiparse a los rápidos cambios en los mercados, responder a una nueva competencia y a su proliferación o a reorientar las tecnologías y la dirección estratégica de su negocio hacia las cambiantes necesidades de los clientes y las nuevas normas del sector

[10] MORECROFT, John y STERMAN, John. *Modelling for learning organizations*. Portland: 1994. *Business dynamics: Systems thinking and modeling for a complex world.* McGraw Hill, 2000.

(Fleisher, 2001). La misma idea la expresa así Gilad: las organizaciones con frecuencia fallan porque no son capaces de leer las señales típicamente débiles y ambiguas que son ubicuas en sus entornos y mercados.

Al introducir la expresión «gestión estratégica», Ansoff (1975) destacó la necesidad de centrarse en la capacidad de las organizaciones para anticiparse a las amenazas y oportunidades, con el fin de hacer frente a la turbulencia del ambiente que rodea la empresa. De hecho, diversos estudios de campo confirman este punto de vista. Las organizaciones con éxito estarían entre las que detectan los eventos más importantes a través de «señales de alerta». Cuando la incertidumbre es elevada, los directivos informan de una mayor frecuencia en el monitoreo y vigilancia del entorno y un mayor uso de fuentes de información personal. Los altos directivos en empresas de elevado rendimiento responden a la incertidumbre estratégica vigilando el entorno con mayor frecuencia y amplitud que sus equivalentes en empresas de bajo rendimiento (Daft *et al.,* 1988).

Pero en la práctica este reto no presenta una solución sencilla (Ansoff *et al.,* 1979; Porter, 1980). Incluso las organizaciones que han implementado sistemas de IC a menudo no logran anticipar sorpresas estratégicas (Gilad, 1988; Blanco y Lesca, 1998). En ambos casos (con y sin sistemas de IC), la mayoría de ellas parecen sufrir a la vez de sobrecarga de información y de falta de información estratégica, lo que para Blanco y Lesca puede llevar a cuestionar sus estrategias de recolección de información, aunque en opinión de quien suscribe el presente artículo esa situación también se debe a carencias en los otros dos ejes antes expuestos. Aquí vamos a profundizar un poco en la identificación y selección de las señales de cambio como base de la anticipación y en su gestión, superando barreras y «ángulos muertos».

Ansoff constató la existencia de una serie de filtros en la organización (tabla 1) que impedían que las señales pertinentes llegaran a tiempo a los decisores. Estas aportaciones siguen hoy teniendo gran valor –he tenido la posibilidad de constatarlo personalmente–. Tal es el caso del rápido crecimiento internacional en las últimas dos décadas de un nuevo competidor en el sector de bebidas de gaseosa, el grupo familiar peruano AJE, gracias a aprovechar oportunidades de cambios en el modelo tradicional de negocio. Dicho crecimiento se ha producido existiendo personas dentro de uno de los competidores afectados que me contaban fueron conscientes de la aparición de la amenaza pero no disponían de mecanismos en dicha organización para sensibilizar de ello a la alta dirección y catalizar un cambio. Este es un ejemplo en el que se constata cómo no basta el conocimiento de los hechos –las señales del cambio–, también es necesario poner el significado e implicaciones de los mismos al alcance de la alta dirección para que esta enderece el rumbo estratégico antes de que sea tarde. Ello supone, entre otros retos, superar estos filtros de Ansoff y comunicar no los hechos sino la inteligencia sobre los mismos.

Tabla 1. Barreras a señales tempranas de cambios: el proceso IC contribuye a reducirlas.

Filtro o barrera	Causa de la existencia del filtro
Filtro de vigilancia	Error al centrar el foco de atención. No hay directrices ni prioridades
Filtro de mentalidad	No se reconoce la importancia de la novedad porque sale del modelo o esquema mental predeterminado. Se reduce la información
Filtro del poder	En la toma de decisiones lleva a los actores menos poderosos en la organización a contener la expresión de sus percepciones

Fuente: I. Ansoff, 1984.

La existencia de un proceso de IC también contribuye a reducir esas barreras que señalaba Ansoff a esas señales tempranas o «débiles» de los cambios y a comunicar no solo las evidencias sino sus implicaciones para el negocio; en suma, la inteligencia. En este sentido, el apoyarse en evidencias y en un proceso trasparente para todos permite la credibilidad del equipo que impulsa el ejercicio de la IC al tiempo que minimiza el posible filtro de poder al integrar a los decisores en el propio proceso de IC. Por eso, el equipo de trabajo de IC debe procurar en todo momento diferenciar lo que son valoraciones o interpretaciones sobre los hechos de estos mismos. Llegado el caso, debe documentarse explícitamente, de manera que los decisores siempre tengan claro el proceso o cadena de valor de la transformación de la información[11]. Es decir, las fuentes de donde parten los datos e informaciones, en suma, las evidencias reunidas y las percepciones y significados formulados a partir de estas que se manejan para su decisión.

El supuesto subyacente de las señales de alerta temprana o *early warning signals* (EWS) es que las discontinuidades no surgen sin previo aviso. Estas señales de advertencia se pueden describir como «señales débiles» pues tienen valor en tanto son escasas, dispersas y fragmentadas; ahí todavía existe capacidad de anticipación y margen para la reacción. El concepto de «señales débiles» (Ansoff, 1975) tiene como objetivo la detección precoz de las señales que podrían dar lugar a sorpresas estratégicas y a un acontecimiento que tuviera el potencial de poner en peligro la estrategia de una organización. El proceso de IC debe integrar una respuesta organizada y sistemática a la detección de esas señales.

[11] Este concepto es del ingeniero francés Paul Degoul, director durante años de la ARIST Alsace y de ADIT.

Un problema importante para las organizaciones es resolver la selección de esas señales de alerta temprana o *early warning signals* (EWS). Para concluir, Blanco y Lesca constatan que las EWS no se pueden abordar objetivamente: más bien como un constructo que implica el conocimiento de los individuos. Por lo tanto, la selección debe contemplarse necesariamente como un proceso colectivo en el que la interpretación juega un papel importante. Esto les lleva a formular a la vez implicaciones prácticas y teóricas. En el mismo sentido se pronuncian Mendonça *et al.* cuando indican que el significado práctico de información de la señal débil es que pueda ser transformada en conocimiento significativo para la acción. Sin embargo, constatan que, como el valor de esta información no se materializa de forma automática, la realización de este potencial requiere un marco colectivo cognitivo por el cual las señales débiles pueden ser aprehendidas y evaluadas para, a partir de ahí, poder actuar en consecuencia. La teoría de los grupos de interés o *stakeholders* ha sido propuesta por Comai y Tena para comprender los actores en una industria específica dentro de un sistema de EWS.

Por todo lo cual, el planteamiento de cómo enfocar desde el proceso de IC la respuesta a las EWS no es obvio, como ya se ha señalado. Su solución, se ha comprobado, no puede descansar solo en tecnologías de la información: estas son un instrumento, no un fin, pueden contribuir a la productividad del equipo humano pero no sustituirlo. La combinación de tecnologías de la información y equipo humano viene mostrándose como el enfoque con mayor potencial.

Como consecuencia de la existencia de esos filtros comentados denunciados por Ansoff, aparecen en los directivos determinados ángulos muertos o puntos ciegos de percepción errónea en su visión del entorno. Este concepto de *blind spot* fue planteado por Porter (1980, págs. 59 y 60), quien utilizó el término para referirse a elementos de conocimiento del entorno que no son ciertos pero que aún guían la estrategia de negocio. En concreto, este autor indicaba que «son áreas en las que un competidor o no ve la importancia de los acontecimientos en absoluto (como por ejemplo un movimiento estratégico) o los percibe en forma incorrecta o solo los percibe con mucha lentitud».

Detrás del análisis de ángulos muertos o puntos ciegos, subyace una suposición acerca de los sesgos inherentes a la toma de decisiones entre altos directivos de las organizaciones (empresas e instituciones), los cuales superan a los de sus empleados o extraños. Sus fundamentos se encuentran en los filtros de Ansoff. Ben Gilad, en 1994 y posteriormente, desarrolló un método de análisis en tres pasos de esos ángulos muertos que se ha incorporado a la caja de herramientas del analista de IC. A partir de un primer examen de las cinco fuerzas de un mercado y de sus factores conductores, realiza un análisis de las suposiciones y percepciones de los directivos de una determinada empresa para identificar en

ellos esos posibles ángulos muertos en un tercer paso. El deterioro de la capacidad de los dirigentes para ver la realidad tal cual es y el análisis más objetivo de los analistas y planificadores de nivel medio (con menos ego involucrado) significan que ese tercer paso del análisis de puntos ciegos puede ser una herramienta para gestionar esos ángulos muertos potenciales.

Influencia y seguridad desde la empresa

Constatando los beneficios para el comercio y desarrollo mundial de la globalización no es menos cierto que la misma comporta un aumento de los riesgos a los que las empresas tienen que hacer frente en mercados conflictivos o lejanos. Es obvio que la complejidad e incertidumbre aumentan en aquellos países en los que o no existe o es incompleta la cadena de valor de la información y por tanto el rendimiento de las fuentes convencionales es mucho más reducido. Por otro lado, solo como ejemplo, acontecimientos recientes como los vividos en 2012 por la española Repsol YPF en Argentina (complejidad de *drivers* políticos y económicos y posterior entrada en el escenario de un competidor «tapado», Chevron) o la situación límite vivida a comienzos de 2013 con la ocupación de la planta gasística de BP, la noruega Statoil y Sonatrach en Tiguentourine, en el sur de Argelia (nuevamente los desencadenantes fueron factores sociopolíticos), son reflejo de esa creciente complejidad e incertidumbre, del potencial existente para la IC y de la necesidad de acentuar la gestión de los riesgos. Pero hoy la seguridad también debe ser tenida en cuenta en el propio mercado de la UE. En este sentido, tomemos como ejemplo algunos de los consejos sobre seguridad económica que las Cámaras de Comercio de Francia, V. Chardon y Bauquis proponen a las empresas y entidades de investigación a partir de tres objetivos:

- La identificación y análisis de las amenazas cuando las empresas francesas sean el blanco.
- La protección de las empresas e instituciones de investigación por su tamaño o sector en el que operan; de hecho, cualquier negocio puede estar sujeto a «ataques» cuando sea destacado innovador y opere en un sector competitivo. Lo mismo se aplica a las instituciones de investigación.
- La difusión de una cultura de la seguridad del patrimonio tangible e intangible en todas las empresas, tanto en grandes grupos como en las pymes e instituciones de investigación.

La poderosa tendencia de las organizaciones hacia su dependencia de la gestión del conocimiento, su reflejo en el creciente valor de la gestión de los activos intelectuales intangibles y el comercio electrónico global ponen de relieve al mismo tiempo las amenazas de distinto tipo a dicho patrimonio intelectual y su necesidad de protección desde una óptica

global. Un ejemplo de ello se manifiesta en el concepto francés de *intelligence economique* antes comentado. Esta incluye, como se ha visto, dos dimensiones adicionales a la vigilancia o monitoreo del entorno y a la generación de inteligencia para la decisión, que son:

- La capacidad de influencia, es decir, la técnica del uso de la información para proyectar la influencia de las organizaciones en los mercados.
- La protección de los activos de información, es decir, la capacidad de la empresa para conservar la información relativa a sus conocimientos, su experiencia, su estrategia y la prevención de riesgos relacionados con la negligencia o dolo en el manejo de esa información y conocimientos de la empresa.

Aquí nos limitaremos, partiendo de esa constatación, a exponer las negativas consecuencias de un tipo de delito tradicional para la seguridad de las empresas e instituciones de investigación, tal es el espionaje industrial. Esta realidad, que hoy adopta nuevas formas con los delitos cibernéticos, requiere la necesidad de responder con políticas activas de protección que aborden también los activos intangibles de la organización. Una de las derivadas de la IC es que la organización como colectivo pasa a ser más consciente de lo que es realmente importante preservar –activos tangibles e intangibles–, del conocimiento, dónde pueden estar los puntos más vulnerables y, como consecuencia, cómo protegerlos más adecuadamente.

El quebranto de la legalidad que plantea el espionaje industrial y sus negativas consecuencias sobre la IC en la empresa

A lo largo de la historia se han producido atentados al patrimonio intangible y tangible de las organizaciones. El intento de utilizar atajos vulnerando la legalidad para robar el saber hacer más singular del competidor tiene múltiples antecedentes. De hecho, ahora trataremos mediante ejemplos cómo este tipo de delitos tienen hoy una importancia que no se puede desdeñar. Lo que llama la atención es que en este campo, dichos quebrantos de la ley, lo que se denomina «espionaje industrial», llegan en los medios de comunicación a eclipsar el trabajo de la gran mayoría de los profesionales, asociaciones y entidades de formación que respetando la legalidad se dedican a generar valor para sus organizaciones analizando la información obtenida de fuentes de acceso público. Además, como resalta Gilad, esa connotación negativa es el resultado del desconocimiento y confusión en medios de comunicación generalistas del significado del concepto de inteligencia con el propio del ámbito militar, donde la obtención de la información es el fin sin perjuicio del medio. Ahí es donde puede aparecer el delito si se extrapola a la esfera civil, ya que es información obtenida ilícitamente y por tanto rechazable por principio.

Esos mismos medios pueden ignorar que la acepción y valor para la empresa están en el resultado del análisis de la información, esto es, la IC. En cualquier caso, dicha confusión viene suponiendo un indudable freno a un mayor conocimiento de la IC y su papel en la empresa. Se recogen aquí algunos ejemplos y datos económicos de esos delitos.

Caso 4: La alemana Enercon GmbH fue espiada por encargo de un competidor norteamericano.

Los hechos sitúan este acto delictivo en marzo de 1994. Por aquel entonces, su tecnología propia de aerogeneradores de tracción directa (sin engranajes) y velocidad variable presentaba ventajas inigualables en el mantenimiento de las máquinas que le permitían una estrategia de diferenciación. Su producto se vendía con precios por encima del resto. En ese período 1993-1994, el fabricante alemán negociaba con New World Power Corp. (NWP) la exportación de su máquina E-40 a los EE. UU. Lo que ignoraban los alemanes es que su competidor norteamericano Kenetech, tras obtener violando la ley los detalles íntimos de una E-40 y armado de los mismos, se dirigió a la batalla defensiva contra las exportaciones previstas denunciando una infracción de una de sus patentes ante el organismo federal U. S. Int. Trade Commission. El litigio duró años y mantuvo a Enercon fuera del mercado de los EE. UU.

Posteriormente a estos hechos, les llegó a Wobben y sus abogados estadounidenses –posiblemente accidentalmente– la evidencia de la otra parte. Además de una gran cantidad de fotos que muestran el interior completo de la E-40, fue también el informe de espionaje de ocho páginas de Ruth Heffernan. En él se describe en detalle la forma en que ella y sus colegas holandeses del competidor de EE. UU. Kenetech Jans-Robert «Bob» y Ubbo de Witt de Oldenburg espiaron el sistema de Enercon. Según este «bandonaron Groningen en la madrugada del lunes, 21 de marzo de 1994, con Bob, en Oldenburg recogieron a Ubbo, físico y meteorólogo, quien había trabajado como *freelance* para Kenetech. Tenía contacto con un agricultor que posee en su terreno una Enercon-40 y estaba en uso». El resto de los hechos se resume en la entrada nocturna y delictiva de esas personas en dicha máquina, el descubrimiento de los hechos, su denuncia y el escándalo que mereció en su día la condena del Parlamento Europeo.

Fuente: Adaptado por el autor del original de Schröm, Oliver en Die Zeit, 1999.

Caso 5: Condenada por robar secretos a Motorola con acusación no probada de venderlos a China.

Jin Hanjuan, ciudadana nacionalizada estadounidense, estaba a punto de abordar un vuelo con destino a Beijing el 28 de febrero del 2007 cuando un control al azar la detuvo en seco. De acuerdo con el expediente judicial

y una declaración jurada del FBI presentada como un caso de espionaje económico en su contra, cuando los funcionarios de aduanas en el aeropuerto O'Hare de Chicago inspeccionaron las bolsas de la ingeniero de *software* de 40 años de edad, se encontraron más de 1.000 documentos confidenciales que se alega han sido robados de Motorola, el grupo de electrónica de EE. UU. para la que la Sra. Jin había trabajado hasta dos días antes del vuelo.

Los documentos de la Corte dicen que los funcionarios chinos también descubrieron manuales militares, catálogos de una empresa europea de productos militares, documentos que detallan aplicaciones militares chinas para equipos electrónicos, etc. que han sido redactados por una empresa de telecomunicaciones china no identificada, y 30.000 dólares en efectivo[12]. En la acusación penal contra la Sra. Jin, celebrada en un tribunal de Chicago, Motorola alegaba que los costos de investigación y desarrollo de la información en poder de la acusada era de más de 600 millones de dólares. La compañía perdería importantes ingresos globales cuando el contenido se hiciera público, agrega. Por su parte, la Sra. Jin se ha declarado no culpable.

En otro caso civil presentado por Motorola, la Sra. Jin es una de los acusados con Huawei, el fabricante chino de equipos de telecomunicaciones, a través de una alegación de que ella y los demás estaban «secretamente comprometidos» en el desarrollo de productos de la compañía china en el tiempo en que ella era empleada de Motorola. Huawei ha dicho que el caso presentado por Motorola es «improcedente» y se ha negado a comentar sobre el caso criminal.

Fuente: Extracto traducido del original de *Financial Times,* 1 de febrero de 2011.

Las pérdidas económicas que implican estos delitos son, como se ha visto en los dos casos, significativas. Las cifras que se manejan son muy dispares según las fuentes. Un informe al Congreso de los EE. UU. de 2002 recoge algunas estimaciones (*Xerox white paper,* 2003). Los autores de un reportaje de *Financial Times* en 2011 constatan una creciente preocupación por la aparición de estos casos; algunos de los más sonados recientemente han implicado a Renault y su tecnología de baterías para coches eléctricos o a Google y su código fuente asaltado por ciberataques, pero en sectores muy diferentes también se presentan casos

[12] Bloomberg añadió posteriormente a partir del juicio que su billete de vuelo a China era solo de ida, que los beneficiarios podrían ser la empresa china Kai Sun News Technology Co., también conocida como SunKaisens, y el Ejército de China, y la tecnología objeto la iDEN. El 29 agosto de 2012 el juez, tras examinar los hechos probados, condenó a la acusada a cuatro años de prisión por robo de secretos pero la exculpó de los delitos de venta de los mismos a empresas chinas. http://www.huffingtonpost.com/2012/08/29/hanjuan-jin-sentenced-for_n_1840304.html.

como la acusación de espionaje en 2009 de Starwood Hotels and Resorts a Worldwide Hilton.

Entre otras medidas de protección ante estos delitos, el trabajo del *Financial Times* plantea reducir al mínimo la posibilidad de fugas ya sea a través de métodos elaborados con ayuda de tecnologías de la información o, a veces, a partir de ideas que se deban más al sentido común. Otro planteamiento puede ser abandonar toda esperanza de que todas las fugas se puedan evitar y concentrarse en un proceso continuado de innovación sobre las tecnologías más avanzadas y productos que sean difíciles de reproducir por una persona ajena debido a su complejidad y al uso de ideas novedosas.

En cualquier caso, este tipo de delitos ha llevado a algunos países de la OCDE a transmitir activamente consejos de prevención y protección a sus empresas contra el espionaje. Tal es el caso de Canadá, cuyos servicios nacionales de investigación de la seguridad los tienen publicados en Internet[13].

Implicaciones para los territorios: la inteligencia territorial

El desarrollo de un territorio depende de varios factores y variables: la información y el conocimiento generado en él juegan un papel relevante. Hacer uso de este conocimiento y de esta información mediante la coordinación de los actores que trabajan y participan en una misma región se ha venido a denominar *inteligencia territorial* (IT). Aunque la IT engloba más aspectos que la gestión de información, esta es una de sus piedras angulares (Eva Otol, 2012).

Este término surgió en Francia en los años 90 y se utiliza para nombrar la función y el proceso de inteligencia llevado a cabo por las administraciones públicas a escala local, regional o estatal. El objetivo es, mediante el uso de la información, conocer el territorio y sus recursos para crear riqueza y planificar políticas de desarrollo y sostenibilidad (Bertacchini, 2004). Para T. Ferrari, la IT consiste en abordar de forma sistemática el desarrollo de un territorio mediante el trabajo de sus actores en red dirigido al desarrollo sostenible del mismo.

No se puede entender este concepto de IT sin partir de conceptos como planificación territorial estratégica, triple hélice, capital del territorio, *clusters,* distritos o polos de especialización económica por competencias e impulso a la innovación e IC. El Informe Carayon de 2003 dedica una parte importante a la IE y el territorio. El concepto de «inteligencia del territorio» sirve en definitiva para impulsar la innovación en el terri-

[13] Las direcciones son: www.csis-scrs.gc.ca/nwsrm/wr/wr2-eng.asp y www.csis-scrs.gc.ca/nwsrm/wr/wr3-eng.asp.

torio. En la práctica, se traduce en la recogida y análisis de la información sobre el entorno con un enfoque de inteligencia competitiva y la confrontación del punto de vista de los actores locales para generar las políticas más coherentes a aplicar.

Para Ferrari, la inteligencia territorial es el dominio de los métodos y recursos de inteligencia económica al servicio de los territorios, y su despliegue se realiza con el objetivo de:

- Identificar y contribuir a poner en marcha proyectos creadores de empleo, riqueza y actividad en cuanto a la estrategia.
- Anticipar los cambios, riesgos y evoluciones futuras en cuanto a la visión prospectiva y salvaguardia del patrimonio.
- Valorizar el territorio, el rendimiento más atractivo, en cuanto a la influencia.
- Animar el desarrollo tecnológico y económico del territorio en cuanto a las redes.

Perspectivas de evolución

El presente y futuro de la IC están ligados al modo en que sea capaz de servir a las decisiones estratégicas e integrar al decisor. En muchos casos, se constata una falta de orientación a su cliente. Ese déficit en la atención que se presta al cliente y a su implicación en el proceso de IC limita la generación de inteligencia y el proceso deriva hacia un mero suministro de información y documentación y, a partir de ahí, a la marginalidad en la organización.

Es por eso que la conversión de la información en inteligencia se ha convertido en uno de los temas centrales hoy de la IC. S. Wright lo ha trabajado recientemente a partir de una reflexión sobre cómo aprovechar los activos intangibles singulares de una organización: su conocimiento explícito, implícito, adquirido y derivado y de un concepto como es el tradicional de ventaja competitiva basada en la inteligencia o IBCA. Para Gilad, esto se hace a través de la interpretación –o lo que muchos llaman análisis– de la información. Para este autor, la definición correcta de la inteligencia debe ser por lo tanto la de un punto de vista sobre los hechos y, en ese sentido, debe distinguirse nítidamente de la información. Es por eso que habla de dos corrientes: una mayoritaria, la *reporting school*, con énfasis en la recolección y organización de la información, y otra que responde a su posición, la *analysis school,* centrada en la generación de inteligencia.

Madureira pone el énfasis en la inmediatez[14] o tiempo de generación de la IC. Para él la ventaja competitiva de la IC no vendrá del acceso a los datos

[14] Debo este término al ing. Marcelino Huerta, antiguo gerente de Famosa.

ni solo de la calidad de los análisis, sino del equilibrio entre la velocidad y la calidad de la visión, llamémosle *agilidad insight.* Esto significa ser los primeros en detectar una oportunidad o una amenaza y transformarla en percepciones y comprensión aplicables que pueden derivarse en estrategia y ponerse en práctica para ganar posición en el mercado.

El profesor J. E. Prescott, tras analizar la evolución de la IC, habla de una tendencia a convertirse en una capacidad central de las empresas, su integración generalizada en los programas formativos de las escuelas de negocios, el énfasis en atributos como lo cualitativo o estratégico y su comunicación mediante insumos directos al decisor proporcionados desde unidades de IC, marketing o planificación. Este autor en la década pasada ha trabajado en el establecimiento de un cuerpo de contenidos estandarizados que definan los contenidos curriculares de la enseñanza de la IC.

Si esta es una visión más académica, desde la práctica empresarial surgen otras propuestas no menos interesantes para el futuro de la IC. Así, por ejemplo, la que hace el norteamericano M. Brenner desde la corporación Air Products and Chemicals, quien ve la eficacia de los especialistas en IC como facilitadores o *coachers* de sesiones de toma de decisión en grupo. Este planteamiento es respaldado por L. Fahey cuando explica cómo la inteligencia, en última instancia, no es un resultado de los profesionales de inteligencia por sí solos, sino que es cocreada a través de la interacción entre los profesionales de inteligencia y tomadores de decisiones. Por eso insiste: «El resultado clave de la inteligencia es la comprensión –*insight*–». Esto es todo en lo que consiste el juego: ese *insight*[15] involucra a los tomadores de decisiones.

Precisamente en línea con la creación de mecanismos que impliquen la participación conjunta de especialistas de IC y decisores y *staff* de los mismos, aparece una forma de desarrollar la técnica de análisis de escenarios que son la sala de guerra o *war room.* Precisamente por su capacidad para hacer frente a la incertidumbre tiene un gran potencial en este momento de la actividad empresarial.

En el ámbito académico, están surgiendo interesantes experiencias de integración de profesionales de la biblioteconomía desde las bibliotecas universitarias, quienes se suman temporalmente a los grupos de investigación para facilitarles el acceso a los resultados de análisis.

Esta necesidad de obtener los resultados del análisis, unida a una explosión de conocimiento científico, tecnológico y de mercado, obliga a incorporar de forma creciente herramientas de *software* de minería de textos científico-técnicos o *tech mining* o herramientas de análisis sintáctico y semántico, para la comprensión de pautas emergentes y sus relaciones.

[15] Comprensión, visión o percepción de los hechos y de sus implicaciones para el negocio.

Por último, la normalización se está abriendo paso en este ámbito desde la I+D+i. Así, la UNE 166.006:2011 en su última revisión se ha abierto a la IC. Los trabajos en curso del grupo del Comité Europeo de Normalización, CEN 389, sobre *strategic intelligence management* apuntan hacia una pronta presencia internacional de referentes normativos para las empresas en este ámbito.

Dedicado a Antonio Rico Gil, economista y maestro, in memoriam (1947-2013).

Bibliografía

AENOR. *Gestión de la I+D+i: Sistema de vigilancia tecnológica e inteligencia competitiva.* UNE 166.006:2011, 2011.

AGUILAR, F.J. *Scanning the business environment*. New York: Macmillan Co., 1967.

ANSOFF I. «Managing strategic surprise by response to weak signals». *California Management Review,* 18 (2), 1975, pp. 21-33.

— *Implanting strategic management.* New Jersey: Prentice Hall International, 1984.

BERTACCHINI, Y. «Le territoire, une entreprise d'intelligence collective à organiser vers la formation du capital formel». *Revue Communication & Organisation,* n° 25, *Les vallées: sens, territoires & signes,* GREC/O, ISIC. Universidad de Burdeos, 3, 1.er semestre de 2004. Recuperado en 20100513 de http://isdm.univ-tln.fr.

BERNHARDT, D. «Tailoring competitive intelligence to executive needs». *Long Range Planning,* vol. 27, pp. 1, 5-17, febrero de 1994.

BLANCO, S., CARON-FASAN, M. y LESCA, H. «Developing capabilities to create collective intelligence within organizations». *Journal of Competitive Intelligence and Management,* vol. 1, nº 1. SCIP, primavera de 2003.

BLANCO, S. y LESCA, H. *Business intelligence: Integrating knowledge into the selection of early warning signals.* 1998. Recuperado el 17/11/2002 de http://www.veille-strategique.org/docs/1998-Blanco-Lesca-Articlewksp.pdf.

CARAYON, B. *Intelligence économique, compétitivité et cohésion sociale.* París: La Documentation Française, 2003, 176 págs. Recuperado el 14/06/2004 de http://www.ladocfrancaise.gouv.fr/brp/notices/034000484.shtml.

CHARDON, V. y BAUQUIS. *Intelligence économique. Guide du Routard.* Hachette, 2012.

CHRISTENSEN, C. M. *et al. Seeing what's next*. Harvard Business School Press, 2004.

COMAI, A. y TENA, J. *Mapping and anticipating the competitive landscape.* Barcelona: Emecom, 2006.

DAFT, R. L., SORMUNEN, J. y PARKS, D. «Chief executives scanning environmental characteristics and company performance: an empirical study». *Strategic Management Journal,* vol. 9, 1988, pp. 123-139.

DAY, G. y SCHOEMAKER, P. J. H. *Visión periférica.* Ediciones Deusto, 2006.

«Aproximación a la inteligencia competitiva. Inteligencia y seguridad». Revista de análisis y prospectiva. Equipo CNI, 2010, 9, pp. 19-40.

ESCORSA, P y MASPONS, R. *De la vigilancia tecnológica a la inteligencia competitiva.* Madrid: Prentice Hall, 2001.

FAHEY, L. «The future directions of competitive intelligence: Some reflections». *Competitive Intelligence Magazine.* SCIP, vol. 12, 2009, 1, pp. 17-22.

FERRARI, T. *Intelligence territoriale.* ADIT. Documentación curso formación en IC para Madri+d, 2007.

FLEISHER, Craig S. «An introduction to the management and practice of competitive intelligence (CI)», cap. 1, de la monografía editada por el autor y David Blenkhorn *Managing frontiers in competitive intelligence*. Westport, CT: Quorum, 2001.

FLEISHER, Craig S. y BENSOUSSAN, Babette. *Strategic and competitive analysis: Methods and techniques for analyzing business competition.* Prentice Hall, 2002, 457 págs.

FLEISHER, Craig S. y BLENKHORN, D. «What are the enduring issues in competitive intelligence (CI)?», cap. 1, de la monografía editada por estos autores, *Controversies in competitive intelligence*. Westport, CT: Praeger Publishers, 2003.

FLEISHER, Craig S. y WRIGHT, Sheila. «Causes of competitive analysis failure». 36-50. *Proceedings III European CI Symposium, ECIS.* Estocolmo: 2009. Recuperado el 23 de enero de 2013. http://www.bth.se/fou/forskinfo.nsf/all/d44c704148b7adbac12576e0003d87e8/$file/ECISproceedingsFinal3.pdf.pdf.

— «Industrial espionage: Data out of the door». *Financial Times,* 1 de febrero de 2011.

GILAD, Ben. «The future of competitive intelligence: Contest for the profession's soul». *Competitive Intelligence Magazine,* 11 (5), 2008, pp. 21-25.

GILAD, B. y GILAD, T. *The business intelligence system: A new tool for competitive advantage*. Amacom Books, 1988, 242 páginas.

HALAL, W. E. «Organizational intelligence: What is it, and how can managers use it?». *Knowledge Management Review,* vol. 1, marzo-abril de 1998. Una copia del mismo se encuentra publicada en www.strategy-business.com/article/12644?gko=4a546.

HAMEL, G. y PRAHALAD, C. K. (1994). *Competing for the future*. Harvard Business School Press, 1994.

HARBULOT, C. y BAUMARD, P. «Perspective historique de l'intelligence économique». *Revue intelligence économique.* École de Guerre Économique, 1997.

HERRING, J. «Key intelligence topics: A process to identify and define intelligence needs». *Competitive Intelligence Review,* vol. 10 (2), 1999, pp. 4–14.

JAWORSKI, B.J., MACINNIS, D. y KOHLI, A. «Generating competitive intelligence in organizations». *Journal of Market-Focused Management*, 5, 2002, pp. 279– 307.

JUHARI, A. y STEPHENS, D. «Tracing the origins of competitive intelligence throughout history». *Journal of Competitive Intelligence and Management.* vol. 3, 4, 2006, pp. 61-82.

KAHANER, L. *Competitive intelligence: How to gather, analyze, and use information to move your business to the top*. Nueva York: Touchstone -Simon & Schuster, 1996.

LESCA, H. y LESCA, N. *Les signaux faibles et la veille anticipative pour les décideurs.* París: Lavoisier, 2011.

MADUREIRA, L. «Social market intelligence. An introduction to future ready CI» . *SCIP insight e-bulletin.* Vol. 5, 1, enero de 2013.

MASSON, J. L. *Inteligencia competitiva. Bases teóricas y revisión de literatura.* Barcelona: Univ. Autónoma Barcelona. Dpto. de Economía de la Empresa. Barcelona, 2005.

MENDONÇA, S., CARDOSO, G. y CARAÇA, J. «Some notes on the strategic strength of weak signal analysis». *LINI working papers,* n.º 2, 2007, recuperado el 23.01.2013 de http://www.lini-research.org/np4/?newsId=9&fileName=SMENDONCA_ETAL_LINI_WP2.pdf.

MICHAELI, R. *Competitive intelligence. Strategische wettbewerbsvorteile erzielen durch systematische konkurrenz-, markt- und technologieanalysen.* Berlin-Heidelberg: Springer Verlag, 2006. Existe traducción al inglés en la misma editorial desde enero 2013, edición 2012.

ORTOLL, Eva «Inteligencia territorial: iniciativas y modelos». *Revista de los Estudios de Ciencias de la Información y de la Comunicación.* UOC, 9 de marzo de 2012. Recuperado el 20 de febrero de 2013 de http://www.uoc.edu/divulgacio/comein/es/numero09/articles/Article-Eva-Ortoll.html.

PALOP, F. y VICENTE, J. M. «Vigilancia tecnológica e inteligencia competitiva: Su potencial para la empresa española». *Colección Estudios*, n.º 15. Madrid: Fundación COTEC, 1999.

PALOP MARRO, F. y MARTÍNEZ, J. F. *Guía metodológica de práctica de la vigilancia tecnológica e inteligencia competitiva.* Erica, 2012.

PRESCOTT, J. E. «Competitive intelligence: Its role and function within organizations», en la monografía editada por el autor *Advances in com-*

petitive intelligence. Viena: Society of Competitive Intelligence Professionals, 1989, pp. 1-14.

— «The evolution of competitive intelligence». *Journal of the APMP.* Verano de 1999, pp. 37-52.

PORTER, M. *Competitive strategy*. Free Press, 1980.

MARTÍN, R. A. «Modelo normalizado de unidad de inteligencia competitiva y manual de operaciones: una propuesta*». Inteligencia y Seguridad. Revista de análisis y prospectiva,* vol. 9, 2010, pp. 67-93.

MARTIN, R. «Strategy and the uncertainty excuse». *Harvard Business Review, HBR Blog Network,* 8 de enero de 2013. Recuperado de http://blogs.hbr.org/.

ROUACH, D. *La veille technologique et l'intelligence économique*. París: Presses Universitaires de France, 1996.

SENGE, Peter M. *The fifth discipline*. Doubleday/Currency, 1990.

SINGH, A. y BEURSCHGENS, A. «Benchmark your CI capabilities using a self-diagnosis framework». *Competitive Intelligence Review,* 2006.

SCHROM, O. «Verrat unter freunden». *Die Zeit.* (dossier), 1999. Recuperado el 4 de abril de 2006 de www.zeit.de/archiv/1999/40/199940.nsa_2_.xml?page=all.

STONER, J. A. F. y WANKEL, C. *Administración. Planeación y toma decisiones.* México: Editorial Prentice-Hall Hispanoamericana S. A., 3.ª edición, 1989.

VOLGESTEIN, F. «Search and destroy». *Fortune Magazine,* 2 de mayo de 2005.

WILENSKY, H. *Organizational intelligence: Knowledge and policy in Government and industry.* New York: Basic Books, 1967, 226 páginas.

WRIGHT, S. «Converting input to insight: organising for intelligence-based competitive advantage». En WRIGHT, S. (ed.): *Competitive intelligence, analysis and strategy: creating organisational agility.* Abingdon: Routledge, 2013, pp. 1-35.

— «Economic espionage and trade secret theft: Defending against the pickpockets of the new millennium». *Xerox white paper,* Xerox Corporation, 2003, p. 10. Recuperado el 17 de enero de 2013 de http://www.xerox.com/downloads/wpaper/x/xgs_business_insight_economic_espionage.pdf.

Capítulo V

LOS RIESGOS ECONÓMICOS DE LA CIBERGUERRA

Henning Wegener

Resumen

La creciente aceptación e introducción de las tecnologías digitales en la planificación y el armamento militares da paso a la perspectiva de una ciberguerra en la cual, habida cuenta de la interdependencia global de las estructuras de red, podría, inevitable y profundamente, afectar a la economía y a esenciales activos de la sociedad.

La utilización militar hostil de estas tecnologías podría de hecho, y de derecho, no estar claramente diferenciada de los ciberconflictos de carácter general y despertar serias dudas sobre su control y legitimidad, abriendo así posibilidades ciertas de causar daños de importante consideración.

Existe el perenne dilema de que el crecimiento exponencial y el velocísimo desarrollo de las tecnologías cibernéticas y los nuevos usos sofisticados entren en conflicto con el crecimiento exponencial y la sofisticación de las posibilidades de ataques. El asombroso crecimiento cuantitativo y cualitativo de los sistemas y las infraestructuras cibernéticos hacia una *segunda revolución digital* viene acompañado de un crecimiento, igual o incluso superior, de posibles ataques y, con ellos, de vulnerabilidades.

Sin embargo, los beneficios de la era digital se acumulan solo si existe confianza en el funcionamiento, la fiabilidad, la integridad y la seguridad de las tecnologías subyacentes: es por ello que la seguridad digital se ha

convertido en un desafío global. Este artículo describe los presentes y posibles futuros desarrollos cibernéticos, así como el panorama de creciente amenaza en términos de nuevas formas de ataque, nuevos atacantes y nuevas dimensiones de riesgos y pérdidas económicas.

El artículo argumenta que el uso militar y deliberado de las nuevas tecnologías con fines cibernéticamente beligerantes o, cuando menos, su componente ofensivo debieran ser deslegitimados, o reducida su importancia; si bien el mejor proceder para todos los interesados, incluyendo los actores económicos, debería fundamentarse en optimizar las estrategias para evitar o reducir los posibles daños cibernéticos.

Los conceptos fundamentales –en toda forma de ciberconflicto– son: la autodefensa, la resistencia, la mejora en la seguridad de la industria de tecnologías de la información, la elaboración de normas que incluyan parámetros estándar de seguridad en la nube, redundancias técnicas, restricciones, cooperación nacional e internacional, respuestas de emergencia, intercambio efectivo de información y sistemas de alerta, incremento de los esfuerzos para armonizar las leyes penales y las sanciones en materia cibernética, avances en el refuerzo de la legislación internacional y el establecimiento de normas internacionales de conducta para la era cibernética. El artículo concluye subrayando la necesidad de crear una cultura de ciberseguridad y presenta unas líneas generales sobre los conceptos de ciberestabilidad y ciberpaz.

Palabras clave

Ciberguerra, ciberseguridad, ciberconflicto, ciberataque, infraestructura cibernética, infraestructura nacional crítica, nuevas tecnologías digitales, ciberlegislación, panorama de amenazas, resistencia, cultura de ciberseguridad, ciberley, ciberestabilidad, ciberpaz.

Abstract

The increasing acceptance and introduction of digital technologies in military planning and armament opens the perspective of a cyber warfare that, given the global interdependence of net structures, would unavoidably and deeply affect the economy and vital societal assets. Hostile military use of these technologies could, for factual and legal reasons, not be cleanly separated from cyber conflict in general and raises serious questions of controllability and legitimacy, thus opening up highly disturbing damage perspectives. There is the perennial dilemma that the exponential growth and ultra-rapid development of cyber technologies and new sophisticated uses are in conflict with the equally exponential growth and sophistication of attack options. The amazing quantitative and qualitative growth of cyber systems and cyber infrastructures in a *second digital revolution* comes accompanied by an equal or even superior growth in attack options and thus in vulnerabilities. Yet, the benefits of the digital age accrue only if there is trust in the functioning, reliability, integrity and safety of the underlying technologies: thus, cyber security has come to be a global challenge. The article describes actual and possible future cyber developments and the evolving threat landscape in terms of new attack modes, new perpetrators, and new dimensions of economic risk and loss.

The article argues that the deliberate military use of digital technologies in a cyber war mode should be delegitimized or that at least its offensive component be deemphasized, but that the best course for all stakeholders, including economic actors, would be to optimize strategies for the prevention and mitigation of cyber damage. The key concepts –for all forms of cyber conflict– are self-defense, resilience, security improvements in the IT industry, standard setting including standards for cloud safety, technical redundancies, constraint, national and international cooperation, emergency responses, effective information exchange and warning systems, increased efforts to harmonize cyber penal law and sanctions, advances in international law enforcement, and building international norms of behavior for the cyber age The article concludes emphasizing the need for a universal culture of cybersecurity, and offers an outline of a concept of cyber stability and «cyber peace».

Key word

Cyber war, cyber security, cyber conflict, cyber attack, cyber infrastructure, critical national infrastructure, new digital technologies, cyber law, threat landscape, resilience, culture of cyber security, cyber law, cyber stability, cyber peace.

Ciberguerra y ciberconflicto: la dimensión económica

Un número anterior de esta serie de *Cuadernos de Estrategia,* publicado en diciembre de 2010, centraba su análisis de las ciberamenazas en la dimensión de la seguridad nacional[1]; el presente ensayo examinará las consecuencias de la inseguridad cibernética y los ciberconflictos en la seguridad económica y en la inteligencia económica. Como quiera que las amenazas que subyacen son las mismas o similares, y considerando que la seguridad económica es, en definitiva, un ingrediente esencial para la seguridad nacional, este análisis servirá de aportación a la antedicha publicación, cuyo valor persiste con entera validez en el tiempo, no obstante lo cual, algunos desarrollos y cifras más recientes se han incorporado, como es natural.

Concebido literalmente, el tema que nos ocupa parece centrarse en los daños económicos que pueden resultar de un uso hostil de las tecnologías cibernéticas dentro de un contexto *militar,* lo cual podría suponer una relación directa entre la economía y la guerra.

Sin duda alguna, la historia nos demuestra que la guerra, tradicionalmente llevada a cabo con armas convencionales, ha representado siempre enormes riesgos y daños para los activos económicos de los países beligerantes:; tanto por sus efectos indirectos en las infraestructuras como en los hábitos de consumo, los procesos económicos y las relaciones comerciales, así como, en general, en el funcionamiento de las sociedades. También los daños secundarios «no intencionados», en los cuales los efectos sobre objetivos estrictamente militares han afectado ampliamente a la sociedad, incluyendo las infraestructuras básicas, así como aquellos que forman parte de una estrategia deliberada que persigue la destrucción de las redes de infraestructuras de países enemigos, con especial atención a la industria armamentística y la economía de guerra, o incluso aquellos destinados a quebrantar la moral del adversario y a minar el deseo de sus pueblos de luchar y resistir.

La guerra moderna ha absorbido de forma creciente a las sociedades en su conjunto. Su intencionado efecto destructivo y devastador culminó, sin duda, en la Segunda Guerra Mundial: una «guerra total» en la que el poder prácticamente ilimitado de los sistemas armamentísticos, incluidas las armas nucleares, y el deseo estratégico de los bandos supusieron la destrucción a gran escala de los territorios enemigos y sus activos económicos, incluyendo sus ciudades, poblaciones enteras, con nuevas dimensiones de violencia y sufrimiento humano.

[1] *Ciberseguridad, retos y amenazas a la seguridad nacional en el ciberespacio. Cuadernos de Estrategia,* n.º 149. Madrid: Instituto Español de Estudios Estratégicos, Ministerio de Defensa.

Al adentrarnos en la era digital, son otras las reglas que gobiernan. Los ataques digitales, incluyendo aquellos con objetivos militares, son, primordialmente, no violentos y de un coste relativamente bajo («bits en lugar de bombas»), y se desarrollan exclusivamente a través de la invasión electrónica de sistemas y estructuras de red. Esto es también aplicable a efectos militares. Las tecnologías de la información y comunicación (TIC) han revolucionado los asuntos militares, incluyendo la información sobre los campos de batalla y sus comunicaciones y los sistemas armamentísticos, al tiempo que han incrementado la vulnerabilidad a este tipo de invasiones.

Un ataque digital llega desde un enemigo invisible: es difícil de identificar y de seguir; es asimétrico, difícil de evaluar en lo que respecta a su amplitud y efectos finales, lo que hace incierto tratar de evaluar sus efectos más allá de las consecuencias económicamente mensurables. Si bien es cierto que de ello se desprende un menor derramamiento de sangre y una menor destrucción física, no lo es menos que sus consecuencias podrían, de hecho, ser desastrosas y dañar profundamente la economía.

En muchas ocasiones en las que autores se aventuran a definir la ciberguerra, esta es descrita como una acción política llevada a cabo por naciones cuyo fin es el de causar al adversario significativos daños militares: daños a redes informáticas militares, a sistemas de mando y control, a redes de defensa aérea y a sistemas de armamento centrados en redes, todo ello a través de medios digitales[2].

Más de cien países han reconocido haber establecido mandos cibernéticos y entendido que el ciberespacio es el quinto escenario bélico, tan esencial para las operaciones militares como las terrestres, marítimas, aéreas o espaciales. Es conocido que más de 30 han desarrollado doctrinas específicas sobre la ciberguerra y más de un centenar tienen la habilidad técnica para desarrollar ofensivas militares efectivas. El sentimiento generalizado es que la ciberguerra es una acción militar que supone una opción portentosa y real y, en consecuencia, debe ser tomada muy en serio; si bien los escenarios y predicciones acerca de su aceptación difieren.

Un asunto a tener en cuenta sobre esta materia es el crecimiento autónomo de los mandos cibernéticos y las doctrinas de ciberguerra aplicables que podrían seguir los esquemas militares al uso, que parecen padecer autismo, siendo así insensibles al contexto cibernético interconectado. El hecho de pensar en términos de ciberguerra podría conducir a una trampa terminológica; regresaremos a este preocupante aspecto.

[2] *Cyberwar*, Wikipedia. Ver también: GLENNY, Misha. «Das ende der nettigkeiten. Cyberkrieg und sicherheit im Internet». *Internationale Politik*, noviembre/diciembre de 2012, p. 80.

Sin embargo, una breve revisión y yuxtaposición de las diferentes definiciones de «ciberguerra» permite apreciar que estas clarifican poco y que, en el mejor de los casos, «ciberguerra» continúa siendo un término elusivo. La más simple y directa conclusión es que estamos hablando de ataques digitales a sistemas e infraestructuras cibernéticas.

Casi cualquier ulterior criterio de definición es susceptible de ser dudoso o ambivalente. ¿Ataques por motivos políticos?; si se trata de espionaje, incluido el ejercido contra industrias armamentísticas e infraestructuras nacionales, muchos de quienes los definen alegan que los motivos políticos y económicos están, por naturaleza, imbricados, por lo que el beneficio económico o los hurtos de datos informáticos bien pueden ser la causa principal[3].

El terrorismo informático (un concepto al que regresaremos en este análisis) tiene ciertamente motivaciones políticas, pero no persigue objetivos bélicos entre estados. ¿Acciones por parte de países o Gobiernos?; en efecto, los ataques pueden ser promovidos por países, pero el escenario más probable y efectivo es que una asociación criminal –si se quiere «mercenarios digitales»– son empleados, al menos como coadyuvantes, para infligir un desbaratamiento digital en perversas alianzas con estados turbios y el crimen organizado como proveedor de un «servicio de delitos».

Podrían darse ataques bajo «bandera falsa» cuando organismos estatales o no estatales llevasen a cabo un ataque informático haciéndose pasar por otros países: el malentendido resultante podría conducir a unas consecuencias que escapan a la imaginación, toda vez que los malentendidos que generalmente siguen a errores de atribución o a la imputación equivocada de una intromisión inocua pueden interpretarse como la preparación de un ataque a gran escala, que podría ser fatal.

Las ambigüedades son múltiples. ¿Objetivos militares? Indudablemente, si los Gobiernos dirigiesen un ataque concreto contra una nación enemi-

[3] Informes recientes acerca de la explotación cibernética por parte de China no solamente demuestran la enorme e indudablemente alarmante dimensión del espionaje cibernético procedente de aquel país, sino también la gran variedad de agentes que lo perpetran: grandes unidades de espionaje que roban borradores de proyectos tecnológicos, estrategias negociadoras, bases de datos corporativas y del Gobierno de los Estados Unidos del tamaño y cantidad de terabytes, los cuales son, en apariencia, oficiales contratados, en parte independientes, y, tal y como estos estudios afirman, están todos, si no conectados, al menos sí coordinados por una unidad del Ejército chino. Esta oscura relación muestra una mezcla de actores e intenciones que pone en duda la definición y convierte en ambivalente el término de «guerra cibernética». Ver: SANGER, David E., BARBOJA, David y PERLROTH, Nicole. «Chinese Army unit Is seen as tied to hacking against US» («Una unidad del Ejército chino es vista como ligada a hacking contra los Estados Unidos»). *New York Times,* 19 de febrero de 2013, y el *Mandiant report* allí citado y ampliamente comentado en otros órganos.

ga, los centros de cibermando podrían ser la punta de lanza de cualquier ataque; las instalaciones militares serían el centro de cualquier ataque, y los modernos sistemas militares centrados en redes serían con toda certeza el centro preferente.

Ahora bien, ¿qué hay del extenso espionaje militar e industrial? Un apunte esquemático de los principales escenarios prueba que el espectro de objetivos es mucho más amplio y que los planificadores militares de hecho incluyen la implicación de, como mínimo, las infraestructuras críticas, así como los sistemas de comunicaciones no militares dentro de sus listas de objetivos, en tanto que muchos de estos tienen un doble propósito.

Los cuatro escenarios más comúnmente mencionados en los análisis político-militares (la ciberguerra de Estonia de 2007, que incluía ataques masivos a instalaciones gubernamentales e importantes mediante una negación distribuida de saturación del servicio, la combinación de ataques cibernéticos y ataques convencionales en el conflicto de 2009 en Georgia, la persistente amenaza de bajo nivel de espionaje militar o la hipotética ciberguerra del «todo apagado» sobre los recursos de defensa, los gobiernos, la economía y las infraestructuras, tal y como lo describe de una forma un tanto sensacionalista en principio, pero a la postre realista, el análisis de Richard A. Clarke[4]) se definen como ataques con multiobjetivos: mitad civiles y mitad militares, y muestran que la ciberguerra en sentido estricto, desde su pura definición, es muy difícil de situar. La validez heurística del término «ciberguerra» y, en consecuencia, el concepto de la misma son muy limitados, por lo que una evaluación integral de conflictos y ciberamenazas resulta inevitable. Es exactamente esta perspectiva integral la que puede demostrar el enorme potencial destructor de un ataque informático de amplio espectro. Este autor no desea entrar en escenarios apocalípticos, pero la literatura que existe sobre posibles «Pearl Harbour» digitales no puede ser despreciada ni minusvalorada[5].

El factor clave que dificulta cualquier esfuerzo para definir la ciberguerra como una categoría distinta de conducta hostil subyace en la propia tecnología digital, ya que los medios de ataque civiles y militares son idénticos; casi siempre de doble uso, con independencia de los motivos u objetivos. Cualquier ataque a las omnipresentes estructuras de red afecta a todos los participantes digitales de forma imprevisible e incontrolable.

[4] CLARKE, Richard A. y KNAKE, Robert K. *Cyberwar. The next threat to national security and what to do about it* (La nueva amenaza a la seguridad y qué hacer con ella). Nueva York: 2010.

[5] Resulta difícil encontrar literatura reseñable que incluya cálculos y estimaciones fiables; no obstante, se puede dar por sentado que los Gobiernos y las instituciones de seguridad poseen amenazas sustanciales, ocultas los ojos del público.

Hasta ahora, uno puede lamentar la ausencia de una investigación sistemática del efecto cascada de un ciberataque militar limitado y de sus repercusiones internacionales; o, lo que es lo mismo, una escasez de predicciones acerca de la utilización básica de las armas cibernéticas[6]. La interdependencia digital entre varios sectores de la economía es susceptible de crear situaciones en las que el fallo de un sector no solamente puede dañar a otro, sino a varios al mismo tiempo, reforzando las retroalimentaciones. Por ello, está claro que el efecto cascada de cualquier ataque sobre los sistemas y estructuras de red en un mundo íntimamente interconectado puede ser enorme y, como quiera que los medios del atacante pueden también ponerse en riesgo, esto determina que, en el mejor de los casos, ese riesgo pueda ser disuasorio[7]. A lo largo de los tiempos, todos los esfuerzos para definir las «armas cibernéticas» han fracasado, aunque se ha conseguido identificar parcialmente algunos instrumentos de *software* dañino.

La realidad es, por consiguiente, que los ciberataques representan un mayor riesgo para la sociedad en su conjunto y para el tejido socioeconómico que lo que indica cualquier variante de las doctrinas, planificaciones y premoniciones militares.

La creciente dependencia de la tecnología digital sitúa a las instalaciones públicas y privadas, los suministros eléctricos, las telecomunicaciones, la banca y el mundo financiero, los transportes, la industria y las instalaciones médicas, la educación y los Gobiernos en la misma situación de riesgo que las instalaciones militares (más en las infraestructuras críticas que se detallan más adelante). Debemos hablar de una exposición integral de riesgos en nuestros países y sus economías. Desde esta perspectiva, las diferencias entre guerra, terrorismo y delitos cibernéticos se tornan borrosas, por lo que parece más adecuado hablar de ataques y

[6] El tan mencionado virus *stuxnet*, un *software* dañino muy sofisticado específicamente orientado a atacar los sistemas *software* de control producido por Siemens (SCADA) de las instalaciones de enriquecimiento nuclear en Irán, quiebra ese efecto cascada, y puede ser el precursor de ataques informáticos quirúrgicos muy precisos. En cualquier caso, los ataques mediante *stuxnet* no estaban orientados contra instalaciones militares y no aparecieron en Internet, sino que se produjeron a través de *pendrives* introducidos furtivamente en una planta en lo que representó más un problema de control de accesos físico y mal comportamiento interno. A este respecto, ver: FAREWELL, James P. y ROHOZINSKI, Rafal. «The new reality of cyber war» (La nueva realidad de la guerra cibernética). *Survival,* agosto-septiembre de 2012, p.107.

[7] El efecto cascada puede ser menos efectivo si los datos, por ejemplo datos militares, se gestionan a través de redes internas, o si otros elementos de segmentación de red han sido instalados. Sin embargo, el aislamiento es solo relativo, y la defensa de redes siempre debe combatir el mismo enemigo invisible. La misma lógica es aplicable con respecto a los presumibles planes de algunos países para operar por fuera de la estructura mundial de Internet, creando fronteras digitales nacionales en una era «ciberwestfaliana». Tales segmentaciones de red nacionales nunca se completarán, y serán, por ello, ineficaces.

conflictos cibernéticos cuando analizamos el amplio patrón de amenazas que crece ahora, y que influyen tan claramente en la economía. En lenguaje popular, la ciberguerra a menudo se ha entendido en amplio sentido como un reflejo del inespecífico y masivo pánico que un ciberconflicto despierta entre la ciudadanía. Estas intuiciones públicas demuestran que la seguridad, o mejor dicho, la inseguridad cibernética se encuentra entre uno de los grandes retos de nuestro tiempo.

Son estos amplios patrones de amenaza lo que más directamente afecta a la economía a través de una perspectiva integrada de riesgos, y en los que este ensayo se centrará a fin de mantenerse dentro del tema general objeto de este libro.

Un análisis realista del riesgo económico requiere un detallado e integrado análisis de todo el espectro de los riesgos cibernéticos, a través del cual, tanto si el objetivo primordial de un ciberataque es alcanzar un beneficio económico como si no lo es, el análisis debe constituirse en una estrategia integrada para combatir los ciberconflictos. La vital contribución que las tecnologías digitales representan en nuestra era, y especialmente en nuestra seguridad económica, depende del funcionamiento, la integridad y la fiabilidad de estas tecnologías, así como de la confianza que inspiran. En consecuencia, la ciberseguridad debe representar un tema central en este estudio, como sucedía en la publicación de 2010 citada anteriormente.

En consecuencia, indagaremos primero la dimensión hasta la que las tecnologías digitales han traspasado ya los segmentos económicamente relevantes de la sociedad. De manera predictiva, analizaremos, siquiera de forma especulativa, las posibilidades de crecimiento y de cambio del mundo digital en los años venideros. El siguiente capítulo se centrará en las vulnerabilidades y la exposición a riesgos generados por este mundo nunca antes tan interconectado y las subsiguientes amenazas de seguridad conforme estas se van generando. A continuación, se realizará un intento de medir los daños económicos resultantes y la escasamente clara relación existente entre ciberataques y ciberdefensa, como por ejemplo en la industria de seguridad.

En la segunda parte de este estudio, se hará hincapié en las contraestrategias, en mitigar los daños, en la prevención y en analizar en su totalidad la panoplia de la defensa digital. Se pondrá un especial énfasis en los aspectos legales, ya que son pocas las provisiones que se han destinado a ejercer un control normativo efectivo sobre la conflictividad cibernética; como mucho, existe una incipiente comprensión de cómo se aplicaría la legislación internacional[8].

[8] Más adelante se podrán encontrar referencias más detalladas al *Manual Tallin sobre la legislación internacional aplicable a la ciberguerra* (*Tallinn Manual on the international*

La cibernética como modelo de cambio del paradigma económico

Cualquier asesoramiento realista sobre amenazas precisa de una revisión panorámica de la tecnología de última generación empleada por actores económicos clave. Las tecnologías de la información y la comunicación (TIC) significativamente se están convirtiendo en el nuevo paradigma que domina todos los aspectos del esfuerzo humano, proporcionando el sistema operativo universal de las sociedades humanas. La tecnología cibernética se ha convertido en una característica que define nuestros tiempos: la casi dependencia total de las TIC proporciona una importancia vital sobre el rendimiento, la robustez, la seguridad, la fiabilidad de los sistemas y redes digitales y la confianza en su funcionalidad e integridad y en la protección de la privacidad. Estas condiciones se convierten en un entramado para el funcionamiento de la sociedad. Por tanto, la seguridad informática se debe considerar como un arquetípico desafío social de proporciones globales.

El progreso y el desarrollo de las TIC que podemos contemplar en la economía y en todos los foros, incluyendo los asuntos militares, son sobrecogedores y justifican ser designados como una segunda revolución digital.

Como ha sido mencionado por diferentes fuentes y estudios, los rápidos avances debidos a la densidad de integración y el desarrollo de circuitos digitales a gran escala que conforman la tecnología base en la era digital continuarán durante al menos una década más. La Ley de Moore, que duplica el desarrollo informático cada 18 años, se mantiene vigente. Como sucede que estos componentes digitales son crecientemente más pequeños y más baratos, algunos de estos componentes, como microprocesadores, sensores y actuadores, se integran en sistemas técnicos o físicos e interconectados a través de una variedad de redes. Según un reciente documento de Manfred Broy, actualmente, alrededor del 98% de todos los microprocesadores van integrados (y son invisibles) y están conectados a través de sensores (por ejemplo, RFID, identificadores de radiofrecuencia), y actúan con el mundo físico y con internet. Como Broy menciona, «... el mundo físico se funde con el mundo virtual del ciberespacio que conduce a sistemas ciberfísicos y a una Internet de las cosas, datos y servicios»[9]. Con más de 2.300 millones de ordenadores en línea y miles de millones de microprocesadores y microordenadores consiguientemente empleados en sistemas integrados, identificadores de radiofrecuencia y otros sensores, dispositivos móviles, tecnologías de red y de banda ancha en crecimiento, ultraminiaturización de circuitos

law applicable to cyber warfare. Cambridge University Press, 2013), el primer tratado minucioso sobre la materia.

[9] «Cyber physical systems» («Sistemas cibernéticos físicos»), parte 1. *IT. Information Technology,* número especial, 6/2012, pág. 255. Múnich: Manfred Broy, 2012. (*Parte 1).*

digitales y la ubicuidad resultante de nuevos elementos informáticos miniaturizados, y el incesante progreso hacia un «Internet de las cosas», con microordenadores insertados en tejidos o en las monturas de gafas, el espectro de una posible amenaza va infinitamente más allá de los ordenadores tradicionales o la actual Internet.

Básicamente, *todos* los dispositivos y redes digitales son vulnerables, y la creciente interconectividad de los sistemas digitales puede causar fácilmente un efecto «bola de nieve» (como ejemplos, la distribución de errores, deficiencias y fallos, o el daño causado por los ciberataques). Y estos son procesos en desarrollo; somos ya testigos de un crecimiento continuo de actores digitales, y de una curva de crecimiento exponencial en la interconectividad, y toda la penetrabilidad que de forma automática dispara un incremento paralelo de las vulnerabilidades.

El fenómeno de la migración de los procesos informáticos (de líneas telefónicas fijas a móviles y a voz sobre IP-VoIP), la gestión de *software* y el almacenamiento de datos desde ordenadores individuales y profesionales a enormes granjas o centros de servidores informáticos (en red en la nube) con capacidad de peta*bytes* y servicios informáticos en la nube –y convergencia– dan como resultado una indistinguible malla de sistemas móviles y fijos que se añaden a una inmensa estructura de redes global en un universo de conectividad .

Sumando los ordenadores tradicionales, los dispositivos móviles y los sistemas integrados –omnipresentes aunque sofisticados microprocesadores, a menudo miniaturizados al tamaño de un terrón de azúcar–, algunos analistas estiman que el número total de sistemas –civiles y militares– interconectados ha alcanzado o está a punto de alcanzar los 50.000 millones. La propensión exponencial de su potencial conectividad mutua, y por ello de su vulnerabilidad a los ciberataques salvo que se encuentren potencialmente protegidos, es difícil de calcular pero, en cualquier caso, es un asunto considerable y preocupante.

El desarrollo de dispositivos móviles es particularmente notorio. Recientes estadísticas indican que la comercialización a nivel mundial de los teléfonos inteligentes o *smart phones* habrá alcanzado los 650 millones de unidades en 2012, que elevarán la base de abonados a móviles a cerca de 8.500 millones en 2016; una cuota de crecimiento anual superior al 7%, con una penetración en el mercado que pronto superará el 100%. La facturación anual del negocio de telefonía móvil asciende aproximadamente a 250.000 millones de dólares[10], cifra que no incluye a otros dispositivos móviles ni al potencial de innovación de todos los sistemas móviles, como tablet PC, o *smart phones* con tecnología 3G. Estos convierten la informática en ubicua.

[10] Cifras de *Portio research report. Smartphone futures 2012-2016.*

En los países de la OCDE y en los mercados emergentes, casi todas las empresas están conectadas a Internet, y un porcentaje cada vez mayor del valor añadido de los negocios puede atribuirse a actividades relacionadas con Internet. Los países en vías de desarrollo se están poniendo al día cada vez más rápidamente, a menudo basándose en tecnologías móviles.

El aparato productivo de nuestras sociedades está ya en gran medida digitalizado. Equipos informáticos conectados por Internet que operan sistemas integrales de intercambio de información entre equipos dentro de las fábricas, a menudo interconectadas por protocolos inalámbricos conocidos como *sistemas de producción ciberfísicos,* y que crecientemente caracterizan los procesos productivos del hoy y del mañana constituyen la base de la cuarta revolución industrial, a pesar de que este desarrollo es aún incipiente. Los sistemas TI conectados a Internet e integrados, como los RFID, se convierten en motores de la innovación, reemplazando los antiguos modos de control y gestión centralizados de la producción por la autoorganización y los ajustes altamente definidos de los procesos.

Las *smart factories,* fábricas inteligentes, van de la mano de las *smart grids*, redes inteligentes para funciones esenciales de servicio público. Una economía energética adecuada debe moverse hacia el uso de redes inteligentes, un control de la producción y el consumo y unos sistemas de mando basados en el funcionamiento de millones de sensores. Los sistemas inteligentes no son, ni por asomo, propiedad de los países de la OCDE: Nueva Delhi ha introducido recientemente redes inteligentes para el mantenimiento energético de la metrópoli.

La *segunda revolución digital* se manifiesta también en el crecimiento cuantitativo del tráfico de datos, sin precedentes. La nueva dimensión en el almacenamiento, transmisión y procesamiento de la información y la nueva disponibilidad de nuevos servicios TIC se hace posible merced al inmenso crecimiento de los centros de datos, *big data* o «grandes volúmenes de datos», coloquialmente conocidos como *la nube,* que se han convertido en una guía principal del crecimiento económico. Los diversos servicios de la nube y su rápido crecimiento –infraestructuras como servicio (IaaS), *software* como servicio (SaaS)– permiten la reducción en la adquisición y mantenimiento del *hardware* y *software* de las empresas, y ofrecen flexibilidad, ahorro y plena disponibilidad de los datos de las empresas desde cualquier punto.

La explosión de la producción de datos es sin duda fomentada por el fenómeno de *la nube.* La computación en la nube es el segmento de las tecnologías de la información con un desarrollo más veloz que hace prever un crecimiento de datos en la nube multiplicado por seis en los próximos cinco años, de los cuales se espera que solo la Unión Europea pueda ge-

nerar unos ingresos adicionales de 600.000 millones de euros y la creación de dos millones y medio de puestos de trabajo a lo largo del proceso.

El mundo cibernético del mañana

Antes de apreciar en su totalidad las amenazas y los riesgos económicos del ciberconflicto, debemos valorar, siquiera de forma resumida, los avances en los desarrollos cibernéticos, a pesar de que predecir es una tarea arriesgada per se. Sin embargo, podemos trazar las líneas maestras conforme se desarrollan a partir de las tendencias actuales, siempre y cuando se construya un acelerador realista. Es seguro asumir que la miniaturización y la penetración de los dispositivos en el Internet de las cosas, basado en el mucho más potente protocolo IPv6 de Internet, avanzarán a un paso mucho más veloz que la ubicuidad y la penetración de la informática invisible, que el crecimiento de los datos se acelerará y que nuevas formas de informática conducentes a distintas y nuevas estructuras de procesamiento en las redes digitales, por ejemplo las redes neurales, evolucionarán.

Contemplaremos el desarrollo de minúsculos ordenadores con potencial de organizarse a sí mismos y capaces de conectarse con otros instrumentos digitales de forma autónoma, de nuevas comunicaciones hombre-máquina (por citar solo algunas de las tendencias informáticas de nueva generación)[11]. Estos desarrollos generarán una ola de continuo crecimiento explosivo de dispositivos digitales, haciendo pequeña la evolución cuantitativa que hemos conocido hasta ahora. El poder informático, especialmente a través de redes y nubes, se está convirtiendo en algo virtualmente ilimitado. La incorporación de modos *inteligentes* de procesamiento en la industria se acelerarán, y las *redes inteligentes,* todavía hoy en fase experimental, serán un componente habitual en el entorno económico.

La disponibilidad de banda ancha y la amplitud de banda se incrementarán hasta dar servicio a sociedades enteras, incluyendo el mundo en desarrollo, con acceso *on line* efectivo y sólido en muchos países del Tercer Mundo, primordialmente con técnicas móviles[12].

Contemplaremos conexiones de fibra de muy alta velocidad y nuevas conexiones inalámbricas de alta velocidad, dos tecnologías que conformarán el futuro próximo de la conectividad. Los aparatos móviles serán más sofisticados y versátiles, servirán como medios de pago sustituyendo a las contraseñas tradicionales e incluso a las tarjetas inte-

[11] Una relación más completa contemplaría los avances de las nanotecnologías, la ciencia material, la tecnología de sensores basados en semiconductores, la formación y gestión de sistemas virtuales, nuevos conceptos arquitectónicos, etc.

[12] Para ver las actuales cifras porcentuales, consultar *OCDE Internet economy outlook 2012 (Panorama económico de Internet 2012).*

ligentes, y tendrán capacidad de recibir televisión de alta definición en cualquier lugar.

Las tecnologías móviles serán tan eficientes que permitirán el trabajo desde casa con pleno acceso a los datos de las empresas como una de sus características normales, cambiando así la estructura laboral y permitiendo ahorros en infraestructuras y en viajes: *bring your own device* (BYOD) o *trae tu propio aparato*, una forma de trabajo en la que cada empleado podrá acometer sus tareas accediendo a datos y gestionándolos desde cualquier lugar, con plena conexión; lo que ya es factible en algunas compañías, y que se convertirá en un procedimiento rutinario. Nada volverá a ser como antes.

El desarrollo de las amenazas. La nueva realidad económica de la inseguridad cibernética

El anterior análisis ha subrayado el actual y el futuro crecimiento de los sistemas y sus actores, que, estando todos interconectados, constituyen el mundo cibernético. Es por ello evidente que la multiplicación de sistemas y de actores son los principales indicadores de las nuevas oportunidades que existen para poner en peligro la ciberseguridad a gran escala en los contextos militar y civil. El crecimiento de los objetos en este ritmo exponencial indica el crecimiento de las amenazas, igualmente exponencial. Debe tenerse presente que *cualquier* objeto digital, si no está protegido, puede ser objeto de un ataque, y si es parte de una red conectada, dispara múltiples potenciales infecciones y profusos daños.

El tremendo proceso de crecimiento que afecta simultáneamente a los sistemas cibernéticos, sus actores y las estructuras de red ha generado el célebre salto de la cantidad a la calidad. A diferencia de los tradicionales delitos informáticos a la vieja usanza, los ciberatacantes de hoy se aprovechan de la creciente dependencia en el día a día que tenemos de las TI y desarrollan estrategias creativas para explotar las vulnerabilidades de los sistemas de información tecnológica.

El cambio resultante no es sino dramático. Las diferentes dimensiones de la oleada de amenazas requieren ser evaluadas en su conjunto. El crecimiento explosivo de los sistemas y la interconectividad –que ya han sido aquí descritos–, la creciente intensidad, sofisticación y diversidad de los modos de ataque y la tecnología de los ataques, así como los cambios radicales en las características de los actores de ciberconflictos, interaccionan entre sí y multiplican los potenciales daños. Con la *segunda revolución digital*, nos adentramos en un nuevo mundo de peligros que hace ver el análisis de la ciberamenaza de, por ejemplo, hace diez años como idílica.

Todas las operaciones en los ciberconflictos tienen en común que intervienen en el funcionamiento de procesos digitales, ya afecten a los datos, a su almacenamiento, su manejo o su transmisión, ya minen la fiabilidad, la autenticidad, la integridad y la privacidad de los datos y los procesos.

Pero los objetivos de un ataque pueden variar; algunos dejan el normal funcionamiento de los sistemas y procesos informáticos intactos, pues su propósito es el de observar y posiblemente copiar (es decir, «robar») datos. Las aplicaciones clave son el espionaje militar e industrial en las que datos e identidades son robados. Si el ataque permanece sin descubrirse por un cierto periodo de tiempo, puede ser perseguido e incluso más datos se pueden recuperar conforme emerjan: el espionaje y el robo de datos apuntan a este tipo de operaciones encubiertas de larga duración, lo que se conoce como *amenaza persistente*, o en el caso de que sea llevado a cabo por un atacante del ámbito del crimen organizado y desarrolle esta actividad de forma sistemática a lo largo del tiempo, se denomina *amenaza persistente avanzada* (APT).

Otros ataques en los que se emplean, por ejemplo, «bombas lógicas» tienen como objetivo alterar o destruir las funciones del sistema atacado, falsificando su efecto (por ejemplo, las instrucciones operativas de un sistema de armamento) o haciéndolo inoperante. Aún más, otros ataques cambian las funciones operativas normales con propósitos abusivos o ilegales durante un cierto tiempo; por ejemplo, en los fraudes bancarios o de tarjetas de crédito, o de modo más permanente, modificando los sitios web. El envío masivo de *spam,* correo electrónico masivo no solicitado frecuentemente con contenidos comerciales y dirigido a un número indiscriminado de receptores, es a menudo empleado para enviar virus y otro *software* dañino como técnica para llevar a cabo robos financieros, de identidades, de datos y de propiedades intelectuales para fraudes o, simplemente, para llevar a cabo *marketing* engañoso.

Las nuevas formas de ataque

Las formas de conflicto que veremos a continuación, junto con sus tendencias de desarrollo y su dimensión evolutiva, pertenecen a alguno de los siguientes supuestos. Como quiera que el propósito de este estudio no es tratar sus características tecnológicas, las referencias se harán con carácter general. La información y las cifras de actualidad han sido recogidas y puestas a disposición por las compañías globales de ciberseguridad Symantec, Norton, McAfee, Microsoft, Kaspersky Labs, Panda Labs y CISCO, entre otras[13]. Además, muchos servicios de seguridad digital na-

[13] *Symantec Internet security threat report, Norton cybercrime report, McAfee threat report.* Estos informes se emiten periódicamente, y en 2011 y, en parte, en 2012 los datos y los desarrollos se encuentran recogidos en sus últimas ediciones.

cionales, como el alemán BSI, el Departamento de Seguridad Interior de EE. UU. y la agencia europea ENISA[14] recogen y a menudo publican datos.

Al tiempo que estas recopilaciones son extraordinariamente reveladoras, deben ser leídas con cierta cautela. Las empresas de seguridad de las TI, si bien son precisas y concienzudas en sus informes, tienden, no obstante, a realzar los peligros de los ataques en su propio interés. Además, las víctimas tienden a minimizar los incidentes sufridos: negocios como los bancos lo hacen para proteger la confidencialidad de sus operaciones, los particulares lo hacen por vergüenza o por la ausencia de interlocutores y los servicios nacionales de seguridad lo hacen especialmente cuando se trata de redes informáticas relacionadas con secretos militares, sistemas armamentísticos o cuando se ha violado algún dispositivo crítico de seguridad.

Pero es exactamente el aprovechamiento de las posibilidades de espionaje lo que ha mostrado últimamente uno de los factores de crecimiento más altos. Como el acceso a los sistemas de seguridad de los estados, las organizaciones y las empresas encuentran cada vez barreras más franqueables junto a la ubicuidad de las técnicas empleadas para acceder a estos datos, muchas de ellas desarrolladas por organizaciones criminales; es evidente que algunos estados hacen un uso cada vez más agresivo del ciberespionaje.

Existe información detallada de las operaciones cibernéticas de China en EE. UU., en las cuales los intrusos se concentran en infraestructuras corporativas clave con vistas al robo de propiedad intelectual[15].

Durante muchos años, China ha estado practicando espionaje nuclear, recopilando información altamente clasificada sobre largas y documentadas listas de cabezas nucleares, al tiempo que accedían a redes de altas instituciones de defensa y financieras. La forma más común de penetración es a través de ataques con troyanos, en los que se introduce un virus con instrucciones de recoger datos por amplios períodos de tiempo sin ser detectado por los sistemas operativos del objetivo. A la vez que las operaciones de explotación cibernética desarrolladas por China han recibido una publicidad especial por causa de su amplitud y agresividad, todo el resto de grandes potencias también se ven envueltas en intensas batallas de espionaje. Por el momento, los virus con funciones de espio-

[14] Informes de ENISA, como el *ENISA Threat landscape: Responding to the evolving threat environment,* de enero de 2013, que destaca por su amplia base de datos, que incorpora hallazgos de la mayoría de otros informes, y por sus sistemáticos y definitorios análisis de los diferentes tipos de riesgos y amenazas.

[15] Wikipedia, «Chinese intelligence operations in the US». *IISS Strategy Survey 2012, Intelligence agencies and the cyber world,* p. 33. Ver también INKSTER, Nigel: «Chinese intelligence in the cyber age». *Survival,* febrero-marzo de 2013, p. 45. Ver también nota 3 más arriba.

naje disfrutan de un ciclo de negocio positivo; últimamente, las variantes de *spylware madi* y *flame* se han hecho especialmente prominentes[16]: su aspecto muestra que incluso *spylware* relativamente simple es capaz de obtener información muy valiosa y sensible a gran escala. Desde las redes de espionaje manejadas por estados con alta penetración de troyanos, solo queda un paso para el ataque directo, la degradación de los sistemas armamentísticos y el sabotaje, por ejemplo a través de bombas lógicas durmientes, a pesar de que estas deben ser capaces de resistir la vigilancia y la constante actualización de *software* de la parte a la que se pretende atacar a corto plazo.

Todos los informes de las empresas de seguridad convienen en sus últimas ediciones que los ataques malintencionados continúan creciendo con rapidez y, según McAfee, actualmente han alcanzado el mayor punto de todos los tiempos en el quebrantamiento de bases de datos. Al mismo tiempo, existe una creciente sofisticación en los ataques y en el desarrollo de *software* dañino.

El software orientado a los dispositivos móviles se ha convertido en un nuevo foco de los ataques, y se ha casi duplicado en un período de un cuatrimestre.

Con el creciente número de vulnerabilidades en el espacio móvil subiendo –Symantec ha detectado un crecimiento de un 93% en un año– y los diseñadores de *software* dañino creando *software* orientado hacia las oportunidades de los móviles, 2011 fue el primer año en que el software dañino constituyó una amenaza tangible para empresas y consumidores, teniendo en cuenta que los trabajadores tienden a introducir sus *smart phones* y *tablets* en el ambiente laboral más rápidamente de lo que las empresas pueden garantizar su seguridad y gestión. BYOD representa unos enormes y nuevos retos de seguridad, y puede conducir a un posterior aumento a largo plazo de los quebrantamientos de datos. Los nuevos desafíos para los móviles se diseñan para actividades que incluyen la recopilación de datos, el envío de contenidos y el rastreo de los usuarios.

Existen saltos cuantitativos en todas las categorías de modos de ataque. Symantec por sí sola bloqueó más de 5.500 millones de ataques dañinos, con un incremento de un 81% respecto del año anterior. Además de ello, el número de variantes de *software* dañino aumentó hasta 403 millones en ese período.

[16] El virus *duqu*, a menudo citado en el contexto *flame*, reúne también excelentes propiedades para el espionaje y el robo de datos, pero es sustancialmente más complejo y está posiblemente relacionado en su estructura y orígenes con *stuxnet*. Su objetivo primordial es controlar *software* como SCADA. *Duqu* desaparece de los sistemas afectados en 36 días, lo que complica su detección.

El daño financiero a los bancos y a los clientes particulares (fraude con tarjetas de crédito, *phishing* y *carding, spearphishing*, extorsión financiera directa) continúa creciendo rápidamente. El pasado año, los delincuentes informáticos montaron un sistema automatizado de transferencias (ATS) que se empleó para atacar a instituciones financieras europeas y que estaba orientado a atacar una gran institución financiera multinacional de EE.UU. La «transferencia de dinero por móvil» (MMT), un término trampa para noveles sistemas financieros digitales que prestan servicios bancarios a millones de personas en el Tercer Mundo, mostrará, si no se regula rápida y eficientemente, el «lado oscuro» de las finanzas cibernéticas, y se convertirá en el terreno de juego para los ataques y el delito cibernéticos[17].

Dada la aún perdurable cuasimonocultura de los sistemas operativos en los que un productor domina el mercado, las vulnerabilidades que son inherentes a sus productos están ampliamente extendidas y, si se explotan, conducen a sustanciosos daños. La principal fuente de distribución de virus informáticos son, por consiguiente, los inocentes usuarios de ordenadores personales, y aquellos ordenadores de empresa cuyos operadores a menudo no son conscientes de los riesgos que comporta la red.

Los ataques con virus también han sido enormemente facilitados por la enorme presencia de «nuevas redes sociales» que operan como distribuidores gratuitos de la infección. Yendo más allá de los ataques de *spam,* los ciberdelincuentes se han orientado hacia estas redes sociales. Su apariencia muy inocente hace que los usuarios den –erróneamente– por sentado que no corren riesgos, y los atacantes están empleando estos sitios para apuntar a nuevas víctimas. Debido a las técnicas de ingeniería social y la naturaleza vírica de las redes sociales, es mucho más fácil que una amenaza se traslade de una persona a la siguiente. A pesar de todo, aunque el *spam* está ahora mejor controlado por los filtros anti*spam* de los proveedores de servicios de Internet y, además, en muchos países sujetos a legislación anti*spam,* este está todavía desenfrenado: en 2010, más del 86% del tráfico en Internet (62.000 millones de mensajes diarios globalmente) eran *spam* (con un porcentaje ligeramente inferior en 2011, un 75% que representó 42.000 millones de mensajes)[18], lo que supone que, al inundar las cuentas de Internet, causa un daño apreciable en tiempo de producción perdido, aparte del potencial existente para difundir los ataques de virus.

[17] BRONK, Christopher, MONK, Cody y VILLASEÑOR, John. «The dark side of cyber finance». *Survival,* abril-mayo de 2012, p. 129. Un virus específico, *gauss,* apunta a las transacciones financieras, pero existen otros.

[18] Cifras de Symantec. El *spam* puede haber crecido menos velozmente, también porque existe una mayor presión sobre los *spammers*; algunos *botnets* enormes especializados en *spam* se han retirado en los dos últimos años. Por el contrario, el contenido del *spam* delictivo se ha hecho más sofisticado.

Existe otro movimiento indiscriminado ajeno al *spam*: los atacantes individualizan sus ataques, centrándose en aquellas víctimas sobre las que han acumulado y procesado conocimientos a través de datos y robos personalizados. Un método de individualización es el *spear phishing:* el término denota un ataque vía correo electrónico orientado hacia personas que se sabe que frecuentan determinados negocios *on line* y de las que pueden poseer información relevante sobre cuentas bancarias, negocios concretos o cadenas de distribución. Se denominan así porque el movimiento hacia el objetivo es preciso y estrecho, como la punta de una lanza.

A pesar de que los datos de tarjetas de crédito no se pueden robar, las direcciones de correo electrónico se encuentran comprometidas y pueden ser vendidas en el mercado negro. Más aún, la información recolectada a través de *spear phishing* puede generar ataques de *phishing* más sofisticados a otros usuarios actuando sobre mensajes aparentemente legítimos procedentes de un minorista o un banco con el que mantengan relaciones comerciales. Los ataques dirigidos se orientan de manera creciente hacia pequeñas empresas, pues estas pueden estar peor protegidas u ocupan puestos importantes en determinadas cadenas de suministros.

Al mismo tiempo, el código dañino está cada vez menos programado para causar daños directos irreparables. Por el contrario, los atacantes tratan de someter bajo su control a los ordenadores para así poder continuar afectándolos a través de infecciones con troyanos y control remoto.

Un elemento importante y efectivo en esos esquemas son los ataques mediante DDoS (denegación de servicio distribuida). En este método de ataque, el atacante inunda al servidor con paquetes de datos inservibles para, de esta manera, sobrecargar los sistemas con el fin de provocar interrupciones comerciales en los sistemas y las estructuras de red de la víctima. En el contexto empresarial, tales ataques se pueden desencadenar por parte de competidores, personal insatisfecho o grupos de personas motivadas por otras razones. Obstruir masivamente la fluida operatividad de los sitios de red puede dar como resultado considerables consecuencias económicas, especialmente en empresas que hagan uso o estén basadas en el comercio electrónico. En escenarios de conflictos militares o políticos, los ataques DDoS –un elemento central del ataque ocurrido en Estonia en 2007, en el que, sin embargo, el daño económico fue menor– pueden paralizar instalaciones de defensa y comunicaciones y neutralizar o destruir sistemas armamentísticos, paralizar servicios gubernamentales, provocar fallos en infraestructuras críticas y sectores económicos y también, en consecuencia y en casos extremos, conducir a la pérdida masiva de vidas.

Mientras que los últimos informes de las empresas de seguridad apuntan a las nuevas amenazas, los dispositivos móviles –y a través de ellos todo

el universo interconectado– aún no han cuantificado las nuevas vulnerabilidades que surgen del explosivo crecimiento de los centros en la nube.

Más allá de la amenaza a los móviles, la inseguridad causada por la migración masiva de datos a la nube ha sido en los últimos tiempos un tema candente en discusiones sobre seguridad, como lo demuestran las palabras de un informe de 2009 de ENISA[19]: «Las concentraciones masivas de recursos y datos suponen un objetivo más atractivo para los atacantes», a pesar de que la agencia cree «que las defensas basadas en la nube pueden ser más robustas, escalables y coste-efectivas».

Esta lista de nuevos modos de ataque supone la emergencia de una amplia serie de nuevos y sofisticados programas de *software* destructivo que aparecen con una inaudita rapidez y sofisticación[20] y con precisión sobre los objetivos. Por descontado, las fronteras nacionales no son ya relevantes ante este tipo de amenazas, y resulta imposible circunscribir la protección de las tecnologías de la información y sus infraestructuras a las políticas nacionales. Los autores, vendedores y beneficiarios de los virus informáticos y otros códigos dañinos, operan globalmente, por lo que la defensa digital debe operar de igual modo.

El nuevo enemigo: actores colectivos del ciberconflicto

La delincuencia en Internet se conduce cada vez más de una forma profesional y comercial. Los ataques a objetivos son cada vez más frecuentemente realizados por delincuentes organizados. Los intereses financieros son la fuerza motriz. Los ciberconflictos se están convirtiendo en una poderosa rama de la escena internacional de la delincuencia organizada. Los consorcios de delincuentes comandan ejércitos de expertos cibernéticos y generadores de *software* dañinos, que sistemáticamente organizan campañas lucrativas de delincuencia organizada. Tras años de operar, han constituido equipos profesionales para el desarrollo de *software* dañino sofisticado, beneficiándose de los recursos generados por la delincuencia masiva. Esto da lugar también a ataques de magnitudes nuevas. Ya en 2004, el 16% de las actividades de *hacking* se orientaban contra empresas de comercio electrónico; esto representó un incremento de un 400% con respecto al año anterior, pero desde entonces, el *hacker* que operaba solo ha desaparecido en las tinieblas y las organizaciones han tomado el relevo.

---

[19] *Cloud computing: benefits, risks and recommendations for information security*. Noviembre de 2009, www.enisa.europa.eu.

[20] Un ejemplo es una nueva tecnología para segmentar el *software* dañino en minúsculos paquetes de datos que irrumpen en el sistema objetivo desconocidos por los cortafuegos y los sistemas antivirus, pero que se reconstruyen automáticamente una vez que han entrado en el sistema.

Estas sistemáticamente introducen troyanos en grandes cantidades de ordenadores, cada vez más, y también en dispositivos móviles, y de este modo tienen miles, incluso millones de equipos bajo su mando en los que pueden activar *software* dañino y emplearlo para sus ataques: las *botnets* –el término procede de las palabras robot y *net*– están creciendo.

Estos conjuntos de *ordenadores zombis* poseen distintos usos. Sus operadores, conocidos como *botherders*, pueden proceder directamente a generar dinero o bien a recoger inteligencia de espionaje, datos comprometedores o robos de identidades. Las *botnets* aportan una infraestructura efectiva y en creciente uso para distribuir programas de espionaje en una amplia gama de variantes, y a hacer negocios a través de bancos *on line.* Las *botnets* son la plataforma ideal para ataques DDoS, pues estos últimos precisan de un gran número de emisores de correo electrónico activos para alcanzar el deseado efecto de saturación a gran escala.

Las *botnets* pueden ser también alquiladas a otros delincuentes, o a Gobiernos, como mercenarios digitales, creando una opaca amalgama de actores estatal-no estatal. No son la única mercancía del mercado negro disponible para delincuentes y Gobiernos por igual; inmensos paquetes de *software* para ataques agresivos, de direcciones de correo electrónico y números de tarjetas de crédito están disponibles a precios casi de ganga. Tampoco hay escasez de zombis: se estima que uno de cada diez correos electrónicos están afectados por virus importantes y, en consecuencia, los *botherders* pueden sumarse en manadas, funcionando sin el conocimiento de sus propietarios. Ya en 2010, McAfee estimó que el número de ordenadores zombi crece alrededor cinco millones al mes.

En los mejores tiempos del virus Conficker, que era y es capaz de añadir de forma autónoma nuevos ordenadores a la *botnet,* la dimensión de tan solo esa red puede haber alcanzado a más de 10 millones de dispositivos. Sin el empuje que aportan los nuevos actores colectivos, este crecimiento sería inconcebible.

Un aspecto alarmante del nuevo escenario de delitos informáticos es la antes citada proeza técnica y financiera para desarrollar *software* dañino por delante de las ciberdefensas, y a pesar de la indudable eficiencia de la industria internacional de seguridad digital. Al mismo tiempo, la dependencia digital de las sociedades modernas es creciente, pues las infraestructuras son cada vez más dependientes de la red (por ejemplo las redes inteligentes). Incluso el aspecto estrictamente numérico es de por sí preocupante: los informes de McAfee indican que las variantes identificadas de *software* dañino se multiplican cada año por cinco.

En consecuencia, el eterno dilema entre ataque y defensa cobra un nuevo significado, especialmente a causa de estos nuevos operadores colectivos en el ciberespacio, y los defensores de un ciberespacio libre de

delitos no siempre prevalecen[21]. El potencial de ataque de estas fuerzas perversas y organizadas también da una idea de las posibilidades de una ciberguerra real si los estados y la delincuencia organizada cooperan.

Existen diversos análisis con teorías sobre los países o lugares de residencia de estas organizaciones delictivas y que se basan en parte en la URL de los mensajes atacantes. Sin embargo, habida cuenta de las ilimitadas posibilidades de saltar de una estación a otra y las entradas procedentes de varios países emisores, este estudio omite tales atribuciones.

Con todos estos desarrollos ha quedado evidentemente claro que el término *seguridad* ha alcanzado un significado completamente nuevo y una nueva dimensión en el ciberespacio: las fronteras nacionales ofrecen hoy menos protección que nunca antes. Conceptos tales como seguridad interna y externa resultan crecientemente difíciles de definir y, en muchos casos, pueden fundirse.

El ciberterrorismo puede también subsumirse bajo las nuevas amenazas colectivas. Bajo la definición más extendida, el terrorismo digital denota el empleo de ataques vía Internet por grupos ideológicos y políticos que apuntan hacia una quiebra a gran escala de los sistemas y las redes, generando potencialmente destrucción, alarma y pánico. Si el objetivo de estos terroristas no es conseguir un beneficio económico, no estarían de forma genuina dentro del contenido de este estudio. Si son motivos económicos, por ejemplo obtener fondos para la financiación de actividades terroristas, significa que esencialmente no son distintos de otros activistas criminales y solo formarían parte del ciberconflicto integral y del panorama de amenazas aquí descrito. En ningún caso esto significa que se trivialicen los peligros que representan, especialmente en los ataques contra infraestructuras críticas, y por ello están con todo derecho dentro de los objetivos de los Gobiernos en sus campañas antiterroristas y de seguridad en general[22].

Medir el coste del ciberconflicto: ¿es posible cuantificarlo?

Varias empresas internacionales de ciberseguridad periódicamente acometen poner un precio al daño económico global causado por el conflicto digital de acuerdo con sus propias actividades y predicciones.

[21] «Hay, y siempre habrá, una carrera permanente en el ciberespacio entre los atacantes y los defensores. Desgraciadamente, en este momento los atacantes van un paso por delante» –*ENISA Threat Landscape,* enero de 2013, antes citado.

[22] CANDAU ROMERO, Javier. «Estrategias nacionales de ciberseguridad. Ciberterrorismo». En: *Ciberseguridad, retos y amenazas a la seguridad nacional en el ciberespacio. Cuadernos de Estrategia,* n.º 149. Madrid: Instituto Español de Estudios Estratégicos, 2010.

El *Informe Norton de ciberdelitos* (*Norton cyber crime report 2012*) estima que las pérdidas financieras inmediatas alcanzan los 110.000 millones de dólares anuales en 24 países (Symantec alcanza los 114.000 millones), con 556 millones de víctimas afectadas; pero si se añaden a ello los fondos correspondientes al tiempo invertido en tratar de encontrar respuesta a los incidentes y resolver los delitos informáticos, la cifra alcanza aproximadamente los 390.000 millones de dólares.

Cualquiera que sea la metodología exacta para calcular estas cifras, es cierto que con independencia del número de países que esta cubra, el coste de los daños a largo plazo y la interrupción de los negocios, el dinero gastado directamente en responder a los incidentes y el daño causado a la reputación de las empresas no han sido totalmente considerados, y si así lo fuera, en todos los países alcanzaría importantes proporciones adicionales. Además, y como se ha señalado anteriormente, cualquier estadística sobre daños habrá de incluir el inmenso número de casos de ataques no identificados ni evaluados[23].

Tampoco parece que se cubran medidas preventivas y de defensa. Si tomamos como ejemplo los esfuerzos del Gobierno de EE. UU. por realzar sus capacidades en ciberseguridad (protegiendo infraestructuras críticas, operaciones de seguridad informática, compartiendo información y análisis, etc.), la asignación presupuestaria para el Departamento de Seguridad Nacional únicamente para estos fines asciende a 1.200 millones de dólares para el año fiscal de 2013[24], seguro que menos que el sector privado, donde todas las empresas incluidas deben invertir en seguridad y vigilancia cibernéticas. Se deben extrapolar estas cantidades a la comunidad internacional en su conjunto. La industria de la ciberseguridad por sí sola supone un negocio de miles de millones de euros o de dólares.

Calcular los presupuestos para salvaguardar instalaciones militares, sistemas de comunicaciones y armamento será incluso más difícil. Pero es evidente que la disponibilidad y mantenimiento de las propias comunicaciones militares y las estructuras de mando, junto con la capacidad de neutralizar acciones militares hostiles (ciberdefensa), deben ser contempladas –y lo son– en los cálculos y la planificación.

---

[23] La Comisión Europea, a través de su vicepresidenta Neelie Kroes, contempla en la actualidad que las empresas tengan la obligación legal de denunciar los ciberataques (*News agencies*, 26 de noviembre de 2012). La Comisión Europea prepara una directiva en este sentido. En los países de la UE, más de 40.000 empresas deberían cumplir con la obligación de informar. Esta iniciativa ha encontrado resistencia por parte de las industrias y los proveedores de servicios de información tecnológica. ENISA ha estimado que el 25% de los ataques en la UE y los EE. UU no se denuncian ante las autoridades legales. Para consultar una iniciativa reclamando la denuncia voluntaria por parte de las empresas, ver nota al pie n.º 55 más adelante.

[24] www.dhs.gov.

Considerando las incertidumbres de los cálculos, no sorprende que no se disponga de cifras globales fidedignas. No obstante, en la reciente primera Cumbre Mundial de Ciberseguridad organizada por el East-West Institute en Dallas, Texas, en 2010, portavoces autorizados valoraron el daño total de la inseguridad cibernética en alrededor de un billón de dólares anuales, y es esta la cifra estimada que desde entonces se ha barajado sin que haya habido serias objeciones. En la misma línea de magnitudes, un portavoz autorizado de la Cámara de Representantes de EE. UU. ha estimado que las pérdidas anuales causadas por el ciberespionaje –presumiblemente causadas por intrusos chinos– han alcanzado los 300.000 millones de dólares en 2012, sin pormenorizar las cifras[25]. En el Foro Económico Mundial de Davos 2013, se ha considerado como cierto que a lo largo de la próxima década existe un 10% de posibilidades de que se produzca un apagón digital de primera magnitud –de origen presumiblemente delictivo– que alcanzará el cuarto de billón de dólares[26]. Estas cifras, y al menos su orden de magnitud, son enormes.

Mientras que *la primera parte* ha analizado las actuales y futuras ciberamenazas y su enorme coste económico y ha subrayado el hecho de que una situación de riesgo integral requeriría también una respuesta integral y extensa, esta *segunda parte* se centrará en combatir los ciberconflictos, el desarrollo de estrategias para la ciberdefensa y el diseño de estrategias para mitigar las consecuencias.

Los límites legales a la ciberguerra *stricto sensu*

Pese a que hemos encontrado el concepto de ciberguerra ambiguo y de dudosa importancia para este análisis de riesgos económicos, se enumera un breve resumen de las restricciones del derecho internacional sobre acciones cibernéticas hostiles, pues estas pueden limitar la potencialidad de los daños.

El derecho internacional, y especialmente el derecho que rige los conflictos armados, precede a la era cibernética, pero dado que el ciberespacio es cada vez más considerado como un nuevo teatro de operaciones bélicas, se acepta generalmente que el *jus ad bellum* (el derecho sobre el empleo de la fuerza) y el *jus in bello* (el derecho en la guerra), adaptados adecuadamente, también gobiernan las hostilidades en el ciberespacio. Existe abundante literatura académica sobre las analogías que pueden y deben extraerse de la Carta de las Naciones Unidas, las Convenciones de La Haya y Ginebra, las Convenciones del Comité Internacional de la Cruz Roja, los protocolos adicionales y otros tratados sobre el derecho

[25] Artículo en *El País* y prensa de EE.UU., 21 de febrero de 2013.

[26] Citado por la vicepresidenta Kroes en la Conferencia sobre la Ciberseguridad Global en Bruselas, el 30 de enero de 2013.

humanitario, resoluciones de la Asamblea General de las Naciones Unidas anunciando principios generales de conducta para los países, la jurisprudencia internacional existente y el derecho consuetudinario internacional. Algunos Gobiernos han publicado manuales y estrategias que también definen restricciones, pero que igualmente proporcionan las bases para enormes inversiones en armamento cibernético. Gran parte del debate se centra en las definiciones de «ataque» y «ataque armado», pero también en las definiciones cibernéticamente adecuadas, asentadas sobre los principios de las leyes de los conflictos armados (necesidad, distinción, proporcionalidad, no discriminación, prohibición de atacar objetivos civiles y a ciertas personas, objetos y actividades, neutralidad, etc.)[27]. Los puntos de vista expresados abarcan desde la aceptación de amplias opciones de ataque, en las que apuntar a infraestructuras críticas se considera dentro de los márgenes de la legalidad[28], a interpretaciones más restrictivas[29].

No tiene sentido discutir estas diferentes perspectivas a la vista de que el principal trabajo de referencia es ya claramente el recientemente publicado *Tallinn manual on the international law applicable to cyber warfare*[30] (*Manual Tallin sobre la legislación internacional aplicable a la ciberguerra*) elaborado por el Grupo Internacional de Expertos invitado por el CCDCOE, Centro de Excelencia de Ciberdefensa Cooperativa de la OTAN. Este pormenorizado tratado busca establecer 95 «reglas» que puedan cubrir los principios de *jus ad bellum* y *jus in bello* para los ciberconflictos de forma exhaustiva.

El Manual posee un mérito obvio: la prestigiosa reunión de coautores propone bajo el régimen internacional de *lege lata* (según la ley existente) definiciones y reglas plausibles, y pone fin a muchas viejas controversias. Sin embargo, al tratar sobre las relaciones entre civiles y militares y al tratar de definir los valores de ambos así como debatir sobre la no

27 Para un resumen de estos asuntos, ver WESTBY, Jody R. «A call for geo-cyber stability», *en* la Unión Internacional de Telecomunicaciones (UIT) (Hamadoun Touré y el Panel Permanente de Seguimiento de la Seguridad de la Información, Federación Mundial de Científicos), *The quest for cyber peace,* Ginebra: UIT, 2011, pág. 66. En la misma publicación, ver: BARLETTA, G. A., BARLETTA, W. A. y TSYGICHKO, V. N. «Cyber conflict», pág. 53.

28 Para una evaluación prudente, que incide en la complejidad de diseñar las líneas en el debate sobre el uso de la fuerza, ver WAXMAN, Matthew C. «Cyber attacks and the use of force: Back to the future of art. 2(4)» («Los ataques informáticos y el uso de la fuerza del art. 2(4)»). *The Yale Journal of International Law*, vol. 36, 2011, p. 421.

29 AMATO, Anthony D. «International law, cybernetics and cyberspace» («Derecho internacional, cibernética y ciberespacio»). *76 International Law Studies,* 1999, pág. 59. En esta obra el autor predijo que «los ataques en Internet pronto serán vistos como claramente ilegales desde la legislación internacional y la legislación internacional consuetudinaria puede haber alcanzado ya ese punto»; pero ciertamente los desarrollos desde entonces no han ido por ahí.

30 Ver nota 7 al pie, más arriba.

discriminación, etc., han de admitir que las «armas» cibernéticas «por su propia naturaleza causan efectos que son imposibles de controlar y que, por ello, se pueden extender de forma incontrolada a ordenadores civiles, así como a otros ordenadores protegidos y a redes informáticas, creando una cadena de efectos incontrolables» (pág. 122), y que los objetivos más susceptibles de serlo, especialmente infraestructuras críticas y cibernéticas, son de doble uso, y que el ataque sobre las mismas origina más «daños colaterales» de aquellos que deben asumirse en un conflicto convencional.

¿Podría una infraestructura crítica de uso mixto, militar y civil, ser objetivo si apoyase a otros objetivos protegidos por las Convenciones de Ginebra? El Manual parece otorgar preferencia a los propósitos militares. Reglas tales como «la población civil como tal, así como los individuos civiles, no serán objeto de ciberataques» (regla 32) podrían, de este modo, perder su efecto protector. Las reglas 14 y 55, que especifican que las operaciones cibernéticas en legítima defensa deben ser necesarias y «proporcionadas», se empañarían si, por defecto de control sobre las mismas, la proporcionalidad sobre las mismas no pudiera medirse de forma fidedigna. Otras incertidumbres son las relativas a actores ocultos –no estatales–, al estatus de combatiente, a la definición de «objetos económicos que sostienen la guerra», la neutralidad y la autodefensa anticipativa: ¿cuándo podría ser considerado como inminente un ciberataque lanzado a velocidad del rayo?

Los autores han sido más afortunados al definir «ataque» y «ataque armado», empleando la regla de los «efectos» en el segundo caso (el hecho de que una operación cibernética constituya o no un ataque armado depende de su magnitud y sus efectos, regla 13)[31]. No obstante, incluso aquí las ambigüedades son alarmantes. La regla de «ataques armados» es tan amplia que reduce las barreras hacia la guerra; no es prudente y sí peligroso para la estabilidad internacional tratar conflictos que no supongan un riesgo evidente para las vidas humanas o un elemento de trastorno social como «ataques armados», con las consecuencias que ello conllevaría bajo el derecho internacional[32].

[31] El Manual también deja claro que no todos los ciberataques transfronterizos, ni tan siquiera aquellos dirigidos desde un Estado, constituyen una violación de la legislación de conflictos armados o, en general, de las leyes internacionales. Así pues, el ciberespionaje en tiempos de paz o en conflictos armados no está previsto en la legislación internacional (excepción hecha de casos especiales, por ejemplo, cuando se es indiferente a la inviolabilidad de los archivos y las comunicaciones diplomáticas). Uno de los elementos importantes de los ciberconflictos, la intrusión masiva en sistemas digitales con propósitos de espionaje, una amenaza avanzada persistente (APT), debe por ello ser juzgada bajo las leyes cibernéticas y sanciones nacionales, tal y como define la Convención de Budapest.

[32] BARLETTA, BARLETTA y TSYGICHKO, *op .cit.,* pág. 60.

En su conjunto, el Manual, lejos de limitar la opción de la ciberguerra cibernética, más bien subraya las grandes posibilidades de los ciberataques y el daño incontrolado que estos pueden infligir. Se han estipulado muy pocas restricciones: al contrario, las incertidumbres y el riesgo para las estructuras cibernéticas civiles se hacen más obvias. Esto se refiere específicamente a las infraestructuras críticas nacionales, que no solamente están mayoritariamente en manos privadas, o lo que es lo mismo, configuran buena parte de las economías nacionales, sino que indirectamente penetran en el tejido social, tanto que las economías dependen cada vez más de ellas. Los ataques cibernéticos sobre estas estructuras no solamente generan daños económicos masivos, sino que además comprometen seriamente la seguridad de la sociedad, poniendo en peligro la vida humana.

Más importante aún es que el Manual acepta la opción de la guerra en el ciberespacio de forma irreflexiva, y elude la cuestión sobre si el desenfrenado armamento cibernético que se prevé emplear en el futuro es un sabio camino a emprender por las naciones civilizadas. Naturalmente, el Manual comienza por asumir la afirmación subyacente de que hostilidades cibernéticas patrocinadas por los estados respetarán las directrices de Naciones Unidas y solo serán empleadas en legítima defensa. No obstante, la impresión final es que la transferencia al por mayor de la legislación tradicional sobre conflictos armados y el pensamiento en términos militares termina siendo un pretexto de legitimidad para las ciberguerras del futuro, y se desentiende del enorme dinamismo de los desarrollos digitales así como de la creciente vulnerabilidad social, con lo impredecible de sus consecuencias.

Una interpretación similar se puede detectar en los manuales cibernéticos que muchos Gobiernos han preparado, en la medida en que son públicamente accesibles.

Algunos países están incorporando capacidades ofensivas cibernéticas dentro de las estrategias bélicas convencionales, previendo respuestas militares convencionales o sabotaje a la información en Internet, incluso con independencia de que se produzca un «ataque armado» o bajas humanas. Otros reclaman el uso ilimitado de armas cibernéticas («explotar el potencial completo», «efecto máximo», «procesos de fuego conjunto», «represalia», «golpe de castigo»...) que indican que sus planeamientos siguen líneas militares («doctrina de combate») con sus correspondientes analogías y esquemas de pensamiento[33]. Sin embargo, conceptos como disuasión, represalia o reglas de enfrentamiento no tienen en cuenta la

[33] Una breve lista de las varias «modalidades de ciberguerra» ha sido ofrecido por el secretario general de la Unión Internacional de Telecomunicaciones, Touré, en «The international response to cyber war», *en The quest for cyber peace* («La respuesta internacional a la ciberguerra», en *La búsqueda de la ciberpaz*), *op. cit.* pág. 86.

especificidad de los ataques cibernéticos ni, por ejemplo, los problemas de atribución y proporcionalidad.

Afortunadamente, estos conceptos no permanecen sin contradecirse. El potencial de destrucción y la imprevisibilidad de las opciones de ciberataques son cada vez más reconocidos, y han matizado el punto de vista puramente militar o se encuentran yuxtapuestos al mismo. En muchos documentos de doctrina militar y política, la prevención de la ciberguerra, la priorización de la ciberdefensa y la cooperación de todos los agentes interesados están ahora avanzando hacia un primer plano. Un ejemplo interesante es la Estrategia de Operaciones en Ciberguerra del Departamento de Defensa de EE. UU., de julio de 2011, que opta claramente por la defensa digital, la estrecha colaboración entre agencias gubernamentales, el Gobierno y la industria y la cooperación internacional.

Documentos de la cumbre de la OTAN como la Declaración de Lisboa de 20 de noviembre de 2010 no ocultan las necesidades de defensa, y sin embargo, ponen especial énfasis en la protección cibernética central y en la optimización de la ciberdefensa colectiva y la alianza interna, así como en la cooperación internacional (§ 40). Es también significativo que los ciberataques no están subsumidos dentro del concepto de ataque recogido en el art. 5 del Tratado de la OTAN, sino más bien se menciona en el contexto del régimen consultivo contemplado en el art. 4[34].

Esto indica que el control de los ataques digitales está claramente admitido en muchos sectores como parte esencial de un nuevo paradigma de seguridad que coloca al frente la prevención, la resistencia y el fortalecimiento de infraestructuras digitales amenazadas, y a un entramado de nuevas y amplias redes de cooperación en defensa.

Como este artículo fundamentará más adelante, este movimiento hacia una posición defensiva debería llevarnos a introducir el concepto de ciberpaz como principio de una conducta pacífica en el ciberespacio.

Optar por el lado positivo de la antinomia guerra-paz implica un cambio importante en la perspectiva y la escala de prioridades, ya que orienta la

[34] Otro buen ejemplo de este emergente instinto de prudencia puede encontrarse en los informes actuales sobre un proyecto de directiva presidencial de los EE. UU. que incorpora disposiciones legales relativas a las Fuerzas Armadas en la defensa o la represalia contra un ciberataque importante, respetando plenamente el derecho internacional. Estas normas supuestamente otorgarán al presidente amplios poderes, incluso para un ataque preventivo, pero a la vista de las consecuencias y los problemas de atribuciones, reflejan también una actitud de moderación sustancial, excluyendo la represalia «automática» y reservando la prerrogativa del presidente para ordenar ataques en su condición de comandante en jefe. SANGER, David E. y SHANKER, Tom. «Broad powers seen for Obama in cyberstrikes». *New York Times,* 2 de febrero de 2013. Ver también CONDLIFFE, Jamie E. «Obama has signed a secret directive to stymie cyber attacks». *Washington Post,* 15 de noviembre de 2012.

mentalidad hacia los beneficios y el potencial positivo de la sociedad de la información y aporta un objetivo en este sentido, denunciando la connotación negativa de la ciberguerra y de los términos y calamidades afines –podríamos decir que la deslegitiman– y fomentando el movimiento dinámico hacia una cultura mundial de ciberseguridad.

En un intento por invertir las perspectivas beligerantes antes descritas, uno debe ser consciente de que las infraestructuras digitales son ahora omnipresentes, e inevitablemente también serán utilizadas con propósitos hostiles y no pacíficos.

En consecuencia, el objetivo último es restringir tales usos e incorporar los límites más estrictos para cualquier situación de ataque. Como el mismo término «ciberguerra» invita a pensar en categorías militares, debe hacerse un esfuerzo para combatir este automatismo mental y fundamentar una petición para lograr una conducta pacífica en el ciberespacio.

Ciberdefensa activa y pasiva

Si un país ejecuta un «ataque armado» –o si se piensa que tal ataque se ha producido–, la víctima, el país atacado, tiene, bajo la carta de las Naciones Unidas, el derecho a la legítima defensa proporcional. Pero si el ataque causa daños a intereses privados, por ejemplo a una empresa o a una infraestructura privada –energía, banca, aviación, etc. (para una definición más precisa, ver nota al pie 42)–, ¿puede el atacado responder a la agresión? ¿Y puede acaso hacerlo si existe incertidumbre en cuanto a la atribución y el atacante es, o puede ser, un actor no estatal o, simplemente, un delincuente informático común? Aquí entra en juego la legislación nacional sobre delitos cibernéticos, con sus sanciones penales y las herramientas de aplicación de la ley. El debate sobre si la defensa activa es legal, incluso si implica intrusión en los sistemas y redes y causa daños, se ha librado durante algún tiempo[35].

Algunas tácticas de defensa activa que han sido propuestas podrían incluir la intrusión en los sistemas para recuperar los datos, cerrando los sistemas, saboteando los datos, infectando al atacante con *software* dañino, apropiándose de la *botnet* del atacante o contratando una *botnet* para atacarle. Enviar datos a un atacante (siempre que no sea con *software* dañino) puede no ser ilegal, pero el resto de las acciones defensivas probablemente lo son. Emprender acciones contra un atacante delictivo en respuesta a un ataque criminal no es necesariamente legal en la mayoría de jurisdicciones. Más aún, estas acciones pueden desencadenar otras acciones legales (especialmente si existen *botnets* involucradas) tales

[35] Ver artículo de Jody R. Westby en el blog de *Forbes* http://www.forbes.com/sites/jodywestby/2012/11/29/caution-active-response-to-cyber-attacks-has-high-risk/.

como las que afectan a la propiedad intelectual, *spam*, fraude, legislación contractual y leyes de responsabilidad civil. Además, pueden causarse daños colaterales a sistemas de terceros[36].

Algunas de las justificaciones que se han sugerido para tácticas de defensa activa incluyen la autodefensa, la persecución y la propiedad de los datos robados. Sin embargo, ninguna de estas justificaciones son lógicas, la propia justicia no es válida y el camino a seguir es, por el contrario, hacer que los sistemas y las redes sean más resistentes, mejorar la ciberdefensa (pasiva) y aplicar las legislaciones nacionales e internacionales[37].

Un sistema emergente de gestión integral de la ciberseguridad

Tras la anterior excursión al territorio de la ciberguerra, con sus ambigüedades, déficits y aterradoras implicaciones, la discusión una vez más se centra en el panorama de la amenaza mundial, con los ciberconflictos procedentes de los estados, actores no estatales –o una combinación de ambos–, los grupos terroristas, consorcios de la delincuencia organizada y delincuentes informáticos en general.

Dada la penetración casi total de las tecnologías cibernéticas en nuestras sociedades, se puede observar cada vez más cómo las organizaciones internacionales, los Gobiernos, la economía en general, la industria de las tecnologías de la información y la industria de seguridad TIC, así como la sociedad civil –la *stakeholder community* o comunidad de intereses, término comúnmente aceptado– unen sus fuerzas para combatir y mitigar las amenazas en el ciberespacio. En un documento de longitud limitada, este movimiento, en parte concertado y en parte autónomo, es imposible de cubrir; por lo tanto, haremos un esfuerzo por enumerar y evaluar sus principales formas de manifestación. Las palabras clave primordiales son: ciberdefensa, autoprotección y resistencia (*resilience*).

Resistencia (*resilience)* es la política orientada a la defensa que maximiza la capacidad de los sistemas objetivo para prevenir, disuadir y resistir ciberataques y, si estos se producen, minimizar y mitigar sus efectos; es un concepto multidimensional que posee componentes técnicos, organi-

[36] Ejemplos tomados de Westby, anterior nota al pie.

[37] Si el origen de un ataque económico se atribuye con una certeza razonable, algunas contramedidas económicas, como la suspensión de relaciones, la negativa al suministro, la retirada de los beneficios comerciales o –en el caso de un Gobierno– la supresión del estatus de nación más favorecida u otras medidas comerciales punitivas pueden ser legítimas. En respuesta a la oleada actual de ataques informáticos sobre activos de empresas e infraestructuras de EE. UU., el presidente Obama ha hablado recientemente de tales medidas.

zativos, políticos y legales que precisan combinarse para ser eficaces[38]. Debatiremos a su vez los requisitos del marco legal, aquellos de legítima defensa a nivel de empresas y usuarios finales, la mejora del diseño técnico de resistencia a los ataques, la capacidad de establecer estándares y buenas prácticas, los beneficios de las redundancias, la asistencia y cooperación social, la cooperación internacional y el cumplimiento de las leyes, el papel del intercambio de la información, los sistemas de alerta y respuestas a emergencias y, lo que es de vital importancia, la protección de infraestructuras críticas, nacionales y transfronterizas.

Creación de un marco legal armonizado para combatir los ciberdelitos y ciberconflictos

El ciberespacio no podía continuar como un espacio alegal, y con la llegada de las tecnologías de la información y la comunicación los legisladores se han enfrentado a una doble tarea: introducir las nuevas tecnologías dentro de sus sistemas legales nacionales y proporcionar un marco legal internacional armonizado para las causas penales y las sanciones y el cumplimiento de la ley, puesto que los ataques informáticos pueden suceder en cualquier parte del mundo. La mayoría de los países industrializados tienen ahora leyes contra los ciberdelitos, muchas de ellas muy adecuadas, pero con variaciones significativas al definir lo que constituye un ciberdelito en su detección e identificación y en las disposiciones procedimentales aplicables, que hasta hace poco han dificultado significativamente la investigación de estos delitos. El Convenio sobre Delitos Informáticos del Consejo de Europa[39] (en la Convención de Budapest se firmó en 2001 y entró en vigor en 2004) ha supuesto un avance de primera magnitud en la armonización global de la legislación sobre ciberdelitos, y me uno al profesor González Cussac en su elogio a este instrumento; también estoy de acuerdo con él en que los nuevos desarrollos y modos de ataque digitales con el tiempo harán necesaria una revisión del texto, a pesar de su validez actual[40].

Sin embargo, al escribir este artículo, la Convención solo ha sido firmada y ratificada por 39 países, y están pendientes 10 ratificaciones. Son significativas las ausencias de Rusia, China y, como tantas veces, de Israel,

[38] La Comisión Europea, pionera en construir estrategias digitales para los 27 miembros de la Unión Europea unificando así sus políticas digitales y de defensa, utiliza el concepto de «resistencia» como una finalidad primordial, por ejemplo, creando –a través de ENISA– una Asociación Europea Público-Privada de Resistencia (EP3R), y sitúa su reciente borrador de la Estrategia de Ciberseguridad de la UE bajo la plataforma «Alcanzando la resistencia cibernética».

[39] www.conventions.coe.int.

[40] *Estrategias legales frente a las ciberamenazas*, *Cuadernos de Estrategia*, n.º 149, *op. cit.*, p. 116.

así como la mayoría de los países del Tercer Mundo, quizás, porque son reticentes a adoptar un documento de origen europeo. El juego de herramientas de la UIT para la legislación de la delincuencia informática (*toolkit for cybercrime legislation)* se ha desarrollado como una alternativa que propone un lenguaje jurídico armonizado con el Convenio y las normas jurídicas sobre delitos informáticos de las naciones industrializadas. La utilización creciente de estos textos o la adopción de un lenguaje autónomo comparable por parte de los países que aún no han suscrito el Convenio ayudarán a que este proceso de armonización avance pronto. Es crucial. La Convención, naturalmente, deberá traducirse conforme a la legislación nacional de los países que ratifiquen los compromisos jurídicos internacionales.

Autoprotección

La ciberdefensa comienza en el hogar o en la empresa. Entre las obligaciones evidentes de un director de sistemas, se encuentra la introducción de tecnologías avanzadas de cortafuegos, antivirus y de incidentes, cifrado de información confidencial, control de acceso a las instalaciones y los equipos que incluya una rigurosa y bien diferenciada gestión de contraseñas («necesidad de conocer»), así como otras técnicas sofisticadas de autenticación. Si se permite BYOD (*bring your own device*), controles rigurosos deberán controlar estos equipos. Se requiere especial vigilancia sobre los sistemas SCADA de las infraestructuras críticas pues son especialmente vulnerables a los ataques de actores estatales, no estatales y terroristas, con un propósito agresivo de tipo militar o de cualquier otro. Esto debería ser obvio; no obstante, la experiencia demuestra que el robo de información confidencial tanto en las empresas como en agencias gubernamentales es, sobre todo, debido a la negligencia de personal interno. Más de nueve de cada diez brechas de seguridad podrían haberse evitado si las organizaciones hubieran seguido las mejores prácticas sobre la protección de datos y seguridad de la información[41].

Una de las tres causas principales de pérdida de datos es el robo o la pérdida física de sus equipos. Además, un informe de la industria alemana muestra que solo una pequeña parte de los correos electrónicos que contienen información altamente sensible, como proyectos de diseño industrial, van cifrados. Se da una falta sistemática de cifrado de los dispositivos móviles de las empresas. En muchos casos, no se prevén sistemas redundantes que en caso de ataque puedan conservar o restablecer rápidamente la funcionalidad de los sistemas o las conexiones.

[41] Cifras de ENISA.

Diseñar para la seguridad

Una importante laguna para los atacantes, casi desde el inicio, es que los diseñadores de *hardware* y *software*, centrándose principalmente en los beneficios de diseño que surgen de los avances técnicos para un mejor desarrollo, han puesto menos interés y esfuerzo en la seguridad de la información y la privacidad.

Además, la construcción de la seguridad desde el principio puede acarrear un coste adicional que reduce los márgenes de beneficios. Tradicionalmente, ha existido una brecha entre la producción y las industrias de seguridad favorecida por la ausencia de conciencia de los usuarios finales de los riesgos para la seguridad de la información y la privacidad inherentes a sus equipos; durante mucho tiempo, ha existido una incongruencia entre la seguridad objetiva y la percibida. Muchas empresas pequeñas pueden no tener los medios o las habilidades profesionales para instalar los medios de protección por sí solas.

Estas brechas de seguridad se están llenando actualmente por una industria más consciente de la seguridad, por una mayor conciencia de los usuarios finales, mayor cooperación e incluso iniciativas comunes de las distintas partes interesadas (véase, por ejemplo, la reciente adquisición de la importante empresa de seguridad McAfee por parte de Intel).

Incluso sería erróneo no dar crédito a las principales alianzas industriales formadas para promover la seguridad y el desarrollo seguro de *hardware*, *software* y arquitectura de redes, ejercicios colectivos que comenzaron en los años noventa del pasado siglo. El más importante es el Trusted Computing Group, con más de 100 miembros, colaboradores o usuarios de la industria. Su módulo –*trusted platform module* (TPM)– está normalizado con la ISO/IEC[42].

No obstante, dado el panorama de las amenazas, la obligación de la industria de *hardware* y *software* de «diseñar para la seguridad» permanece, como también es permanente la responsabilidad de instituciones públicas y privadas y de los países de establecer contratos de seguridad y políticas y estándares de certificación de seguridad[43].

[42] www.trustedcomputinggroup.org. El TPM se usa en los sistemas operativos de la mayoría de los grandes suministradores. El Trusted Computing se enfrenta, sin embargo, a serias críticas por parte de la comunidad de *software* libre en la medida en que fideliza a los clientes.

[43] En su *Agenda de seguridad global,* la UIT se compromete al «desarrollo de estrategias para la creación de unos criterios mínimos de seguridad mundialmente aceptados, y esquemas de acreditación para aplicaciones y sistemas de *software* y *hardware*». Ver también el capítulo *Designing for security* in *information security in the context of the digital divide,* recomendaciones presentadas ante la Cumbre Mundial de la Sociedad de la Información (noviembre de 2005) por el Panel Permanente de Seguridad Informática de la Federación Mundial de Científicos, Doc. WSIS-05/TUNIS/CONTR/01, en www.itu.int.

Sería especialmente útil asegurar el diseño de sistemas SCADA a través de esfuerzos colectivos. Todo esto se basa en la percepción de que todavía existe una escasez de métodos de análisis y diseño, científicamente probados, para dominar las enormes complejidades de los futuros sistemas digitales interconectados, especialmente en lo que se refiere a la seguridad física, la fiabilidad, el funcionamiento y la seguridad. La industria de la seguridad de las tecnologías de la información requiere una alta cualificación para estar al día, a un nivel altamente profesional, de los desafíos que debe enfrentar cada vez más. Las compañías de seguridad representan un negocio en rápida expansión, altamente exigente y competitivo, de miles de millones de dólares.

Establecimiento de estándares y buenas prácticas

La actuación de los Gobiernos y la propia organización de las empresas han creado un universo de estándares técnicos y operativos para asegurar las estructuras de las infraestructuras IT. Muchas de estas son de carácter voluntario, pero un sistema de certificaciones ofrece incentivos para adoptar una visibilidad pública. Las empresas que no apuestan por la excelencia en este área y que, en consecuencia, sufren ataques e intromisiones en sus datos no solamente pierden dinero, sino también reputación y clientes. Los estándares más importantes para la gestión de las tecnologías de la información y la comunicación, de aplicación prácticamente mundial, han sido elaborados por ISO/IEL[44] en las series 27000 y 13335 para el antes citado trusted platform module, en sus normas 11889-1 a 11889-4 sobre tecnologías de la información (2009). En EE. UU., el establecimiento de normas está a cargo del American National Standards Institute (ANSI). Durante años, la comunidad de usuarios, desarrolladores y proveedores de tecnología de Internet se han unido a la Internet Engineering Task Force (asociada a la Sociedad Internet) para el desarrollo y la promoción de estándares para la infraestructura de Internet, enrutamiento y la seguridad del transporte de datos. Además, en los problemas específicos de la informática distribuida, existe el Open Grid Forum para el establecimiento de estándares en informática y arquitectura de redes.

El International Information Systems Security Certification Consortium (ISC) (Consorcio Internacional de Certificación de la Seguridad de Sistemas Informáticos), descrito como «la mayor organización mundial de seguridad de tecnologías de la información» («la seguridad trasciende a la tecnología»), promueve la idea de normalización mediante la concesión de certificados de excelencia en operaciones seguras de tecnologías de la información (*certified Information Security professional,* CISSP, profesio-

[44] www.iso.org, www.iec.ch. El miembro español de ambas es AENOR, que también establece estándares propios (en este contexto, ver UNE 71502) y otorga certificaciones.

nal titulado en Seguridad De La Información); las áreas de elección para estos certificados también incluyen el desarrollo de *software* y el diseño y la arquitectura de seguridad. Actualmente, 85.285 miembros de 143 países poseen estos certificados. Los emisores de certificados, más allá de las agencias normativas tradicionales, los institutos, las asociaciones, las empresas particulares o los organismos intergubernamentales, son muchos, lo que, obviamente, refleja la necesidad de reconocer la excelencia y la generación de confianza. Una recopilación indicativa en la página web de Wikipedia del CISSP reúne 70 certificaciones diferentes[45].

Protección de infraestructuras críticas

CIIP, la protección de infraestructuras críticas de información[46]. Ha estado durante muchos años en el centro de atención de las políticas de seguridad de la información y de las estrategias para mejorar la resistencia, tanto por parte de los Gobiernos y organismos internacionales como por los propios operadores de estas infraestructuras. De hecho, en un contexto de ciberguerra sería la pieza clave de las estrategias defensivas y de todos los esfuerzos para optimizar la resistencia de los sistemas. Dada su importancia vital para el funcionamiento de la sociedad, la creciente vulnerabilidad de las infraestructuras en un ambiente interconectado y dependiente de Internet y los posibles efectos cascada que sus fallos pueden producir, es fácilmente comprensible esta prioridad. Las infraestructuras críticas son de las primeras en la línea de fuego de un ataque militar, terrorista y de consorcios criminales (crimen organizado), en este último caso como base para el chantaje.

En EE. UU., las directivas presidenciales desde la época del presidente Clinton han ordenado las medidas de protección necesarias. Asegurar las infraestructuras críticas y los sistemas de información es una parte fundamental del mandato del Departamento de Seguridad Nacional (DHS), ampliamente dotado en cada presupuesto anual. Las políticas CIIP

[45] La *Revista de Seguridad en Informática y Comunicaciones*, www.revistasic.com, una excelente publicación y con certeza la mejor sobre seguridad informática en España, ayuda al lector no profesional a mantener la pista de estas diversas distinciones conforme son recibidas por empresas españolas. La editora de esta publicación, SIC, organiza también conferencias sobre ciberseguridad en España de forma periódica.

[46] Se entiende que estas infraestructuras generalmente, y en el más amplio sentido, incluyen la generación de transmisión y distribución de electricidad, la producción, transporte y distribución de gas, la producción, transporte y distribución de petróleo, las telecomunicaciones, el suministro de agua potable y no potable (alcantarillado), el filtrado de aguas de superficie (por ejemplo, diques y compuertas), la agricultura, la producción y distribución alimentaria, la calefacción (por ejemplo, gas natural, diésel, hospitales, sistemas de transporte por ambulancia, redes ferroviarias, aeropuertos, puertos o navegación interior), servicios financieros y servicios de seguridad (Policía y Ejércitos). El componente energético se considera la parte más vulnerable.

ocupan un lugar destacado en la página de DHS www.dhs.gov. Limitando intensos esfuerzos anteriores, el presidente de EE. UU., el 13 de febrero de 2013, firmó una orden ejecutiva (EO) *sobre la mejora de la ciberseguridad de las infraestructuras críticas* y una directiva presidencial de política (PPD) *sobre seguridad de infraestructuras críticas y resistencia* cuyas lecturas resultan instructivas.

Otro actor de la mayor importancia es la Comisión Europea, asistida por su Agencia Europea de Seguridad de las Redes y de la Información (ENISA). Consciente de las diferencias aún existentes en los sistemas y los niveles de protección en los 27 países miembros, la UE ha estado durante tiempo trabajando en CIIP y en la armonización de las normas de protección.

En 2009, la Comisión adoptó un Plan de Acción y Comunicación sobre CIIP[47] y organizó una Conferencia Ministerial sobre CIIP[48]. Ya hemos mencionado el European Public-Private Partnership for Resilience (Consorcio Europeo Público-Privado de Resistencia). ENISA ha venido organizando varios Ejercicios Europeos de Ciberseguridad, con amplia participación de Gobiernos y del sector privado, el último de ellos en 2012[49]. Con el objetivo de fortalecer la comunidad de gestión de incidentes informáticos. El 7 de febrero de 2013 la Comisión publicó, en un comunicado conjunto con los demás órganos principales de la UE, la Ciberestrategia de la UE, que en un amplio repaso persigue establecer unos requisitos comunes mínimos a nivel nacional para cada miembro de los sistemas de información y de red (NIS), incidiendo sobremanera en la resistencia y la protección de las infraestructuras[50]. El Parlamento Europeo está también activo, y celebró su última reunión sobre CIIP el 6 de febrero de 2013.

Durante más de una década, la Unión Internacional de Telecomunicaciones (UIT) ha estado trabajando en la protección de infraestructuras críticas desde una perspectiva global y, últimamente, en referencia con su *Agenda global de ciberseguridad,* a pesar de lo cual aún no se ha logrado concebir un marco regulador uniforme. Sin embargo, existe una gran cantidad de estudios, publicaciones e informes de conferencias que son fácilmente localizables en la página web de la UIT, así como en la de su rama ejecutiva, el Consorcio Internacional Multilateral contra las Ciberamenazas (International Multilateral Partnership Against Cyber Threats,

[47] COM/2009/149, incluida por el Consejo de Europa en su resolución 2009/C 321/01. Ver también la Directiva 2008/114/CE sobre la Protección de Infraestructuras Críticas Europeas.

[48] www.tallinnciipeu.eu/?id=conference.

[49] Para localizaciones clave, ver www.enisa.europa.eu.

[50] JOIN (2013 1 final). La Estrategia viene acompañada de un borrador de directiva sobre medidas destinadas a asegurar un alto nivel común de medidas de protección cibernética.

IMPACT)[51]. El estudio anterior no es sino indicativo, y complementarlo con una descripción de las iniciativas nacionales excedería las posibilidades de este capítulo. Aun así, muchos, si no la mayoría de los países que participan en el mundo cibernético, se ocupan de CIIP en sus organismos nacionales como complemento de los esfuerzos internacionales. La Agencia Federal Alemana de Seguridad de la Información, por ejemplo, maneja una plataforma de Internet especializada en CIIP y patrocina una serie de publicaciones[52].

Resistencia en la informática en la nube y los dispositivos móviles

Los rápidos avances de la informática en la nube en enormes centros de datos y la masiva migración hacia dispositivos móviles que se ha descrito en anteriores secciones de este capítulo plantean la utilidad de analizar la resistencia a los ataques de estos nuevos centros de gestión de datos y operaciones cibernéticas, y señalar las novedades al respecto.

La computación o informática en la nube es una nueva modalidad para suministrar recursos informáticos, no una nueva tecnología. La concentración de datos y la prestación de servicios, escalables según la demanda, ofrecen enormes beneficios económicos, y por ello han atraído inversiones masivas a nivel mundial. Las previsiones mundiales de servicios en nube en 2013 indican un volumen previsible de negocio de 44.200 millones de dólares. ENISA lo ha expresado de forma palpable: las economías de escala y flexibilidad de la nube son al mismo tiempo un amigo y un enemigo desde el punto de vista de la seguridad. La concentración masiva de recursos y datos ofrece un objetivo más atractivo a los atacantes, pero las defensas basadas en la nube pueden ser más robustas, escalables y rentables. Los ataques contra centros de datos de estas dimensiones ofrecen nuevas e importantes oportunidades a un ataque terrorista o militar, lo que incluye la manipulación del suministro de energía y supondría una pérdida masiva de datos (siempre que se superen las redundancias de suministro eléctrico), la destrucción física o la intrusión cibernética en las bases de datos. Los temores de los clientes aumentan, ya que las masas de datos se mueven de forma aparentemente arbitraria e imposible de seguir entre unos y otros paneles, y el personal supervisor se convierte en anónimo y la confianza en la integridad y la privacidad de los datos se torna más difícil de mantener. Los riesgos de la informática en la nube son serios y suponen un importante desafío en lo que concierne a la seguridad.

[51] www.itu.int; www.itu.int/ITU-D/cyb/cybersecurity/impact.html.

[52] www.bsi.bund.de, para la plataforma CIIP. Ver: www.kritis.bund.de.

Por todo ello, no resulta sorprendente que la seguridad en la nube se haya convertido en un tema central en el actual debate sobre seguridad informática. En un mundo tan competitivo como el de la nube, los suministradores y las compañías de seguridad se superan unas a otras en la generación de confianza. Sin duda, pueden demostrar que existe una prima en la gestión de la seguridad en la nube. Toda clase de medidas de seguridad resultan más baratas cuando se implantan a gran escala, y la misma cantidad invertida en seguridad consigue una mejor protección (un perímetro físico y control de acceso más barato, mejor escalado de los recursos, más oportunidades de respuesta rápida, una gestión más eficaz de la amenaza, etc.). Los clientes, entre los cuales están también los Gobiernos, toman sus opciones económicas en gran medida a la luz de la resistencia de los servicios de seguridad ofrecidos, la reputación de confidencialidad y la transparencia de los procedimientos internos.

Últimamente destaca un importante factor diferenciador de las empresas europeas, ya que estas juzgan la protección legal de los datos en Europa mejor que en EE. UU., habida cuenta de la política de datos más intrusiva del Departamento de Seguridad Nacional.

Hoy en día la seguridad en la nube parece ser un asunto de todos. Las referencias de este artículo al trabajo analítico y a las recomendaciones sobre la materia están por ello limitadas a los recientes estudios de ENISA: el *Cloud computing: benefits, risks and recommendations for information security* antes citado y el *Critical cloud computing: A CIIP perspective on cloud computing* (14 de febrero de 2013), ambos en www.enisa.europa.eu.

Antes se han citado cifras sobre el impresionante crecimiento del número de dispositivos móviles y las consecuencias derivadas de la migración hacia las tecnologías móviles. También se ha destacado que la amenaza hacia los móviles es desproporcionada, por lo que los ciberataques a móviles son una característica dominante del panorama actual de amenazas. A pesar de que son extraordinariamente vulnerables a los ataques, los dispositivos móviles han permanecido virtualmente desprotegidos durante mucho tiempo. Solo bajo esta coyuntura aparece en el mercado el *software* antiataque para los sistemas operativos de móviles. Sin embargo, el futuro no puede asentarse en la descarga de *software* en dispositivos móviles individuales, sino en la vigilancia centralizada de los clientes móviles desde la nube, como demuestra una alianza entre Vodafone y BAE Systems que se está introduciendo en el mercado a través de una asociación estratégica de cinco años[53]. La promesa de esta aproximación a la vigilancia de la nube es que no se refiere solo a *smart phones,* sino también a *tablets* y, eventualmente, a RFID, los sistemas de

[53] «BAE and Vodafone in cyber safety deal», *Financial Times,* «And news services», 18 de febrero de 2013.

control en fábricas inteligentes y otros sistemas ciberfísicos que podrían ser protegidos eficazmente.

Cooperación nacional e internacional en ciberseguridad

Habida cuenta de la naturaleza transparente y global de las estructuras de red digitales, un asunto de indudable necesidad es conseguir una amplia cooperación nacional e internacional de la comunidad de interesados en combatir y mitigar las consecuencias derivadas de ciberconflictos, como se reconoce a nivel mundial. Los patrones de cooperación existentes actualmente, y que deben mejorarse, incluyen intercambios efectivos de información, como la notificación de incidentes, asistencia mutua –también para activar redundancias–, respuestas a incidentes organizados, sistemas de alarma, puntos de contacto dentro y entre las naciones, mejora de la cooperación en el cumplimiento de las leyes y requisitos organizativos para hacer funcionar todos estos desiderátums.

Estas medidas, y otras relacionadas, parecen bastante sencillas, y su utilidad con vistas a una estrategia de prevención, defensa, sanción y mitigación de los incidentes propios de un conflicto digital es bastante evidente por sí sola. Por ello, no sorprende que las categorías y el número de actores involucrados en ellas sean enormes y muy diversas. Nos encontramos aquí con procesos de continua expansión, difíciles de resumir en un análisis breve. Baste con mencionar unos cuantos desarrollos que indican las próximas tendencias.

Encomendado por la Cumbre Mundial sobre la Sociedad de la Información para coordinar las respuestas internacionales sobre la ciberseguridad, la UIT ha elaborado una *Agenda global de ciberseguridad* que promueve muchas de las tareas de cooperación a nivel mundial, que culminan en un marco de una estrategia global de las múltiples partes interesadas para la cooperación y el diálogo internacionales. Esta agenda persigue sus objetivos de forma dinámica, como puede desprenderse de las páginas web de la UIT.

Un elemento importante de esta estrategia de cooperación es aquel que afecta a la información crítica a través de fronteras. El mecanismo clave es el enfoque «24/7» (24 horas durante 7 días), la disponibilidad permanente de puntos de contacto en caso de gestión de incidentes informáticos. El primer plan internacional se desarrolló con el G-8 en 1998: el grupo de G8 creó una red de expertos en el cumplimiento de las leyes de entre sus miembros, funcionando las 24 horas, pero también se unieron otros Gobiernos. En la UE, el primer programa 24/7 vino acompañado de la decisión marco del Consejo sobre ataques contra los sistemas de información de 2003. Un enfoque más sistemático forma parte del Convenio de Delitos Cibernéticos (Budapest) que, aparte de armonizar el derecho penal sustantivo de los delitos informáticos, ha aportado poderes

legislativos procesales necesarios para investigar y procesar delitos domésticos, pero también ha establecido un régimen ágil y eficaz de cooperación internacional y asistencia mutua (art. 23 y siguientes del Convenio) para el «seguimiento y rastreo» que incluye normas sobe la conservación expedita de los datos almacenados y en tráfico, etc. En el art. 35 se establece una red permanente 24/7 con equipos adecuados y personal capacitado a fin de asegurar la disponibilidad de apoyo inmediato con fines de investigación y procesamiento, incluida la recopilación de pruebas y la localización de sospechosos. Muchos Gobiernos participan en la puesta en marcha del 24/7, incluso más allá de las obligaciones que impone el tratado ya existente.

Un elemento de creciente importancia en la notificación de incidentes, asistencia mutua, alerta temprana, información de riesgo, etc. son los Equipos de Respuesta a Emergencias Informáticas (Computer Emergency Response Teams, CERT), también conocidos como Equipos de Respuesta a Incidentes de Seguridad Informática (Computer Security Incidents Response Teams, CSIRT). Liderados por la Universidad Carnegie Mellon y con fondos del Departamento de Defensa de EE. UU., los CERT nacieron en 1988 y son hoy una red de dimensiones globales. En muchos países existe una CERT del Gobierno central que se ocupa de la coordinación con otros CERT nacionales, y específicamente con asegurar infraestructuras digitales del Gobierno.

Los CERT son equipos de expertos en tecnologías de la información que siguen y procesan la información sobre incidentes informáticos; analizan, recomiendan, coordinan y prestan asistencia para combatir ciberataques y reparar los daños, y a menudo emiten boletines informativos y advertencias sobre nuevas amenazas. Por todo el mundo existen actualmente más de 250 organizaciones que emplean esta denominación, y que se ocupan de dar respuesta a la seguridad informática.

En muchos paises, la industria y las instituciones académicas han tomado la iniciativa de establecer CERT. En EE. UU., el Departamento de Seguridad Nacional ha establecido el US CERT, que coordina el CERT/CC, en parte financiado a nivel federal por la comunidad US CERT y liderado por la Carnegie Mellon. En Alemania, una tarea similar es llevada a cabo por el BSI, a través del CERT-Bund. En España, funciona el Centro de Respuesta a Incidentes de Seguridad TIC de INTECO, un órgano del Ministerio de Industria, y su oficina ejecutiva Red.es. Como parte de su *Agenda global de ciberseguridad,* la UIT apoya a los países en vías de desarrollo en la creación de sus CERT nacionales. En septiembre de 2012, la Unión Europea estableció un CERT-EU, en un principio para proteger sus propias entidades pero también para asociarse con CERT nacionales y gubernamentales del área de la UE. Al mismo tiempo, en su *Agenda digital* de 2010 la Unión Europea convocó a sus miembros a establecer sus propios CERT nacionales, un desarrollo que debía completarse en 2012,

allanando así el camino para una red comunitaria eficaz de respuesta a incidentes.

En un movimiento paralelo, en febrero de 2013, la UE ha creado un Centro Europeo de Delincuencia Informática (EC3), en EUROPOL, cuya finalidad se centra específicamente en grupos organizados que buscan grandes beneficios y un impacto hostil en infraestructuras con mayores poderes de investigación.

Para el futuro es necesario universalizar el movimiento CERT y hacer que los CERT sean más operativos y estén interconectados; pero también que, desde luego, constituyan un arma defensiva de primer nivel contra los ataques informáticos y para minimizar los ciberconflictos[54].

En el momento en que se elabora este capítulo, uno no puede sino observar un crecimiento de los ataques informáticos a Gobiernos e industrias, mayoritariamente con APT (amenazas persistentes avanzadas), como también una creciente toma de conciencia de que todos los interesados deben hacerse más activos y próximos en el intercambio de información y en compartir los recursos de defensa digital.

Un ejemplo notable de los amplios esfuerzos de autoayuda de la industria es la alianza colectiva para la ciberseguridad pilotada en Europa por René Obermann, consejero delegado de Deutsche Telecom, quien ha solicitado que se comuniquen voluntariamente más informes sobre incidentes y que haya una mayor transparencia[55].

Una cultura de ciberseguridad: normas de conducta en la era digital

Hasta el momento, solo *algunos* de los aspectos legales generales han sido considerados: el derecho internacional define con ambigüedad los límites de la ciberguerra y «ataque armado», así como la armonización de la legislación sobre delitos informáticos en sus dimensiones nacionales y transfronterizas. Naturalmente, aunque no se mencione, en la mayoría de países es válido un régimen de derecho civil que rige los daños y perjuicios, así como el pertinente derecho internacional privado.

[54] Desde 1990, los CERT están coordinando e intercambiando información desde una organización internacional informal, FIRST (Forum of Incident Response and Security Teams); pero existe espacio para una coordinación más efectiva. Ya en 2004, este autor recomendó que el enfoque CERT no solamente debería ser universal sino que, más allá de la asistencia y el procesamiento de información individuales, debería desarrollar un enfoque de «lecciones aprendidas». Ver: WEGENER, Henning. *Learning lessons from cyber attacks: Broadening the CERT framework*, en www.unibw.de/infosecur.

[55] Ver, por ejemplo: OBERMANN, René. «Uniting for cyber defence», *New York Times, op. ed.,* 21 de febrero de 2013.

Pero todo esto está lejos de cumplir los requisitos de un régimen de funcionamiento en el ciberespacio capaz de combatir y soportar los ciberconflictos. En términos legales, la nueva área del ciberespacio inicialmente era un vacío necesitado de un marco detallado de normas no solo para los estados, sino para todas las partes interesadas. La tarea consistía en desarrollar, con el tiempo, una serie de normas de conducta de convivencia –de una cultura de ciberespacio y de seguridad digital– que incluyese un marco legal global para gestionar y controlar el omnipresente e infinito potencial de las tecnologías digitales. En consecuencia, existe poca o ninguna capacidad para controlar por ley la escalada de ciberconflictos o garantizar el uso pacífico del ciberespacio y, como hemos visto, existen ambigüedades al concebir cómo debe aplicarse la legislación internacional existente. Sin duda, esto representa un peligroso y precario estado de cosas. El grupo sobre seguridad digital en el que sigo participando activamente, la Federación Mundial de Científicos, desde el principio reclamó que Naciones Unidas dirija los esfuerzos para la creación de una ley universal e integral del ciberespacio[56]. Sin embargo, por una serie de razones, un tratado único no ha demostrado ser una opción realista.

Afortunadamente, la reflexión colectiva sobre los procesos necesarios para la estrategia digital ha evolucionado notablemente. Para hacer corta una larga historia, una nueva era de diplomacia cibernética comenzó en torno a 2008, con un consenso internacional emergente manifiestamente hacia la concentración de los esfuerzos como una alternativa al establecimiento formal de tratados globales: la elaboración de medidas de fomento de la confianza o códigos de conducta como instrumentos normativos. Podemos estar asistiendo a un punto de inflexión en la diplomacia de seguridad informática.

La opinión predominante es que las CBM (*confidence building measures*) –las medidas de confianza– y los códigos de conducta abren una ventana a las oportunidades para progresar realmente hacia definiciones comunes y normas de comportamiento. Las CBM tienen capacidad para reducir amenazas, aumentar la transparencia y hacer predecible la conducta de los países; además, son flexibles, voluntarias y ofrecen una geometría variable en función de sus participantes –es posible incluir actores no

[56] *Towards a universal order of cyber space: Managing the threat from cyber crime to cyber war,* Doc. WSIS-03/GENEVA/CONTR/6-E, www.itu.int/dms_pub/itu-s/md/03/wsis/c/S03-WSIS-C-0006!!PDF-E.pdf, también en www.unibw.de/infosecur. Ver también: KAMAL, Ahmad. *The law of cyber space: An invitation to the table of negotiations.* Génova: UNITAR, 2005, www.un.int/kamal/thelawofcyberspace. Rusia ha abogado desde 1998, en una serie de resoluciones en Naciones Unidas, por un tratado, proponiendo contenidos hasta cierto punto conflictivos y probablemente de imposible aplicación. Ver Res. A/53/70 hasta A/65/41. Estas resoluciones, sin embargo, tuvieron el incuestionable mérito de mantener vivo el debate, en el sentido de que se requería un esfuerzo normativo universal a gran escala.

estatales– y seguimiento: a diferencia de la elaboración de tratados coherente, los participantes son libres para adoptar soluciones parciales y ponerlas en práctica sin demoras, independientemente o con otras partes interesadas que piensen de igual modo. Las CBM apoyadas por estados no requieren ratificación, invitan a la imitación y, en su grado máximo (y mejor), son políticamente vinculantes. Están por ello excepcionalmente indicadas para fomentar la creación de consenso internacional a escala evolutiva. Un paquete bien negociado de CBM con una masa crítica de participantes puede poner en marcha un proceso de cambio gradual y mayor sensibilidad. La clarificación de las normas de comportamiento puede servir como un incentivo para ir a más.

Actualmente existen numerosas actividades internacionales paralelas que conjuntamente contribuyen a la creación de un consenso. Baste con citar algunas. En 2011 se constituyó un grupo de expertos de Naciones Unidas, con el mandato concreto de «definir medidas cooperativas (...) incluyendo normas, reglas, principios de responsabilidad de los estados y mensajes de fomento de la confianza en el espacio de la información»[57], que informará en 2013. Los Gobiernos han proporcionado numerosas aportaciones al grupo a petición del secretario general de Naciones Unidas[58]; sus puntos de vista han apoyado firmemente la idea de identificar CBM. En poco tiempo, han surgido oleadas de declaraciones nacionales de otros países en este mismo sentido: desde Australia, el Reino Unido, Alemania y, al menos de manera implícita, EE.UU., entre otros[59]. Un portavoz autorizado de la India se ha unido al concierto[60]. China, Rusia, Tayikistán y Uzbekistán reflejaron los trabajos del Consejo de Cooperación de Shanghái y remitieron al secretario general de Naciones Unidas en septiembre de 2011 un borrador de código internacional de conducta sobre seguridad informática[61]. A pesar de que el documento, en virtud de la elección de sus autores, no desprendía un excesivo aroma de correc-

57 A/Res/66/24 de 13 diciembre de 2011.

58 A/66/152 y A/66/152, add.1.

59 Ver la anterior nota al pie y las expresiones positivas en la sesión del Diálogo de Shangri-La, *IISS news,* julio de 2012. Para Alemania, ver también «Challenges in cyber security: Risks, strategies and conference building», *Conference report.* Berlín: 13 y 14 de diciembre de 2011.
www.auswaertiges-amt.de/DE/Aussenpolitik/Friedenspolitik/Abruestung/Projekte/Cybersicherheit.html. El Ministerio Federal de Asuntos Exteriores de Alemania, además, apoya un proyecto de UNIDIR sobre ciberseguridad internacional y CMB en 2012.

60 GUPTA, Arvind. *CBMs in cyber space: What should be India's approach?* IDSA, Institute for Defence Studies and Analysis, 27 de junio de 2012.

61 A/66/359. Ver también el acuerdo entre los Gobiernos de los estados miembros de la Organización de Cooperación de Shanghái sobre Cooperación en el campo de la Seguridad Internacional de Información, firmado en Ekaterinburgo el 15 de junio de 2009.

ción política, el catálogo de compromisos ofrecidos mediante suscripción voluntaria no debe ser desdeñado.

Al mismo tiempo, los países miembros han organizado conferencias de prestigio internacional en las que se ha aireado la idea de las CBM y catálogos más o menos detallados con los contenidos o aportaciones a las CBM que han figurado en los resúmenes de las conferencias (Londres, Berlín, Pekín, Viena, Budapest). Además del ejercicio de las Naciones Unidas en curso, las organizaciones regionales también se están involucrando en el acto. Por ejemplo, el foro regional ASEAN, con sus miembros representativos y participantes, 27 naciones que trascienden sobradamente el ámbito geográfico de Asia, se ha inmerso de lleno en el tema CBM[62], y la OSCE, consciente de su anterior experiencia con CMB orientales y occidentales, está trabajando activamente en un borrador de código de conducta (ver *A comprehensive approach to cyber security*[63]).

También la APEC[64], así como la Organización de Cooperación de Shanghái[65], está trabajando en acuerdos regionales. El Consejo de Europa, famoso por su contribución a una ley penal mundial sobre delitos cibernéticos a través del Convenio sobre el Ciberdelito, ha adoptado 10 principios sobre la gobernanza en Internet[66], y el UNIDIR ayuda a suministrar el sustento académico para estos esfuerzos[67]. Las ONG en el área cibernética, así como investigadores individuales, ofrecen sus propios catálogos de conducta. Obviamente, estos catálogos no pueden reproducirse ni analizarse aquí, pero representan herramientas efectivas para estimular el debate y facilitar las negociaciones de CBM[68]. Es de esperar que el actual

[62] La secretaria de Estado, Clinton, en el encuentro de ASEAN en Pnom Penh el 12 de julio de 2012: «Este foro incluye algunos de los mayores actores cibernéticos del mundo. Por ello, es un lugar apropiado para un diálogo sostenido y lleno de contenidos sobre asuntos que atañen al ciberespacio. En los años que nos aguardan, debemos trabajar juntos en apoyo de normas y estándares responsables, y perseguir medidas prácticas para reforzar la confianza y reducir los riesgos». El ARF organizará un Seminario sobre Medidas de Fortalecimiento de la Confianza en el Ciberespacio en Seúl el próximo mes de septiembre. En mayo de este año, los ministros de Defensa de ASEAN han reclamado un «plan director ASEAN sobre conectividad segura».

[63] www.osce.org/event/cyber_sec2011.

[64] Ver el APEC TEL *Strategic Action Plan* (Plan de Acción Estratégica 2010-2015, www.apec.org).

[65] No se pudo detectar ninguna página web en inglés. Resulta mejor recoger la información de las páginas web de los países miembros.

[66] www.coe.int.

[67] El UNIDIR (United Nations Institute for Disarmament Research, www.unidir.org) organiza conferencias y participa en otras. Particularmente relevante es la conferencia 2012 sobre *The role of confidence-building measures in assuring cyber stability (El papel de las medidas de fomento de confianza en la garantía de ciberestabilidad).*

[68] Para una posible lista de principios que debieran incorporarse a un código de conducta global, ver: WEGENER, Henning. *La 'ciberguerra' se puede evitar.* Madrid: Política Exterior, n.º 146, marzo-abril de 2012, p. 140; del mismo autor, *Die diplomatie des cy-*

dinamismo en promover negociaciones sobre tales medidas de fomento de la confianza y códigos de conducta se mantenga y que pronto se alcance un acuerdo sobre un escenario apropiado para la negociación.

Con el fin de aportar al lector al menos algunas ideas sobre los contenidos de los actuales esfuerzos normativos, se incluye una breve referencia de una corta lista publicada por el secretario General de la UIT:

1. Todos los Gobiernos deben comprometerse a dotar a su pueblo del acceso a las comunicaciones.
2. Todo Gobierno se comprometerá a proteger a su pueblo en el ciberespacio.
3. Todo Gobierno se comprometerá a no acoger terroristas ni delincuentes en su territorio.
4. Todos los países deben comprometerse a no ser los primeros en lanzar un ataque cibernético contra otros países.
5. Todos los países deben comprometerse a colaborar entre sí dentro de un marco de cooperación internacional para asegurar la paz.

Para la UIT, esta concisa lista constituye la esencia de la ciberestabilidad, y una parte importante de la paz digital. En el mismo sentido se orienta la Declaración Erice *sobre principios de ciberestabilidad y ciberpaz,* que emana de la Federación Mundial de Científicos, cuya lista de principios culmina en un llamamiento a «evitar el uso del ciberespacio para el conflicto». La ciberguerra puede evitarse, y no debería ser considerada como un instrumento legítimo de conflictos militares. Eso supondría un largo camino para aliviar la ambivalencia de la tecnología cibernética y podría reducir sensiblemente los riesgos y las preocupaciones económicas. La paz en el ciberespacio –la *ciberpaz*– es la mejor elección[69].

ber-friedens, 2011, en www.unibw.de/infosecur, y también: «Regulating cyber behavior: Some initial reflections on codes of conduct and confidence-building measures» («Regulando la conducta cibernética: algunas reflexiones Iniciales sobre códigos de conducta y medidas de fomento de confianza»), agosto de 2012. *The science and culture series,* Sigapur: World Scientific, 2013, en prensa.

[69] Ver también WEGENER, Henning. *A concept of cyber peace in the quest for cyber peace, op. cit.*(«Un concepto de paz cibernética en la búsqueda de la paz cibernética»), 2011. En la misma publicación, la Declaración de Erice está también reimpresa.

Composición del grupo de trabajo

Coordinador:	**Don Eduardo Olier Arenas** *Presidente del Instituto Choiseul España* *Director de la cátedra de Geoeconomía de la Universidad CEU San Pablo*
Vocal y secretaria:	**Doña María José Caro Bejarano** *Analista principal del Instituto Español de Estudios Estratégicos*
Vocales:	**Don Antonio M. Díaz Fernández** *Profesor titular de Ciencia Política y de la Administración de la Facultad de Derecho de la Universidad de Cádiz*
	Don Christian Harbulot *Director de l'École de Guerre Économique de París* *Socio gerente de la empresa Spin Partners*
	Don José L. González Cussac *Catedrático de Derecho Penal de la Facultad de Derecho de la Universidad de Valencia*
	Don Fernando Palop Marro *Cofundador de Triz XXI* *Profesor asociado de la Universidad Politécnica de Valencia*

Don Henning Wegener
Exembajador de Alemania en España.
Presidente del Observatorio Permanente para la Ciberseguridad de la Federación Mundial de Científicos

Cuadernos de Estrategia

01 La industria alimentaria civil como administradora de las FAS y su capacidad de defensa estratégica

02 La ingeniería militar de España ante el reto de la investigación y el desarrollo en la defensa nacional

03 La industria española de interés para la defensa ante la entrada en vigor del Acta Única

04 Túnez: su realidad y su influencia en el entorno internacional

05 La Unión Europea Occidental (UEO) (1955-1988)

06 Estrategia regional en el Mediterráneo Occidental

07 Los transportes en la raya de Portugal

08 Estado actual y evaluación económica del triángulo España-Portugal-Marruecos

09 Perestroika y nacionalismos periféricos en la Unión Soviética

10 El escenario espacial en la batalla del año 2000 (I)

11 La gestión de los programas de tecnologías avanzadas

12 El escenario espacial en la batalla del año 2000 (II)

13 Cobertura de la demanda tecnológica derivada de las necesidades de la defensa nacional

14 Ideas y tendencias en la economía internacional y española

15 Identidad y solidaridad nacional
16 Implicaciones económicas del Acta Única 1992
17 Investigación de fenómenos belígenos: método analítico factorial
18 Las telecomunicaciones en Europa, en la década de los años 90
19 La profesión militar desde la perspectiva social y ética
20 El equilibrio de fuerzas en el espacio sur europeo y mediterráneo
21 Efectos económicos de la unificación alemana y sus implicaciones estratégicas
22 La política española de armamento ante la nueva situación internacional
23 Estrategia finisecular española: México y Centroamérica
24 La Ley Reguladora del Régimen del Personal Militar Profesional (cuatro cuestiones concretas)
25 Consecuencias de la reducción de los arsenales militares negociados en Viena, 1989. Amenaza no compartida
26 Estrategia en el área iberoamericana del Atlántico Sur
27 El Espacio Económico Europeo. Fin de la Guerra Fría
28 Sistemas ofensivos y defensivos del espacio (I)
29 Sugerencias a la Ley de Ordenación de las Telecomunicaciones (LOT)
30 La configuración de Europa en el umbral del siglo XXI
31 Estudio de «inteligencia operacional»
32 Cambios y evolución de los hábitos alimenticios de la población española
33 Repercusiones en la estrategia naval española de aceptarse las propuestas del Este en la CSBM, dentro del proceso de la CSCE
34 La energía y el medio ambiente
35 Influencia de las economías de los países mediterráneos del norte de África en sus respectivas políticas defensa
36 La evolución de la seguridad europea en la década de los 90
37 Análisis crítico de una bibliografía básica de sociología militar en España. 1980-1990
38 Recensiones de diversos libros de autores españoles, editados entre 1980-1990, relacionados con temas de las Fuerzas Armadas
39 Las fronteras del mundo hispánico
40 Los transportes y la barrera pirenaica
41 Estructura tecnológica e industrial de defensa, ante la evolución estratégica del fin del siglo XX

42 Las expectativas de la I+D de defensa en el nuevo marco estratégico
43 Costes de un ejército profesional de reclutamiento voluntario. Estudio sobre el Ejército profesional del Reino Unido y (III)
44 Sistemas ofensivos y defensivos del espacio (II)
45 Desequilibrios militares en el Mediterráneo Occidental
46 Seguimiento comparativo del presupuesto de gastos en la década 1982-1991 y su relación con el de Defensa
47 Factores de riesgo en el área mediterránea
48 Las Fuerzas Armadas en los procesos iberoamericanos de cambio democrático (1980-1990)
49 Factores de la estructura de seguridad europea
50 Algunos aspectos del régimen jurídico-económico de las FAS
51 Los transportes combinados
52 Presente y futuro de la conciencia nacional
53 Las corrientes fundamentalistas en el Magreb y su influencia en la política de defensa
54 Evolución y cambio del este europeo
55 Iberoamérica desde su propio sur. (La extensión del Acuerdo de Libre Comercio a Sudamérica)
56 La función de las Fuerzas Armadas ante el panorama internacional de conflictos
57 Simulación en las Fuerzas Armadas españolas, presente y futuro
58 La sociedad y la defensa civil
59 Aportación de España en las cumbres iberoamericanas: Guadalajara 1991-Madrid 1992
60 Presente y futuro de la política de armamentos y la I+D en España
61 El Consejo de Seguridad y la crisis de los países del Este
62 La economía de la defensa ante las vicisitudes actuales de las economías autonómicas
63 Los grandes maestros de la estrategia nuclear y espacial
64 Gasto militar y crecimiento económico. Aproximación al caso español
65 El futuro de la Comunidad Iberoamericana después del V Centenario
66 Los estudios estratégicos en España
67 Tecnologías de doble uso en la industria de la defensa
68 Aportación sociológica de la sociedad española a la defensa nacional

69 Análisis factorial de las causas que originan conflictos bélicos

70 Las conversaciones internacionales Norte-Sur sobre los problemas del Mediterráneo Occidental

71 Integración de la red ferroviaria de la península ibérica en el resto de la red europea

72 El equilibrio aeronaval en el área mediterránea. Zonas de irradiación de poder

73 Evolución del conflicto de Bosnia (1992-1993)

74 El entorno internacional de la Comunidad Iberoamericana

75 Gasto militar e industrialización

76 Obtención de los medios de defensa ante el entorno cambiante

77 La Política Exterior y de Seguridad Común (PESC) de la Unión Europea (UE)

78 La red de carreteras en la penísula ibérica, conexión con el resto de Europa mediante un sistema integrado de transportes

79 El derecho de intervención en los conflictos

80 Dependencias y vulnerabilidades de la economía española: su relación con la defensa nacional

81 La cooperación europea en las empresas de interés de la defensa

82 Los cascos azules en el conflicto de la ex-Yugoslavia

83 El sistema nacional de transportes en el escenario europeo al inicio del siglo XXI

84 El embargo y el bloqueo como formas de actuación de la comunidad internacional en los conflictos

85 La Política Exterior y de Seguridad Común (PESC) para Europa en el marco del Tratado de no Proliferación de Armas Nucleares (TNP)

86 Estrategia y futuro: la paz y seguridad en la Comunidad Iberoamericana

87 Sistema de información para la gestión de los transportes

88 El mar en la defensa económica de España

89 Fuerzas Armadas y sociedad civil. Conflicto de valores

90 Participación española en las fuerzas multinacionales

91 Ceuta y Melilla en las relaciones de España y Marruecos

92 Balance de las primeras cumbres iberoamericanas

93 La cooperación hispano-franco-italiana en el marco de la PESC

94 Consideraciones sobre los estatutos de las Fuerzas Armadas en actividades internacionales

95 La unión económica y monetaria: sus implicaciones
96 Panorama estratégico 1997/98
97 Las nuevas Españas del 98
98 Profesionalización de las Fuerzas Armadas: los problemas sociales
99 Las ideas estratégicas para el inicio del tercer milenio
100 Panorama estratégico 1998/99
100 1998/99 Strategic Panorama
101 La seguridad europea y Rusia
102 La recuperación de la memoria histórica: el nuevo modelo de democracia en Iberoamérica y España al cabo del siglo XX
103 La economía de los países del norte de África: potencialidades y debilidades en el momento actual
104 La profesionalización de las Fuerzas Armadas
105 Claves del pensamiento para la construcción de Europa
106 Magreb: percepción española de la estabilidad en el Mediterráneo, prospectiva hacia el 2010
106-B Maghreb: percepción espagnole de la stabilité en Méditerranée, prospective en vue de L'année 2010
107 Panorama estratégico 1999/2000
107 1999/2000 Strategic Panorama
108 Hacia un nuevo orden de seguridad en Europa
109 Iberoamérica, análisis prospectivo de las políticas de defensa en curso
110 El concepto estratégico de la OTAN: un punto de vista español
111 Ideas sobre prevención de conflitos
112 Panorama Estratégico 2000/2001
112-B Strategic Panorama 2000/2001
113 Diálogo mediterráneo. Percepción española
113-B Le dialogue Méditerranéen. Une perception espagnole
114 Aportaciones a la relación sociedad - Fuerzas Armadas en Iberoamérica
115 La paz, un orden de seguridad, de libertad y de justicia
116 El marco jurídico de las misiones de las Fuerzas Armadas en tiempo de paz
117 Panorama Estratégico 2001/2002
117-B 2001/2002 Strategic Panorama
118 Análisis, estrategia y prospectiva de la Comunidad Iberoamericana

119 Seguridad y defensa en los medios de comunicación social
120 Nuevos riesgos para la sociedad del futuro
121 La industria europea de defensa: presente y futuro
122 La energía en el espacio euromediterráneo
122-B L'énergie sur la scène euroméditerranéenne
123 Presente y futuro de las relaciones cívico-militares en Hispanoamérica
124 Nihilismo y terrorismo
125 El Mediterráneo en el nuevo entorno estratégico
125-B The Mediterranean in the New Strategic Environment
126 Valores, principios y seguridad en la comunidad iberoamericana de naciones
127 Estudios sobre inteligencia: fundamentos para la seguridad internacional
128 Comentarios de estrategia y política militar
129 La seguridad y la defensa de la Unión Europea: retos y oportunidades
130 El papel de la inteligencia ante los retos de la seguridad y defensa internacional
131 Crisis locales y seguridad internacional: El caso haitiano
132 Turquía a las puertas de Europa
133 Lucha contra el terrorismo y derecho internacional
134 Seguridad y defensa en Europa. Implicaciones estratégicas
135 La seguridad de la Unión Europea: nuevos factores de crisis
136 Iberoamérica: nuevas coordenadas, nuevas oportunidades, grandes desafíos
137 Irán, potencia emergente en Oriente Medio. Implicaciones en la estabilidad del Mediterráno
138 La reforma del sector de seguridad: el nexo entre la seguridad, el desarrollo y el buen gobierno
139 Security Sector Reform: the Connection between Security, Development and Good Governance
140 Impacto de los riesgos emergentes en la seguridad marítima
141 La inteligencia, factor clave frente al terrorismo internacional
142 Del desencuentro entre culturas a la Alianza de Civilizaciones. Nuevas aportaciones para la seguridad en el Mediterráneo
143 El auge de Asia: implicaciones estratégicas

144 La cooperación multilateral en el Mediterráneo: un enfoque integral de la seguridad

145 La Política Europea de Seguridad y Defensa (PESD) tras la entrada en vigor del Tratado de Lisboa

145 B The European Security and Defense Policy (ESDP) after the entry into Force of the Lisbon Treaty

146 Respuesta europea y africana a los problemas de seguridad en África

146 B European and African Response to Security Problems in Africa

147 Los actores no estatales y la seguridad internacional: su papel en la resolución de conflictos y crisis

148 Conflictos, opinión pública y medios de comunicación. Análisis de una compleja interacción

149 Ciberseguridad. Retos y amenazas a la seguridad nacional en el ciberespacio

150 Seguridad, modelo energético y cambio climático

151 Las potencias emergentes hoy: hacia un nuevo orden mundial

152 Actores armados no estables: retos a la seguridad

153 Proliferacion de ADM y de tecnología avanzada

154 La defensa del futuro: innovación, tecnología e industria

154 B The Defence of the Future: Innovation, Technoligy and Industry

155 La Cultura de Seguridad y Defensa. Un proyecto en marcha

156 El gran Cáucaso

157 El papel de la mujer y el género en los conflictos

157 B The role of woman and gender in conflicts

158 Los desafíos de la seguridad en Iberoamérica

159 Los potenciadores del riesgo

160 La respuesta del derecho internacional a los problemas actuales de la seguridad global

161 Seguridad alimentaria y seguridad global

161 B Food security and global security