



Monografías 148  
Inteligencia.  
Un enfoque integral

Escuela  
Superior  
de las  
Fuerzas  
Armadas



MINISTERIO DE DEFENSA





# Monografías 148

Inteligencia. Un enfoque integral

Escuela  
Superior  
de las  
Fuerzas  
Armadas



MINISTERIO DE DEFENSA

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

Edita:



<http://publicaciones.defensa.gob.es/>

© Autores y editor, 2016

NIPO: 083-16-252-6 (edición papel)  
ISBN: 978-84-9091-153-2 (edición papel)

Depósito Legal: M-5386-2016

Fecha de edición: abril 2016

Imprime: Imprenta Ministerio de Defensa



NIPO: 083-16-253-1 (edición libro-e)  
ISBN: 978-84-9091-154-9 (edición libro-e)

Las opiniones emitidas en esta publicación son exclusiva responsabilidad de los autores de la misma.

Los derechos de explotación de esta obra están amparados por la Ley de Propiedad Intelectual. Ninguna de las partes de la misma puede ser reproducida, almacenada ni transmitida en ninguna forma ni por medio alguno, electrónico, mecánico o de grabación, incluido fotocopias, o por cualquier otra forma, sin permiso previo, expreso y por escrito de los titulares del © Copyright.

En esta edición se ha utilizado papel 100% reciclado libre de cloro.



# ÍNDICE

## Presentación

### Capítulo primero

Ideas fundamentales sobre inteligencia..... 13

*Juan Bautista Sánchez Gamboa*

**El escenario**..... 15

**El marco estratégico militar**..... 18

**Una aproximación al concepto**..... 20

**Un ejemplo de organización**..... 36

**A modo de conclusión**..... 40

### Capítulo segundo

Finalidad de la inteligencia..... 41

*Valentín Díaz Blanco*

**Introducción**..... 43

**Factores**..... 45

**Actores**..... 47

**Riesgos y amenazas**..... 48

**Inteligencia**..... 52

**Inteligencia integral**..... 54

**La inteligencia en el caso español**..... 58

**La necesidad de una organización adecuada**..... 61

**La comunidad de inteligencia en España**..... 65

**Necesidad de una cultura de inteligencia y seguridad**..... 68

### Capítulo tercero

Campos de actuación de la inteligencia..... 77

*José Manuel Díaz-Caneja Greciano*

**Escenario geopolítico**..... 79

**¿Qué es inteligencia?**..... 80

	Página
<b>El ciclo de inteligencia</b> .....	82
<b>Los flujos de información en el ciclo de inteligencia</b> .....	84
<b>Innovaciones en los procesos de inteligencia</b> .....	87
<b>Implicaciones del escenario actual para inteligencia</b> .....	89
<b>Inteligencia en el proceso de toma de decisiones</b> .....	92
<i>Inteligencia de alertas y su relación con la toma de decisiones</i> .....	94
<i>Factores que influyen en la inteligencia de alertas</i> .....	96
<i>Mejoras del análisis de inteligencia en apoyo a la toma de decisiones</i> ...	102
<b>Influencia de los medios de comunicación</b> .....	105
<i>El papel de los medios de comunicación</i> .....	107
<i>Problemas y obstáculos</i> .....	108
<b>Conclusiones</b> .....	109
<b>Capítulo cuarto</b>	
<b>Actores en la producción de inteligencia</b> .....	113
<i>Isaac Martín Barbero</i>	
<b>Inteligencia: actores en busca de guion</b> .....	115
<b>Entender la inteligencia</b> .....	116
<b>Necesidades de información: atinar es cosa de dos, fallar puede hacerse solo</b> .....	118
<b>De las necesidades de información a los requerimientos de inteligencia. Planificando el trabajo y trabajando el plan</b> .....	120
<b>Tecnología y factor humano: una muy falsa disyuntiva en tiempos de cambio</b> .....	122
<b>Más es mejor, en ocasiones; y más accesible, a menudo, también es mejor</b> .....	124
<b>Análisis: en pugna con todos los enemigos internos y externos</b> .....	125
<i>Herramientas internas del analista de información. Procesos mentales y sesgos cognitivos</i> .....	127
<i>Herramientas externas del analista de información. Técnicas de análisis</i> .....	128
<b>De la predicción a la anticipación: la criticidad del criterio</b> .....	130
<b>Si no está orientada a la acción, no tiene consecuencias operativas y no llega a tiempo; no es inteligencia</b> .....	132
<b>El consumo de inteligencia como objetivo final y punto de partida del proceso</b> .....	133
<b>Capítulo quinto</b>	
<b>Beneficios de la inteligencia en apoyo de la política/estrategia de una organización</b> .....	143
<i>Valentín Martínez Valero</i>	
<b>Introducción</b> .....	145
<b>Ámbitos de aplicación de la inteligencia</b> .....	148
<b>La inteligencia como producto</b> .....	150
<b>La inteligencia como proceso: el ciclo de inteligencia</b> .....	155
<b>Ciclo de inteligencia. Fase de dirección</b> .....	157
<b>Ciclo de inteligencia. Fase de obtención</b> .....	161
<b>Ciclo de inteligencia. Fase elaboración</b> .....	170

	<u>Página</u>
<b>Ciclo de inteligencia. Fase de difusión.....</b>	<b>175</b>
<b>La inteligencia como organización: servicios y comunidad de inteligencia.....</b>	<b>176</b>
Conclusiones.....	181
Composición del grupo de trabajo.....	185
Relación de Monografías del CESEDEN .....	187





## Presentación

*«Entonces la serpiente dijo a la mujer: No moriréis; sino que sabe Dios que el día en que comáis de él serán abiertos vuestros ojos y seréis como dioses, conociendo el bien y el mal.*

*Y vio la mujer que el árbol era bueno para comer, y que era agradable a los ojos y deseable para alcanzar la sabiduría; y tomó de su fruto y comió; y dió también a su marido, el cual comió así como ella».*

*Génesis, 3*

Nos atrevemos a decir que, con toda seguridad, la escena anterior reproduce la primera situación en la que un ser humano decide tomando como referencia el asesoramiento que le proporciona un tercero. En este caso, podríamos decir que el conocimiento que recibe le hace adoptar una decisión errónea, precisamente porque el «asesoramiento» estaba intencionadamente deformado, pero también esa circunstancia forma parte de la propia vida.

Presentamos en este cuaderno un recorrido por diversos aspectos de una disciplina poco conocida, aunque esté en boca de muchos: inteligencia; de cuya esencia puede decirse con propiedad que no es nada en sí misma si no se entiende como conocimiento orientado a apoyar la toma de decisiones de un usuario concreto en unas circunstancias determinadas.

Decidir es elegir entre dos o más opciones ante una situación dada, por lo que, también puede decirse que decidir es renunciar; renunciar a aquellas opciones que desechamos cuando elegimos una de entre todas las posibles. Por ello, estando la inteligencia encaminada a apoyar la toma de decisiones, su impacto en el resultado final es innegable, ya que, como en el caso de Eva, el asesoramiento recibido en forma de inteligencia condicionará la decisión adoptada y, con ello, el resultado final.

Con la intención de aportar ese enfoque integral que recoge el título, se ha tratado de recoger en este documento una visión de inteligencia desde diferentes puntos de vista, en forma tal que, aunque puedan repetirse

algunos aspectos de la disciplina, el lector llegue a comprender todas sus facetas.

El capítulo primero, a modo de introducción, realiza un minucioso recorrido por los fundamentos básicos de la disciplina, deteniéndose en aspectos tales como los diferentes escenarios de seguridad actuales que, de seguro, resultarán muy del interés del lector; pasando por consideraciones acerca de las estrategias de seguridad españolas, así como los cambios forzados por la globalización y el acortamiento de los ciclos de decisión, entre otros aspectos; se presentan igualmente los diferentes niveles de decisión y se expone la necesidad de disponer de la inteligencia adecuada en cada uno de ellos; se analiza brevemente la necesidad de que los diferentes organismos de inteligencia coordinen sus actividades en pro de un mejor servicio a la nación, y se finaliza, a modo de ejemplo, con la presentación de la arquitectura de inteligencia en la Fuerzas Armadas españolas. En sus conclusiones, el autor señala muy acertadamente que, entre otros atributos, «la inteligencia en beneficio de la seguridad del Estado ha de ser integral, multidisciplinar, oportuna, colaborativa...»; y, quizás mucho más importante aún, que, en el mundo de la inteligencia se impulsa actualmente la creación de comunidades, grupos de trabajo, equipos multidisciplinarios, virtuales o no, que trabajen y compartan conocimiento, integrados en un sistema con una dirección única, con unidad de acción, en beneficio de la seguridad de todos.

En el segundo capítulo, se realiza un detenido estudio de la situación de seguridad, tanto en el ámbito nacional como en el nivel internacional, considerando los riesgos y amenazas a las que se enfrentan las sociedades actuales, derivando de ello la necesidad de disponer del conocimiento necesario para hacerles frente adecuadamente. Además de los actores, se presentan y analizan igualmente los factores (geográfico, demográfico, económico, etc.) que influyen en los primeros, de forma determinante en muchas ocasiones. Se contemplan en detalle los riesgos y amenazas consideradas en las estrategias de seguridad publicadas en los últimos años en España, así como los factores potenciadores de aquellas. A lo largo de un detallado estudio de las premisas y desarrollo correspondiente realizado en el marco de la Estrategia de Seguridad Nacional, se llega a identificar y exponer de forma minuciosa el concepto de inteligencia integral, que desemboca también en la necesidad de que exista una perfecta coordinación de los diferentes organismos de inteligencia para la constitución de una auténtica comunidad de inteligencia en España. En línea con ello, se realiza un repaso de las recomendaciones de la Comisión de Investigación del 11-M, y del «escaso fruto de las mismas», en palabras del autor, quien, como se ha dicho anteriormente, concluye con que, en España, no solo debe existir una comunidad de inteligencia bien organizada, eficaz y eficiente, sino también con la necesidad de que exista una «reserva de inteligencia» y una fuerte «cultura de inteligencia y seguridad», aunque finaliza reconociendo que «queda mucho camino para esa comunidad de inteligencia y esa cultura de inteligencia».

«Los campos de actuación de la inteligencia» es el título con que el autor del tercer capítulo expone la importancia de la inteligencia en el proceso de la toma de decisiones a la hora de definir y adoptar la estrategia/política de las organizaciones. Se resalta la importancia de actividades, como el análisis, de muy poca o nula visibilidad, pero esencial dentro del conjunto de actividades que conforman el denominado ciclo de inteligencia. Ciclo que el autor analiza desde una perspectiva moderna, en contraposición al modelo tradicional, más rígido, pero más universalmente aceptado; se plantean diversas alternativas encaminadas a «redefinir» el ciclo, todas ellas interesantes.

Otro de los aspectos interesantes de este capítulo es el análisis que se realiza de las implicaciones del escenario de seguridad actual en los procesos de inteligencia y en el personal que participa en los mismos; de igual manera, es novedoso el estudio que se presenta referente al papel que juega la inteligencia en el proceso de toma de decisiones en diferentes situaciones o campos de aplicación, destacando el dedicado al estudio de la Inteligencia de Alertas, con los factores que influyen en la misma, pasando a proponer posibles maneras de mejorar el análisis de inteligencia en apoyo a la toma de decisiones, y finalizando con el papel e influencia de los medios de comunicación en la actividad de inteligencia.

A la detallada presentación de los diferentes actores, humanos y materiales, que participan en el proceso de producción de inteligencia, se dedica el cuarto capítulo, destacando del estudio realizado las consideraciones que se formulan en referencia a aquellos que juegan el papel más decisivo: los recursos humanos, en todos sus roles, pero especialmente, los analistas de inteligencia. Con todo, son las relaciones entre el personal dedicado a inteligencia y los clientes o usuarios del producto, elemento de reflexión, dado que, de la calidad e intensidad de las mismas depende en gran medida el nivel de satisfacción de estos últimos.

Por otra parte, el autor recoge dos cuestiones que impregnan la argumentación: el impacto de la tecnología en el proceso de inteligencia y el alcance del proceso de inteligencia en las tomas de decisiones. Así, respecto a lo primero, se entiende que la tecnología ha tenido un impacto directo en el propio trabajo de inteligencia, con el desarrollo de multitud de herramientas informáticas que ayudan a automatizar partes del proceso y otorgan agilidad al mismo; y, por otro lado, el autor explica que ha «optado por la deconstrucción del llamado ciclo de inteligencia para presentar cada una de sus fases, la relación entre ellas, y los actores implicados en las mismas desde el punto de vista de su necesaria imbricación, y también con el propósito práctico de poder abogar por la introducción de la inteligencia –su uso y su puesta en práctica en cualquier marco conceptual– para toda organización, independientemente de su tamaño». Puede resumirse su visión de la inteligencia en una frase que emplea muy acertadamente: «Si no está orientada a la acción, no tiene consecuencias operativas y no llega a tiempo; no es inteligencia».

Finaliza el documento con el capítulo dedicado a presentar los beneficios de la inteligencia en apoyo a la política/estrategia de las organizaciones. Se consideran en el mismo las amenazas actuales y el incremento del nivel de incertidumbre respecto a tiempos pretéritos, lo que revaloriza aún más, si cabe, el papel que la inteligencia representa en la toma de decisiones. Para proporcionar al lector una guía completa en su recorrido por el mundo de la inteligencia, se le presentan un completo conjunto de conceptos fundamentales acerca de la disciplina; de sus ámbitos de aplicación; de lo que inteligencia puede, y no puede, proporcionar al usuario; así como una detallada descripción de la tipología de inteligencia, desde la que se precisa para el apoyo a la toma de decisiones en todos los niveles (estratégico, operacional y táctico), y sus características diferenciales, hasta la clasificación de la misma en razón al origen de la información (fuente) en la que se basa, pasando por sus diferentes clases.

De igual manera, se realiza un recorrido completo por el término «inteligencia», en sus acepciones de «producto», «actividad» y «servicio», para asegurar que el lector llegue a diferenciarlos, y aprehender la importancia de su correcto empleo. Por otra parte, se presentan una serie de disciplinas que, con el transcurso de los años, y debido principalmente a la introducción en el mundo empresarial de conceptos y métodos aplicados principalmente en el ámbito gubernamental, han adquirido carta de naturaleza y una indiscutible y creciente importancia: inteligencia de negocios, inteligencia competitiva, inteligencia empresarial, inteligencia tecnológica, inteligencia comercial o de mercado, inteligencia económica.

Se lleva a cabo un breve análisis de la inteligencia como servicio, en referencia a los diferentes organismos dedicados a dicha función en España, finalizando el mismo con un llamamiento a la implantación de una fuerte, cohesionada y eficiente comunidad de inteligencia; al desarrollo de una auténtica cultura de inteligencia; a la creación de una Universidad Nacional de Inteligencia, u órgano académico equivalente; así como al desarrollo e implantación de una fuerte «reserva de inteligencia» en el tejido social de la nación.

Somos conscientes de que, el lector que recorra todos y cada uno de los capítulos que componen este documento, encontrará repeticiones en más de una ocasión; pero también lo somos de que, prácticamente en ninguno de esos casos, hallará discrepancias sino, más bien, visiones desde ángulos diferentes, lo que, a nuestro juicio, enriquece el texto más que estropearlo.

En cualquier caso, el objetivo común de los autores al embarcarse en la aventura de redactar este texto no ha sido otro que el divulgar, de la manera más sencilla y completa posible, una materia que es objeto de deseo, tema de tertulia y, casi siempre, una gran incógnita. Esperamos y deseamos sinceramente que, por lo menos, este último aspecto quede desterrado después de la lectura atenta de este documento.

## Capítulo primero

### Ideas fundamentales sobre inteligencia

Juan Bautista Sánchez Gamboa

#### Resumen

Se trata de un recorrido por los fundamentos básicos de la inteligencia, deteniéndose en aspectos tales como los diferentes escenarios de seguridad actuales; pasando por consideraciones acerca de las estrategias de seguridad españolas, así como los cambios forzados por la globalización y el acortamiento de los ciclos de decisión, entre otros aspectos; se presentan igualmente los diferentes niveles de decisión y se expone la necesidad de disponer de la inteligencia adecuada en cada uno de ellos; se analiza brevemente la necesidad de que los diferentes organismos de inteligencia coordinen sus actividades en pro de un mejor servicio a la nación, y se finaliza, a modo de ejemplo, con la presentación de la arquitectura de inteligencia en la Fuerzas Armadas españolas. Se señala que, entre otros atributos, «la inteligencia en beneficio de la seguridad del Estado ha de ser integral, multidisciplinar, oportuna, colaborativa...»; y, quizás algo mucho más importante aún, que, en el mundo de la inteligencia se impulsa actualmente la creación de comunidades, grupos de trabajo, equipos multidisciplinarios, virtuales o no, que trabajen y compartan conocimiento, integrados en un sistema con una dirección única, con unidad de acción, en beneficio de la seguridad de todos.

**Palabras clave**

Inteligencia, unidad de acción, oportunidad, objetividad, accesibilidad, globalización, escenario, sistema, organización funcional, interacción, multidisciplinar.

**Abstract**

This is a journey through the basics of intelligence, stopping on aspects such as the different security scenarios we are currently facing, passing through considerations about the Spanish security strategies, and changes forced by globalization and shortening decision cycles, among others. Different levels of decision making are also reviewed, setting out the needs for an adequate intelligence to each level. It analyses briefly the need for the various intelligence agencies to coordinate their activities for a better service to the nation. And it ends, by way of example, with the presentation of the intelligence architecture within the Spanish Armed Forces. It notes that, among other attributes, «*Intelligence for the benefit of State Security must be comprehensive, multidisciplinary, timely, collaborative ...*»; and perhaps much more importantly, the world of intelligence is currently promoting the creation of communities, working groups, multidisciplinary teams, virtual or not that work and share knowledge, integrated into a system with a single management with unity of action in the interest of everyone's safety.

**Keywords**

Intelligence, unity of action, opportunity, objectivity, accessibility, globalization, scenario, system, functional organization, interaction, multidisciplinary.

Estoy convencido de que no hay nadie que dude de la importancia de la inteligencia, y menos cuando nuestra sociedad se encuentra actualmente en la tesitura de dar respuesta a retos como el que supone la lucha contra el terrorismo, un fenómeno extenso, que se manifiesta en un espacio muy amplio pero no continuo, en general con una base ideológica común, pero que no es homogéneo, ni en sus objetivos, ni en sus procedimientos, ni dispone de una estructura general a la que combatir.

### El escenario

*«We live in a dynamic world in which the pace, scope, and complexity of change are increasing. The continued march of globalization, the growing number of independent actors and advanced technology have increased global connectivity, interdependence and complexity creating greater uncertainties, systemic risk and less predictable future»<sup>1</sup>.*

En un periodo pretérito, el sistema de relaciones internacionales se podía explicar siguiendo un modelo estático en el que –simplificando– dos actores fuertes y expansionistas interactuaban, muchas veces a través de terceros, en defensa de sus intereses, sin que elementos transnacionales perturbaran su hegemonía. Cierto es que ningún modelo es único y puro, porque son intentos de explicar realidades donde conviven otros modelos diferentes, e incluso un mismo modelo impele hacia el cambio creando sus propios mecanismos evolutivos: así, el mundo bipolar creó las bases para la multipolaridad, a través de exitosas estrategias integradoras que dieron lugar, por ejemplo, a la constitución de múltiples organizaciones internacionales de todo tipo. Sin duda, ello contribuyó a evitar la guerra. No obstante, la ruptura del equilibrio al caer el sistema, supuso, de un lado, la desmembración y desaparición de uno de los actores principales, dejando al segundo el liderazgo de un mundo inestable y desequilibrado. La característica de aquel periodo era, en términos de geopolítica global –aunque suponga una simplificación de un largo periodo en el que sucedieron multitud de eventos de carácter histórico diversos y trascendentes– la estabilidad, el estatismo. En el marco de un escenario internacional anárquico, en ausencia de un derecho internacional aceptado por todos y con falta de mecanismos eficientes de represión para quienes lo vulneran –que parece eficaz contra los Estados, pero que es inútil frente a estructuras paraestatales– el modelo antiguo, junto con el equilibrio de poder entre los fuertes, era un mecanismo realista para mantener la paz, al menos entre los actores más poderosos. Ello se lograba con una política de poder, del fuerte al débil, en la que la autonomía de los subordinados queda sometida a un reparto tácito entre los grandes en el que no son consultados como actores, ni contemplados sus intereses. El modelo anterior, basado en el establecimiento de zonas de influencia y

---

<sup>1</sup> J. M. McConnell, Director of National Intelligence. Visión 2015.

su lucha por ellas, tenía como referente a los Estados. En ese modelo, estatista, era difícil que apareciera con virulencia el fenómeno terrorista actual, si bien sus semillas ya estaban plantadas. Cada vez es más evidente que las organizaciones estatales clásicas, las fronteras, se han visto superadas por el cambio. Los Estados con sus herramientas, por poderosas que sean, tienen dificultades para controlar sus espacios de soberanía, superados en un mundo dinámico, opuesto al estático del pasado inmediato. La comunicación global, los flujos migratorios, los procesos de integración regional y, a la vez, las descentralizaciones administrativas, hacen perder peso al Estado. Ciertamente no es un proceso generalizado o, más bien, que no se produce al mismo ritmo en todo el globo. Las coyunturas revolucionarias, que constituían un acelerador de la historia, están presentes ahora, en forma distinta a la lucha de clases, pero con carácter casi universal, el terrorismo yihadista es un ejemplo claro. Los atentados del 11 de septiembre, el 11 de marzo en Madrid, los atentados de Londres, el de París, son un ejemplo de la porosidad de la seguridad clásica frente a las nuevas amenazas.

Vamos a aproximarnos a un ejemplo de actualidad; no es lo mismo el Dáesh que el Frente Al Nusra, Al Qaeda en el Sinaí tenía objetivos distintos que Al Qaeda en el Magreb, Al Shabab busca otra cosa diferente a la que pretende Boko Haram, o el Movimiento para la Unidad y la Yihad en África Occidental, o Al Murabitún. Unos quieren controlar territorios, otros derribar gobiernos. Unos utilizan tácticas de guerrilla, otros son más próximos a la guerra convencional... se hace uso del terror, se ataca en el corazón de las capitales europeas, reclutan en nuestro entorno y allá donde estén (incluso en Australia, por citar un lugar lejano). Unos se alimentan de capital aportado por seguidores, otros por tráfico ilícito... Tiene el atractivo de la ideología que lo sustenta y la motivación de sus combatientes es innegable ¿sería posible dar una respuesta única a un fenómeno con tantas variables? Evidentemente, no. Dado que la inteligencia es base de la lucha contra esos fenómenos, y esta solo se produce a partir de información fiable y oportuna, las organizaciones de inteligencia deben disponer de una capacidad multidisciplinar que permita anticiparse a un enemigo que se mueve en un escenario mutante, porque vivimos en un mundo dinámico en el que el ritmo, amplitud y complejidad del cambio se incrementan y la oportunidad en la acción es una de las claves del éxito.

La globalización, el creciente número de actores y la tecnología avanzada han aumentado espectacularmente la conectividad global, la interdependencia y la complejidad de las relaciones, creando grandes incertidumbres, riesgos sistémicos y un futuro menos previsible.

Si consideramos el globo como un sistema, los cambios demográficos y sociales, la integración económica, la innovación tecnológica, son factores de cambio en este mundo dinámico, factores de cambio que configuran también la amenaza y la facilitan. Estos cambios han conducido a la necesidad de contar con tiempos de respuesta y alarma reducidos y ciclos de decisión cortos. Además, si bien cada uno de estos factores puede ser motor del cambio por



sí mismo, la interacción entre los mismos unido al potente factor psicológico de la ideología, amplifica los efectos creando, desde el punto de vista de la seguridad, riesgos y amenazas, a veces imprevisibles, que evidentemente van más allá de fronteras y organizaciones estatales. Es en ese sistema global donde se ubican los grupos terroristas en sus diversas maneras. Si antes la guerrilla, en el concepto maoísta, debía ser con respecto al pueblo como el pez al agua, ahora, el terror se mueve en el océano global con gran impunidad. En este ambiente, la clave para conseguir una ventaja estratégica en la lucha contra este y otros fenómenos similares es la habilidad para, rápida y ajustadamente, adaptarse a cambios complejos y anticiparse a la acción.

Nos encontramos en un escenario incierto que muta a gran velocidad, donde la adaptación ha de ser sistemática. Los riesgos y amenazas adquieren carácter transnacional y precisan de la interacción bilateral o multilateral entre Estados para hacerles frente. La diversificación y complejidad de la amenaza y de los riesgos exige la unidad de acción por parte del Estado, que debe materializarse en un Sistema de Seguridad Nacional, apoyado por una comunidad de inteligencia abierta a las capacidades que la sociedad dispone, integradora, ágil y capaz de dar respuesta oportuna y eficaz a los riesgos y amenazas emergentes.

Parece coherente ante esta situación, ante esta aceleración de la historia, y los riesgos y amenazas que plantea, adaptarse mediante una visión integral, capaz de definir el problema y de darle solución incluso antes de que se produzca, y ante esto se precisa alinear las capacidades nacionales con otras, en nuestro caso, europeas, bilaterales y multinacionales.

Citando parte del resumen ejecutivo de la *Estrategia de Seguridad Nacional de 2011*:

*«Los límites entre seguridad interior y la seguridad exterior se han difuminado. Las políticas nacionales en los ámbitos tradicionales de la seguridad ya no son suficientes para salvaguardarla en el siglo XXI. Solo un enfoque integral, que conciba la seguridad de una manera amplia e interdisciplinar a nivel nacional, europeo e internacional, puede responder a los complejos retos a los que nos enfrentamos».*

El escenario amplio, interdisciplinar, se extiende a áreas ya no geográficas sino del conocimiento en toda su extensión; desde los aspectos culturales a los económicos, tecnológicos o militares. Pero, además, no se trata de buscar equilibrios que eviten resultados de ganar-perder, sino de hallar soluciones para que, de ellas, surja el beneficio de todos, ganar-ganar, aproximándose posturas en campos nacionales, bilaterales o multinacionales para solventar problemas comunes como, por ejemplo: la inmigración ilegal, la radicalización o el terrorismo.

Es preciso actuar sobre todos los aspectos y no se puede hacer desde una única perspectiva sino desde distintas para abarcar la globalidad del proble-

ma: el enfoque integral se debe aplicar también a la lucha contra la radicalización violenta.

### El marco estratégico militar

La Directiva de Política de Defensa establece alguno de los elementos a considerar para garantizar los intereses del Estado. Entre ellos, la participación en las estructuras multinacionales de seguridad y defensa, incrementando además, las relaciones bilaterales con países que comparten intereses comunes con España, mejorar el esfuerzo conjunto en operaciones, reducir el riesgo de ataques cibernéticos y –muy importante– reforzar los sistemas de obtención de información y de elaboración de inteligencia.

Hoy en día no solo se contempla la posibilidad del conflicto convencional, sino que también se consideran otros actores no estatales, la proliferación de armas de destrucción masiva, el crimen organizado, la competición por recursos energéticos o las injerencias en espacios comunes no sometidos a soberanía nacional, pero también las acciones subversivas. El conflicto convencional, la guerra clásica, son también una posibilidad dentro del marco de la lucha contra el fenómeno terrorista –véase la guerra de Irak o Siria– y está sometida al proceso de cambio de los tiempos. Como todo estado de necesidad, la guerra es un proceso adaptativo que necesita ser estudiado permanentemente, y para el que no vale siempre la misma respuesta, ni aun en los mismos supuestos. Si nos fijamos en los últimos cien años, la humanidad ha conocido guerras que se han llamado convencionales, subversivas, revolucionarias, civiles, de liberación o independencia y en el momento actual se sufren ciber-ataques, y se participa en guerras asimétricas, surgen las «guerras híbridas» y pronto podría haber ciberguerras.

La característica principal del entorno estratégico actual es la complejidad de los elementos que intervienen en él. Los clásicos «factores de la decisión»: situación, terreno, enemigo y medios, conforme se abre el objetivo, para pasar del campo táctico, al operacional y de allí al estratégico se complican enormemente y varían del Sahel al Cuerno de África y de allí a la península del Sinaí o a Mosul. Este ambiente complejo difumina en ocasiones la tradicional percepción de la amenaza, la identificación del esfuerzo enemigo o la determinación de su centro de gravedad, en términos tácticos, y dificulta la identificación del estado final del conflicto con la idea clásica de victoria o derrota. Ante la complejidad y diversidad de la amenaza se precisa un conocimiento capaz de abordar un espectro de materias que difícilmente una sola organización estatal podría abarcar. Por ejemplo, hasta hace poco se ponía en duda la relación entre crimen organizado y terrorismo cuando hoy grupos como el de Moktar bel Moktar viven de esto o ¿cómo se puede considerar el tráfico de petróleo procedente de las zonas controladas por el Dáesh o la producción de amapola en Afghanistan?

En un entorno rápidamente mutable las estructuras orgánicas se vuelven obsoletas prematuramente, pecando el organizador de responder a las lecciones aprendidas en la última de las guerras o de las crisis y no a los retos del futuro inmediato. Para paliar este fenómeno se precisa la ventaja en la información y la anticipación que proporciona la inteligencia; así se podrá evitar o, en su caso, ganar la batalla decisiva que será la primera y, con un poco de fortuna, la última.

Todo, tanto lo nacional, como lo bilateral, como lo multinacional en materia de seguridad, ha de ser visto desde el prisma del cambio en el que estamos inmersos sin perder un instante la vista de la amenaza que muta y se adapta al cambio. Todas las instituciones deben participar en un proceso de revisión permanente para anticiparse a una realidad cambiante, una especie de «Larga Marcha»<sup>2</sup> pero de avance continuo.

*«Cuando el ritmo del cambio externo a tu organización sobrepasa al interno, el fin está próximo»<sup>3</sup>.*

El escenario es, como ya he dicho, de tiempos de alarma y respuesta reducidos, y de ciclos de decisión cortos, siendo la clave del éxito la anticipación, que se facilita a través de la inteligencia oportuna. Además, la guerra, el conflicto, la crisis, la defensa de los intereses nacionales tiene múltiples actores que deben trabajar integrados para dar respuesta a situaciones complejas. La *Estrategia de Seguridad Nacional 2013* da una respuesta al crear la estructura del Sistema de Seguridad Nacional (Consejo de Seguridad Nacional y Comités especializados). Los procesos administrativos para la construcción de este sistema serán largos e insoslayables, pero todo responde a una necesidad y se dirige a satisfacer un principio básico que es el de la «unidad de acción».

Hablamos de tiempos de alarma y respuesta reducidos, de ciclos de decisión cortos; hablamos de «anticipación». Si nos dotamos de la organización, hay que alimentarla con el conocimiento. La información, la inteligencia precisa y oportuna es clave en todo proceso de toma de decisiones, es la base de todo el edificio de la seguridad nacional. Solo hay que enumerar los riesgos y las amenazas a las que hay que hacer frente para darse cuenta del reto. Un compromiso que va más allá de límites fronterizos, ya que muchos de estos riesgos y amenazas son de carácter transnacional.

Los riesgos y amenazas definen de forma genérica los objetos de interés de la inteligencia; aquello que debe atender precisa y oportunamente para facilitar la decisión de la autoridad que corresponda, del decisor en cualquier caso.

---

<sup>2</sup> La «Larga Marcha» fue el viaje a través del interior de China que siguieron las tropas del Ejército Rojo chino, las fuerzas armadas del Partido Comunista de China (PCCh), entre los años 1934 y 1935, huyendo del ejército de la República de China.

<sup>3</sup> Jack Welch ex CEO de General Electric.

## Una aproximación al concepto

La inteligencia produce conocimiento sobre el escenario de que se trate, sea el campo de batalla militar, el comercial o industrial, el político, o cualquiera que podamos imaginar, y sobre los actores de esos escenarios. Intenta descubrir las intenciones e intereses de estos actores, su capacidad y motivación. Tiene que dar a conocer cómo interactúan estos con otros actores de diferentes escenarios y la dinámica de sus relaciones con los demás. La inteligencia debe mirar hacia adelante, para permitir al decisor tener la iniciativa, basándose en el estudio metódico del pasado y el seguimiento preciso de la situación actual. En este sentido, la inteligencia se suele calificar de básica, que provee información del contexto, de elementos que constituyen referencia para el planeamiento, actual, que refleja la situación presente. Esta última es dinámica, y requiere tiempos de respuesta muy cortos para facilitar la toma oportuna de decisiones.

«Ciencia es la opinión verdadera acompañada de razón» Platón.

La inteligencia es una disciplina que abarca aspectos como el razonamiento lógico desarrollado por programas informáticos, los procesos de análisis metódicos de la información, el tratamiento automatizado de datos, la obtención de información por sistemas clásicos o tecnológicamente avanzados, y no puede definirse más que como una disciplina científica. Se puede entender inteligencia como una disciplina científica que se aplica a campos variados, militar, económico, social, político... cuyo objeto es proporcionar elementos de juicio a quien debe tomar las decisiones para fundamentar estas.

«El fin de la investigación no es la acumulación de hechos, sino su comprensión y que esta solo se obtiene arriesgando y desarrollando hipótesis precisas que tengan un contenido empírico más amplio que sus predecesores».

Como paso previo, puede ser preciso determinar a qué nos referimos cuando hablamos de inteligencia en este texto, porque difiere su interpretación según quien y en qué contexto se nombre. Sin ir más lejos, las definiciones que proporciona la Real Academia de la Lengua, en las acepciones más aproximadas al sujeto que queremos estudiar, no nos aclaran en su totalidad el concepto «inteligencia». Así la define el Diccionario como:

- La capacidad de entender o comprender.
- Resolver problemas.
- El trato y correspondencia secreta de dos o más personas o naciones entre sí.

Ninguna de estas acepciones llega a satisfacer plenamente el concepto inteligencia, en el sentido que pretende este trabajo, toda vez que la inteligencia que tratamos requiere de la capacidad de entender o comprender, pero con una finalidad que es la de poner en manos de quien decide elementos de

juicio basados en el conocimiento adquirido para fundamentar sus decisiones. Pero, siguiendo con las definiciones, si intentamos profundizar o hallar la respuesta apoyándonos en qué entiende la Academia por un servicio de inteligencia, encontramos que se define como una «Organización del Estado que proporciona al poder ejecutivo análisis e información para mejorar la toma de decisiones estratégicas orientada a prevenir o neutralizar amenazas y a defender los intereses nacionales». Así, la Real Academia limita el servicio en un nivel concreto que es el del poder ejecutivo y con una finalidad específica «mejorar la toma de decisiones estratégicas». Hemos avanzado en el sentido de comprender que la inteligencia es un apoyo a la decisión, que proporciona análisis e información con una finalidad concreta. Quizás esta definición pueda ser reduccionista al tratar de definir un único servicio en un único nivel cuando normalmente hay más de una organización; que, entre las distintas organizaciones dedicadas a inteligencia, puede haberlas no estatales; y porque las necesidades de información y análisis no solo son inherentes al poder ejecutivo, sino a otros organismos e instituciones del Estado y del ámbito privado, que requieren, tanto en el campo de la seguridad como en el puramente competitivo, información analizada para facilitar las decisiones. Yendo al campo militar, la definición tampoco encaja y, aunque los límites entre los tres niveles clásicos<sup>4</sup> de conducción de la guerra, como veremos más adelante, se difuminan cuando se trata de inteligencia, existe una clasificación de la misma en estratégica, operacional y táctica, que se refiere al nivel de responsabilidad del usuario al que se sirve. La doctrina de la Organización del Tratado del Atlántico Norte define estos niveles<sup>5</sup>:

- *Strategic Intelligence as intelligence required for the planning and the provision of indications and warning, at the national and/or international levels.*
- *Operational intelligence is defined as intelligence required for the planning and conducting of campaigns at the operational level, focusing on detailed reporting regarding the capabilities and intentions of actors and hazards to develop commanders understanding and to assist in his decision-making.*
- *Tactical intelligence is required for the planning and execution of operations at the tactical level to achieve short-term mission, task or action.*

En la organización militar, los tres niveles de conducción de las operaciones clásicos: estratégico, operacional y táctico corresponden con sus equivalentes en «inteligencia». Las fronteras entre estos niveles, desde el punto de vista de la inteligencia, se han difuminado completamente, gracias a los excelentes medios de transmisión de información existentes que permiten disponer de la información adquirida casi en tiempo real, vertical y también horizontalmente. Así, un mando de nivel táctico puede aprovechar información obtenida por un medio de carácter estratégico y viceversa. Es decir, hoy en día, un sistema satélite, o un vehículo sin piloto, adquiere información

---

<sup>4</sup> Estratégico, operacional y táctico.

<sup>5</sup> AJP2 capítulo 3.

que puede ser explotada simultáneamente por un jefe de compañía sobre el terreno, y producir inteligencia a nivel táctico para cumplimentar su misión y, en el nivel operacional o estratégico la misma información, ser utilizada para producir inteligencia y facilitar la decisión en esos niveles de mando, pero también, recíprocamente, información obtenida por elementos de reconocimiento de ese jefe de compañía, a nivel táctico, puede ser explotada por quien decide en lo alto de la pirámide de la estructura.

La inteligencia puede ser definida también como el producto resultante de la obtención y del procesamiento de información sobre la situación, capacidades e intenciones de personas u organizaciones, incluyendo Estados y entidades no estatales, en el ámbito nacional o internacional, con capacidad o intención de influir en otros, para identificar amenazas y ofrecer oportunidades para la explotación por los usuarios<sup>6</sup>.

*«Intelligence plays a critical role by providing the processed information required to develop understanding. This includes answering the main intelligence question of what, where, why, how, who and when, and providing the context and narrative of events»<sup>7</sup>.*

La inteligencia contribuye a facilitar la comprensión de forma continua y coordinada de una situación compleja y a fundamentar las decisiones. Es una ayuda para llegar a comprender qué sucede, por qué sucede y qué puede suceder, constituyendo una herramienta clave para quien decide, esté en el nivel de decisión y en el ambiente, político, económico, militar, de seguridad que sea.

«La necesidad de saber, es una característica innata al ser humano. Al igual que la capacidad de anticiparse a los acontecimientos. Lamentablemente, a lo largo de la historia, la primera característica ha sufrido un desarrollo mucho mayor que la segunda. De este modo, con el paso de los siglos, el ser humano ha ido aprendiendo que el proceso de interpretación y percepción de la realidad es enteramente subjetivo; estando condicionado por la percepción de lo que supone una amenaza para conseguir la maximización de los intereses propios. Hoy sabemos que la toma de decisiones que no se basa en patrones estables, se rige por meras elecciones al azar con un 50% de acierto, pero también con un 50% de error. De este modo, partiendo de patrones estables basados en referencias pasadas, adquiridas por la experiencia propia o de otros, desde el principio de los tiempos, sabemos que los monarcas, caudillos y comerciantes de los distintos pueblos, posteriormente Estados y entidades empresariales, han buscado la manera de «ver lo que hay al otro lado de la colina», tanto para conseguir ventajas en la toma de decisiones, como para evitar sorpresas estratégicas, por medio de una su-

---

<sup>6</sup> Traducción de la definición del AJP2.

<sup>7</sup> Joint doctrine publication 2-00 understanding and intelligence support to joint operations. UK.

perioridad en la información. Este sería uno de los elementos principales del término inteligencia; la reducción de la incertidumbre en cualquier proceso de toma de decisiones. En el estudio en profundidad de estos argumentos encontramos otra de las bases que configuran la naturaleza del término inteligencia: la concepción del «otro». La inteligencia, por sí misma, supone el intento de maximizar lo propio con respecto del «otro», que es considerado extraño, ajeno al grupo. Según esta concepción, la inteligencia existe porque unos actores tratan de conseguir información reservada de otros ocultando la suya propia. El uso de la inteligencia supone la toma de conciencia del «otro», de la diversidad de intereses y de la diversidad de interpretaciones de la realidad. La inteligencia es fruto de la subjetividad del ser humano y es usada como una herramienta contra lo diferente. Y este es el origen de la conRAINTELIGENCIA<sup>8</sup>, de la protección de los intereses propios ante los esfuerzos de otros por conseguir los suyos, y de las actividades realizadas para maximizar la situación propia con respecto a la de los demás.

En resumen, el término inteligencia posee dos partes diferenciadas que completan su esencia. La naturaleza del concepto inmutable desde la antigüedad, la cual está basada en la información y la prevención y que consiste en proporcionar información útil que ayude al proceso de toma de decisiones. Tanto en las acciones destinadas a proteger la propia información de los esfuerzos de conocimiento del «otro», como en las acciones encubiertas, destinadas a maximizar los intereses propios. Por otro lado, el carácter del término, que puede ser revolucionario y es dependiente de la estructura en la que se lleva a cabo el trabajo de inteligencia, donde distintas organizaciones tienen métodos propios que caracterizan e individualizan su aplicación y uso en otros sistemas. En ocasiones, este carácter se puede ver influenciado por los cambios (culturales, tecnológicos, profesionales, entre otros) que, a través de los tiempos, la actividad ha sufrido. Por tanto, la esencia de la inteligencia expuesta anteriormente es independiente de los cambios temporales que la aplicación de esta herramienta ha sufrido a lo largo del tiempo en las diversas organizaciones donde se ha implantado. Todo lo demás son añadidos, como lo son los servicios de inteligencia. Es cierto que los servicios de inteligencia realizan inteligencia, pero no toda la inteligencia la realizan exclusivamente los llamados servicios de inteligencia. De hecho, los términos inteligencia y servicios de inteligencia no son equivalentes. La distinción principal reside en que si bien la función principal de la inteligencia es que los encargados de tomar decisiones en cualquier organización, dispongan de mayores alternativas de elección consiguiendo superioridad estratégica a través de una superioridad informacional; los servicios de inteligencia no son más que una herramienta de la maquinaria del Estado que realiza labores de inteligencia. Cuando Sherman Kent afirmaba que la

---

<sup>8</sup> ConRAINTELIGENCIA son las acciones dedicadas a evitar las amenazas a la seguridad llevadas a cabo por servicios de inteligencia hostiles, organizaciones o individuos dedicados al espionaje, sabotaje, subversión o terrorismo.

inteligencia era información concerniente a la seguridad nacional en 1949, los actores no estatales se encontraban relegados a un segundo plano y la lucha de Bloques situaba a los servicios de inteligencia estatales en el ojo del huracán. Hoy, sesenta y cinco años después, los servicios de inteligencia siguen siendo la punta de lanza de la seguridad del Estado y así seguirá siendo, pero ya no son los únicos actores a tener en cuenta en el juego de la inteligencia. Así, en la naturaleza de los servicios de inteligencia (que no de la inteligencia) se encuentra la respuesta al porqué de las diferencias en su estructura. Porque los servicios de inteligencia son un reflejo de la organización política y el espacio temporal en el que operan y, cada servicio de inteligencia del mundo tiene unas peculiaridades distintas, protocolos propios y estructuras dispares. Por tanto, si durante la Guerra Fría los servicios de inteligencia, de cada lado del telón de acero, debían prestar gran atención al desarrollo de las capacidades militares del enemigo, las amenazas y riesgos que caracterizan el entorno internacional en este comienzo del siglo XXI inclinan la balanza de los objetivos de la inteligencia hacia las intenciones. En gran medida, hoy la realidad es mucho más compleja, lo cual tiene un claro impacto en la idea de interés nacional (concepto determinante en las políticas exteriores de cada país y muy ligado al ascenso del Estado nación como forma moderna de asociación exclusiva de los Estados). Este concepto queda en entredicho, no solo por la proliferación de actores no estatales en la esfera internacional y el consecuente aumento de distintos intereses contrapuestos (acelerado también por la falta de cohesión social dentro de las propias fronteras estatales), sino también por cuestiones como la lucha por los recursos escasos, la escasez de alimentos, las fuentes de energía, o como las cuestiones medioambientales. En definitiva, riesgos que superan las fronteras nacionales y la capacidad de dar respuestas unilaterales y unidimensionales. Nos encontramos ante un entorno más complejo, más problemático y más interdependiente donde la cooperación y la competición van de la mano»<sup>9</sup>.

El objeto, la finalidad de la inteligencia, será distinto según su campo de aplicación, pero los procesos, el método, aun con variantes, siempre sigue los mismos pasos. Es esta una de las razones por las que, independientemente del adjetivo que se añada (inteligencia militar, económica, etc.) la inteligencia puede estudiarse como una disciplina científica. A lo largo de la historia, la inteligencia se ha utilizado de forma intuitiva o sistemática porque siempre ha sido preciso disipar la «niebla de la guerra»<sup>10</sup> para poder aplicar el esfuerzo allí donde el enemigo era más débil, o anticiparse a sus movimientos.

<sup>9</sup> José M<sup>a</sup> Blanco Navarro, Gustavo Díaz Matey «Presente y futuro de los estudios de inteligencia en España»... *Documento Marco 11/2015* 4. Instituto Español de Estudios Estratégicos.

<sup>10</sup> Clausewitz menciona en su obra *De la Guerra* que la naturaleza ambigua de la información durante el transcurso de la guerra hace que los comandantes tomen decisiones fundamentadas en la intuición (Fingerspitzengefühl). La definición de «niebla de la guerra» ha ido evolucionando desde que en 1827 escribiera sus ocho libros sobre la naturaleza de la



En multitud de ocasiones lo obvio es esencial; de hecho, no hay dificultad en comprender la obviedad de que, para poder llevar a cabo cualquier actividad, se precisa disponer de sensores que capten la información necesaria, desde la espacio-temporal, para dar un paso al andar, hasta la que se precisa para los más complejos procesos intelectivos y que, además, esa información haya de ser rápidamente transmitida y comparada con otras, obtenidas en situaciones similares, para que, al final, tras el análisis casi instantáneo de la misma, una orden motora ponga en marcha la musculatura y el pie se apoye en el lugar preciso sin que nos caigamos ni tropecemos. Esto no difiere en nada del proceso que requiere la complejidad de una decisión de carácter político, económico o militar.

La sencillez del ciclo de inteligencia<sup>11</sup>, de cada una de sus fases, su obviedad, esconde rigor, precisa una aproximación sistemática, un método, sin el que el proceso de elaboración de inteligencia podría bien no llegar a ningún resultado o, lo que es peor, conducir a decisiones erróneas por falsear el resultado. El método está inspirado en unos principios, entre los que podemos considerar como esencial, y piedra angular del todo, el de unidad de acción o unidad de esfuerzo que debe contar con una única dirección.

En ese sentido, el director de Inteligencia Nacional de los Estados Unidos, refiriéndose a la comunidad de inteligencia norteamericana<sup>12</sup> hablaba de transformarla en «*a globally networked and integrated intelligence enterprise*»<sup>13</sup> para lograr la ventaja en la decisión porque la seguridad<sup>14</sup> depende en gran medida de anticipación y en evitar que el adversario pueda llevar a cabo sus planes. Totalmente alineado con esas ideas, está el enfoque que tiene la

---

guerra. En las batallas de mediados del siglo XIX los informes que llegaban al comandante procedían de diversas vías, generalmente de subordinados que llegaban de diferentes partes del frente. Las informaciones recibidas de las operaciones de reconocimiento son incompletas, subjetivas, fragmentadas e imprecisas en la mayor parte de las ocasiones.

<sup>11</sup> Intelligence cycle

The sequence of activities whereby information is obtained, assembled, converted into intelligence and made available to users. This sequence comprises the following four phases:

a) Direction – Determination of intelligence requirements, planning the collection effort, issuance of orders and requests to collection agencies and maintenance of a continuous check of the productivity of such agencies.

b) Collection- The exploitation of sources by collection agencies and the delivery of the information obtained to the appropriate processing unit for use in the production of intelligence.

c) Processing- The conversion of information into intelligence through collation, evaluation, analysis, integration and interpretation.

d) Dissemination- The timely conveyance of intelligence, in an appropriate form and by any suitable means, to those who need it. (AAP-06 2012).

<sup>12</sup> Conjunto de agencias estatales dedicadas a inteligencia en los Estados Unidos.

<sup>13</sup> J. M. McConnell (Director of National Intelligence). Vision 2015.

<sup>14</sup> Seguridad es la condición que se alcanza cuando determinada información, material, personal, actividades e instalaciones están protegidas contra el espionaje, sabotaje, subversión o terrorismo.

*Estrategia de Seguridad Nacional 2013* española. Este documento prevé «una nueva estructura institucional capacitada para abordar las cuestiones estratégicas de la seguridad y de la gestión de las crisis necesitadas de una respuesta rápida, coordinada e integral» y señala como primer principio informador de la estrategia la unidad de acción «que supone la implicación, la coordinación y la armonización de todos los recursos del Estado..., así como la colaboración público-privada y la implicación de la sociedad en general». El segundo de los principios informadores de la Estrategia de Seguridad Nacional<sup>15</sup> mencionados en ella es el de anticipación y prevención «que han de orientar la acción del Gobierno a la detección y la reconducción de situaciones que pueden representar un potencial riesgo o amenaza para la seguridad nacional». Ambos, unidad de acción, que implica una dirección única, y la anticipación y prevención son principios clave en inteligencia.

Los campos de batalla, no son como los tableros de ajedrez, donde cada contrincante es capaz de ver las fuerzas y el dispositivo enemigo y conoce de antemano su objetivo. En el campo de batalla, las piezas, las unidades, se ocultan y se mueven sigilosamente, las reglas del juego no son uniformes y las capacidades de los adversarios son diferentes. Y, aunque se pueda conocer el objetivo que pretende el enemigo, se desconoce cómo actuará para conseguirlo. Si nosotros pretendemos lograr un efecto sobre él deberemos tener en consideración datos, información y, tras su análisis, obtener la inteligencia precisa para que el responsable disponga de elementos de juicio que le permitan tomar, junto con otros factores, las decisiones oportunas.

Si fuéramos capaces de abarcar el globo terráqueo, se nos presentaría un escenario absolutamente complejo donde fenómenos naturales, sociales, políticos, económicos y culturales interactúan entre intereses y ambiciones.

---

<sup>15</sup> Los principios informadores de la Estrategia son:

1. Unidad de acción que supone la implicación, la coordinación y la armonización de todos los actores y los recursos del Estado bajo la dirección del presidente del Gobierno, así como la colaboración público-privada y la implicación de la sociedad en general. El enfoque integral de la seguridad, comprensivo de todas sus dimensiones, justifica este principio de acción y precisa, a su vez, de una gestión completa a través de un sistema de seguridad nacional impulsado y liderado por el presidente del Gobierno;
2. Anticipación y prevención, que han de orientar la acción del Gobierno a la detección y la reconducción de situaciones que pueden representar un potencial riesgo o amenaza para la seguridad nacional;
3. Eficiencia y sostenibilidad en el uso de los recursos, un principio que, si bien debe presidir en todo momento la actuación administrativa, cobra especial significación en un contexto como el presente. Se sustenta en la priorización de los recursos y la optimización de su empleo, precisa el control y la evaluación de los resultados y orienta la organización administrativa;
4. Resiliencia o capacidad de resistencia y recuperación, principio relativo a la aptitud de los recursos humanos y materiales para afrontar con flexibilidad y fortaleza las situaciones de crisis y sobreponerse a ellas minimizando y absorbiendo sus consecuencias negativas.

Tanto el campo de batalla moderno, como el globo no pueden ser abarcados con una sola mirada. En otras épocas, el general, desde un puesto dominante en el campo de batalla, era capaz de tomar las decisiones al abarcar la totalidad del mismo, muchas veces de forma intuitiva; ahora, para ser capaces de comprender el escenario, hace falta más de una mirada. Si en un proceso motor, como el de dar un paso, apenas se requiere decidir hacia donde nos movemos; si el general del siglo XIX, como el jugador de ajedrez, era capaz de dar órdenes sin precisar más que de su propia apreciación de la situación, la batalla moderna y el mundo actual, en su complejidad, requieren organizaciones especializadas orientadas hacia distintas áreas dotadas de voluntad integradora para poder sumar capacidades de las que no disponen y ser capaces de mantener entre sí una colaboración ágil, siendo innovadoras para mantener siempre la ventaja intelectual, organizativa y tecnológica sobre el adversario potencial o real.

*«It is impossible to capture all complexities of modern intelligence in a single document»<sup>16</sup>.*

La complejidad de la materia de la inteligencia, no permite simplificaciones ni soluciones simples.

En el estudio comparativo efectuado en el documento del Instituto Español de Estudios Estratégicos «A qué responden las estrategias de seguridad nacionales»<sup>17</sup> se realiza un análisis comparativo, «de alcance limitado», de distintas estrategias<sup>18</sup>. El autor determina en él que todas ellas ponen énfasis en la importancia de la «anticipación» y la «prevención» y, también, que los documentos son coincidentes en defender un enfoque integral de la seguridad donde hay que superar la mera coordinación y lograr la integración de los instrumentos nacionales para hacer frente a las amenazas; integración que se indica ha de ser horizontal y también vertical. Para lograr esa integración, se proponen similares reformas administrativas. En primer lugar, potenciando el papel de la Presidencia del Gobierno u oficina del primer ministro en el ámbito de la seguridad nacional y residenciando en ella los órganos de apoyo a los Consejos de Seguridad Nacional. En segundo lugar, crean-

<sup>16</sup> Allied Joint Doctrine for intelligence, counter- intelligence and security AJP2.

<sup>17</sup> Amador Enseñat y Berea. «A qué responden las estrategias de seguridad nacionales». IEE 2012.

<sup>18</sup> La canadiense de 2004 (*Securing an Open Society: Canada's National Security Policy*), la holandesa de 2007 (*National Security: Strategy and Work Programme 2007-2008*), las tres, elaboradas en menos de dos años, por el Reino Unido: las del gobierno laborista de 2008 (*The National Security Strategy of the United Kingdom. Security in an interdependent world*) y su actualización de 2009 (*The National Security Strategy of the United Kingdom: Update 2009. Security for the Next Generation*), así como la del gobierno de coalición conservador-liberaldemócrata de 2010 (*A Strong Britain in an Age of Uncertainty: The National Security Strategy*), el *Libro blanco francés de 2008 (Défense et Sécurité nationale: le Livre Blanc)*, la norteamericana de 2010 (*National Security Strategy*) y la española de 2011 (*La Estrategia Española de Seguridad. Una responsabilidad de todos*).

do órganos, interministeriales<sup>19</sup> para integrar la respuesta de los diferentes departamentos. En tercer lugar, mejorando la integración de los servicios de inteligencia<sup>20</sup>. En cuarto lugar, creando órganos para implicar al sector privado y a la sociedad civil<sup>21</sup>. En quinto lugar, potenciando el papel del Parlamento<sup>22</sup> y, en sexto lugar, creando órganos para facilitar la participación de las capacidades civiles en esa respuesta integrada y su coordinación con los militares. En definitiva, se pretende superar la mera coordinación y lograr la integración de los instrumentos nacionales para hacer frente a la amenaza. Esto afecta directamente a las organizaciones nacionales dedicadas a la inteligencia evidentemente, ya que impulsa a dotarlas de mayor capacidad de anticipación redundante en la seguridad.

Para organizaciones como la OTAN, el reto es afrontar situaciones complejas<sup>23</sup> donde se encuentran actores y amenazas como las siguientes:

- El terrorismo.
- Los Estados hostiles.
- Estados frágiles y Estados fallidos.
- Las amenazas híbridas.
- La globalización.
- Los fenómenos naturales impredecibles.
- La proliferación de armas de destrucción masiva.

De estos, como última en incorporarse, está la «amenaza híbrida», que es definida como aquella que se produce cuando concurren amenazas convencionales clásicas, la guerra irregular y la asimétrica y se combinan en el mismo tiempo y espacio, pero no solo esto, sino que el conflicto puede involucrar a individuos, grupos o Estados con un carácter transnacional que operen global y localmente. Así, nos podemos encontrar con conflictos que incluyan violencia entre distintos grupos locales o regionales, terrorismo, ataques cibernéticos, crimen organizado, insurgencia... en fin, una situación aparentemente caótica, pero que es considerada, y podría ser dirigida, como un todo, donde los objetivos se alcanzan con todos los medios posibles. Como ejemplo de este tipo de situaciones está la de la recuperación<sup>24</sup> de la península de Crimea por Rusia y la desafección de su Gobierno central de las provincias de Doneskt y Lugansk del este ucraniano. Un escenario semejante, de una complejidad tremenda, muestra necesaria una inteligencia todo

---

<sup>19</sup> National Security Council, Conseil de Défense et de Sécurité Nationales o el Consejo de Seguridad Nacional y las Comisiones Interministeriales.

<sup>20</sup> El *Libro blanco francés* propone la creación de un Conseil National du Renseignement.

<sup>21</sup> National Security Forum británico, Conseil Consultatif sur la Défense et de la Sécurité Nationale francés.

<sup>22</sup> En el Reino Unido el Joint Parliamentary Committee on the National Security Strategy.

<sup>23</sup> AJP2 (edition A version 1 ratification draft 2015).

<sup>24</sup> Si se considera la pérdida de Crimea por Ucrania esta ha sido un acto provocado por Rusia.

acimut que utilice un amplio abanico de fuentes<sup>25</sup> de información y agencias para poder entenderlo. Esto implica capacidades tecnológicas avanzadas y, sobre todo, humanas con aptitudes en áreas del conocimiento muy variadas de las que difícilmente una organización estatal sola es capaz de disponer.

Pero no es solo la complejidad del escenario sino también la abundancia de información disponible que, por una parte, es difícil de adquirir en su totalidad por la propia limitación de los medios tecnológicos y humanos disponibles, y, por otra parte, la hacen difícilmente manejable. La habilidad para gestionar y manejar información relevante rápidamente puede ser crítica para lograr la oportunidad en la inteligencia que se genere. Esto requerirá una coordinación perfecta y una aproximación conjunta, eficiente y flexible de distintos elementos trabajando con una misma finalidad. Los «que deciden», en cualquier nivel, necesitarán generar en sus organizaciones estructuras capaces de gestionar esos grandes volúmenes de datos e información, evitando la saturación por sobrecarga<sup>26</sup>, para producir inteligencia oportuna y fiable.

Un escenario complejo exige una aproximación multidisciplinar para su análisis. Compartir los puntos de vista de distintas disciplinas sobre un escenario cualquiera ayuda a aproximarse a la verdad sobre el mismo; implica, no solo a los elementos expertos de inteligencia sino también a otras disciplinas disponibles como, por ejemplo, pueden ser economistas, ingenieros, expertos en psicología social.

La «unidad de acción» en materia de inteligencia se pretende conseguir a través de diversas soluciones desde el punto de vista de la organización, más o menos centralizadas y dirigistas, o descentralizadas y colaborativas, estas últimas proporcionando gran iniciativa a los actores. Un ejemplo claro de la complejidad de las organizaciones estatales descentralizadas dedicadas a la inteligencia es la estadounidense, con más de una decena de agencias, o bien las soluciones centralizadoras de países como Argelia. ¿Cuál es más eficaz? Si la eficacia pudiera medirse en términos de éxito-fracaso deberíamos conocer en profundidad los servicios, y comparar, tarea difícil por la naturaleza discreta de los mismos. Se pueden mencionar los grandes éxitos históricos de los servicios de la antigua Alemania Democrática, como ejemplo de servicio centralizado, consiguiendo información de la Organización del Tratado del Atlántico Norte, o de la eficacia de los servicios del Département de la Sécurité et du Renseignement argelino en la lucha contra el Group Islamique Armé<sup>27</sup>, o de fracasos en las organizaciones descentraliza-

<sup>25</sup> Persona u objeto del que puede ser obtenida información.

<sup>26</sup> Se cifra en 2 zettabytes (4 millardos de gigabytes) el volumen de información disponible a través de Internet. En cinco años la información en red se ha multiplicado aproximadamente por nueve.

<sup>27</sup> The Armed Islamic Group (GIA, from French: Groupe Islamique Armé; Arabic: *جبهة إسلامية* al-Jama'ah al-Islamiyah al-Musallaha) was one of the two main Islamist

das, por ejemplo la norteamericana, al no haber sido capaces de anticipar los ataques del 11 de septiembre del año 2001 o evitar que se produjeran filtraciones, como la del caso Snowden, empleado de la National Security Agency; sin embargo, también podemos encontrar ejemplos negativos en las organizaciones centralizadas, como el error del servicio alemán en la Segunda Guerra Mundial, incapaz de identificar la fecha ni el lugar donde se iba a producir el desembarco aliado sobre el continente europeo, y de éxitos en la colaboración entre distintos servicios de información e inteligencia, como los muchos que, en la lucha contra el terrorismo de la ETA, se han conseguido en España. Podemos, pasado el tiempo, conocer algún hecho que permita aventurar que tal o cual servicio fue eficaz en un determinado caso, o que se fracasó en tal otro, pero es más normal achacar, de forma inmediata, como fracaso de los servicios de inteligencia, la comisión de un atentado, como los del 11 de marzo de 2004 en Madrid, los del 11 de septiembre de 2001 en Nueva York, los del 19 de noviembre en París, del 7 de julio de 2005 en Londres, o la sorpresa estratégica conseguida por Egipto y Siria el 7 de octubre de 1973 en el inicio de la guerra del Yom Kipur. Lo cierto es que los éxitos de los servicios no se suelen conocer con la inmediatez de sus fracasos o, si se conocen, lo es tiempo después de conseguidos. En cualquier caso, el análisis de los fracasos identifica, independientemente de que el sistema de inteligencia sea centralizado o descentralizado, como lección aprendida que la información debe fluir, que deben dejar de existir barreras estructurales (y también prejuicios) que hagan de compuertas a la información de forma que quien debe tomar decisiones en cada caso, aunque sea a través de estructuras u organizaciones complejas, disponga de la inteligencia necesaria oportunamente y pueda tomar las medidas que considere al respecto. Pero, si lo anteriormente expuesto se refería a una actitud defensiva –evitar el ataque terrorista, evitar la sorpresa militar–, la necesidad de conocer a un adversario potencial también requiere, para su mayor eficacia, el esfuerzo conjunto. El adversario debe estudiarse desde múltiples aspectos: político, económico, militar... La seguridad, los aspectos relacionados con ella, están íntimamente relacionados con la sociedad, con la organización estatal, con su política, con su historia, con su economía, y las decisiones dependen de sus dirigentes, que también son objeto de interés de inteligencia. Intereses, ambiciones, miedos, prejuicios dentro del campo social, repercuten en ellos. Aunque pueda parecer anecdótico, hasta la salud de estos puede suponer un factor importante de estudio; un ejemplo de ello fue el seguimiento que se hizo de personajes públicos de primera línea como los líderes de la Unión de Repúblicas Socialistas Soviéticas, Bréznhev o Andrópov, en un periodo crucial de la Guerra Fría, cuando el equilibrio de las superpotencias estaba ca-

---

insurgents groups that fought the Algerian government and army in the Algerian Civil War. It was created from smaller armed groups following the 1992 military coup and arrest and internment of thousands of officials in the Islamist Islamic Salvation Front (FIS) party after that party won the first round of parliamentary elections in December 1991. It was led by a succession of emirs (commanders) who were killed or arrested one after another.

mino de romperse definitivamente y la inestabilidad podía conducir a situaciones de riesgo para la seguridad. El campo es tan amplio que difícilmente puede ser abarcado desde un solo punto de vista y, si lo es, será siempre tamizado por la perspectiva de la disciplina desde la que se estudie, sea la que sea: militar, policial, económica, sociológica. El conjunto requiere visión conjunta para llegar a comprender, primero, y luego comprender, analizar y obtener conclusiones del todo. Para lograr esto se precisa la «unidad de acción» (o unidad de esfuerzo), que no implica necesariamente soluciones orgánicas, pero sí el desarrollo de una idea, la identificación con un propósito común. El principio de unidad de acción es clave en inteligencia. La política de Estado, seguida ya por dos Gobiernos con tendencias distintas, para el desarrollo de la estrategia de seguridad con la creación del Consejo de Seguridad Nacional, pretende la acción coordinada de todos los elementos que juegan un papel en nuestra seguridad. Es evidente que, simultáneamente a la estructuración de un sistema de seguridad nacional, nuestra comunidad de inteligencia juega un papel cada vez mayor y más relevante aportando anticipación y prevención, y no debe quedar atrás en ese proceso.

Los atentados del 11 de septiembre de 2001 contra los Estados Unidos dieron lugar a una profunda y apartidista reflexión en ese país, a un juicio crítico que tuvo su mayor exponente en el informe elaborado por la Comisión Nacional organizada al efecto. Parte de las recomendaciones del informe final de la Comisión se centraron en la comunidad de inteligencia norteamericana, proponiendo medidas que permitieran una mejor coordinación de sus componentes que rompieran las barreras estructurales identificadas. De hecho, de las cinco recomendaciones elevadas en materia de reorganización, tres se refieren a inteligencia y contrainteligencia, y van específicamente dirigidas a reforzar el principio de unidad de acción y proponiendo la creación de la figura del National Intelligence Director:

- *Unifying strategic intelligence and operational planning against Islamist terrorists across the foreign-domestic divide with a National Counterterrorism Center.*
- *Unifying the intelligence community with a new National Intelligence Director.*
- *Unifying the many participants in the counterterrorism effort and their knowledge in a network based information-sharing system that transcends traditional governmental boundaries*<sup>28</sup>.

Más de catorce años después de ese histórico 11 de septiembre, la mayor potencia del mundo se ha ocupado de mejorar su organización de inteligencia, dotándola de esa capacidad de dirección única y estableciendo flujos de información e inteligencia verticales y horizontales que, de algún modo, han roto barreras estructurales. Esto describe algo que va más allá de la constatación de un hecho, constituye la definición de un objetivo: la voluntad de lograr una auténtica y eficaz «comunidad de inteligencia»; también en España,

<sup>28</sup> The 9/11 Commission report Authorized edition. Ed. Norton.

donde la creación del Centro de Inteligencia contra el Terrorismo y el Crimen Organizado (CITCO), dependiente de la Secretaría de Estado de Seguridad, mediante la integración del Centro Nacional de Coordinación Antiterrorista (CNCA) y del Centro de Inteligencia Contra el Crimen Organizado (CICO) ha sido un paso en ese sentido, aunque sea a nivel ministerial. Pero habría que empezar por definir qué es la Comunidad de Inteligencia española. Es fácil, en principio, contestar a esta pregunta: son todos los que trabajan en esta área; es la voluntad de lograr con ellos lo que, parafraseando la definición clásica militar de acción de conjunto como «la concurrencia al mismo fin de cuantos elementos intervienen en la batalla»; en este caso, en la batalla de la información, de la inteligencia; batalla que rompe los límites del interés particular de cualquiera de las partes interesadas por la interrelación que existe entre todas ellas. Interrelación que es tanto mayor cuanto más alto es el nivel, abarcando más y más, al conjunto. Así pues, la comunidad de inteligencia sería el conjunto de gabinetes, centros, unidades, estados mayores, planas mayores, grupos de trabajo, equipos, redes... que adquieren información por medios orgánicos, o no, desde los multinacionales hasta los propios de las más pequeñas unidades u organizaciones, compartiendo y analizando la información adquirida, elaborando inteligencia para satisfacer las necesidades de sus mandos respectivos, y difundiendo los productos obtenidos, todo en un proceso continuo. ¿Es esto posible? Se puede responder afirmativamente: Lo es. Lo es desde el punto de vista teórico; la organización, los medios disponibles, las capacidades tecnológicas, lo permiten. Se trata con ello de maximizar el rendimiento de los recursos, materiales y humanos disponibles, e integrar en una única organización, con una sola dirección, el conjunto de capacidades del que estamos provistos, de sumar los esfuerzos de todos en aras de lograr una mayor eficacia. Pero, para que exista una comunidad debe haber un interés común: ¿Tienen las mismas necesidades de información, de inteligencia –por ejemplo– el presidente del Gobierno, el ministro del Interior, el de Defensa, el de Industria, el jefe de Estado Mayor de la Defensa, los jefes de Estado Mayor de los Ejércitos y la Armada, o el jefe de una unidad desplegada en un teatro de operaciones? evidentemente, no. ¿Los procedimientos de obtención utilizados en la lucha antiterrorista, o en la acción policial, son los mismos que los empleados por una unidad militar? probablemente, tampoco. Sin embargo, desde el presidente del Gobierno hasta el jefe de una pequeña unidad, comparten un interés común: *la seguridad*, cada uno a su nivel. Cada cual, en la comunidad de inteligencia, puede diferir en sus necesidades de inteligencia, en los procedimientos y en sus medios de obtención, pero esto no debe ser considerado una traba, sino algo natural, derivado del área de especialización de cada uno; las partes del conjunto no son iguales, pero todas forman parte del mismo. Cada parte de la comunidad se organiza, se dota, se prepara y actúa en función de sus propias necesidades. Dentro de la comunidad de inteligencia, se encuentra un área de especialización que es la inteligencia militar, de la que forman parte los Ejércitos y la Armada, que cuenta con su propia organización, personal



y recursos específicos con un único objeto: facilitar la toma de decisiones en el ámbito de las operaciones actuales, en el planeamiento de las futuras y alertar sobre posibles escenarios de actuación; su área de competencia principal son las operaciones militares, así como en el Ministerio del Interior se ha creado el CITCO, en el Ministerio de Defensa existe el Centro de Inteligencia de las Fuerzas Armadas. La clave para lograr la unidad de acción en el conjunto de la comunidad de inteligencia es conseguir romper las barreras estructurales entre sus miembros, y para ello falta dotar a la comunidad de inteligencia de una dirección única. La acción de mando, la dirección, en una organización de inteligencia se manifiesta de una forma muy determinante, entre otras cosas, en la decisión sobre qué, sobre cuáles son los objetos, asuntos, actividades o escenarios de interés, reflejados desde las más altas directivas, planes, hasta en las órdenes de operaciones, y en decidir quiénes tienen necesidad de saber sobre ellos. Una vez adoptada la decisión, definido el objeto de interés, el siguiente paso es identificar e integrar a todos los niveles o escalones de decisión que precisan conocer sobre el mismo en los flujos de información que se generen, facilitarles el acceso a la información en un entorno seguro y explotar sus capacidades específicas. Por ejemplo, en el campo militar, las operaciones determinan el objeto, y ahí es clásica la división entre lo futuro y lo presente, cada uno con un tempo distinto y con unas necesidades diversas pero concurrentes. Identificar posibles escenarios de actuación, riesgos, amenazas, conocerlos y disponer de la información básica sobre los mismos es el primer paso, y muchas veces el único, porque, si se identificaron correctamente esos posibles escenarios, la anticipación que proporciona la inteligencia a la autoridad, facilitará la toma de decisiones que eviten la escalada. Pero, puede que se pase de este estadio inicial y entonces la información obtenida, la inteligencia producida, se aplicará a las operaciones en curso y requerirá una actualización continua. Así, la dirección en inteligencia es una función permanente que garantiza la unidad de acción; se inicia mucho antes de comenzar las operaciones, antes siquiera de que se presuman, y se mantiene durante todo su desarrollo, contando para ello con la organización –estructura, arquitectura...– de la inteligencia adecuada.

Esta inteligencia debe basarse en principios como el de accesibilidad; hace ya mucho tiempo que la inteligencia de «caja fuerte y armario blindado», aquella a la que se tenía acceso con dificultades ingentes y que solo unos pocos podían explotar y que era más propia de la Guerra Fría; donde era preciso acumular datos, identificar despliegues de armas y unidades, trabajos de fortificación, frecuencias de radio, en la que había, como alguien dijo, «que contar tanques» o descubrir despliegues, como en la crisis de los misiles en Cuba. La información, la inteligencia desarrollada a partir de aquella, ha de estar al alcance de quien debe resolver, de quien va<sup>29</sup> a tomar decisiones

---

<sup>29</sup> La Crisis de los misiles en Cuba es como se denomina al conflicto entre los Estados Unidos, la Unión Soviética y Cuba en octubre de 1962, generado a raíz del descubrimiento

basándose en ella, de quien la precisa: la inteligencia ha de ser accesible. No tiene ningún valor aquello de lo que no disponemos. En esa época pretérita podía darse el caso de considerarse la inteligencia un fin en sí misma, luego ella misma se anulaba por su inaccesibilidad. Aún restan prejuicios en esta materia constituyendo otro de los vicios de los viejos servicios de inteligencia, vicio próximo, a veces, al «síndrome de Diógenes»<sup>30</sup>, acumulando informes e información sin que nadie pueda explotarlos. Ciertamente es que la política de «armarios abiertos» para facilitar esa accesibilidad exige prudencia; hay que determinar quién puede y debe acceder a cada estante manteniendo siempre el control de acceso. Compartir información e inteligencia dentro de la propia organización, Fuerzas Armadas, Ministerio del Interior, Defensa, es relativamente fácil; compartir entre organismos de un mismo Estado, empieza a ser más complejo; hacerlo de forma bilateral con otros Estados, requiere siempre acuerdos mutuos y control, y hacerlo en un ambiente multinacional exige un gran rigor. Es muy propio que en ambientes multinacionales en operaciones militares se establezcan representaciones oficiales con el fin de compartir información, como son las National Intelligence Cells (NIC,s) pero, incluso en estas operaciones, en las que teóricamente todos tienen la misma necesidad de conocer sobre la misma materia y, en consecuencia, debiera haber la misma necesidad de compartir información, se organizan grupos, algunos formalmente instaurados, como el de los «Five Eyes» con Estados Unidos, Gran Bretaña, Canadá, Nueva Zelanda y Australia. Este ejemplo de «insolidaridad informativa», que puede impedir la accesibilidad a inteligencia que pudiera ser de utilidad, provoca rechazo, crea desconfianza y puede llegar a afectar al buen fin de las operaciones, pero puede tener justificación de carácter histórico o cultural, lo que es muestra de la complejidad del asunto.

Un aspecto clave para compartir información es hacerlo oportunamente. La oportunidad es clave en inteligencia; el ritmo del cambio en el campo de batalla, en la sociedad, en el planeta es tal que la información queda obsoleta en plazos muy breves. Información que ha de ser analizada<sup>31</sup> en tiempos muy cortos por equipos de analistas y transformada en inteligencia. El analista de inteligencia es la figura clave en el ciclo, en él reside la responsabilidad de orientar o iluminar a la persona que decide en cada momento, de proporcionarle inteligencia. El analista de inteligencia ha de vivir permanentemente en la duda metódica hasta aproximarse, muchas veces de forma

---

por parte de Estados Unidos de bases de misiles nucleares soviéticos en territorio cubano. En Rusia se la denomina Crisis del Caribe (en ruso *Карибский кризис*, *Karibskiy krizis*), mientras que en Cuba se le llama Crisis de octubre.

<sup>30</sup> El síndrome de Diógenes es una enfermedad mental, que hace que el individuo que la padece se dedique a acumular basura en su domicilio.

<sup>31</sup> Análisis es el paso en la fase de producción de inteligencia en el que la información es sometida a revisión para identificar hechos significativos para su subsecuente interpretación.

casual, a una verdad que también deberá ser puesta en duda y sometida a su propio juicio, previamente a ponerla en manos de quien decide. Esto implica disponer de una potente estructura de inteligencia, con un sistema nervioso capaz de transmitir la información rápidamente a múltiples centros neurálgicos donde equipos de analistas la exploten oportunamente, adaptándose a los cambios de situaciones fluidas en muy corto plazo. Plazo que es también de decisión que, si no se respeta, impide que la persona que decide pueda resolver, que pueda tomar la decisión adecuada. Para facilitar esto, la tecnología permite poner en manos de uno o múltiples usuarios la información recién obtenida o la inteligencia recién elaborada; además, esa misma tecnología permite al responsable de la custodia de la moderna caja fuerte virtual controlar el acceso a la misma de unos o de otros y determinar qué información o inteligencia pueden explotar en un entorno seguro. Ciertamente que la tecnología es vulnerable, pero lo es menos, y el riesgo que se asume es mucho más reducido que el que se asumía irremediabilmente en la época de los mensajeros a pie o a caballo, o la de las palomas mensajeras, del telégrafo, de los motoristas u otros. Por cierto, la gran ventaja del mensajero a pie, del caballo o de la moto es que reúnen algo que hoy constituye la piedra angular de los sistemas de comunicación, que es la interoperabilidad. La interoperabilidad es uno de los mayores problemas para la intercomunicación de sistemas diferentes, y si a este se une el de los requerimientos de seguridad, en ocasiones extremas, al final podría resultar que el mensajero, utilizando el medio más rápido que tenga a su alcance, pudiera volver a ser de total actualidad. Conseguir la interoperabilidad de los sistemas dentro de un entorno seguro, y que la seguridad de estos no sea un lastre para la operatividad, es difícil de conseguir, lográndose en el marco multinacional y solo en determinadas operaciones al utilizarse sistemas únicos aplicables a la operación concreta. Es preciso alcanzar la interoperabilidad de los sistemas para ser capaces de lograr eficazmente el apoyo mutuo entre diferentes miembros en una operación o dentro de la comunidad de inteligencia y, de paso, conseguir la economía de medios.

Enumerar los principios de cualquier materia suele ser complejo y conduce a error, bien por falta de profundidad en el análisis, bien por subjetividad en la priorización de los mismos o por una conjugación de ambos; subjetividad y escaso análisis. La inteligencia debe ser capaz de comprender escenarios cada vez más complejos y ser capaz de explicar estos de forma objetiva, no sesgada por prejuicios o distorsionada por apreciaciones erróneas. Una aproximación es el modelo de estudio que se utiliza en la Organización del Tratado del Atlántico Norte, que comprende los aspectos políticos, militares, económicos, sociales de infraestructuras y de información (PMESII), pero no solo estos factores son hoy en día suficientes para entender el entorno al estar más enfocados a países o regiones; hoy, los actores no estatales, terroristas o no, requieren ser estudiados con rigor, la interacción entre crimen organizado y terrorismo, el uso del ciberespacio como nuevo campo de batalla, el carácter transnacional de estos, las amenazas provenientes

del medio ambiente o a la salud. Han de ser estudiadas cuestiones de carácter de psicología social, se precisa especialización de carácter técnico en armas nucleares, bacteriológicas o químicas, incluso elementos culturales y artísticos. Los equipos de análisis, militares o no, deben ser capaces de incorporar especialistas en materias diversas para dibujar nítidamente una realidad cambiante.

### Un ejemplo de organización

Incardinada la inteligencia en el Sistema de Seguridad Nacional, esta da también su propia respuesta desde el punto de vista organizativo. Como modelo de organización y de institución centenaria al servicio del estado, las Fuerzas Armadas pueden servir de ejemplo para mostrar un modelo organizativo buscando satisfacer el principio de unidad de acción con una dirección única. La importancia de la inteligencia en las Fuerzas Armadas es obvia; llevando a un extremo, esta se podría afirmar que debe ser la base de su organización, efectivos, armamento, preparación, etc... Si la misión genérica de los Ejércitos es la defensa militar de España, lo es para hacer frente a una amenaza, a un enemigo potencial o real, que ha sido definido por la inteligencia. Para cada escenario la aproximación será distinta: evidentemente de la guerra convencional a la subversiva hay una gran diferencia. La inteligencia militar española se organiza en un sistema, cuya cabeza funcional reside en el Centro de Inteligencia de las Fuerzas Armadas. Este sistema de inteligencia pretende la suma de las capacidades de todos los elementos que trabajan en inteligencia militar en las Fuerzas Armadas españolas. Está orientado por la misión, que tiene una doble faceta de alarma y de apoyo a las operaciones, y puede ponerse como modelo a considerar dentro de la comunidad de inteligencia nacional. Comunidad de inteligencia en el sentido amplio que debe acoger disciplinas que no son exclusivas del mundo de la seguridad y defensa para dar respuesta a este escenario complejo y mutable a gran velocidad donde se ampara el terror. El modelo de estructura del Sistema de Inteligencia de las Fuerzas Armadas es fruto de un proceso evolutivo, recogiendo la experiencia adquirida; es integrador, refuerza la vocación de servicio en apoyo a la decisión y la funcionalidad de la inteligencia. Es integrador porque abarca conceptualmente a todas las capacidades disponibles en las Fuerzas Armadas facilitando al máximo la relación entre ellas; refuerza la vocación de servicio porque pretende poner a disposición de todos los niveles de mando la totalidad de las capacidades disponibles, facilitando la interacción entre sus actores; así, recursos de obtención, análisis y difusión, lejos de estar separados por infranqueables barreras estructurales, actúan bajo una dirección única, de forma que se pueda conseguir la ventaja en la decisión, la anticipación que se solicita, oportuna y objetivamente. El modelo refuerza la funcionalidad de la inteligencia al exigir la máxima fluidez en la gestión de la información por procedimientos automatizados.

La organización de la inteligencia para una operación militar no es fija, es evolutiva. Los actores y los recursos que intervienen en ella cambian al ritmo que se modifica el escenario. Si hacemos un estudio de cualquiera de las operaciones finalizadas o en curso, normalmente, desde la situación inicial, el número de actores que interviene se irá modificando conforme se requiera. A lo largo de todo el proceso debe existir la capacidad de integrar actores y recursos, con oportunidad, para garantizar permanentemente las necesidades de inteligencia de todos los escalones de mando. El ejercicio de la dirección, en su más amplio sentido, permite la continuidad de este apoyo. La organización de la inteligencia para cada escenario debe contemplar a todos y a cada uno de los actores, y ser capaz de integrar todo cuanto requiera, en función de la evolución de la situación y de las necesidades operativas. La dirección trata de identificar las carencias y solventarlas, saber dónde están los recursos e integrarlos, temporalmente o no, en la estructura, en la arquitectura de inteligencia, de cada operación concreta. En el planeamiento de cualquier operación, el analista de inteligencia es el encargado de abrir el telón mostrando el escenario a los que –centros, unidades, organismos, personas– tengan necesidad de conocerlo. En el proceso de análisis se parte siempre de una situación inicial, donde el escenario se percibe de una forma borrosa; es preciso conocerlo en detalle, definirlo. El volumen de información disponible sobre cualquier escenario es tan grande y crece de una manera tal que exige una actuación sistemática sobre ella para permitir al analista acceder a aquello que le es necesario, sin falta alguna, desde cualquier entorno y en condiciones seguras. El análisis es multidisciplinar, y eso implica especialización en áreas de conocimiento y recursos diversos. La dificultad de disponer permanentemente de expertos en áreas de conocimiento específicas exige mecanismos ágiles, que permitan contar oportunamente con las capacidades que se requieran. Para ello, éstas han de estar identificadas previamente. Ninguna de las partes del sistema tiene la posibilidad por sí misma de abarcar todo, pero cada una dispone de ciertas capacidades y, con ellas y las que le proporciona toda la organización, participará de forma que los productos que se obtengan sirvan oportunamente al conjunto. La clave es sumar las capacidades, integrarlas en una sola organización, de geometría variable, capaz de adaptarse a las necesidades. Una organización en la que la información fluya sin obstáculos y llegue a todo aquel que deba conocerla. Una organización que sume las capacidades aportadas por cada una de las partes que la componen, y satisfaga las necesidades de las mismas. Organización cuya médula espinal sea un sistema físico capaz de gestionar la información, los productos derivados de ella, su difusión; que proporcione las herramientas de análisis necesarias; que sea seguro, pero evitando que la seguridad sea una traba; que sea capaz de «entenderse» con sistemas similares cuando se precise; que pueda «crecer» sin quedarse obsoleto... Un sistema capaz de relacionar la información, de ayudar al analista a componer el puzzle que se presenta ante sí.

Por otra parte, la obtención de la información requiere disponer de medios muy variados cuya adquisición y mantenimiento, en algunos casos, precisa un esfuerzo económico muy elevado, tanto que la asociación de varios países para distribuir el esfuerzo en programas concretos es también común en este ámbito. Todos y cada uno de los escalones de mando y de decisión tienen unas necesidades de información, pero los recursos, personal y medios de obtención son escasos, muy especializados y están encuadrados en unidades orgánicas escalonadas. El empleo de los medios orgánicos de obtención responde, en primer lugar, a las necesidades de información de su unidad o de la organización operativa en que estén encuadrados, pero la información obtenida no es exclusiva de ese nivel. La inteligencia desarrollada a partir de información obtenida por una patrulla en el escenario de combate puede tener repercusión en las decisiones que se tomen hasta en los más altos órganos de decisión política y, recíprocamente, la información obtenida por un medio de obtención compartido multinacionalmente, puede tener valor tanto para los más altos niveles de decisión políticos o militares como para una unidad táctica desplegada sobre el terreno. Esto supone la ruptura de las divisiones teóricas entre los tres niveles clásicos: estratégico, operacional y táctico, por lo menos desde el punto de vista de la obtención. El medio puede ser orgánico de un escalón, por ejemplo, estratégico, como un sistema de satélites, pero la información adquirida puede producir inteligencia de aplicación al nivel táctico. Es más, una misma información tiene lecturas distintas dependiendo del nivel en que se analice. La información no es táctica, operacional o estratégica, lo es la inteligencia derivada de la misma en función del escalón de mando, del nivel que la explote. De una misma noticia se pueden extraer conclusiones que interesen a distintos niveles, siempre en función del punto de vista desde el que se trate. Una misma noticia, una misma información, puede presentar múltiples caras, por lo que no puede sustraerse a quien puede tener necesidad de saber sobre un determinado asunto, es decir: el analista ha de tener libre acceso a la información; pero, es más, tampoco se puede determinar con claridad, en todos los casos, qué puede ser de interés para otro, qué información le permitirá elaborar la inteligencia que su mando precisa. La información sobre determinado objeto debe estar al alcance de todo aquel que tenga necesidad de conocer sobre el mismo. En la caja del puzle tenemos piezas que no corresponden con el modelo; es más, no tenemos un modelo: hay que descubrirlo. Imaginemos un escenario en el que intervengan varias unidades de las Fuerzas Armadas: todas ellas tendrán la misma necesidad de conocer lo que ocurre; la información será analizada para ser aplicada al planeamiento, a la preparación, a las operaciones. Todos estarán atentos a lo que se obtenga y a lo que se elabore sobre ese escenario, todos formularán preguntas para completar los vacíos informativos que detecten. Los cuarteles generales responsables de la generación y preparación de la fuerza necesitarán conocer cómo evoluciona la situación. Las necesidades de información que no sean capaces de solventar por sus propios medios se elevarán para que otros cuarteles

generales, centros, organismos, que dispongan de capacidades superiores, se las proporcionen. La información de contacto, la adquirida durante las operaciones, entrará en el flujo establecido llegando a todos. Los órganos de planeamiento adaptarán la organización, el armamento, la logística y la preparación de las unidades en función de la situación; la decisión política en distintos niveles nacionales y multinacionales se apoyará en análisis de expertos. Nos encontramos con un solo objeto de análisis: un escenario en el que actores diversos están interesados, y lo están de forma permanente en tanto la operación esté en curso. Los actores cambian, pero el escenario permanece. La continuidad del apoyo la asegura una estructura permanente que integra a los actores, a las capacidades que estos aportan, y que solventa sus carencias, añadiendo capacidades propias o facilitando el acceso a capacidades ajenas, militares o no. Una estructura plena y permanentemente integrada en la nacional superior y capaz de enlazar con otras similares multinacionales o de países aliados.

Durante la preparación de una unidad para desplazarse al Líbano, se preguntó al jefe de la misma cuáles eran sus necesidades de inteligencia, él respondió que quería saber lo que pasaba al norte del río Litani<sup>32</sup>. Necesitaba saber qué ocurría allá donde sus medios de obtención no llegaban, pero desde donde el cumplimiento de su misión podía verse alterado. No puede haber solución de continuidad en los flujos de información. En el ámbito de la inteligencia, se necesita de la integración del todo; no debe haber zonas de sombra que detraigan del analista partes del puzle que debe construir, no debe haber capacidades que se sustraigan, que no se pongan a disposición del conjunto. Desde las unidades tácticas sobre el terreno hasta los centros de inteligencia, todos deben acceder a toda la información disponible sobre el objeto del que tienen necesidad de conocer. Cada uno extrae de ella la inteligencia que precisa y así, al partir de la misma base, la concordancia en la apreciación de la realidad y, su consecuencia positiva en la toma de decisiones, aumenta. La información ni puede pasar por tamices que limiten el análisis, ni puede ser vista a través de lentes que la deformen. Negar información a quien tiene necesidad de saber, o intentar dirigir las conclusiones de un análisis, aumenta innecesariamente el riesgo de fracaso de la misión. Las consecuencias de análisis distintos son absolutamente distintas, porque las decisiones que se adopten, tanto en el plano táctico como en otros superiores, serán diferentes.

En nuestras Fuerzas Armadas hoy, como siempre, la preocupación por la seguridad de nuestros soldados y unidades es imperativa, y es una prioridad para el mando. La seguridad está basada en la inteligencia; en ese concepto amplio de inteligencia que integra inteligencia y contrainteligencia, y que es una consecuencia suya. Inteligencia que condiciona la organización de la unidad, el armamento y material de que está dotada, la preparación de sus

---

<sup>32</sup> Río del sur del Líbano que delimita por el norte el área de la misión UNIFIL.

hombres y su forma de combatir; es decir: todo. Desde la pequeña unidad a las Fuerzas Armadas en su totalidad, se planea, organiza, dota, prepara y actúa en función de las necesidades derivadas de su empleo en escenarios presentes o futuros, cuyo conocimiento es una exigencia para todos y cada uno de los distintos niveles de decisión. Inteligencia que, de una manera sencilla, no es más que el resultado del análisis de una información aislada o de un conjunto de ellas. El efecto del conocimiento adquirido es la decisión acertada y su consecuencia, el éxito. La información es la materia prima de la inteligencia.

La primera batalla que debemos ganar es, pues, la de la información, que debe ser completa y oportuna. Para ello es precisa una comunidad de inteligencia nacional sin barreras estructurales en la que la inteligencia militar constituya una organización funcional permanente de apoyo a las operaciones, capaz de integrar y dirigir las capacidades disponibles en las Fuerzas Armadas en materia de inteligencia, y de aportar eficazmente su especialización, identificando situaciones potenciales de crisis, contribuyendo así a la seguridad de todos. La Inteligencia Militar –organizada en un sistema funcional único, aunando las capacidades de todos sus componentes, e integrada plenamente dentro de la comunidad de inteligencia nacional, con una única dirección– es un objetivo a alcanzar.

### A modo de conclusión

Integral, multidisciplinar, oportuna, colaborativa... posiblemente otros atributos más, y más convenientes, sean apropiados para definir cómo ha de ser la inteligencia en beneficio de la seguridad del Estado en la lucha contra los movimientos radicales violentos o frente a cualquier otra amenaza emergente en cualquier campo. Los procesos intelectuales, el planeamiento y la decisión, para llegar a la ejecución de un proyecto, a veces compiten con la realidad; con la velocidad del cambio del escenario geopolítico/estratégico en el que nos movemos y con organizaciones y estructuras que responden a situaciones pretéritas. El informe de la Comisión Nacional sobre los ataques terroristas del 11-S es contundente en sus recomendaciones, llamando al cambio y adaptación de sus instituciones de seguridad, a la unidad de acción y a «romper barreras estructurales». Han pasado ya 14 años desde entonces, pero sus recomendaciones están aún vigentes. La disgregación, la falta de unidad de acción, la estanqueidad, conducen al fracaso: actualmente la tecnología permite la interacción entre distintas organizaciones de forma permanente. Los pasos que se están dando para hacer frente a los riesgos y amenazas actuales son integradores.

En el mundo de la inteligencia se impulsa la creación de comunidades, grupos de trabajo, equipos multidisciplinarios virtuales o no, que trabajen y compartan conocimiento, integrados en un sistema con una dirección única, con unidad de acción en beneficio de la seguridad de todos.



## Capítulo segundo

### Finalidad de la inteligencia

Valentín Díaz Blanco

#### Resumen

Este capítulo aborda la finalidad de la inteligencia, entrando en analizar los actores y factores que condicionan y determinan la vida de la sociedad internacional. Posteriormente se plasman los riesgos y amenazas, la mayor parte asimétricos, basados en las recientes Estrategias Españolas de Seguridad (2011 y 2013).

Una segunda parte del capítulo, está dedicada en primer lugar al concepto de inteligencia, a través de las citadas Estrategias de Seguridad y en la nueva Ley de la Seguridad Nacional. Y en segundo lugar, se analiza el caso español, en cuanto a las estructuras de Inteligencia y la necesidad de desarrollar el concepto de «comunidad de inteligencia», como sistema integrado por agencias y organismos, coordinados por una estructura específica y en la que estén integrados otros estamentos y actores diversos y variados, además de la estructuras de seguridad y defensa. Haciendo hincapié al final en la llamada Cultura de Inteligencia y su implantación en la sociedad civil.

#### Palabras clave

Inteligencia, seguridad nacional, comunidad de inteligencia, cultura de inteligencia.

**Abstract**

This chapter treats the purpose of Intelligence, analyzing the key players and factors that condition and determine life in global society. Afterwards we reflect the risks and threats, most of them asymmetrical, based on the recent Spanish Security Strategies (2011 and 2013). The second part of this chapter is dedicated in the first place to the concept of Intelligence, through the aforementioned Security Strategies and the latest Law of National Security.

Secondly we analyze the case of Spain, regarding intelligence structures and the need to develop the concept of «Intelligence Community», as a system integrated by agencies and institutions coordinated by a specific framework in which other diverse actors besides defense and security bodies are integrated. And finally emphasizing on the so-called «Intelligence Culture» and its implementation in civil society.

**Keywords**

Intelligence, National Security, Intelligence Community, Intelligence Culture.

## Introducción

El siglo XXI es una época de gran transformación, quizá la de más repercusión en la historia. La situación mundial actual comprende la interrelación de un conjunto de procesos políticos, económicos, intelectuales, culturales, demográficos, y ambientales nunca antes vista. La confluencia de estos procesos se hace más aguda por la conectividad del mundo presente, que abarca todo el planeta y es producto de la globalización. Cada uno de estos procesos representa una dimensión del orden mundial, aunque hasta ahora han sido los órdenes político y económico los que han construido el marco referente de la actuación pública y así se manifiesta en el sistema internacional de Estados y en las estrategias de seguridad adoptadas por cada nación.

De la mano de la globalización, varios son los factores que han adquirido especial relevancia en el orden mundial.

La globalización ha tenido un efecto directo en la seguridad. La pacificación y la estabilización de regiones muy alejadas de nuestras fronteras son responsabilidad de todos y especialmente de los países más favorecidos.

Por otro lado, la aparición de organizaciones terroristas y formas de terrorismo que, además de querer implantarse como Estados propios, no tienen fronteras en su capacidad de acción y efectos letales que reparten por todo el planeta.

Asimismo, la globalización ha incrementado las inversiones empresariales exteriores, a la vez que ha favorecido el comercio transnacional y la búsqueda de recursos procedentes de los lugares más diversos del planeta, sin olvidar a los flujos de personas que se mueven por el mundo. Todo ello hace que, cada vez más, los intereses de los países se estén localizando lejos de su territorio.

Este panorama ha hecho que los países se asocien en organizaciones supranacionales para proteger sus intereses, a la vez que contribuyen a la paz y a la estabilidad mundial.

Entre las organizaciones supranacionales creadas cabe destacar las organizaciones multinacionales de carácter regional, como la Unión Europea (UE) o el «G7 más Rusia». Recientemente, y ante la crisis económica mundial, ha sido necesario buscar una nueva fórmula más representativa de la situación internacional, que se ha materializado en el «G20». En palabras de Joschka Fischer «la globalización ha provocado un cambio duradero en el reparto de poder y de oportunidades y ha sentado las bases de un nuevo orden mundial para el siglo XXI» (Fischer, 2008). Los Estados están representados en ellas y, a su vez, hacen pesar sus intereses pero, con frecuencia, ven condicionada su política y su papel internacional por los compromisos adquiridos con anterioridad. Este es el caso de la política económica y monetaria de la UE que se decide en el ámbito comunitario, en detrimento, cada vez más mar-

cado, del protagonismo de los Estados miembros, a pesar de la reticencia de algunos de ellos. La globalización se presentó como una oportunidad para limar diferencias entre sociedades desarrolladas y subdesarrolladas, entre sociedades ricas y pobres, entre sociedades industrializadas y agrarias, entre el norte y el sur. Una oportunidad para aprovechar el cambio social en beneficio de la seguridad internacional, pieza clave del desarrollo.

Paradójicamente, cuanto más se conectan entre sí las sociedades más desarrolladas, más distancia se abre entre estas y aquellas sociedades que carecen de las infraestructuras básicas para poder aprovechar las ventajas de la globalización. Además: «Aunque es cierto que la globalización ha logrado una cierta expansión de la prosperidad, la distribución de sus beneficios no es homogénea y la pobreza sigue siendo un problema de dimensión global» (Stiglitz, 2004).

Otro aspecto negativo que se ha adscrito a la globalización es el fanatismo, que reacciona contra el proceso de modernización, visto como una imposición por los poderes económicos y como un neoimperialismo. Todo ello es causa de frustraciones entre los más pobres, que pueden llegar a generar violencia entre grupos sociales que se consideran agraviados. No es la privación absoluta la que conduce a la protesta, sino la privación relativa: la distancia que hay entre la vida que la gente se ve obligada a llevar y lo que cree que podría lograr de una manera realista. Son las expectativas frustradas las que generan la protesta, e incluso la violencia.

Uno de los factores clave en el rápido desarrollo del mundo global actual ha sido las nuevas Tecnologías de la Información y la Comunicación (TIC). A medida que se han ido desarrollando, el cambio social ha ido tomando protagonismo en nuestras sociedades. La información se convierte en un importante recurso en la economía, en la cultura, en la política y, por supuesto, en las relaciones internacionales.

Entre todas las tecnologías de la información y la comunicación, destacan las que han configurado Internet que, en la última década, se ha convertido en un motor de cambio social y económico, cuyas consecuencias en el ámbito de la política no pueden ser ignoradas.

El fenómeno de los «blogs», de los que se calcula que hay 130 millones en todo el mundo, y las páginas de información en general pueden llegar a constituir un auténtico contrapoder. Esa masa de internautas, que no respeta fronteras y que utiliza la red de redes como foro de debate y cadena de transmisión de ideas, conforma un actor no estatal de gran importancia en los países democráticos.

La telefonía móvil también está dando lugar al surgimiento de masas de ciudadanos que aprovechan las nuevas tecnologías para dinamizar a la sociedad a golpe de mensajerías instantáneas con la finalidad de alcanzar cambios políticos.

El análisis de toda esa realidad social del mundo actual implica, en primer lugar, estudiar los factores que influyen en las relaciones internacionales; cuyo conocimiento resulta indispensable para ayudar a encontrar explicaciones racionales al comportamiento de los actores que se relacionan en dicha sociedad, e incluso para tratar de anticipar sus comportamientos. En segundo lugar, implica caracterizar a los actores, protagonistas vivos de la sociedad internacional que van a determinar su estructura, y sin cuya comprensión difícilmente se podrán extraer conclusiones acertadas sobre los caracteres fundamentales del sistema internacional en los albores del siglo XXI, que es donde actúan los servicios de inteligencia.

También la globalización económica en marcha, que pretende la creación de un mercado mundial en el que se supriman todas las barreras arancelarias para permitir la libre circulación de capitales financieros, comerciales y productivos.

Así, el Fondo Monetario Internacional define este proceso como: «el crecimiento de la integración de las economías de todo el mundo mediante el comercio y los flujos financieros, el desplazamiento de la mano de obra y la transferencia de conocimientos tecnológicos a través de las fronteras internacionales y sus efectos culturales, políticos y medioambientales».

### Factores

Los factores que dejan sentir su influencia en los actores que protagonizan la vida de la sociedad internacional, que, en ese sentido, la condicionan y, en buena medida, la determinan, forman una lista bastante numerosa, siempre abierta a nuevas incorporaciones y con una intensidad variable en su importancia y en las relaciones entre ellos. A pesar de esta advertencia relativizadora, resulta conveniente realizar una serie de consideraciones, en relación a alguno de los factores que son citados de forma recurrente por la doctrina científica como explicativos de las relaciones internacionales, porque ello nos va a permitir comenzar a dibujar el contexto en el que se mueven los Estados y sus instituciones –entre ellas, los servicios de inteligencia– en la sociedad internacional actual.

Siguiendo una aproximación tradicional al análisis de los factores, comenzaremos por el geográfico, en sentido amplio, y, dentro de él, hay que subrayar que, al igual que a finales del siglo XIX –momento en el que Ratzel creó una nueva ciencia donde se estudiarían las relaciones entre la geografía y la política–, la geopolítica sigue teniendo hoy una importancia esencial en el análisis de la sociedad internacional; tanta que, en la actualidad, se habla, además de geoestratégica, de geodemografía y, sobre todo, de geoconomía, como sectores de conocimiento que ayudan a explicar y/o a anticipar comportamientos.

El factor demográfico es el segundo de los grandes factores que ayudan a explicar las relaciones internacionales. Dentro de él, el llamado capital hu-

mano juega un papel esencial tanto en las políticas nacionales como internacionales de los Estados y organizaciones internacionales, y ello desde muy diversos puntos de vista: económico, social, ecológico, científico y, por supuesto, militar. Sin embargo, son probablemente los desequilibrios en el reparto y crecimiento demográfico, y sus efectos los que de manera más acuciante vienen a poner a este factor en el primer plano de las preocupaciones de los Estados. Esta situación, que no hace sino empeorar paulatinamente, provoca en el corto plazo enormes movimientos migratorios que generan problemas concretos de distinta naturaleza y de gravedad variable en los países receptores; incluido el ámbito de la seguridad y, dentro de él, muy especialmente, el control de redes mafiosas internacionales de muy distinto tipo y actividad.

El factor económico en sentido amplio –esto es, comercial, financiero y monetario– supone también un elemento de influencia en el comportamiento de los actores internacionales de gran envergadura. No se trata aquí solo de la voluntad de controlar el acceso a la producción y al mercado de materias primas o de las grandes vías de comunicación tales como canales interoceánicos –Suez, Panamá– o grandes vías marítimas –Gibraltar–. Se trata también de la competencia, cada vez más feroz, que el mundo económico globalizado introduce entre las grandes empresas –transnacionales o no– y que, en buena medida, arrastra a los Estados, fundamentalmente del Norte desarrollado, en sus comportamientos de política exterior.

Lo anterior podría no comprenderse bien, sin embargo, sin profundizar algo más en un nuevo factor de importancia creciente en la sociedad internacional como es el técnico y científico. Como muy bien explicara Marcel Merle: «El progreso técnico afecta bajo todas sus formas (política, militar, cultural y económica) al juego de las relaciones internacionales. Acentúa la interdependencia de los elementos constitutivos del sistema y favorece la unificación del campo de actuación de todos los actores. Pero, al mismo tiempo, acentúa los contrastes, las diferencias de poder entre los actores e introduce nuevas fuentes de tensión y nuevos factores de dominación».

Esta doble faceta como generador de confianza, de lazos de unión más profundos y de una mayor interdependencia, de un lado, y de desigualdades cada vez más abismales, así como de tensiones, de desconfianza y temor, de otro, hace que estemos ante un factor complejo y de difícil concreción, a la vez que, en las últimas décadas, se ha convertido en vector fundamental de todo el devenir de la sociedad internacional.

En efecto, en la época de la, tan manida y muy pocas veces bien comprendida, globalización, nada puede entenderse, y mucho menos ella misma, sin un análisis en profundidad de los avances tecnológicos y científicos que la han hecho posible, a ella y a todo lo que conlleva.

Muy unido a lo anterior nos encontramos con el factor mediático, que, si bien existe ya en buena medida desde el siglo XIX en el plano internacional, al

menos en sus albores –como consecuencia de la aparición de los primeros medios de comunicación de masas que generaron el embrión de opinión pública, tan necesaria para definir la democracia–, será en el mundo actual, como consecuencia del desarrollo de las tecnologías de la información, cuando comience a desplegar buena parte de sus efectos, entre los que cabe destacar la creación, por primera vez, de una verdadera y real opinión pública mundial.

Finalmente, el factor ideológico –espiritual, cultural o identitario, en definitiva, no material– que, lejos de haber disminuido o incluso desaparecido su grado de influencia en los actores internacionales tras el final del conflicto Este-Oeste, continúa siendo un factor esencial, del que se destaca la religión y nacionalismo. En un mundo en el que las ideologías tradicionales han ido perdiendo importancia, en el que el orden bipolar ha desaparecido y ha dejado paso a un vacío, a un desorden que bien puede denominarse, con Ramonet, geopolítica del caos, los individuos se refugian en identidades primarias donde encuentran la seguridad del grupo: religión, etnia, nación.

### Actores

Por lo que respecta a los actores que participan en la sociedad internacional actual, podemos estar viviendo una evolución lenta hacia una mayor institucionalización de la misma como consecuencia de una paulatina decadencia del Estado nación como actor fundamental de las relaciones internacionales. En la actualidad, y una vez constatada la heterogeneidad de la sociedad internacional como el elemento estructural más novedoso de la misma, hay que seguir afirmando la primacía del Estado como actor en la esfera internacional y la vigencia de la soberanía de los Estados como principio rector, tanto de esa sociedad como del derecho que la rige.

La globalización ha favorecido la aparición de nuevos actores no estatales, como las grandes empresas multinacionales, que llegan a tener presupuestos mayores que muchos Estados, a la vez que sus crisis pueden llegar a desestabilizar los sistemas financieros internacionales.

Junto a los dos actores principales de la sociedad internacional –Estados y organizaciones internacionales–, toda una serie de actores más o menos importantes participa en la vida internacional. Algunos de ellos actúan de manera regular, y cada vez más intensa, en la esfera internacional, adquiriendo un protagonismo que les permite influir activamente en la formación de la voluntad de los Estados, y que, precisamente por ello, han sido denominados por algunos como «fuerzas transnacionales»: las organizaciones no gubernamentales (ONG) y las empresas transnacionales.

Finalmente, resulta esencial hacer mención a otros entes que actúan en la sociedad internacional, aunque lo hagan desde la ilegalidad: las redes criminales transnacionales. En las últimas décadas, alentadas por facilidades de

todo tipo –desde el final de la Guerra Fría a los avances en la tecnología de la comunicación y, en definitiva, por la globalización misma– las organizaciones criminales desarrollan sus actividades, cada vez más, a escala mundial.

La interconexión, la flexibilidad y la versatilidad en sus actuaciones, son la clave de todos estos grupos que funcionan como redes criminales transnacionales y, entre ellos, por supuesto, también de los grupos terroristas internacionales. De ahí que sean la seguridad nacional e internacional, y por lo tanto la lucha contra estas redes criminales que actúan a escala mundial, uno de los principales retos que deben afrontar los Estados en la actualidad. Ya no basta con la lucha en el interior de cada Estado, la colaboración y la cooperación entre todos los Estados resulta hoy más necesaria que nunca; y ello, en todas y cada una de las facetas de actuación, incluidas aquellas que, de manera tradicional, más celosamente han sido mantenidas como propias de cada Estado: en especial, los servicios de inteligencia de cada país.

Como hemos visto, la sociedad internacional se enfrenta en la actualidad a una serie de riesgos y amenazas estructurales, determinadas en muy buena medida por los actores que en ella se relacionan y por los factores que de un modo u otro determinan y, en ese mismo grado, ayudan a explicar sus comportamientos. ¿Cuáles son esos riesgos y amenazas?

### Riesgos y amenazas

Las amenazas fundamentadas en actores no estatales son de carácter asimétrico en su mayor parte, lo que las hace menos predecibles y más difíciles de controlar y de conocer en toda su extensión. La información sobre ellas es más difícil de obtener y, sin embargo, esa información es la principal herramienta para combatir las. La búsqueda de la información en un mundo globalizado donde, con frecuencia, la amenaza no tiene localización geográfica, se convierte en una dificultad añadida. La obtención de información requiere de la colaboración internacional.

Ningún país tiene capacidad para enfrentarse por sí solo a estas nuevas amenazas. Por ello, todas las estrategias occidentales de seguridad y defensa, incluida la española, se basan en un sistema de actuación multilateral, pero sin descartar situaciones que puedan requerir una respuesta puramente nacional.

La globalización ha obligado a los países a definir estrategias de seguridad nacional de carácter multidisciplinar, que requieren unas capacidades y estructuras distintas de las que se requerían en un ambiente de Guerra Fría.

En el caso español, la Estrategia Española de Seguridad, del año 2011, aprobada por el Gobierno español en junio del mismo año, señalaba que las disfunciones de la globalización, los desequilibrios demográficos, la pobreza y la desigualdad, el cambio climático, los peligros tecnológicos, y las ideolo-



gías radicales y no democráticas, eran factores transnacionales que podían potenciar los efectos de las amenazas y riesgos, e incluso cambiar su naturaleza, a la vez que identificaba las amenazas y riesgos más importantes para la seguridad de nuestro país:

- *Conflictos armados.* España puede tener que participar en tres tipos de conflictos, frente a los que el papel de las Fuerzas Armadas es central: los no compartidos con nuestros aliados; los multilaterales que afecten a intereses directos de España y los derivados de nuestros compromisos internacionales en marcos multilaterales que no afecten directamente a nuestros intereses. La defensa de nuestros intereses y valores es el eje básico que ha de guiar los esfuerzos de España en este campo, desde la triple perspectiva de la anticipación y prevención de conflictos, su gestión y resolución, y la posterior consolidación de la paz. Para ello, España apuesta por un enfoque integral que incluya los elementos diplomáticos, militares, policiales y de cooperación al desarrollo, entre otros.
- *Terrorismo.* El terrorismo amenaza directamente la seguridad de todos los ciudadanos, pretende socavar las instituciones democráticas y puede llegar a causar graves daños en nuestras infraestructuras críticas en un momento determinado. El terrorismo transnacional, señaladamente el «yihadista», aprovecha las características de la nueva sociedad global para intentar perturbar su normal funcionamiento. Aunque ninguno representa una amenaza existencial para el Estado, prevenir, impedir y derrotar el terrorismo es objetivo prioritario nacional, europeo e internacional. Para ello, es necesaria una respuesta estratégica específica e integrada, desde el respeto a los valores democráticos, los derechos humanos y el Estado de derecho. Sus ejes son la anticipación, la prevención, la protección, y la disponibilidad de los medios, la unión de los partidos democráticos, el apoyo a la labor de las Fuerzas y Cuerpos de Seguridad del Estado y de los servicios de inteligencia, y la cooperación internacional.
- *Crimen organizado.* Es una de las amenazas a nuestra seguridad más serias y a veces menos reconocidas. Su creciente interrelación con el terrorismo, los grupos violentos y la delincuencia local hace que todos ellos se potencien entre sí. Para responder a esta amenaza se ha de trabajar en una triple dirección: incrementar los efectivos y los medios, continuar desarrollando una legislación efectiva en este ámbito, y mejorar la coordinación entre organismos nacionales e internacionales.
- *Inseguridad económica y financiera.* La seguridad económica es parte integral y requisito esencial de nuestra seguridad. Las amenazas y riesgos relacionados con la actividad económica y financiera pueden tener su origen en factores como los desequilibrios macroeconómicos –públicos o privados–, la volatilidad de los mercados, la actuación desestabilizadora, especuladora e incluso ilegal de diversos agentes, la deficiente actuación de los organismos supervisores y reguladores, la interdependencia económica, la competencia por los recursos o un modelo de crecimiento

desequilibrado. Tanto la prevención como la mitigación de sus efectos requiere luchar contra las actividades delictivas, asegurar una correcta supervisión y regulación de los mercados, avanzar en la gobernanza económica europea y global, potenciar la presencia internacional de España, garantizar el funcionamiento de los servicios e infraestructuras críticos económicos y financieros, y promover un desarrollo económico sostenible que minimice los desequilibrios y garantice el crecimiento económico y la cohesión social. En relación con esto, la Estrategia ya preveía que «con el fin de analizar la información relevante y facilitar la acción del Estado mediante una mejor toma de decisiones en este ámbito, se crearía un Sistema de Inteligencia Económica (SIE)» que está aún por desarrollar.

- *Vulnerabilidad energética.* Nuestra alta dependencia de combustibles fósiles y la insostenibilidad del actual modelo energético a nivel mundial, por razones medioambientales, entre otras, hacen del factor energético un componente fundamental para nuestra seguridad. Los ejes de acción de la seguridad energética son: la diversificación de las fuentes de energía; el ahorro y la eficiencia energética, con el doble objetivo de reducir la dependencia exterior y mejorar nuestra competitividad económica; y la seguridad de abastecimiento a un precio razonable, limitando la cuota procedente de un mismo país, desarrollando reservas estratégicas, fomentando las interconexiones, impulsando infraestructuras y liberalizando mercados. La mejor garantía de abastecimiento y seguridad energética para España es un mercado europeo integrado de electricidad y gas natural.
- *Proliferación de armas de destrucción masiva.* La proliferación de armas nucleares, radiológicas, biológicas o químicas, es una de las grandes amenazas de nuestra era, especialmente si agentes incontrolados, como las organizaciones terroristas, consiguen acceder a ellas y utilizarlas. Prevenirla y neutralizarla exige un intenso trabajo multidisciplinar. España apoya las diferentes iniciativas internacionales en esa dirección, como el Tratado de No Proliferación Nuclear (TNP) y crear una capacidad de defensa colectiva adecuada contra la proliferación de misiles balísticos.
- *Ciberamenazas.* Cada vez más, una mayor parte de nuestra actividad se desarrolla en el «ciberespacio», donde las amenazas pueden ocasionar graves daños, e incluso podrían paralizar la actividad de un país. Los «ciberataques» más comunes tienen fines comerciales, pero también estamos expuestos a agresiones por parte de grupos criminales, terroristas u otros, e incluso de Estados. Las nuevas tecnologías de la información y comunicación ofrecen nuevos y más sofisticados medios para el espionaje y la contrainteligencia. Mejorar la seguridad en el ciberespacio pasa por fortalecer la legislación, reforzar la capacidad de resistencia y recuperación de los sistemas de gestión y comunicación de las infraestructuras y los servicios críticos, y por fomentar la colaboración público-pri-

vada con este fin. Es necesaria la coordinación de los diversos agentes involucrados, así como impulsar la cooperación internacional con el objetivo de desarrollar acuerdos para el control de las «ciberamenazas».

- *Flujos migratorios no controlados.* El impacto de la inmigración masiva e ilegal puede generar conflictividad social, guetos urbanos por falta de integración –donde la radicalización extremista, religiosa o ideológica, pueden tener su caldo de cultivo–, explotación económica por parte de organizaciones criminales o la desestabilización de algunos sectores productivos.
- *Emergencias y catástrofes.* Las amenazas y riesgos causados por el hombre o de origen natural –potenciados por el cambio climático–, los problemas sanitarios, como las pandemias, o la escasez de recursos básicos, como el agua, en un momento determinado pueden convertirse en riesgos de primer orden para la seguridad y el bienestar de los ciudadanos.
- De especial importancia es la *seguridad de las infraestructuras, suministros y servicios críticos.* Es preciso garantizar su funcionamiento y capacidad de resistencia y recuperación ante posibles amenazas. La colaboración con el sector privado –gestor ya de muchas de ellas– debe ser potenciada.

La Estrategia de Seguridad Nacional, del año 2013, aprobada también por el Gobierno de España en mayo de dicho año, vuelve a reseñar los mismos riesgos y amenazas que la Estrategia del año 2011. Al igual que el documento del año 2011, se vuelven a señalar como factores potenciadores, que pueden generar nuevos riesgos o amenazas o multiplicar y agravar sus efectos, la pobreza, la desigualdad, los extremismos ideológicos, los desequilibrios demográficos, el cambio climático o la generalización del uso nocivo de las nuevas tecnologías. A estos añade el espionaje y la vulnerabilidad del espacio marítimo:

- *El espionaje* se ha adaptado al nuevo escenario del mundo globalizado y aprovecha ahora las posibilidades que ofrecen las tecnologías de la información y comunicación. Las agresiones por parte de Estados, grupos o individuos con la finalidad de lograr información que les permita obtener ventajas estratégicas, políticas o económicas, han sido una constante histórica y siguen siendo una amenaza de primer orden para la seguridad.
- *Vulnerabilidad del espacio marítimo* Los mares y océanos ocupan algo más de las dos terceras partes del planeta. Es un espacio de fácil acceso y, en términos generales, menos regulado y controlado que el espacio aéreo o el terrestre. Sin duda, estas características hacen del espacio marítimo un medio donde los riesgos y amenazas a la seguridad se pueden propagar de manera relativamente fácil y rápida. En los últimos años, la constatación de este hecho ha llevado a la comunidad internacional a realizar un gran esfuerzo en el plano normativo, tecnológico y operativo, orientado a incrementar el control del mar.

Al final del documento de Estrategia de Seguridad Nacional del año 2013, antes referenciado, se instaba a la reforma paulatina del sistema de seguridad nacional y al perfeccionamiento de los instrumentos de gestión de crisis. Así, el Consejo de Seguridad Nacional debía elaborar una propuesta de anteproyecto de Ley Orgánica de Seguridad Nacional.

Esta legislación vio la luz, no en forma de ley orgánica, sino de ley ordinaria, el pasado 29 de septiembre, como Ley 36/2015 de 28 de septiembre, de Seguridad Nacional (BOE 233).

En su preámbulo se refiere a la seguridad nacional como: «un objetivo compartido por las diferentes Administraciones, estatal, autonómica y local, los órganos constitucionales, en especial las Cortes Generales, el sector privado y la sociedad civil, dentro de los proyectos de las organizaciones internacionales de las que formamos parte».

En su artículo 4, punto 3, habla de la estrategia de seguridad nacional en los siguientes términos: «es el marco político estratégico de referencia de la política de seguridad nacional. Contiene el análisis del entorno estratégico, concreta los riesgos y amenazas que afectan a la seguridad de España, define las líneas de acción estratégicas en cada ámbito de actuación y promueve la optimización de los recursos existentes. Se elabora a iniciativa del presidente del Gobierno, quien la somete a la aprobación del Consejo de Ministros, y se revisará cada cinco años o cuando lo aconsejen las circunstancias cambiantes del entorno estratégico. Una vez aprobada, será presentada en las Cortes Generales en los términos previstos en esta ley».

## Inteligencia

Información e inteligencia no son lo mismo. Los medios de comunicación son capaces de ofrecernos hoy ingentes cantidades de información sobre los lugares más remotos y con la mayor inmediatez. También los institutos de investigación, los llamados *think-tanks*, elaboran rigurosos informes a partir de un exhaustivo acopio de datos. Se trata, en ambos casos, de información valiosísima que, de tener que ser usada en un proceso de toma de decisiones, debería ser evaluada y matizada convenientemente.

La información es el punto de partida del llamado ciclo de inteligencia. Por tanto, para empezar a trabajar, el informador y el analista de inteligencia parten de una materia prima muy semejante. Sin embargo, puesto que cada uno aplica metodologías, herramientas y principios de actuación diferentes, y las organizaciones de las que dependen buscan objetivos dispares y destinatarios distintos, al final, el producto de ambos procesos –información e inteligencia– apenas tiene puntos en común.

La rapidez con la que evolucionan los escenarios de seguridad, la cantidad de información que deben manejar los responsables de la toma de decisio-

nes, la variedad y las características de los nuevos riesgos y amenazas, así como la posibilidad de acciones de desinformación, con la finalidad de inducir errores al evaluar el escenario de seguridad, hacen que los cometidos de los servicios de inteligencia sean cada vez más complejos. El proceso de producción de inteligencia requiere el uso de un método que permita tratar la información eficientemente para aportar un conocimiento veraz y exacto al usuario final.

El valor añadido de la inteligencia no se mide únicamente por su capacidad de anticipar acontecimientos, sino por aportar un nivel de conocimiento especializado, basado en el recurso a fuentes y procedimientos solo al alcance, en muchos casos, de los servicios de inteligencia. La finalidad de los servicios de inteligencia es poner a disposición de una autoridad información convenientemente elaborada, de forma oportuna, para que pueda tomar decisiones relacionadas con la seguridad y defensa nacional de forma que asuma el menor riesgo posible en la decisión. Esta información analizada, integrada e interpretada se denomina inteligencia. La inteligencia aporta a las autoridades un conocimiento que permite la toma de decisiones que reducen los riesgos y amenazas a la seguridad nacional, no solo por el conocimiento de la situación sobre la que se ha de decidir y sobre su evolución futura, sino por el valor añadido que supone la información secreta.

La actuación de los Estados en un mundo cada vez más complejo, heterogéneo e interdependiente, debe realizarse en gran medida a través de la cooperación multilateral, si bien, esta cooperación no elimina la necesidad para cada Estado de poseer una estructura de inteligencia propia que desarrolle las actividades acordes con sus funciones y que, fundamentalmente, sirva para consolidar cada una de las fases del llamado Ciclo de la Inteligencia (Navarro, 2004), desde la obtención de información a su análisis crítico, estudio en profundidad y extracción de conclusiones.

Hoy más que nunca, en una sociedad internacional marcada por los flujos constantes y multiformes de información que la nueva era surgida de la revolución de la tecnología de la información permite, los servicios de inteligencia juegan un papel esencial para ofrecer a los órganos de poder evaluaciones coherentes de la realidad, derivadas de interpretaciones lógicas de todo el flujo de información, que les ayuden a adoptar decisiones correctas ante problemas determinados.

Esta nueva realidad genera consecuencias muy poderosas, en relación a los servicios de inteligencia que, ya que al realizar su labor se ven obligados a ser cada vez más flexibles ante las nuevas situaciones, retos y factores que influyen en el comportamiento de los actores que se relacionan en la sociedad internacional y cuya actuación tratan de anticipar a través de una amplia recopilación de información y un posterior análisis más certero.

## Inteligencia integral

Los Estados formulan sus objetivos y estrategias de seguridad nacional, los recursos, las acciones y los medios para alcanzarlos a través de una política de defensa, que es una componente de la política general del Estado. Esta política consta de dos ámbitos: la defensa militar, frente a toda amenaza o agresión armada de cualquier enemigo, que corresponde a las Fuerzas Armadas; y la defensa civil contra las amenazas interiores, que corresponde a los cuerpos y fuerzas de seguridad del Estado. Pero también se suele entender por defensa civil la disposición permanente de todos los recursos humanos y materiales de una nación contra las amenazas interiores y exteriores, de modo tal que la política de defensa se puede concretar en política económica de defensa, política diplomática de defensa, política de educación para la defensa, política de solidaridad internacional para la defensa... En definitiva, los ejércitos son agentes fundamentales de la defensa pero no los únicos, ya que, según este concepto de defensa, la política militar es solo un subconjunto de la política de defensa, que, a su vez, es uno de los subconjuntos de la política nacional.

En ese marco, la función de los servicios de inteligencia ha experimentado un salto cualitativo de especial significación. Los horrores de un siglo XX sangriento han terminado por desacreditar la guerra como instrumento de poder en beneficio de intereses más o menos legítimos. El anhelo de paz y la conciencia de interdependencia que alienta un mundo cada vez más globalizado exigen su concurso para atender a los cada vez más amplios espacios de seguridad, preservando la paz y la estabilidad de los pueblos y de las naciones que comparten valores primordiales.

En consecuencia, el viejo concepto de inteligencia/espionaje que se centraba en las meras tareas informativas sobre «lo secreto» hace tiempo que fue superado para dar paso a otro de horizonte mucho más abierto que exige una mayor integración con el objetivo de realizar nuevas y complejas tareas, desarrolladas con fundamento científico, adaptadas a la obtención y tratamiento de la información procedente de nuevos y numerosos ámbitos a los que hoy es posible acceder por multitud de «fuentes abiertas» (OSINT) que proporcionan volúmenes ingentes de informaciones fáciles de obtener, pero difíciles de seleccionar, contrastar y analizar adecuadamente.

Es, por tanto, una ardua tarea que exige costosos esfuerzos tanto en personal altamente cualificado, como en sofisticados medios materiales puestos a su servicio para «aprehender» la realidad sobre la que se proyectan los riesgos, las amenazas y los conflictos. Una labor que consiste, en definitiva, en aislar los hechos significativos, estudiarlos en función de su pertinencia, oportunidad y relevancia, e interrelacionarlos, en busca de la «inteligencia», del «conocimiento», que haga posible superar las incertidumbres y apoyar, así, las políticas adecuadas para prevenir riesgos, neutralizar amenazas y gestionar, en su caso, las situaciones de crisis.

En definitiva, la realidad ha determinado que se haya desarrollado una clara conciencia de la necesidad de dar respuestas globales a fenómenos globales. Y esta convicción acabó por asentarse, de forma generalizada, tras la brutal realidad de los hechos acaecidos el 11 de septiembre de 2001, y el 11 de marzo de 2004. En esas luctuosas fechas, quedó confirmado lo que ya anticipara Henry Kissinger tiempo atrás: «ni siquiera la superpotencia hegemónica, Estados Unidos, sería capaz, en adelante, de afrontar, en soledad, amenazas que, por su naturaleza y alcance, son capaces de poner en riesgo la paz y la estabilidad mundiales».

En consecuencia, el número y la entidad de las funciones genéricas de los servicios de inteligencia se han visto incrementados; mientras que la interdependencia, fruto de la globalización, ha hecho más necesaria que nunca la cooperación concertada, tanto en el plano nacional como en el internacional.

De manera que, en orden a la eficacia y a la economía de medios, la gestión de tan ingente volumen de información impone una rigurosa aplicación tanto de los principios tradicionales como de los medios que hoy ofrecen las nuevas tecnologías informáticas a las tareas de señalamiento de objetivos, a la construcción de los nuevos marcos de referencia –que han de mantenerse actualizados– y, en definitiva, a la realización de una labor de planeamiento de la obtención y de la elaboración de «inteligencia», ejecutada de forma rigurosa, flexible, abierta a la complementariedad y a la cooperación entre las distintas agencias, tanto en el plano nacional como en el internacional, y capaz de adaptarse a la volatilidad de las situaciones, a los cambios imprevistos de escenario y a la aparición de nuevos riesgos y amenazas.

Nunca, pues, antes de ahora, se percibió con tanta claridad la necesidad y la urgencia de articular auténticas y eficaces comunidades de inteligencia capaces de desarrollar, en su seno, esfuerzos complementarios, sinérgicos, interactivos, con el apoyo de los diferentes actores sociales y orientados al logro de los objetivos e intereses compartidos; porque, como afirma Robertson «a pesar de que continuará siendo necesario actuar localmente, hoy se hace imprescindible pensar en términos globales y promover y perfeccionar foros de reflexión y sistemas de información e inteligencia compartidos, que hagan posible la complementariedad y la coordinación de esfuerzos en favor de intereses comunes». Y es que, si la información y la inteligencia pertenecen al orden del conocimiento, la inteligencia, además es «una organización física, de seres vivos que persigue, como fin, una clase especial de conocimiento». Una organización que se hace aún más necesaria a la hora de elaborar «inteligencia compartida».

En la *Estrategia Española de Seguridad (2011)* se señalaba que la seguridad española reposaba sobre seis conceptos básicos:

- *Enfoque integral*: Es necesario integrar todas y cada una de las dimensiones de la seguridad, haciéndolas converger hacia objetivos comunes y conscientes de las múltiples relaciones que existen entre ellas.

- *Coordinación*: La cooperación y colaboración entre las Administraciones públicas es imprescindible para lograr el máximo rendimiento de los recursos disponibles. Adicionalmente, dado que muchas infraestructuras, suministros y servicios críticos están en manos privadas, es imprescindible la cooperación entre el Estado y las empresas privadas, además de la colaboración ciudadana y la de las organizaciones sociales.
- *Eficiencia en el uso de los recursos*: En un contexto de limitación del gasto público, el Estado deberá asegurar el buen uso de los recursos y racionalizar el empleo de los instrumentos existentes.
- *Anticipación y prevención*: No todas las amenazas pueden preverse, pero algunas pueden prevenirse y evitarse. El Estado debe disponer de los medios necesarios para alertar y prevenir de todo aquello que pueda poner en peligro la seguridad de España y de sus ciudadanos.
- *Capacidad de resistencia y recuperación*: Surgirán retos, amenazas y desafíos hoy imprevisibles. Para hacerles frente hay que disponer de sistemas e instrumentos resistentes y flexibles, susceptibles de adaptarse a las diversas circunstancias.
- *Interdependencia responsable*: Mediante la colaboración con nuestros socios europeos e internacionales, debemos establecer mecanismos de gobernanza para crear y fortalecer marcos e instrumentos multilaterales que garanticen la seguridad internacional. Por su capacidad de interlocución y por su posición estratégica, España tiene importantes atributos con los que contribuir a estos objetivos.

De esos conceptos básicos se concluía que era necesario superar la compartimentación, duplicidades y solapamientos de las políticas y del entramado institucional existente. El objetivo es consolidar una visión más integrada de los diversos factores que inciden en la seguridad y de los mecanismos de respuesta, para garantizar una gestión mejor coordinada y eficaz de los mismos, a lo que se añadía la esencial colaboración y cooperación entre todos los actores afectados.

Ese planteamiento tiene continuidad en la Estrategia de Seguridad Nacional, del año 2013, donde se define la seguridad nacional como una forma integral y amplia, y se concibe como un servicio público objeto de una política de Estado, que precisa de la colaboración de la sociedad en su conjunto, cuyos principios informadores son:

1. *Unidad de acción*, que supone la implicación, la coordinación y la armonización de todos los actores y los recursos del Estado bajo la dirección del presidente del Gobierno, así como la colaboración público-privada y la implicación de la sociedad en general. El enfoque integral de la seguridad, comprensivo de todas sus dimensiones, justifica este principio de acción y precisa, a su vez, de una gestión completa a través de un sistema de seguridad nacional impulsado y liderado por el presidente del Gobierno;



2. *Anticipación y prevención*, que han de orientar la acción del Gobierno a la detección y la reconducción de situaciones que pueden representar un potencial riesgo o amenaza para la seguridad nacional;

3. *Eficiencia y sostenibilidad en el uso de los recursos*, un principio que, si bien debe presidir en todo momento la actuación administrativa, cobra especial significación en un contexto como el presente. Se sustenta en la priorización de los recursos y la optimización de su empleo, precisa el control y la evaluación de los resultados y orienta la organización administrativa;

4. *Resiliencia o capacidad de resistencia y recuperación*, principio relativo a la aptitud de los recursos humanos y materiales para afrontar con flexibilidad y fortaleza las situaciones de crisis y sobreponerse a ellas minimizando y absorbiendo sus consecuencias negativas.

Esos principios informadores, junto al análisis de los riesgos y amenazas y tendencias globales, y a las capacidades de respuesta existentes, permite diseñar unas líneas de acción estratégicas de respuestas efectivas e integrales a los retos existentes para la seguridad nacional, muchas de ellas basadas en una mejora de las capacidades de investigación e inteligencia, mediante la adecuación de los instrumentos nacionales precisos de coordinación, dirección y supervisión, con la finalidad de lograr el mayor grado de efectividad posible de las instituciones y los poderes públicos.

Por último, la nueva Ley de Seguridad Nacional establece en un preámbulo: «El superior interés nacional requiere mejorar la coordinación de las diferentes Administraciones públicas, buscando marcos de prevención y respuesta que ayuden a resolver los problemas que plantea una actuación compartimentada, organizando a diversos niveles y de manera integral, la acción coordinada de los agentes e instrumentos al servicio de la seguridad nacional.

Esta Ley se dicta con el propósito de responder a esta demanda, que viene siendo expresada por los agentes de la seguridad nacional integrados en las Administraciones públicas, por el sector privado y por la sociedad en general. No afecta a la regulación de los distintos agentes e instrumentos que ya son objeto de normas sectoriales específicas, sino que facilita su inserción armónica en el esquema de organización general, establecido por la Estrategia de Seguridad Nacional, de 31 de mayo de 2013, bajo la denominación de Sistema de Seguridad Nacional, y liderado por el presidente del Gobierno».

El artículo 5 se dedica a la «Cultura de Seguridad Nacional» y se hace mención a la inteligencia, en el sentido de que por otro lado: «la realidad demuestra que los desafíos para la seguridad nacional que afectan a la sociedad revisten en ocasiones una elevada complejidad, que desborda las fronteras de categorías tradicionales como la defensa, la seguridad pública, la acción exterior y la inteligencia, así como de otras más recientemente incorporadas a la preocupación por la seguridad, como el medio ambiente, la energía, los transportes, el ciberespacio y la estabilidad económica».

Ya que ciertos riesgos y amenazas, adquieren una dimensión de acusada transversalidad o combinan estos rasgos con su naturaleza abierta e incierta. Todo lo cual aconseja una respuesta coordinada de los distintos agentes e instrumentos de la seguridad nacional.

Así se establece en el artículo 24, la posibilidad de declarar «la situación de interés para la seguridad nacional», de todo o una parte del territorio nacional por un periodo limitado y prorrogable. Situación en la que está prevista la aportación de recursos humanos y materiales, tanto públicos, como privados, aunque no de forma permanente; estando prevista su regulación en una futura ley reguladora de la preparación y disposición de la contribución de recursos a la seguridad nacional.

### La inteligencia en el caso español

España ha padecido al igual que otros países las consecuencias de no tener una verdadera comunidad de inteligencia. Un devastador ataque terrorista en marzo de 2004, el apoyo a una intervención bélica basado en un asesoramiento inadecuado y una carencia, menos visible pero igualmente perjudicial, de una inteligencia económica que dé respuesta a las necesidades de nuestra creciente proyección exterior.

Todos estos errores tienen una casuística plural; sin embargo, su base común es la falta de concepción del papel que la inteligencia debe jugar en el entramado de la política española de inicios del siglo XXI.

La inteligencia española nace en 1977 en el contexto del final de una dictadura, algo muy distinto al de otros países occidentales, cuya inteligencia surge tras la Segunda Guerra Mundial. En lo estructural, la inteligencia española nació sin un modelo previo, convirtiéndose en un mero agregado de burocracias (Defensa, Interior y Asuntos Exteriores) que competían por una nueva área de la Administración que aparecía como era la informativa-inteligencia.

En lo funcional se produjeron enormes tensiones y solapamientos, sin que fructificase ninguno de los intentos de la Presidencia por poner un poco de orden y distribuir cuáles eran los cometidos de cada una de las agencias. Los objetivos de nuestra inteligencia también fueron cambiando muy rápidamente.

Preocupados inicialmente por la involución y el terrorismo, no es hasta mediados de los ochenta cuando el Gobierno indica al entonces CESID que comience a salir de España y desarrolle una estructura en el exterior; es así fácil de entender que el bagaje acumulado por el ahora CNI no pueda admitir parangón con sus contrapartes europeas o norteamericanas.

Pero, aunque haya puntos de partida bien diferenciados, tanto las comunidades de inteligencia españolas como las occidentales deben ser sometidas a una profunda revisión, puesto que las condiciones que justificaron su crea-

ción han cambiado profundamente (transición a una democracia versus terrorismo global en el caso de España, y guerra fría versus terrorismo global en la mayoría de los países occidentales).

Desde 2001 España ha tenido dos momentos clave para poder reflexionar sobre cómo configurar su inteligencia: la creación del Centro Nacional de Inteligencia en 2002 y los trabajos de la comisión de investigación del 11-M.

Así dicha comisión de investigación recomendaba, entre otras, las siguientes medidas:

1. En referencia a la mejora de la seguridad del Estado frente al terrorismo internacional:
  - a. Una acción eficaz contra el terrorismo necesita una coordinación elemental entre las distintas fuerzas y cuerpos de seguridad y los servicios de inteligencia con que cuenta el país. Para ello, entre otras acciones sería necesario que:
    - i. las líneas de investigación y las bases de datos se compartan entre sí para optimizar los recursos disponibles y evitar, en algunos casos, que un mismo objetivo sea trabajado doblemente por cuerpos distintos, con diversos enfoques y dispar resultado;
    - ii. los confidentes de unos cuerpos sean conocidas por los otros; el resultado de las investigaciones sobre armas y explosivos o financiación terrorista se unifique para permitir una acción conjunta;
    - iii. la información de que disponen unos y otros en materia de inmigración, actividades de terroristas internacionales de origen islamista recluidos en cárceles españolas o de delincuentes comunes captados por la yihad sea completa, coordinada y compartida por todos.
2. En el ámbito policial y de inteligencia:
  - a. Se requiere una reorganización de los servicios de la Guardia Civil y de la Policía, junto con una mayor especialización en la lucha contra el terrorismo internacional, en particular mediante una colaboración estrecha con las Universidades, otros centros de estudios y expertos, y el trabajo desarrollado por el nuevo Centro de Formación, Adiestramiento y Reciclaje de los agentes.
  - b. Se ha de buscar una formación policial especializada y homologada para la lucha antiterrorista, mediante una cooperación estrecha con las Universidades, centros de estudios y expertos. En tal sentido, se propone la creación, dentro de las actuales infraestructuras formativas, de la Escuela Antiterrorista, un centro de formación, adiestramiento y reciclaje que, con carácter estable y altamente cualificado, impartirá la formación teórico-práctica, multidisciplinar y conjunta de

las distintas promociones de fuerzas y cuerpos de seguridad dedicadas a la lucha antiterrorista en sus distintas escalas, grados y funciones, que permitiría también la formación en la materia de policías y servicios de seguridad de otros países.

- c. Resulta imprescindible que se produzca una más intensa y programada cooperación de los servicios de inteligencia de los distintos Estados que componen la Unión Europea. En la arquitectura institucional que diseña la Constitución, parece que el mejor órgano para llevarla a cabo es la Secretaría General del Consejo de Ministros.
- d. Los aspectos antiterroristas del control fronterizo deben desarrollarse e incluir una dimensión de inteligencia con vistas a obtener y compartir datos de manera sistemática con los cuerpos y fuerzas de seguridad de los Estados fronterizos, especialmente en el marco de la Unión Europea.

### 3. En política exterior para la seguridad.

- a. Reforzar la coordinación contra el terrorismo, no solo entre países miembros de la UE y a escala internacional. Especialmente a través de convenios de colaboración con los Estados árabes y muy principalmente con Marruecos, Argelia y Túnez, en materia de inteligencia, acceso a bases conjuntas, armonización de legislaciones, investigaciones compartidas e instrucciones judiciales en estrecha colaboración.
- b. También hay que extender a otros países la creación e intercambio de enlaces policiales y judiciales, como ya se ha acordado con Marruecos. Sería conveniente promover la celebración de encuentros periódicos, como se ha hecho en el pasado, para la puesta en común de los servicios de inteligencia y fuerzas de seguridad de los países del Mediterráneo, principalmente Argelia, Túnez, Marruecos, Francia, Italia y España.

Sin embargo, el fruto ha sido escaso. En primer lugar, la reforma de 2002, que, por mucho que sea vista como una consecuencia de los atentados contra los Estados Unidos de septiembre de 2001, no tiene este referente, buscaba poner fin a una situación de continua provisionalidad que se remonta a 1977, cuando a trompicones nace el CESID.

La segunda ocasión coincide con los trabajos de la comisión del 11-M, y su aportación para la mejora del sistema de inteligencia ha sido mínima. Las propuestas de la comisión, referenciadas en parte anteriormente, no están basadas en unas conclusiones comunes y consensuadas por parte de los diferentes grupos. Además, fueron elaboradas por políticos no expertos en inteligencia y cuyo mandato, por lo demás, nunca fue reflexionar sobre la mejora del sistema de inteligencia español; de hecho, uno de los avances más reseñables, como es la creación del Centro Nacional de Coordinación Antiterrorista (CNCA, actualmente CITCO –Centro de Inteligencia contra el

Terrorismo y el Crimen Organizado—, por la unión con las estructuras de lucha contra la delincuencia organizada), tiene lugar fuera de la comisión.

España debe, por lo tanto, iniciar una verdadera reflexión sobre el papel de su comunidad de inteligencia en el proceso de elaboración de diferentes políticas a un ritmo que al menos se pueda acercar al que están marcando los políticos de Reino Unido o Australia.

### La necesidad de una organización adecuada

Con el fin de aplicar las líneas de acción estratégicas diseñadas en los informes de estrategia de seguridad nacional y en la Ley de Seguridad Nacional, surge la necesidad de cooperar como único método de ser efectivos. La cooperación refuerza la lealtad y la confianza entre los países y aumenta, de manera significativa, la seguridad entre ellos, lo que se refleja simpáticamente en el entorno geográfico, generando un escenario de paz y progreso, que está en la base de todas las aspiraciones humanas.

No existe un único modelo de cooperación, ni tampoco un modelo ideal de cooperación que dé una respuesta óptima a todas las necesidades de inteligencia. Este modelo dependerá de las circunstancias particulares del objetivo a cubrir, de los actores que tomarán parte, de su vocación de temporalidad o permanencia, de la coincidencia de intereses, etc.

En definitiva, la forma de cooperación será, para cada momento, una, y no necesariamente siempre la misma. La que funcionó bien en una circunstancia no tiene por qué servir para otra, cuando las condiciones son distintas, ni tampoco deberemos descartar las que funcionaron bien, pues podría ser que fueran útiles de nuevo.

La variedad de las estructuras de coordinación es grande; y ello es debido, en primer término, a la configuración de cada tipo de Estado, al número y naturaleza de los distintos servicios y agencias que han de coordinar, e incluso a la escalonada aparición en el tiempo de cada uno de ellos. De manera que no debe extrañar que resulte difícil establecer homologaciones entre órganos de coordinación de diferentes países, más allá de las funciones genéricas y de los niveles en los que desarrollan su función. Pero dicha cooperación no debe limitarse solo al ámbito público, entre las diferencias agencias y organismos, la cooperación debe ser abierta al sector privado. Las empresas privadas son hoy en día el motor de la economía de los países debido a su creatividad e innovación constante.

El concepto de «comunidad de inteligencia» surge de la necesidad de coordinar las actividades de inteligencia e información relacionadas con la seguridad nacional, de manera que sean planeadas y desarrolladas de forma que garanticen tanto la eficacia como la eficiencia en el logro de sus objetivos. Las estructuras de coordinación existen en casi todos los países, dando lugar a di-

ferentes modelos de organización cuya configuración depende principalmente de las competencias asignadas a las instituciones del Estado, el número y naturaleza de los distintos servicios, e incluso del origen de cada uno de ellos.

Una comunidad de inteligencia (CI) consiste en un sistema integrado por agencias y organismos relevantes en tal materia, coordinados por una estructura con esa específica función. Pero la coordinación no es sencilla, y su organización, aun orientada por criterios funcionales, puede conducir a resultados opuestos a los pretendidos: injerencias en las competencias propias de cada uno de los actores, rigidez en los procedimientos de intercomunicación, distanciamiento entre productores y usuarios de inteligencia, escasez o proliferación excesiva de órganos específicos de coordinación de nivel intermedio, disminución de la intercomunicación horizontal, deficiente delimitación de los ámbitos competenciales por excesiva compartimentación o por indefinición de los puntos de vista adecuados a cada finalidad que fomenta la dispersión, las extralimitaciones y el trabajo redundante.

Podemos considerar el concepto de comunidad de inteligencia como un sistema, es decir, un conjunto de servicios de inteligencia e información relacionados entre sí, con una ordenación lógica y finalidad común. Como todo sistema, posee la cualidad de que su eficiencia es mayor que la suma de la eficiencia de todos sus componentes (sinergia). Es decir, la comunidad de inteligencia tiene ventajas que no se encuentran en ninguno de sus componentes, a la vez que cada uno de sus elementos puede ver potenciada su capacidad. La comunidad de inteligencia no puede considerarse como un sistema cerrado, totalmente independiente, sino que está en constante interrelación con otros sistemas más amplios como el sistema de seguridad y defensa, del que, a su vez, es un componente.

La coordinación que permita conformar una auténtica y eficaz CI ha de pasar, necesariamente, por el acierto en la elección de una arquitectura en la que estén perfectamente determinados sus miembros, y en la que los órganos y mecanismos de coordinación cumplan una serie de condiciones entre las que cabe destacar: que tengan sus funciones claramente definidas en los tres niveles fundamentales: de planeamiento, operacional y de difusión; que proyecten su acción sobre todos los espacios definidos por el binomio seguridad-defensa; que promuevan una comunicación rápida y fluida entre los órganos de análisis y las instancias decisorias; y que fomenten la permeabilidad entre los miembros de la comunidad de inteligencia y entre esta y el resto de la administración y los sectores políticos, económicos y sociales. Y, todo ello, desarrollando redes de cooperación interinstitucional que respondan a criterios de eficacia. Es decir, redes compatibles, de alta conectividad, ágiles, flexibles, bien articuladas, adaptables, seguras, y que posibiliten acciones de la comunidad de inteligencia adecuadas y en tiempo eficaz.

Pero tales requisitos no son suficientes; además se han de cumplir otras condiciones indispensables: que exista homogeneidad conceptual y termi-

nológica en materia de inteligencia, principios y procedimientos básicos comunes que faciliten el entendimiento y la cooperación, fluido intercambio informativo en el seno de la CI y, sin menoscabo de la seguridad, aperturas hacia la sociedad capaces de promover en ella una verdadera «cultura de inteligencia».

Entre estas últimas condiciones señaladas, conviene reparar, de forma especial en aquella que se refiere al intercambio y puesta en común de la materia a compartir. Y conviene hacerlo porque justamente es en este empeño donde aparecen serias dificultades en las relaciones entre agencias que, con frecuencia, han de trabajar sobre un mismo objetivo. Ciertamente, cada una de ellas lo ha de hacer desde la perspectiva de la finalidad concreta que se corresponde con sus misiones. Pero lo cierto es que la realidad es indivisible, el objeto de estudio, en tales casos, es uno y de él se ha de obtener la necesaria información en bruto que permita, tras su análisis y evaluación, actuar en consecuencia a cada agencia.

Compartir información procedente de fuentes abiertas o relacionada con las actividades de los individuos organizaciones y grupos legalmente intervenidas o reguladas por las distintas administraciones, sin menoscabo de los requisitos que exigen cumplir las leyes que protegen el derecho a la intimidad, y al margen de las trabas de carácter burocrático que puedan existir en algunos casos, no suele ofrecer excesivas dificultades.

Otra cosa ocurre cuando se trata de compartir o intercambiar información en bruto obtenida por fuentes humanas (HUMINT siglas en inglés de Human Intelligence) o mediante herramientas, sistemas y procedimientos técnicos especiales aun siendo, unas y otros, actuados conforme a ley. En este caso, las dificultades aumentan considerablemente; en primer lugar, por razón de la propia sensibilidad de tales fuentes y por la correlativa necesidad de protegerlas. En segundo, porque determinadas informaciones en bruto se encuentran con frecuencia directamente relacionadas con operaciones en curso que podrían verse comprometidas al ser utilizadas por otras instancias. Y, por último –no se debe ocultar– a consecuencia de reticencias hacia la cooperación derivadas de celotipias, suspicacias y prejuicios (ciertamente no deseables) que existen entre las agencias e instituciones de todos los países y, en mayor medida, en aquellos con escasa tradición en materia de cooperación coordinada.

En materia de análisis, es decir, cuando se trata del intercambio del producto «inteligencia», las dificultades son menores. Las difusiones suelen circular en horizontal con más facilidad, tanto en el ámbito doméstico como en el internacional. Las dificultades surgen aquí cuando los órganos de análisis de las agencias centrales y las autoridades de coordinación de la CI han de elaborar inteligencia estratégica central integrando informes y documentos procedentes de las agencias y servicios miembros. Pero esto puede verse paliado o incluso superado –de hecho ya ocurre en los países donde exis-

ten— promoviendo, desde tales instancias, grupos de trabajo de análisis y evaluación participados por las agencias afectadas en cada caso.

No obstante lo dicho en relación con las dificultades derivadas del intercambio de información sin elaborar, la necesidad de actuar globalmente contra amenazas de tanta gravedad como el terrorismo transnacional y el crimen organizado de análoga proyección, aconseja la existencia de bases de datos interoperables en el seno de la comunidad. Sin perjuicio de que las agencias o unidades puedan establecer, en ellas, áreas de informaciones restringidas por razones de seguridad operacional, pero que permitan el acceso a las restantes de los miembros de la CI que pudieran verse necesitados de ellas.

La razón de ser de la comunidad de inteligencia es evitar la dispersión de esfuerzos, y procurar que todas las actividades de sus miembros se desarrollen de forma coordinada con la finalidad de alcanzar el mayor grado de eficacia y eficiencia en la consecución de los objetivos de seguridad. Por abundantes y apropiados que sean los medios puestos a disposición de los servicios de inteligencia e información, solo se alcanzarán unos resultados óptimos si el conjunto actúa ordenadamente. Para lograr una coordinación adecuada de la comunidad de inteligencia es imprescindible definir las competencias de cada uno de sus miembros, de forma que se eviten duplicidades no deseadas y se satisfagan todas las necesidades de inteligencia. La coordinación puede lograrse más fácilmente en las primeras fases del planeamiento, al definir los objetivos y la forma de alcanzarlos, pero requiere una atención continuada. No es suficiente con la coordinación inicial; es un proceso permanente que, en muchas ocasiones, requerirá un contacto directo entre las personas responsables de las distintas actividades. Por lo tanto, es necesario tener previstos unos protocolos de comunicación flexibles que faciliten las relaciones necesarias para lograr una coordinación correcta, evitando una excesiva burocratización.

En la sociedad global, todo depende de todos. La ciencia, la tecnología, el sistema financiero, la industria y el comercio, la política y la evolución de los espacios de seguridad y defensa ofrecen incertidumbres que afectan a lo público y a lo privado —que tan imbricados se hallan en el emergente «estado de mercado»— que preocupan a los especialistas de unos y otros campos y que, consecuentemente, son objeto de reflexión también en el seno de las comunidades académicas. Y esta circunstancia no puede ser olvidada por la CI. Contar con tales aportaciones, establecer cauces de diálogo con los especialistas y estudiosos de tales ámbitos, diseñar, en definitiva, esquemas de cooperación y asesoramiento externo entre todos ellos, enriquece los procesos de elaboración de inteligencia y contribuye, decisivamente, a oxigenar espacios a veces excesivamente clausurados, al proporcionar nuevas perspectivas, opiniones tal vez contradictorias, matices quizá inadvertidos, que contribuyen a aventar el riesgo cierto de que las agencias —y la propia comunidad— se vean envueltas en una especie de «opinión de grupo» acrítica, autocomplaciente y remansada en sí misma.



Los partidarios del «no» a una reserva de inteligencia centralizada, alegan que habría que volcar esfuerzos muy costosos de contrainteligencia para garantizar la seguridad de la documentación que habría de ser tratada y las conductas del personal externo que tendría acceso a ella; y argumentan que tal opción supondría recaer en una dinámica centralizadora que restaría, a las agencias, autonomía, capacidad de reacción y adaptabilidad en cuestión de riesgos y escenarios cuya aparición es difícilmente previsible, y en los que, llegado el caso, la amenaza o el conflicto se va a materializar y a desarrollar, cada vez con más frecuencia, en la forma dispersa y arrítmica propia de la «guerra en red», que exige respuestas en las que la capacidad de alerta temprana y de iniciativa se encuentran en relación directa con la flexibilidad y el grado de descentralización de los sistemas de mando y control.

Se hace, pues, necesario promover y desarrollar una «cultura de inteligencia» que sustituya la filosofía de la acción aislada por la de la intercomunicación y la acción concertada, desde el conocimiento y aprecio de la específica labor de cada instancia, de la complementariedad de unas y otras y de la trascendental importancia que para el éxito tiene una acertada acción de conjunto. Esto ayudará a desarrollar, en el seno de la CI, actitudes positivas que se verán reforzadas si, al tiempo, el conocimiento y aprecio de la labor que los servicios de información e inteligencia desarrollan en defensa de la paz y de la seguridad va creciendo en la sociedad a la que sirven. Las actitudes, como es sabido, inclinan a la acción dirigida al logro del objeto perseguido; y la acción continuada, coherente y coordinada desarrolla hábitos de cooperación que garantizan su eficiencia.

En nuestro mundo fuertemente globalizado, los nuevos conceptos de «seguridad colectiva» y «defensa compartida» exigen la cooperación internacional frente a fenómenos a los que, como en el caso del terrorismo internacional, las respuestas unilaterales resultan ineficaces cuando no imposibles. Y lo mismo ocurre en relación con otros graves riesgos y amenazas que se cierren sobre la paz y la estabilidad mundiales.

### La comunidad de inteligencia en España

Como se ha visto anteriormente, la inteligencia no deja de ser un instrumento de ayuda a la decisión del político, por lo que la estructuración de la comunidad debe estar en función de cuáles sean las necesidades que este manifiesta; así, una comunidad de inteligencia debe tener dos dimensiones bien diferenciadas: la política y la técnica, y que es como debería configurarse la comunidad de inteligencia española en la actualidad.

También y como ha quedado patente, una comunidad de inteligencia no es un mero agregado de organismos de inteligencia y órganos políticos consumidores de ella, es un sistema que interactúa y que debe ser un conjunto que entregue un producto superior y diferente al que podrían entregar sus par-

tes si actuasen de forma individual. Sin embargo, a pesar de esta obviedad y de que este concepto esté presente en el discurso habitual de políticos y medios de comunicación, el hecho cierto es que las comunidades de inteligencia no existen, no tienen entidad jurídica y no están recogidas –con muy contadas excepciones– en las diferentes legislaciones nacionales.

Estamos, por lo tanto, ante un concepto manoseado que ha sido empleado intuitivamente por los políticos para referirse al conjunto de organizaciones que generan algún tipo de información y que comprende a lo que se conoce como las siete tribus: inteligencia estratégica, militar, cuerpos policiales, ONG, empresas, academia y ciudadanos.

Así, el país más desarrollado en materia de inteligencia como sería Estados Unidos, tan solo hace una relación de las organizaciones que configuran esta comunidad; una situación que avanza algo con la creación del Homeland Security Department.

Las nuevas legislaciones de algunos países latinoamericanos hacen referencia a sistemas nacionales de inteligencia que recogen a las organizaciones de seguridad, pero olvidan otras; una estructura muy similar se encuentra en algunas recientes leyes que regulan los servicios de inteligencia de la Europa del Este, si bien estas no dejan de ser formulaciones jurídicas con poca o nula virtualidad.

Por todo esto, estamos ante la necesidad de reformar de arriba abajo las comunidades de inteligencia cuando estas no han cobrado entidad propia y ni siquiera se han conceptualizado. Esta posibilidad de construcción casi *ex novo* nos muestra grandes ventajas, pero también evidentes inconvenientes.

España tampoco cuenta con una comunidad de inteligencia, entendiendo esta como esa estructura formal de coordinación y cooperación entre las distintas agencias encargadas de la obtención, análisis y difusión de la información a los dirigentes políticos.

Aunque siempre estuvo en nuestro discurso político, la primera vez que en España se intenta dotar de cierta entidad a esa idea de comunidad de inteligencia es a mediados de los años ochenta. Con el objetivo de coordinar la pluralidad de informaciones sobre lucha antiterrorista que le llegan al presidente desde La Moncloa se gesta una mínima unidad de seis personas (dos guardias civiles, dos policías y dos agentes del CESID); sin embargo, las diferentes agencias boicotearon estos intentos hasta que consiguieron que cesaran tras los fastos de 1992.

Continuaron los proyectos, pero no será hasta una década después, en mayo de 2002, con la Ley del Centro Nacional de Inteligencia, cuando reaparezca la noción de comunidad de inteligencia en España.

Para su definitivo nacimiento, el legislador español eligió una forma indirecta y bastante peculiar. Evitó dar una definición de comunidad de inteligencia y

optó por establecer que la comunidad «está llamada a crearse» a partir de la Comisión Delegada del Gobierno para Asuntos de Inteligencia, estructura de la que sí indica cuáles son sus componentes y a la que dota de cierto contenido.

Esta forma de gestar la comunidad de inteligencia se debe a la clara conciencia por parte de los diputados socialistas y populares encargados de la reforma de la imposibilidad de realizar un diseño acabado de ella con una estricta distribución de funciones.

Se buscaba, en definitiva, aprobar un marco legal lo suficientemente difuso como para que ulteriormente los sucesivos Gobiernos pudieran llenarlo de contenido, evitando que una clara distribución de competencias y responsabilidades generara una enorme resistencia entre las Administraciones implicadas, sobre todo con el CNI, reproduciendo pasadas luchas burocráticas entre ministerios.

Como ya se ha destacado de forma reiterada, los servicios de inteligencia no están únicamente para proteger a los Estados de las amenazas, sino para ayudarles a aprovechar las oportunidades que pueda presentarles el entorno; pero las necesidades de seguridad son siempre más prioritarias que las derivadas de las potencialidades de otro tipo.

En la última década España ha incrementado de forma abrumadora su presencia económica en el exterior, siendo varios los ministerios implicados. Los embajadores son la cabeza del Estado en el extranjero y nuestras acciones en el exterior una prolongación de la política nacional. Por esto, se les preguntó a los embajadores si consideraban que el CNI debía tener un papel más relevante en nuestros intereses económicos en el extranjero; un 75% considera que sí, pero solo un 18,8% cree que efectivamente sea una pauta habitual del CNI.

Esta percepción es llamativa, ya que la Ley del Centro Nacional de Inteligencia de 2002 establece en su artículo 4.a) que una de las misiones del Centro es «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». No obstante, los embajadores reconocen que las empresas españolas tampoco favorecen el incremento de esta buena relación. Mientras un 100% de los embajadores preguntados entiende que las empresas deben informar al CNI de aquello que tengan conocimiento y que pueda ser relevante para los intereses de España, apenas un 10% considera que estas lo hagan.

Por este motivo es muy necesario que los servicios de inteligencia reciban indicaciones claras de los dirigentes políticos para incorporar la inteligencia económica e industrial en su catálogo real de tareas más allá de las que pueda hacer la Directiva de Inteligencia; evidentemente todo esto si consideran que debe tener la relevancia que parece que embajadas y empresas manifiestan.

Para mantener un contacto continuo de la Presidencia con las empresas españolas con fuertes inversiones en el exterior se han establecido diferentes observatorios, uno por zona geográfica prioritaria para España, y que consisten en reuniones de periodicidad mensual en La Moncloa con los responsables de estas empresas. Sin embargo, los canales de comunicación de la comunidad de inteligencia con empresas y diferentes actores económicos españoles parecen bastante exigüos.

Situación algo diferente se produce respecto al Ministerio de Asuntos Exteriores, con una mayor tradición en suministrar este tipo de información y que cuenta para esto con estructuras como la Dirección General de Relaciones Económicas Internacionales.

Parece que los representantes de las empresas españolas en el exterior se sienten más cómodos relacionándose con los embajadores que con las antenas del CNI. La relación óptima, muy pocas veces encontrada, es la de una empresa española con un buen trato con el embajador y de este con el CNI, estableciéndose una adecuada distribución de competencias entre uno y otro.

Sin embargo, las empresas españolas no se fían excesivamente del CNI por dos grandes motivos: no confían en aquellos a quienes no pagan, cosa que sí sucede con las consultoras con las que trabajan y, en segundo lugar, aunque va cambiando esta percepción, porque el CNI sigue teniendo para ellos la imagen de un servicio de espionaje y no es contemplado como una agencia estatal más cuyo trabajo pudiera ser de interés para las inversiones españolas en el extranjero. También es cierto que, cuando a las empresas españolas en el exterior les surgen problemas serios, acuden al CNI en busca de ayuda.

Las escasas relaciones de empresas con el Centro se producen por contactos personales de la dirección o alguna área específica. La falta de cauces establecidos y adecuados convierte a la relación personal en la base de esta actividad, lo que genera una excesiva precariedad, inestabilidad y dependencia de factores personales. Esta es, sin duda, una asignatura pendiente del servicio de inteligencia: implicarse más en esta parcela o bien explicitar a los potenciales consumidores lo que realmente puede aportar en esta área, eliminando la continua frustración de estos actores ante la para ellos débil inteligencia económica que reciben del CNI.

### **Necesidad de una cultura de inteligencia y seguridad**

La Estrategia Española de Seguridad destacaba, muy acertadamente y de una manera explícita, la importancia de la información, la comunicación y la cultura, señalando:

*«El libre acceso a la información y el desarrollo de una política de comunicación responsable son cruciales para la seguridad. Las autoridades*

*públicas deben fomentar la transparencia informativa en estas cuestiones y hacer consciente a la ciudadanía de las amenazas y riesgos a la seguridad, pero sin fomentar el discurso del miedo ni favorecer a los violentos dándoles publicidad o ampliando el eco de sus actividades».*

En cuanto a la cultura de seguridad, la Estrategia Española de Seguridad señalaba:

*«Las amenazas y los riesgos a los que se enfrenta nuestro país han cambiado de forma drástica en las últimas décadas y sus orígenes son múltiples y heterogéneos, desde el terrorismo yihadista hasta las redes del crimen organizado, pasando por los ciberataques. Vivir en una sociedad moderna requiere de unas actitudes, aptitudes y conocimientos hasta ahora desconocidos. Es necesario promover una mayor cultura de seguridad e impulsar la educación de los profesionales de sectores muy diversos y, en general, de los ciudadanos, en estas materias».*

La nueva Estrategia de Seguridad Nacional, aunque no trate esta cuestión de una manera tan directa sí que contiene claras referencias. Las tres primeras las encontramos en la carta o introducción del presidente del Gobierno:

- ✓ En la primera frase de la Estrategia señala que «la seguridad es un fundamento esencial para el desarrollo y el progreso de una sociedad libre. Por eso, resulta imprescindible un entendimiento básico y generalizado de la importancia de la seguridad como garantía del bienestar de los ciudadanos y de la estabilidad del propio Estado».
- ✓ Cuatro párrafos después señala: «Una sociedad responsable y concienciada de su seguridad está en mejores condiciones para hacer frente a los desafíos actuales y ganar en términos de desarrollo y prosperidad».
- ✓ Finalmente indica que «es esencial promover la participación del ciudadano y la colaboración público-privada».

En definitiva, aunque no cite expresamente la palabra «cultura» es evidente que se destaca la necesidad (tanto de conocimientos como de actitudes y aptitudes como señalaba la antigua estrategia), y el mandato de promover esa cultura desde los poderes públicos, de una manera generalizada (profesionales, empresas, asociaciones, ONG, ciudadanos...).

Pero las menciones a la materia no quedan ahí. A lo largo del texto se encuentran multitud de referencias:

- En materia de inmigración. «El nuevo escenario exige esfuerzos de pedagogía y protección por parte de las Administraciones, así como una promoción activa del enfoque de la inmigración como suma positiva en el ámbito económico, social y cultural».
- En materia de defensa nacional establece como línea de acción estratégica el «fomento de la conciencia y cultura de defensa, pilares del apoyo de la sociedad española a la defensa nacional, prestando especial atención a la juventud».

- En materia de ciberseguridad plantea «la implantación de una cultura de ciberseguridad sólida. Se concienciará a los ciudadanos, profesionales y empresas de la importancia de la seguridad de la información y del uso responsable de las nuevas tecnologías y de los servicios de la sociedad del conocimiento».
- En materia de crimen organizado, «la sensibilización y concienciación de la sociedad de que la lucha contra este fenómeno es global, trasciende nuestras fronteras y puede precisar el despliegue de efectivos en terceros países».
- En materia de contrainteligencia, «la sensibilización permanente y a todos los niveles del personal, tanto de las Administraciones públicas como de las empresas y organizaciones, que maneja información clasificada o que, por su relevancia, pueda ser objeto de agresión» y «protección y sensibilización de los ciudadanos españoles que desarrollan sus actividades fuera del territorio nacional y que, por tanto, puedan ser más vulnerables a las acciones hostiles de otros Estados, grupos o individuos».
- En materia de protección ante emergencias y catástrofes, «la promoción de una cultura de prevención entre los ciudadanos, que incluirá conocimientos y actitudes de autoprotección, reforzando las capacidades de resiliencia ante emergencias súbitas e inesperadas. También se promoverán programas de educación para la prevención en centros escolares».

Y no acaban ahí las referencias. Entre los principios del Sistema de Seguridad Nacional, tres de un total de ocho están directamente relacionados con la cultura de seguridad:

- La implicación de la sociedad civil y el fomento de una cultura de seguridad.
- La gestión de la información y del conocimiento.
- La necesidad de transparencia.

De esta forma, atendiendo a las amenazas existentes en la mayoría de las estrategias de seguridad a nivel internacional, y sin ánimo académico, podríamos pensar en la existencia de una cultura de seguridad nacional, por desarrollar, formada a su vez por una serie de culturas específicas, que aún conservando su independencia deberían estar coordinadas, integradas y subordinadas a esa cultura superior.

Así, podríamos considerar a la cultura de defensa, la cultura de inteligencia, la cultura de seguridad interior, la cultura de seguridad económica y financiera, la cultura de emergencias y catástrofes, o la cultura de seguridad energética, como algunas de las culturas integrantes de la cultura de seguridad nacional.

Sobre la cultura de defensa poco cabe señalar que no se haya indicado ya. La ingente labor del Ministerio de Defensa en esta materia, y las continuas actividades del CESEDEN y del Instituto Español de Estudios Estratégicos, pueden servir de modelo y espejo para el resto de las áreas implicadas. La

experiencia, el conocimiento, y la calidad de los trabajos desarrollados, además de la propia importancia de la defensa, pueden y deben ser la guía para todos.

La cultura de inteligencia, explicitada en la propia página web del CNI, y cuyo contenido se actualizó recientemente, se viene desarrollando en los últimos años. Señala:

### *«Cultura de inteligencia*

*Política de sensibilización pública iniciada en 2003 por el Centro Nacional de Inteligencia (CNI) con el objetivo de mejorar el conocimiento de la sociedad en lo que respecta a la labor y misiones del servicio de inteligencia. Asimismo, la cultura de inteligencia pretende concienciar sobre la importancia de la función de inteligencia como herramienta clave en la toma de decisiones estratégicas, tanto a nivel estatal como en el ámbito privado.*

*La cultura de inteligencia se enmarca en una iniciativa más global, la llamada cultura de seguridad, que es compartida por los integrantes de la comunidad de inteligencia española. El objetivo común es que todos los actores sociales adquieran conciencia de que tienen un papel activo en la salvaguarda de la seguridad, y que solo la suma de esfuerzos puede garantizar la seguridad y la defensa de los valores que compartimos.*

### *Objetivos:*

*La cultura de inteligencia pretende dar a conocer a la sociedad las funciones y misiones del servicio de inteligencia como institución que forma parte del Estado democrático y que actúa al amparo de la legislación y controlado por esta. Intenta demostrar también la importancia del análisis y de la inteligencia como herramienta para la toma de decisiones estratégicas en un entorno cada vez más globalizado e incierto.*

*Al mismo tiempo, la cultura de inteligencia trata de propiciar la transferencia de conocimientos y experiencias entre los miembros de los servicios de inteligencia y los representantes de los ámbitos académicos y empresariales, con la convicción de que este intercambio resultará enriquecedor para todas las partes».*

Incluso en ámbitos en que parecía complicado que se produjera la intervención de la comunidad universitaria, como los asuntos de inteligencia, se está asistiendo una apertura y acercamiento que ha culminado en la creación de másteres sobre la materia, en varias universidades, con mayor o menor calidad en cada caso.

Y anteriormente se produjo la creación de la Cátedra Servicios de Inteligencia y Sistemas Democráticos (Universidad Rey Juan Carlos) y del Instituto Juan Velázquez de Velasco de Investigación en Inteligencia para la Seguridad y la Defensa (Universidad Carlos III de Madrid).

Fruto de la colaboración entre ambas instituciones nació la publicación *Inteligencia y seguridad: Revista de análisis y prospectiva*, referencia nacional en materia de inteligencia. Con origen en el citado ámbito académico se vienen desarrollando congresos anuales en materia de inteligencia.

Otras iniciativas, lanzadas por los propios analistas ya formados, y potenciales integrantes de las llamadas reservas de inteligencia o de una comunidad de inteligencia ampliada, son la creación de la Asociación de Analistas de Inteligencia (ASAI) o el lanzamiento de un *hashtag* #esINT en Twitter mediante el cual poder identificar mensajes y contenidos relacionados con la inteligencia en un sentido amplio, abierto tanto a profesionales de la seguridad como de la empresa privada.

A la hora de determinar las posibles culturas, es preciso señalar en todo caso algunas cuestiones:

- o Mientras que algunas tienen carácter claramente finalista, como la cultura de seguridad o la cultura de defensa, otras (como en el caso de la inteligencia) tienen carácter dual y transversal, son más un medio que un fin en sí mismas. Su finalidad es obtener información, su conversión en inteligencia y conocimiento, pero con objeto de garantizar la defensa y la seguridad. La inteligencia debe calar también en las acciones de la seguridad y de la defensa. Tampoco sería del todo adecuado pensar orgánicamente a la hora de establecer responsabilidades en cada una de las culturas. Simplemente dos ejemplos:
  - ✓ La Guardia Civil no solo se limita a la seguridad interior, sino que en multitud de ocasiones despliega sus efectivos en misiones internacionales.
  - ✓ Nuestras Fuerzas Armadas no se limitan únicamente a la defensa en sentido estricto y clásico, sino que apoyan, por ejemplo en catástrofes (especialmente a través de la acción de la Unidad Militar de Emergencias) o de grave crisis de seguridad (patrullas en los días posteriores a los atentados del 11-M).
- o No conviene olvidar la existencia de otras amenazas que obligan a potenciar la cultura actualmente inexistente, y más en los momentos actuales, como podrían ser la cultura de seguridad económica y financiera, la seguridad energética, etc.

La construcción de una cultura de inteligencia y seguridad nacional implicaría los siguientes elementos:

- a. Existencia de una estructura de inteligencia y seguridad nacional, cuestión que resuelve la Estrategia y que en parte aclara la reciente Ley Orgánica de Seguridad Nacional.
- b. Información y comunicación en materia de seguridad nacional. Mandato claro en la Estrategia que debe implementarse.



- c. Educación y formación. Acciones orientadas a profesionales, a jóvenes, a estudiantes en edad escolar, a empresas, a ciudadanos. Muchas de ellas son citadas en la propia Estrategia.
- d. Investigación y publicaciones. La seguridad nacional como objeto de estudio académico y profesional.
- e. Cuerpo doctrinal. Principios, valores, procedimientos. Los pilares los señala la Estrategia.
- f. Lenguaje común. Existiendo por ejemplo un Glosario de Inteligencia, no sucede lo mismo en este ámbito.
- g. Comunidad. Conjunto de personas internas a organizaciones o externas que están comprometidas con la creación y difusión de esta cultura.

Y los requisitos previos para el desarrollo de una cultura de inteligencia y de seguridad nacional, deben ser:

- I. Disponer de una clara cultura organizacional, y que la misma sea difundida. Es preciso el desarrollo de gestión del conocimiento en las propias organizaciones. Es decir, antes de poder trasladar valores, principios y prácticas al ciudadano es necesario abordar de manera más profunda esta materia a nivel interno en las Administraciones públicas.
- II. Es clave que las organizaciones dispongan de una gestión estratégica. Únicamente conociendo dónde se quiere llegar será posible elegir el camino. La cultura de la inteligencia y la seguridad debe estar reflejada y apoyada por el sistema estratégico.
- III. Debe existir una clara conciencia en las organizaciones sobre el interés de una proyección hacia el exterior, que incluya entre otros actores, al ámbito académico, medios de comunicación, y ciudadanos.
- IV. Cultura es colaboración. Se debe tratar de cambiar un viejo paradigma en materia de colaboración y cooperación, y lo que es un error: su planteamiento como un objetivo, un mandato o exigencia. La colaboración y cooperación debe orientarse a «una forma de ser», a su desarrollo como una «actitud» y «aptitud».
- V. Finalmente, el desarrollo de una cultura de inteligencia y seguridad nacional debe estar guiada por criterios éticos, no es una vía para la manipulación o el marketing institucional.

Así y como se ha visto, que la finalidad de la inteligencia no es otra que la capacidad de anticipar noticias de acontecimientos, con un nivel de conocimiento especializado, basado en el recurso de fuentes y procedimientos solo al alcance, en estos momentos y en muchos casos, de los servicios de inteligencia.

Pero hay muchos sectores más que pueden y deben aportar inteligencia, y no solo desde el punto de vista de la seguridad, sino en otros diversos factores referenciados.

Queda mucho camino para esa comunidad de inteligencia y esa cultura de inteligencia.

## Bibliografía

- BALLESTEROS MARTÍN, Miguel Ángel y Joyanes Aguilar, Luis. *Los efectos de la globalización en el ámbito de la seguridad y la defensa*. Cuaderno de Estrategia nº. 10 de Inteligencia y Seguridad (julio-diciembre 2011) del Instituto Español de Estudios Estratégicos (IEEE), organismo del Ministerio de Defensa de España dependiente del Centro Superior de Estudios de la Defensa Nacional (CESEDEN) y del secretario general de Política de Defensa. Pp. 11 a 28.
- BOE. Boletín Oficial del Estado nº. 313, 31 de diciembre de 1987. Tratado sobre no proliferación (TNP), Instrumento de 13 de diciembre de 1987, de Adhesión de España al Tratado sobre la no proliferación de las armas nucleares, hecho en Londres, Moscú y Washington el 1 de julio de 1968.
- DÍAZ FERNÁNDEZ, Antonio M. *El papel de la comunidad de inteligencia en la toma de decisiones de la política exterior y de seguridad de España*, Documento de Trabajo 3/2006, Fundación Alternativas, Observatorio de Política Exterior Española (OPEX), 78 pp.
- ESTRATEGIA DE SEGURIDAD EUROPEA, «Una Europa segura en un mundo mejor», aprobada por los presidentes de gobierno y primeros ministros en el Consejo de la UE el 12 de diciembre de 2003; también conocida por «Documento Solana».
- ESTRATEGIA DE SEGURIDAD EUROPEA, Informe sobre la aplicación de la Estrategia Europea de Seguridad aprobado por el Consejo de Europa. «Ofrecer seguridad en un mundo en evolución». Bruselas, 11 de diciembre de 2008.
- ESTRATEGIA ESPAÑOLA DE SEGURIDAD 2011 «Una responsabilidad de todos», publicada en la web del Ministerio de Defensa español <http://www.defensa.gob.es/>.
- ESTRATEGIA DE SEGURIDAD NACIONAL 2013 «Un proyecto compartido», publicada en la web de Presidencia del Gobierno español <http://www.la-moncloa.gob.es/>.
- FISCHER, Joschka. «Europa y el nuevo orden mundial», artículo publicado en *El País* el 7 de diciembre de 2008.
- KISSINGER, Henry. «Reconsideración del Nuevo Orden Mundial». Fondo de Cultura Económica USA, 1/7/1999 - 72 pp.
- LEY 36/2015 de 28 de septiembre, de Seguridad Nacional (BOE 233 de 29/09/2015).
- MERLE, Marcel. *Sociología de las relaciones internacionales*. Madrid (España), Alianza 1984. 461 pp.

- NAVARRO BONILLA, Diego. «El ciclo de inteligencia y sus límites». Cuaderno Constitucional de la Cátedra Fadrique Furió Ceriol nº. 48. Universidad Carlos III Madrid. 15 pp.
- RAMONET, Ignacio. *Geopolítica del Caos*. Editorial: Debate. 400 pp.
- RAMONET, Ignacio. *Guerras del siglo XXI. Nuevos miedos, nuevas amenazas*. Barcelona, Mondadori, 2002.
- RATZEL, Friedrich. *Antropogeografía* (1891) y *Geografía Política* (1897), Editorial Verlag Von J. Engelhorn de Stuttgart (1909).
- ROBERTSON, Roland. «Globalization: Time-Space and Homogeneity», *Global Modernities*, eds. Mike Featherstone, Scott Lash and Ronald Robertson (London: Sage, 1995), pp. 25-44.
- SANZ ROLDÁN, Félix. Secretario de Estado, Director del Centro Nacional de Inteligencia español (CNI). «Opinión e inteligencia», Documento de Opinión nº. 45/2012 fechado el 06/06/2012, 4 pp. Publicado por el Instituto Español de Estudios Estratégicos (IEEE), organismo del Ministerio de Defensa de España dependiente del Centro Superior de Estudios de la Defensa Nacional (CESEDEN) y del secretario general de Política de Defensa.
- STIGLITZ, Joseph E. (2004). *El malestar de la globalización*. Madrid: Santillana. Ediciones Generales.
- VARIOS AUTORES: Grupo de trabajo número 5/03. *Estudios sobre inteligencia: fundamentos para la seguridad internacional*. Cuaderno de Estrategia nº. 127 del Instituto Español de Estudios Estratégicos (IEEE), organismo del Ministerio de Defensa de España dependiente del Centro Superior de Estudios de la Defensa Nacional (CESEDEN) y del secretario general de Política de Defensa. 177 pp.
- VARIOS AUTORES: Grupo de trabajo número 5/04. *El papel de la inteligencia ante los retos de la seguridad y la defensa internacional*. Cuaderno de Estrategia nº. 130 del Instituto Español de Estudios Estratégicos (IEEE), organismo del Ministerio de Defensa de España dependiente del Centro Superior de Estudios de la Defensa Nacional (CESEDEN) y del secretario general de Política de Defensa. 175 pp.



## Capítulo tercero

### Campos de actuación de la inteligencia

José Manuel Díaz-Caneja Greciano

#### Resumen

Durante siglos, la inteligencia o información elaborada ha sido uno de los pilares fundamentales en los procesos de toma de decisiones por parte de los responsables políticos en todos los ámbitos, principalmente a la hora de proporcionar una seguridad lo más eficaz posible, a la sociedad de la que eran responsables.

La inteligencia puede ser considerada, en términos generales, como el complejo proceso de comprender el significado de la información disponible, para su empleo en un proceso de toma de decisiones o de planeamiento.

La identificación de amenazas globales y el alcanzar una comprensión de su impacto, requiere algo más que simplemente compartir información. Es necesaria una mayor colaboración en la fusión de información y en la producción de inteligencia.

#### Palabras clave

Inteligencia, toma de decisiones, análisis, alertas.

**Abstract**

During centuries, intelligence or information produced has been one of the cornerstones in a decision making process for policy makers at all levels, primarily in providing security as effective as possible, to the society which they were responsible.

Intelligence can be considered, in general terms, as the complex process of understanding the meaning of the information available to be used in a decision making process or planning.

The identification of global threats and the achievement of an understanding of their impact require more than simply sharing information. Greater collaboration in the fusion of information and production of intelligence is necessary.

**Keywords**

Intelligence, decision making, analysis, warning.

## Escenario geopolítico

Desde la antigüedad se ha resaltado el poder que supone disponer de información por adelantado del enemigo o competidor que permita prever sus posibles actuaciones, como aspecto esencial para obtener la victoria en el campo de batalla, o más importante aún evitar el enfrentamiento.

Durante siglos, la inteligencia o información elaborada ha sido uno de los pilares fundamentales en los procesos de toma de decisiones por parte de los responsables políticos en todos los ámbitos, principalmente a la hora de proporcionar una seguridad, lo más eficaz posible, a la sociedad de la que eran responsables.

La percepción del concepto de seguridad en Europa durante el siglo XX ha sufrido modificaciones, como consecuencia de los acontecimientos que se han producido en el ámbito internacional, donde el papel de la inteligencia cobra cada vez más importancia a la hora de detectar y prevenir amenazas.

El escenario actual, en el cual los Estados tienen que proporcionar seguridad ante una gran variedad de enemigos difusos, y para los cuales las fronteras nacionales no son un obstáculo, es complejo, debido a la cada vez mayor número de población que vive en grandes ciudades, al movimiento de la gente, el invisible trasiego de información de un punto a otro del planeta, y la constante interacción de sistemas adaptativos complejos (CAS)<sup>1</sup> así como la manera en que interactúan y colisionan entre ellos<sup>2</sup>.

El mundo globalizado actual se puede entender mejor como compuesto por sistemas adaptativos complejos (CAS), donde cada uno de ellos es una red<sup>3</sup> de muchos agentes (los cuales pueden representar células, especies, individuos, empresas, naciones, etc.) funcionando en paralelo, constantemente actuando y reaccionando a lo que otros agentes están haciendo. El control de un CAS tiende a ser altamente disperso y descentralizado. Si tiene que haber, o queremos definir, una conducta coherente en el sistema, esta surge de la competición y la cooperación entre los agentes que forman parte del sistema. El comportamiento general del sistema es el resultado de un gran número de decisiones realizadas a cada momento por muchos agentes individuales<sup>4</sup>.

Esta situación provoca que los Estados con sus propios recursos, y excesivamente burocratizados, se vean impotentes para hacer frente a unas amenazas que están estructuradas en redes interconectadas. Pero es que además, este escenario, que es de pesadilla para los gobiernos, es visto por sus

<sup>1</sup> En inglés, Complex Adaptive Systems (CAS).

<sup>2</sup> HALL, W. M., & Citrenbaum, G. (2010). *Intelligence Analysis: How to Think in Complex Environments*. Santa Barbara: Praeger Security International, pp. 10-16.

<sup>3</sup> Cada vez está más difundido el empleo del término inglés *network*.

<sup>4</sup> WALDROP, M. M. (1992). *Complexity: The Emergencing Science at the Edge of Order and Chaos*. New York: Simon & Schuster.

contrarios como un santuario en el cual, y desde el cual, pueden operar con facilidad, debido a que el entorno actual, con sus grandes ciudades, el volumen enorme de transacciones comerciales, las dinámicas de la población y la disparidad étnica, permiten, por ejemplo, que con bastante facilidad un pequeño grupo terrorista pase desapercibido dentro de las actividades que tienen lugar en una ciudad un día cualquiera.

Esta necesidad que tienen los gobiernos de proporcionar seguridad a su población en un sentido más amplio, ha traído como consecuencia la potenciación de sus servicios de inteligencia, ya no solamente para que tengan las capacidades suficientes para actuar dentro de sus fronteras, sino que sean capaces de colaborar, intercambiar información y llevar a cabo operaciones conjuntas con los servicios homónimos de otros Estados.

### ¿Qué es inteligencia?

La película de George Lucas, *La Guerra de las Galaxias*, describe el paso final de una operación de inteligencia. La heroína, la princesa Leia, obtiene los planos de la última máquina de guerra del malvado Imperio Galáctico, la Estrella de la Muerte, del robot R2-D2, el cual está actuando como un buzón móvil<sup>5</sup>. Leia entrega los planos a las fuerzas rebeldes, cuyos analistas de inteligencia informan al mando rebelde sobre los planos, señalan los puntos débiles de la Estrella de la Muerte, y presentan un brillante análisis de las defensas enemigas. Los pilotos rebeldes lanzan torpedos de protones al punto débil y el objetivo es destruido.

La escena anterior resume con mucha precisión cómo es visto normalmente el ciclo de inteligencia. Los agentes que obtienen la información y ejecutan la operación se llevan la gloria. Los analistas de inteligencia, trabajando detrás del telón, analizan los problemas importantes para resolverlos y hacer que todo funcione.

Aunque el foco popular está en la obtención de la información y en la ejecución de operaciones en base a ella, el éxito en operaciones como la de Bin Laden en el 2011, no puede hacernos olvidar que la mayoría de los grandes fallos en inteligencia, como puede ser el caso de las armas de destrucción masiva de Irak, son debidos a un inadecuado o inexistente análisis.

La información estaba normalmente allí, al menos cuando se hace un análisis *post mortem*<sup>6</sup> se encuentra, pero desafortunadamente habría que haber examinado y descartado una gran cantidad de material irrelevante.

---

<sup>5</sup> Un buzón móvil es un escondite temporal para material que está en tránsito entre dos agentes clandestinos de inteligencia, que no se pueden arriesgar a un encuentro cara a cara. Una lata próxima a un banco en un parque es un ejemplo típico.

<sup>6</sup> Un análisis *post mortem* es aquel que se lleva a cabo posteriormente a que se haya producido un hecho, para intentar detectar en que se falló. Un ejemplo muy conocido es el



Cuando hablamos de inteligencia, muchas veces también lo hacemos de información, pero ambos términos no son sinónimos. Según figura en la página web del Centro Nacional de Inteligencia (CNI), el término información debe diferenciarse del de inteligencia, ya que información equivale a la noticia de un hecho en su sentido más amplio<sup>7</sup>.

Mientras el concepto información debe de entenderse como el elemento de partida para la elaboración de inteligencia, esta se considerada que es el resultado de valorar, analizar, integrar e interpretar la información<sup>8</sup>.

Pero la inteligencia está en relación con la reducción de la incertidumbre en el conflicto. Debido a que el conflicto puede consistir en cualquier acción competitiva u opuesta, como resultado de la divergencia de ideas o intereses de dos o más actores, el conflicto no tiene por qué ser físico.

Si existe la negociación o la competición, entonces dos o más grupos están en conflicto. Pueden existir diferentes niveles de conflicto, desde la competición amistosa hasta la guerra. Reducir la incertidumbre requiere que la inteligencia obtenga información que el oponente en el conflicto prefiere ocultar.

Sin embargo, en muchas ocasiones la información necesaria es inaccesible, ya que otros países, grupos políticos o competidores son conscientes de que ciertos tipos de información podrían tener un gran valor para aquellos que podrían ser adversarios actuales o potenciales en un futuro próximo<sup>9</sup>. Como consecuencia, las organizaciones, y no necesariamente solo las estatales, toman grandes medidas para denegar, limitar, o incluso falsificar ciertos tipos de información y datos.

Así, unido a los problemas metodológicos de obtener y utilizar la información obtenida por lo medios de obtención, los responsables de planificación se encuentran con el gran problema de obtener información que otros desean denegar a los extraños. Son estos actos para denegar cierto tipo de información a otros, lo que ha provocado el nacimiento y crecimiento de las organizaciones de inteligencia. Sin la inaccesibilidad para ciertos tipos de información, las organizaciones de inteligencia hoy en día serían innecesarias, ya que gracias a los avances tecnológicos, gran parte de la información necesaria para el planeamiento puede estar disponible o bien en otras agencias gubernamentales o en fuentes abiertas.

---

análisis (investigación) que se llevó a cabo en los Estados Unidos, después de los ataques del 11-S.

<sup>7</sup> CENTRO NACIONAL DE INTELIGENCIA. ¿Qué diferencia hay entre información e inteligencia? Disponible en <http://www.cni.es/es/preguntasfrecuentes>. Fecha de la consulta el 09/01/2016.

<sup>8</sup> *Ibidem*.

<sup>9</sup> CLAUSER, Jerome (2008). *An Introduction to Intelligence Research and Analysis*. Plymouth UK: The Scarecrow Press, p. 10.

Las organizaciones de inteligencia deben emplear un amplio abanico de medios de obtención, que pueden ir desde sofisticados sensores como pueden ser los aparatos aéreos no tripulados a fuentes humanas. Debido a la gran variedad de medios de obtención empleados y a la gran cantidad de datos que se obtienen, las organizaciones de inteligencia deben gastar mucho tiempo y esfuerzo en asegurar la calidad de los datos obtenidos. Cualquier estimación o proyección de inteligencia es tan fiable como lo son los datos en los cuales está basada; por ello, establecer la fiabilidad de los datos es una de las principales funciones de las organizaciones de inteligencia.

La inteligencia puede ser considerada, en términos generales, como el complejo proceso de comprender el significado de la información disponible. Un objetivo típico de inteligencia es el determinar unos hechos y luego desarrollar inferencias (hipótesis, estimaciones, conclusiones o predicciones) precisas, fiables y válidas, para su empleo en un proceso de toma de decisiones o de planeamiento.

La mayoría de los métodos que se emplean en inteligencia son muy similares a los que puede emplear por ejemplo una analista de mercados financieros, la diferencia es que, cuando la información precisa no está disponible a través de medios tradicionales, se puede emplear un amplio abanico de tecnología especializada.

Como la inteligencia es sobre el conflicto, apoya a operaciones tales como de combate o de planeamiento militar, negociaciones diplomáticas, comerciales y a las fuerzas y cuerpos de seguridad. El primer consumidor de inteligencia es la persona que actuará en base a la información, el ejecutivo, el político, el militar o el policía.

Una de las cosas que distingue a la inteligencia de las simples noticias es su apoyo a las operaciones, y que además la persona que necesita inteligencia para llevar a cabo sus operaciones (o actividades) debe de hacer algo en base a ella, es decir, tiene que tomar una decisión.

Por último, la inteligencia es siempre en relación a un objetivo, el centro del problema sobre el cual queremos respuestas.

### El ciclo de inteligencia

Se entiende por «ciclo de inteligencia» la secuencia mediante la cual se obtiene información, se transforma en inteligencia y se pone a disposición de los usuarios. El ciclo de inteligencia consta de cuatro fases: dirección, obtención, elaboración y difusión<sup>10</sup>.

<sup>10</sup> CENTRO NACIONAL DE INTELIGENCIA. El Ciclo de Inteligencia. Disponible en <http://www.cni.es/es/queescni/ciclo/>. Fecha de la consulta 08/01/2016. La versión de la Agencia Central de Inteligencia (CIA) de los Estados Unidos consta de cinco fases: Planeamiento y dirección, obtención, procesamiento, análisis y producción, y difusión.



Figura 3-1. Ciclo de inteligencia. Elaboración propia. Fuente: [www.cni.es](http://www.cni.es)

Independientemente del modelo de ciclo que se tome, este se pone en marcha cuando existen unos requisitos o necesidades para definir un problema de inteligencia. Puede tomar la forma de una pregunta muy general o más concreta.

Luego viene la fase de planeamiento o dirección, en la cual se determina como el resto de componentes del ciclo colaboran en la solución del problema. Se encomiendan misiones a los medios de obtención para conseguir la información necesaria. La información en bruto, una vez obtenida, tiene que ser procesada, antes de que se ponga en marcha la fase de análisis. Por ejemplo, si la información es una grabación procedente de una interceptación telefónica a un miembro del gobierno sirio, tiene que ser traducida y transcrita a un documento.

Todo este material obtenido y procesado, junto con material anterior relevante, se utiliza para crear productos de inteligencia en la fase de elaboración. Un analista diseñará posibles escenarios futuros<sup>11</sup> basados en la situación actual de Siria, realizará perfiles de los líderes sirios, y evaluará sus respuestas más probables ante posibles acontecimientos futuros.

El producto final de inteligencia debe ser difundido al que lo solicitó, ya sea en un documento escrito o mediante una conferencia informativa. Posteriormente viene un periodo de transición hasta que surgen nuevos requerimientos o necesidades de información, las cuales inician un nuevo ciclo.

<sup>11</sup> El diseño de escenarios consiste en prever posibles futuros que podrían ocurrir. Como mínimo se deben diseñar dos, el más probable y el más peligroso. Para profundizar en el diseño de escenarios ver el libro de Heuer, R. J., & Pherson, R. H. *Structured Analytic Techniques for Intelligence Analysis*. 2011. Washington: CQ Press.

### Los flujos de información en el ciclo de inteligencia

«Durante muchos años el ciclo de inteligencia llegó a ser casi como un concepto teológico, sin que nadie se cuestionara su validez. Sin embargo, actualmente, muchos profesionales de inteligencia no dudan en reconocer que el proceso de transformación de la información en inteligencia no funciona realmente como un ciclo»<sup>12</sup>.

El principal problema del ciclo de inteligencia es que define rígidamente una serie de pasos, los cuales constriñen el flujo de información. Además, separa totalmente a los especialistas en medios de obtención, de los encargados de alimentar las bases de datos y de los analistas, lo que provoca que en muchas ocasiones sea difícil encontrar al responsable del siguiente paso. Esto trae como consecuencia que todos los involucrados evitan responsabilizarse de la calidad del producto final.

Otro problema existente es que, en muchas ocasiones, el bucle de retroalimentación, presente en cualquier ciclo, brilla por su ausencia. Existe un vacío entre la difusión y las necesidades iniciales de inteligencia formuladas, debido a que los solicitantes están fuera del bucle, y normalmente no existe un procedimiento para que comuniquen si el producto final de inteligencia satisface sus necesidades, o necesitan que se modifique, sin que eso suponga el punto de partida para un nuevo ciclo.

Todo esto es debido al desconocimiento mutuo dentro de las estructuras gubernamentales, entre los oficiales de inteligencia y los responsables de tomar decisiones, a los cuales apoyan, ya sean políticos, policías o militares, si bien es cierto que el vacío en estos últimos es menos acentuado.

Que el sistema funcione depende de que los clientes<sup>13</sup> den a conocer sus necesidades. En las estructuras militares y policiales existen procedimientos establecidos para que se produzca. Sin embargo, a nivel de altos cargos políticos en muchos casos no es así, ya que las contribuciones o comunicación de las necesidades de información son más informales y además normalmente pasan por varios intermediarios antes de llegar al personal de inteligencia, con las distorsiones que ello provoca.

En muchas ocasiones, y principalmente debido al desconocimiento por parte de los responsables de tomar decisiones de las capacidades y procedimien-

---

<sup>12</sup> CLARK, R. M. (2010). *Intelligence Analysis: A Target Centric Approach*. Washintong: CQ Press, p. 11.

<sup>13</sup> A lo largo del texto se encontrará el término cliente, para definir a cualquier persona, ya sea un cargo político, un mando militar o policial, o incluso una organización o parte de ella, que tiene unas necesidades de inteligencia, las cuales deben de ser satisfechas, ya que esa inteligencia es necesaria tanto como apoyo para el proceso de toma de decisiones, como para el planeamiento.

tos de los órganos de inteligencia, son los analistas y sus jefes quienes acaban determinando esas necesidades de inteligencia de sus clientes.

Según Treverton y Gabbard, el ciclo de inteligencia comienza con los jefes, cuyas inquietudes, por medio de las primeras fases del ciclo, se convierten en misiones para los distintos medios de obtención. Las informaciones y datos adquiridos por los distintos medios de obtención son procesadas en varios niveles para, en última instancia, llevarse a cabo un análisis de las informaciones obtenidas de todas las fuentes. Una vez elaborado el producto de inteligencia correspondiente, este es difundido<sup>14</sup>.

Como se observa en la figura 3-2, el ciclo distingue entre fuentes de inteligencia (medios de obtención) y proceso de análisis (en España denominado fase de elaboración) que se emplea para transformar los datos en bruto en inteligencia.

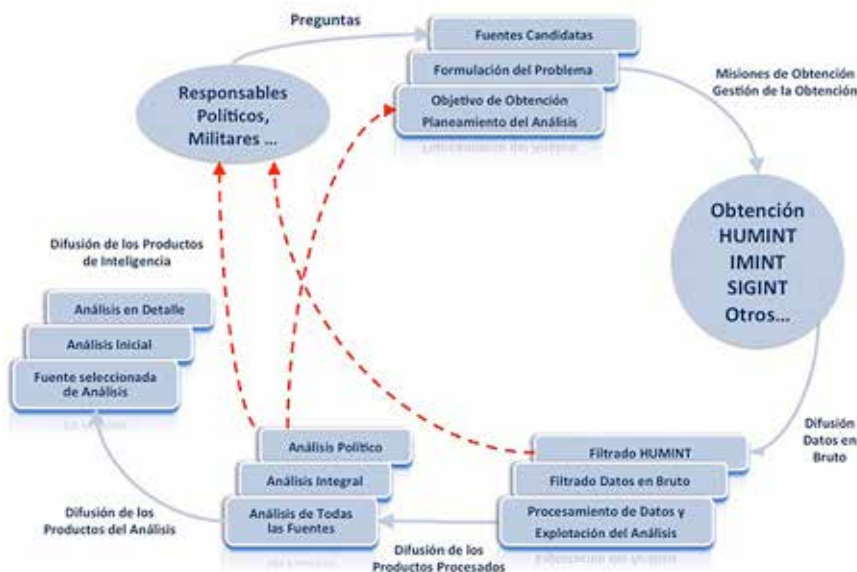


Figura 3-2. El ciclo de inteligencia. Fuente: TREVERTON, G. F., & GABBARD, B.C. (2008). *Assesing the Tradecraft of Intelligence Analysis*. Santa Monica: RAND Corporation, p. 3

Las líneas punteadas de la figura resaltan la posibilidad que existe, y que muchas veces se materializa, de que el ciclo sea cortocircuitado, ya que en ocasiones, la información a varios niveles, incluyendo información en bruto sin procesamiento previo, pasa a los jefes, sin que se haya realizado un filtrado previo por los analistas y se haya puesto en contexto, provocando que

<sup>14</sup> TREVERTON, G. F., & GABBARD, B.C. (2008). *Assesing the Tradecraft of Intelligence Analysis*. Santa Monica: RAND Corporation, p. 3.

estos, ante la premura de tiempo, tomen como inteligencia lo que únicamente es información sin analizar.

A lo largo de la historia, líderes muy carismáticos y dinámicos han sido vulnerables a este problema. Franklin Roosevelt, Winston Churchill y Henry Kissinger son ejemplos de grandes estadistas que ocasionalmente hicieron sus propios análisis.

Michael Herman cuenta como Churchill, durante la II Guerra Mundial, leyendo los mensajes descriptados del mariscal de campo Erwin Rommel, llegó a la conclusión de que los alemanes estaban desesperadamente cortos de suministros en el norte de África. Basando su interpretación en estos productos en bruto de Inteligencia de Señales (SIGINT)<sup>15</sup> sin analizar, presionó a sus generales para que llevaran a cabo operaciones ofensivas contra Rommel. Churchill no se dio cuenta de lo que sus propios analistas de inteligencia podrían haberle dicho rápidamente: Rommel exageraba continuamente sus carencias, como una manera de asegurar que sus solicitudes de suministros y refuerzos fueran atendidas<sup>16</sup>.

Hoy en día, esta situación se puede reproducir en múltiples organizaciones, debido a los grandes avances de la tecnología, que permite que los clientes de cualquier organización de inteligencia realicen su propia obtención, lo que puede resultar que le den mayor importancia y valor sobre cualquier otra, y que puede traer como consecuencia que sean más vulnerables a la decepción y el engaño, al realizar también ellos mismos su propio análisis, en ocasiones con resultados desafortunados.

Otro problema existente con el ciclo de inteligencia, es que está basado en la búsqueda de soluciones para un problema de manera lineal, en la creencia de que es necesario seguir un proceso secuencial y ordenado desde el planteamiento inicial del problema, una necesidad de inteligencia, hasta la solución, la difusión del producto final.

Muchos expertos en inteligencia destacan que el fallo de este enfoque lineal es que no tiene en cuenta el proceso cognitivo real que se lleva a cabo. La mente no trabaja de manera lineal, sino que va saltando de una parte a otra del problema. En el caso de un oficial de inteligencia, ante la falta de información adecuada en la fase de análisis, saltará a la de obtención para pedir aclaraciones, de allí podrá saltar a la de requisitos, para volver de nuevo a la de obtención, y vuelta a la de análisis. Como se observa, este proceso no se asemeja a un ciclo<sup>17</sup>.

---

<sup>15</sup> SIGINT es la inteligencia elaborada a partir de la obtención y explotación de emisiones o señales electromagnéticas.

<sup>16</sup> HERMAN, Michael (1996). *Intelligence Power in Peace and War*. Cambridge. Cambridge University Press, p. 99.

<sup>17</sup> LAHNERMAN, W. J. (2006). *The Future of Intelligence Analysis*. Maryland: University of Maryland, Center for International and Security Studies.

En el mundo actual con los grandes avances que se producen cada poco tiempo en las tecnologías de la información, el ciclo de inteligencia es cada vez menos relevante, siendo habitual la constitución de redes informales<sup>18</sup>, con los mismos intereses, para la búsqueda de soluciones a un problema determinado, y que, debido al empleo de tecnología web segura<sup>19</sup>, permite desarrollar un proceso de inteligencia no lineal.

### Innovaciones en los procesos de inteligencia

Una alternativa al tradicional ciclo de inteligencia, y que facilitaría el flujo de información, y la confección de un producto de inteligencia de calidad, es incorporar a todos los actores implicados al proceso de inteligencia, incluidos los solicitantes de información, los responsables de tomar decisiones, los especialistas en medios de obtención, los analistas de inteligencia, etc.



Figura 3-3. Proceso de Inteligencia Centrado en el Objetivo. Fuente: CLARK, R. M. *Intelligence Analysis: A Target Centric Approach*. O. C., p. 14

<sup>18</sup> Estas redes informales se las suele denominar comunidades de interés.

<sup>19</sup> Un buen ejemplo lo constituye la página <https://www.cimicweb.org/>, desarrollada por la OTAN, que con el objetivo del alcanzar un conocimiento profundo en situaciones de crisis complejas, y fomentar la colaboración cívico-militar, permite el intercambio de información entre todos los actores involucrados, tanto a nivel interno de la OTAN, como externo, organizaciones estatales e incluso Organizaciones No Gubernamentales (ONG).

Para incluir a todo este personal en el proceso, el ciclo tiene que ser redefinido, pero no en una rígida estructura orgánica tradicional, si no de tal manera que aprovechen los avances actuales en las tecnologías de la información para manejar problemas complejos.

Uno de los autores defensores de esta idea es el autor norteamericano Robert M. Clark, que en su libro sobre análisis de inteligencia<sup>20</sup>, lo denomina «inteligencia como un proceso centrado en el objetivo»<sup>21</sup>.

La figura 3-3 muestra este nuevo enfoque del proceso de inteligencia centrado en el objetivo. La finalidad de este enfoque es diseñar una imagen común del objetivo, de la cual todos los participantes puedan extraer los elementos que necesiten para su trabajo, y a la cual puedan contribuir desde sus capacidades y conocimiento. No es un proceso lineal, es proceso colaborativo en red, con todos los participantes centrados en el objetivo.

En cualquier operación de inteligencia el análisis está implícito, pero no todo el trabajo es hecho por los analistas. Los clientes (o solicitantes de inteligencia), así como los especialistas en obtener la información, también participan, y lo harán a pesar de que el analista no esté de acuerdo. Esto es debido a que ambos tienen su particular visión del objetivo, y quieren que esta se incluya en el producto analítico final.

Sin embargo, alguien tiene que hacer que el proceso funcione coherentemente, crear y mantener actualizada esa imagen común del objetivo, recibir las necesidades de inteligencia, descomponerlas en requisitos de información que deben ser obtenidos, aceptar las nuevas informaciones e incorporarlas a la imagen del objetivo, extraer inteligencia procesable<sup>22</sup> y asegurarse que llega al solicitante. Según Clark todo esto es cometido del analista, el cual pasaría a desarrollar más un trabajo de gestión de la información y conducción de la misma hacia los otros participantes.

Las ideas de Clark tuvieron gran repercusión y han sido el punto de partida de otros teóricos en asuntos de inteligencia como Wayne Michael Hall y Gary Citrenbaum, los cuales a lo largo de su libro destacan la brecha existente y la falta de cooperación entre los analistas y los especialistas de los medios de obtención. Esta realidad, conlleva que los medios de obtención reciban poca orientación por parte de los analistas sobre lo que es necesario buscar, donde buscarlo y cuando buscarlo, provocando un despilfarro del esfuerzo de obtención por un lado, y por otro que no se mejore el conocimiento del objetivo, con la finalidad de producir inteligencia útil<sup>23</sup>.

<sup>20</sup> CLARK, R. M., O. C., p. 13.

<sup>21</sup> En inglés: Intelligence as a Target-Centric Process.

<sup>22</sup> El término de inteligencia procesable se refiere a la información concreta y específica que deja vía libre a líneas de actuación y su rápida ejecución.

<sup>23</sup> HALL, W. M., & CITRENBAUM, O. C., p. 18.



Con un enfoque en equipo, el trabajo es más interactivo que con el proceso del tradicional ciclo de inteligencia, además de ser más eficaz para manejar problemas complejos, ya que todos los participantes comparten un conocimiento común del objetivo, y son más capaces de identificar vacíos en ese conocimiento.

«El enfoque centrado en el objetivo es un proceso más resistente y flexible, debido a la colaboración de todos sus miembros, no hay un solo punto de fallo, ya que en cualquier momento un miembro de la red puede actuar como facilitador de información, y la responsabilidad final del producto es de todo el equipo»<sup>24</sup>.

Por otro lado, este enfoque es capaz de satisfacer a una gran variedad de clientes desde una única base de conocimientos. En inteligencia, es normal que exista un gran número de solicitantes de información para un problema determinado, y cada solicitante tiene sus propias necesidades. Por ejemplo, en un momento dado las Fuerzas Armadas de un país, su Ministerio de Economía y el de Asuntos Exteriores pueden necesitar información sobre un determinado país. El objetivo es común, pero las necesidades de información de cada organización son únicas.

Las principales ventajas que aporta este enfoque centrado en el objetivo son:

1. Es colaborativo por diseño, lo que facilita el intercambio de información y permite incrementar la confianza mutua y la comprensión entre todos los participantes en el mismo.
2. Es un modelo que se puede aplicar tanto dentro de la estructura de inteligencia nacional, como a nivel internacional, cuando existe un asunto de intereses común a varios países.
3. Facilita el trabajar con grandes volúmenes de información, ya que el enfoque de trabajo en red, permite expandir el equipo incorporando especialistas en las áreas que sea necesario, con la finalidad de filtrar la información disponible y desechar la irrelevante.
4. Permite satisfacer más rápidamente las solicitudes de información más detalladas y que cada vez es más habitual recibir por parte de los clientes, sobre un determinado objetivo de inteligencia<sup>25</sup>.

### Implicaciones del escenario actual para inteligencia

Como se ha visto anteriormente, el escenario actual, caracterizado por unas amenazas difusas a la seguridad de los Estados, siendo estos incapaces de

<sup>24</sup> CLARK R. M., O. C., p. 15.

<sup>25</sup> DÍAZ-CANEJA GRECIANO, José Manuel (2014). *La Cooperación de Inteligencia en la UE*. Madrid: Instituto Español de Estudios Estratégicos. Disponible en [http://www.ieee.es/Galerias/fichero/docs\\_opinion/2014/DIEEE0151-2014\\_CooperacionInteligencia\\_UE\\_JMDiaz\\_Caneja.pdf](http://www.ieee.es/Galerias/fichero/docs_opinion/2014/DIEEE0151-2014_CooperacionInteligencia_UE_JMDiaz_Caneja.pdf).

afrentarlas eficazmente únicamente con sus recursos, tiene unas especiales implicaciones para las estructuras de inteligencia según Hall y Citrenbaum<sup>26</sup>:

- El personal de inteligencia afronta una gran variedad de cambios, de tal manera que están obligados a ser intelectualmente más agresivos.
- Deben aprender a anticiparse al adversario en sus pensamientos, decisiones y acciones.
- Debe aprender y entender cómo percibe el líder enemigo, piensa, planea, decide, actúa y recibe retroalimentación de sus acciones.
- Principalmente los analistas deben aprender a dirigir la obtención, el objetivo debe ser el establecimiento de esa red cooperativa/colaborativa propia, buscando la implicación de los solicitantes de inteligencia, los especialistas en medios de obtención de información, así como contar en todo momento con el apoyo de expertos.
- Es necesario alcanzar un profundo conocimiento de la red oponente/enemiga, para ser capaces de identificar sus nodos, vínculos y procesos, con la finalidad de identificar aquellos más vulnerables y que puedan ser interferidos.

Por otro lado si hablamos más concretamente de terrorismo o crimen organizado, estos son fenómenos complejos que involucran a un gran número de actores no estatales, vinculados por organizaciones conectadas en red, las cuales operan como redes transnacionales dentro de una galaxia de redes afines.

Estas entidades plantean amenazas a la seguridad de las naciones estado y a la seguridad colectiva global. A esto se le suma que «los enfoques tradicionales de inteligencia y seguridad han separado siempre la inteligencia criminal de la de seguridad nacional, así como las inquietudes sobre seguridad interna e internacional, lo que trae como consecuencia una brecha que es aprovechada por las organizaciones terroristas y criminales para operar a escala global»<sup>27</sup>.

Por ello, es necesario cerrar la brecha existente entre la inteligencia tradicional y las estructuras de seguridad, siendo necesario un enfoque en red para la producción de inteligencia, de interés para distintos servicios u organismos.

Este enfoque debe de estar basado en la búsqueda e identificación proactiva de amenazas emergentes y proporcionar alerta temprana, integrando las informaciones y el análisis a partir de un equipo multidisciplinar de personal de diversos servicios e incluso naciones, cuya finalidad, como se ha dicho,

<sup>26</sup> HALL, W. M., & CITRENBUM, G., O. C., pp. 29-47.

<sup>27</sup> SULLIVAN, J. P. (2005). «Terrorism Early Warning and Co-Production of Counterterrorism Intelligence». Montreal, Québec, Canadá. Disponible en [http://www.projectwhitehorse.com/pdfs/6.%20CASIS\\_Sullivan\\_paper1.pdf](http://www.projectwhitehorse.com/pdfs/6.%20CASIS_Sullivan_paper1.pdf).

es anticipar amenazas y desarrollar estrategias de obtención de inteligencia acordes a esas amenazas.

La identificación de amenazas globales y el alcanzar una comprensión de su impacto, requiere algo más que simplemente compartir información. Es necesaria una mayor colaboración en la fusión de información y en la producción de inteligencia entre los nodos cooperativos que están distribuidos en las ubicaciones donde los terroristas o redes criminales operan, planean o buscan para atacar.

Por ejemplo, una organización terrorista puede planear sus ataques en Europa, mientras obtiene su apoyo logístico y financiero en Sudamérica y Asia. Puede simultáneamente llevar a cabo acciones de reconocimiento en su ciudad objetivo en el norte de África, reclutar y entrenar a sus miembros en Irak, y todo ello mientras recibe órdenes desde otra ubicación diferente.

El desarrollo de la inteligencia necesaria para anticipar, prevenir, interferir o mitigar los efectos de un ataque, requiere la producción de inteligencia de una manera colaborativa e integrada del esfuerzo de un gran número de agencias a lo largo de un área dispersa.

El núcleo central de producción de inteligencia, ya sea para afrontar una amenaza terrorista o más convencional, es la fase de elaboración, y más concretamente el análisis y la síntesis, o en lenguaje más claro, el proceso de descomposición de la información en sus elementos constituyentes, su procesamiento en componentes manejables, la búsqueda de vínculos con elementos relacionados, ponerlos en contexto y sintetizar los resultados en inteligencia procesable.

El principal problema de todo lo expuesto, es la competición existente a nivel de organización y burocracia. Las estructuras en red compiten con sus jerárquicas predecesoras. La inercia burocrática dificulta las acciones encaminadas hacia la colaboración. A ello se añade las luchas intergubernamentales entre las distintas agencias por ostentar la supremacía. Y, si estamos hablando de cooperación a nivel internacional, la cosa se complica más, por los diferentes intereses nacionales y una desconfianza mutua endémica.

Mucha de la información necesaria para comprender la dinámica de una amenaza, e incluso para reconocer que una amenaza existe, requiere intercambios de información multilaterales. Para alcanzar un eficaz intercambio de información e inteligencia es necesario el desarrollo de nuevas capacidades analíticas, procesos y políticas. Se necesitan instrumentos intergubernamentales para explotar completamente el intercambio de información, tanto a nivel nacional como internacional.

Según Treverton, otro aspecto importante es que actualmente las estructuras de inteligencia están dedicadas a trabajar a nivel operacional, táctico o actual. En la mayoría de los casos, se echa en falta un análisis a largo plazo. En otras palabras, la mayoría de los recursos están dedicados al informe de

inteligencia, en vez de intentar alcanzar un profundo conocimiento de nuestros adversarios<sup>28</sup>.

Esta situación es debida al complejo entorno de seguridad, la naturaleza de las necesidades de los responsables, las prácticas individuales o de la organización y el éxito de las actividades técnicas de obtención, con unas capacidades actuales inimaginables hace unas décadas. El principal motivo de la falta de análisis a largo plazo es debido a que la mayoría de los consumidores de inteligencia es lo que quieren (o, por lo menos, es lo que obtienen, ya que no preguntan por análisis a largo plazo).

Un estudio reciente realizado por la Iniciativa para la Consolidación de la Paz llegó a la conclusión de que: «los esfuerzos actuales de la UE en la alerta temprana y su correspondiente respuesta se caracterizan por el corto plazo y un proceso de toma de decisiones *ad hoc*. Carecen de priorizaciones basadas en las evidencias, y un proceso de toma de decisiones de poca calidad contribuye a la formulación de políticas ineficientes»<sup>29</sup>.

Muchos estudios en estas áreas tan interrelacionadas como son inteligencia, el proceso de toma de decisiones y planificación consideran, quizás de manera muy optimista, que un mejor análisis facilitaría una mejora en el proceso de toma de decisiones, así como una mejor orientación del personal de inteligencia responsable de gestionar los sistemas de alerta temprana y producir los informes de inteligencia correspondientes.

En multitud de ocasiones hay que tomar decisiones en un ambiente de incertidumbre, por lo que será difícil discernir cuando el proceso ha sido correcto y cuando no. Pero sí resulta posible identificar bajo qué condiciones el proceso resulta más fiable o menos.

### Inteligencia en el proceso de toma de decisiones

Una de las funciones que puede llevar a cabo el personal de inteligencia es apoyar en un proceso de toma de decisiones. Es decir, ante la identificación de una posible amenaza, el personal de inteligencia elabora el correspondiente producto, basado en el análisis de toda la información disponible, en el cual alerta de una posible amenaza en un futuro próximo; dicho producto llega a su destinatario, quien podría emplearlo para tomar la decisión correspondiente.

<sup>28</sup> TREVERTON, G. F. & GABBARD, B. C., O. C., p. 4.

<sup>29</sup> MONTANARO, Lucía y SCHÜNEMANN, Julia (2011). *Walk the Talk. The EU needs an effective Early Warning system to match its ambitions to prevent conflict and promote peace*. Fride & International Alert /Initiative for Peacebuilding-Early Warning, p. 12. Disponible en <http://www.ifp-ew.eu/>.

Según lo dicho anteriormente, «se pueden identificar cuatro tareas dentro lo que se podría llamar el bucle de alerta-respuesta»<sup>30</sup>, representado en la figura 3.4, y que, como se ve, están relacionadas con un proceso de toma de decisiones en base a la información e inteligencia disponible.

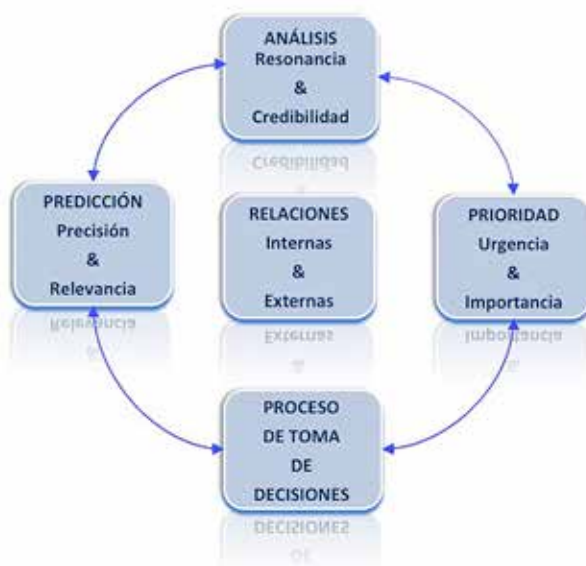


Figura 3-4. Bucle de alerta-respuesta

Todas las tareas y los actores involucrados en el bucle están interconectados y las tareas vinculadas, de tal manera que el fallo en una etapa es probable que conduzca a errores en las etapas posteriores. Por ejemplo, las predicciones inexactas que se han comunicado a los responsables, inevitablemente, afectarán a la eficacia de las decisiones que se tomen y, por supuesto, a la política preventiva que se esté llevando a cabo.

A la inversa, los responsables pueden influir negativamente en la capacidad de los analistas para producir inteligencia, si no les informan lo suficiente acerca de la información que necesitan y cuándo. Por lo tanto, sería engañoso centrarse solo en la etapa de toma de decisiones, con el fin de determinar si el proceso es de calidad y cómo afecta al comportamiento de una hipotética política preventiva que se quisiera llevar a cabo.

<sup>30</sup> Versión basada en la de DE FRANCO, Chiara y MEYER, Cristoph O. (2011). *Forecasting, Warning, and Responding to Transnational Risks*. Basingstoke: Palgrave Macmillan, p 7. Disponible en <http://www.palgraveconnect.com/pc/doi/finder/10.1057/9780230316911>. Fecha de la consulta 21/12/2015.

Al mismo tiempo, también los actores involucrados en el proceso de alerta-respuesta están unidos entre sí, a través de la evolución de sus relaciones según pasa el tiempo. Tanto los analistas de inteligencia como sus clientes desarrollan una historia compartida, ya que interactúan y se comunican, lo que significa que las experiencias de los distintos actores entre sí fomentan el establecimiento de reputaciones y patrones de comportamiento. Esto, a su vez, puede crear, tanto incentivos como desincentivos para una comunicación efectiva y de confianza a lo largo del tiempo.

Los analistas dentro de las burocracias suelen ser muy receptivos a lo que ellos perciben como las agendas políticas, así como a las preferencias de sus clientes, y consideran las implicaciones que sus productos pueden suponer para la política de la organización, así como para el éxito o fracaso de sus carreras.

Por el contrario, los clientes no confían simple y directamente en los productos de inteligencia que reciben, sino que revisan las conclusiones o hipótesis en ellos reflejadas, de acuerdo con las informaciones que reciben de sus propias fuentes y las comparan con sus propias visiones del asunto en cuestión. Además, sobre todo cuando hablamos de altos cargos políticos, consideran muy a menudo la utilidad política de los conocimientos de los analistas como limitada, para evitar la culpa en caso de fracaso, y reclamar el reconocimiento por el éxito.

### *Inteligencia de alertas y su relación con la toma de decisiones*

Cynthia Grabo, una veterana analista de la Agencia de Defensa de Norteamérica (DIA), define alerta como «un intangible, una teoría, una deducción, una percepción, una creencia. Es el resultado del razonamiento o de la lógica, una hipótesis cuya validez no puede ser ni refutada ni confirmada hasta que es demasiado tarde»<sup>31</sup>.

La sorpresa es una característica de cualquier conflicto. La ventaja competitiva que proporciona el confundir a un adversario sobre las verdaderas intenciones y capacidades propias, supone un poderoso incentivo para engañar al enemigo en cualquier lugar y momento. Como se ha dicho, esto por sí solo explica la necesidad de la inteligencia como una disciplina y una profesión. Sin embargo, el ignorar o malinterpretar los indicadores de las intenciones de un adversario puede tener consecuencias nefastas, como se ha demostrado a lo largo de la historia.

La historia militar revela que en pocas ocasiones la sorpresa fue total; siempre hubo señales que, en caso de haber sido correctamente interpretadas,

---

<sup>31</sup> GRABO, Cynthia M. (2002). *Anticipating Surprise*. Analysis for Strategic Warning: Washington DC, Joint Military College, p. 4. Disponible en [http://www.ni-u.edu/ni\\_press/pdf/Anticipating\\_Surprise\\_Analysis.pdf](http://www.ni-u.edu/ni_press/pdf/Anticipating_Surprise_Analysis.pdf).

hubieran apoyado otro tipo de decisiones o, por lo menos, se habría conseguido mitigar las consecuencias. En muchas ocasiones, la sorpresa fue favorecida debido a una falta de voluntad de abandonar las ideas preconcebidas y las decisiones adoptadas, a pesar de las señales identificadas sobre el terreno que las contradecían.

Hoy en día, la metodología de indicadores y alertas, con su origen militar, es una técnica bien asentada en ese campo, pero que, además, se muestra de gran utilidad para hacer frente a otro tipo de amenazas, como puede ser el crimen organizado, el terrorismo o incluso en el ámbito empresarial para identificar los planes de nuestros competidores.

La idea central que subyace detrás del análisis de indicadores y alertas es que los acontecimientos y fenómenos raramente ocurren en el vacío; afectan y son afectados por fuerzas y condiciones del entorno, algunos de los cuales son observables. Una correcta interpretación de los indicios en su contexto alerta sobre una posible amenaza emergente o futura. Con el apoyo de un análisis de indicadores y alertas, se puede facilitar un proceso de toma de decisiones que permita identificar y llevar a cabo las acciones apropiadas, para tratar con las amenazas y riesgos antes de que sean inmanejables.

Cuando hablamos de indicadores y alertas es importante no confundirlos con hechos o informaciones. En el caso de que un enemigo esté movilizándolo sus fuerzas armadas, esto es una información; cuando llegamos a la conclusión, basado en esta información y otros indicios, de que el enemigo se está preparando para atacar, esto es una alerta.

En resumen, una alerta es el resultado de un análisis de inteligencia sobre una amenaza o riesgo, en relación con un adversario en particular o un escenario. Pero no solo lo anterior, sino que también permite la identificación de oportunidades y su explotación, mediante la ejecución de las acciones que correspondan.

Hay que distinguir la inteligencia de alertas de los otros tipos de inteligencia, por su alcance y campo de aplicación, clientes y función que desempeña. En relación con el alcance, como se observa en la figura 3-5, la inteligencia de alertas está enfocada en el futuro. Por el contrario, la inteligencia básica y actual están enfocadas en describir realidades pasadas y presentes.

La inteligencia de alertas es especulativa, ya que trata de identificar una oportunidad o amenaza futura, por lo que cae dentro del campo de la inteligencia estimativa y predictiva, pero con diferencias. Mientras la inteligencia estimativa y predictiva miran hacia el futuro con un foco muy amplio para tratar de prever las posibles amenazas en sentido amplio, la inteligencia de alertas está focalizada en dar respuesta a una amenaza concreta. Esto último hace que la inteligencia de alertas sea muy indicada para apoyar a los responsables de tomar decisiones.

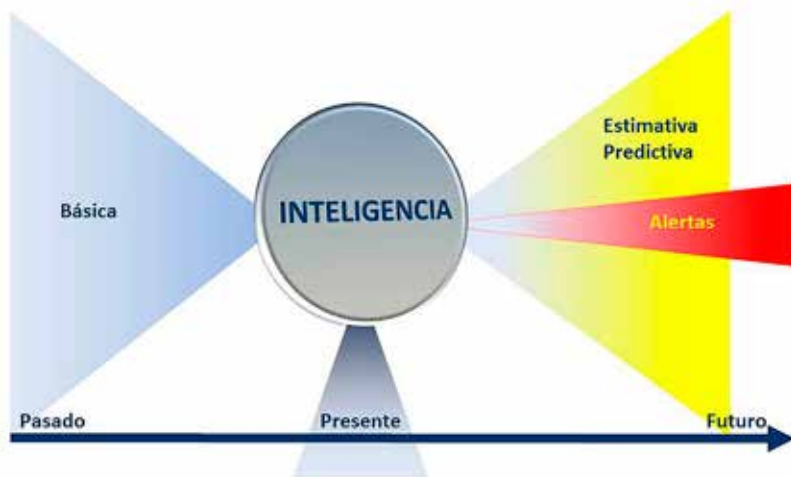


Figura 3-5. Tipos de Inteligencia según el objetivo y el foco. Elaboración propia

### *Factores que influyen en la inteligencia de alertas*

La alerta temprana se basa en una buena predicción de la probabilidad y severidad de que un conflicto, una crisis latente, o una amenaza, se materialicen. Como se ha dicho anteriormente, la predicción de conflictos, por ejemplo, puede llevarse a cabo con un sistema de indicadores de alerta que proporciona resultados cuantitativos o, por otro lado, por un sistema más cualitativo, basado en predicciones de expertos sobre las dinámicas del conflicto. En la mayoría de las organizaciones estatales e internacionales, el último suele ser el enfoque predominante.

Los expertos pueden ser analistas de inteligencia, diplomáticos en las embajadas, representantes especiales, personal militar en misiones, periodistas y ONG. Independientemente del método que se esté utilizando y qué tipos de expertos estén involucrados, la previsión para los propósitos preventivos presenta grandes retos en relación con la precisión y la relevancia.

La precisión es el grado en que una predicción es correcta a la hora de describir los posibles escenarios, sus causas, consecuencias y el momento en que se producirán. La precisión en relación con una predicción solo puede medirse a posteriori, a pesar de que, a priori, podemos medir la confianza de los expertos en la cantidad y calidad de las evidencias disponibles, junto con la fiabilidad en el pasado de las teorías o modelos aplicables, para dar sentido a esas pruebas.

«El problema es que los nuevos riesgos son más difíciles de pronosticar con precisión, ya que las teorías podrían no haber sido probadas previamente y pudieran no ser aplicables. El desafío analítico para los analistas es saber



cuándo los acontecimientos del pasado pueden ser extrapolados hacia el futuro y cuándo deberían reemplazarles escenarios de pesadilla»<sup>32</sup>.

En relación con la precisión de una predicción surgen varios problemas:

- Ciertas amenazas, países o regiones están «fuera del radar» de los analistas, ya que los recursos están excesivamente concentrados en unos pocos asuntos de interés. Esto provoca una escasez de información detallada, con suficiente antelación, acerca de los eventos que podrían provocar la materialización de una amenaza.
- Ciertos tipos de amenazas y riesgos son más difíciles de predecir que otros.
- En muchas ocasiones, la información relevante para la predicción no es compartida entre los analistas, que trabajan en diferentes áreas de la organización de inteligencia.
- Los analistas pueden carecer del conocimiento suficiente del asunto objeto de análisis, así como de la formación necesaria para comprender el sentido de los datos. Además, podrían verse influenciados por sesgos de distinto tipo.

La relevancia se refiere, tanto a la utilidad de las informaciones incluidas en la alerta, con respecto al proceso de toma de decisiones encaminadas a la prevención, como en la medida en que se refiere a las cuestiones y áreas consideradas prioritarias por los receptores del producto. Ciertas predicciones pueden carecer de relevancia para los tomadores de decisiones, ya sea porque dejan de lado los riesgos considerados importantes o porque son demasiado vagas en la evaluación de lo que va a pasar, cuándo, cómo y con qué probabilidad.

La relevancia normalmente aumenta con la especificidad de las predicciones, pero no implica necesariamente que tengan que ir emparejadas con recomendaciones. Decir simplemente que el país «X» puede volverse inestable, sin decir más sobre cuestiones de probabilidad, cuándo y las consecuencias derivadas del mismo, no es muy útil para los planificadores de políticas y los que tiene que tomar las decisiones, los cuales están siempre contemplando cuándo y cómo actuar.

El problema es que, en muchas ocasiones, la realidad de la predicción no es siempre compatible con las necesidades de los que tiene que decidir. La buena predicción de los acontecimientos socio-políticos es, por su naturaleza, vaga e incierta, mientras que a los tomadores de decisiones les gustaría tener no solo evaluaciones fiables, si no también muy precisas y concretas de cuándo es probable que las cosas sucedan, cómo y con qué tipo de consecuencias: «En muchos casos, existe un conflicto entre lo que la inteligencia,

---

<sup>32</sup> BETTS, Richard K. (2007). *Enemies of Intelligence: Knowledge & Power in American National Security*. New York: Columbia University Press, p. 56.

en su mejor momento, puede producir y lo que los tomadores de decisiones buscan y necesitan»<sup>33</sup>.

En relación con la relevancia, los principales problemas son:

- Insuficiente intercambio de criterios de relevancia entre los productores de alertas y sus clientes, en parte por la preocupación de preservar la objetividad de los analistas.
- Conocimiento inadecuado de los instrumentos a disposición de los clientes.
- Presión sobre los analistas para reducir al mínimo el margen de error, lo que aumenta los incentivos para las predicciones vagas o que no impliquen acciones concretas.

Una vez que se ha elaborado una predicción y se monitorizan los indicadores correspondientes, para confirmar o denegar su cumplimiento, el siguiente paso consiste en la comunicación de un determinado riesgo a los que tienen la capacidad de actuar sobre él. Por lo general, es el aspecto más descuidado en el análisis *post mortem*, ya que los investigadores buscan señales de peligro, pero no investigan si estos signos fueron traducidos en actos comunicativos intencionados de alerta. Además, si estas advertencias llegaron en realidad al destinatario y fueron entendidas como tal, nunca es examinado<sup>34</sup>.

Este aspecto es clave cuando tratamos con alertas: la comunicación de la alerta por parte del analista a su cliente. De tal manera, que el producto resultante del análisis solo llega a convertirse en alerta cuando llega a los destinatarios y es comprendido por estos. Como señala Grabo «una alerta que solo existe en la mente del analista es inútil».<sup>35</sup>

Así como detectar discontinuidades requiere audacia analítica, comunicarlás requiere un cierto grado de valentía. Un exagente de Inteligencia Nacional de Estados Unidos avisó a su personal: «usted tiene que estar acostumbrado a ser el chico más tonto en la habitación»<sup>36</sup>. Lo que tenía en mente era que sus subordinados no eran los únicos que pensaban en el futuro, sus clientes también lo hacen, y con gran confianza en su criterio.

<sup>33</sup> JERVIS, Robert (2010). *Why Intelligence Fails: Lessons from the Iranian Revolution and the Iraq War*. Ithaca and London: Cornell University Press.

<sup>34</sup> MEYER, Christoph O., OTTO, Florian, BRANTE, DE FRANCO, Chiara. (2010). *Re-Casting the Warning-Response-Problem: Persuasion and Preventive Policy*. *International Studies Review*, vol. 12, nº. 4, pp. 556-578. Disponible en <http://onlinelibrary.wiley.com/doi/10.1111/j.1468-2486.2010.00960.x/abstract> . Fecha de la consulta 11/12/2015.

<sup>35</sup> GRABO, Cynthia M., O. C., p. 14.

<sup>36</sup> ERDMANN, Drew, y MENDONCA, Lenny (2009). *Focused on foresight: An Interview with the US national intelligence officer for warning*. *McKinsey Quarterly*. Disponible en [http://www.mckinsey.com/insights/public\\_sector/focused\\_on\\_foresight\\_an\\_interview\\_with\\_the\\_uss\\_national\\_intelligence\\_officer\\_for\\_warning](http://www.mckinsey.com/insights/public_sector/focused_on_foresight_an_interview_with_the_uss_national_intelligence_officer_for_warning) . Fecha de la consulta 11/12/2015.

Como el estallido de una guerra en general presenta discontinuidades para establecer patrones, alertar es, en muchas ocasiones, un proceso de desafiar las asunciones preestablecidas de los clientes y, en consecuencia, se corre el riesgo de ser visto «fuera de onda». El desafío es convencer a este último de que la advertencia debe ser tomada como creíble y que merece mayor atención.

Cuenta Grabo en su libro que «un experimentado oficial de inteligencia en el campo del análisis político, señaló hace muchos años que, no importa lo que haya salido mal, siempre la culpa es de inteligencia. Cuando ocurrió el desastre, el analista podría recordar al responsable que había advertido de la posibilidad o que se había mencionado que esto podría suceder, en varias reuniones en el último mes. Y él respondió: bueno, no lo dijo con bastante frecuencia o lo suficientemente alto»<sup>37</sup>.

A la hora de comunicar una alerta, es muy importante el mensaje de resonancia, y que es cuando la alerta es adaptada, de tal manera que persuade al cliente para que acepte el análisis y la interpretación de las pruebas o evidencias. Las alertas sobre amenazas inminentes, se tienen más en cuenta cuando ponen de manifiesto las consecuencias que al destinatario le importan, en lugar de aquellas que solo el analista de inteligencia considera más importantes.

Tienen también más probabilidades de tener impacto cuando incluyen pruebas que el destinatario considera más creíbles y traduce el análisis en un lenguaje que es comprensible. Por lo tanto, los analistas necesitan no solo habilidades comunicativas, si no también saber cómo procesan la información los que toman las decisiones, aprender cuáles son sus visiones del mundo y asunciones acerca de ciertos asuntos y, sobre todo, para qué cuestiones exigen mayor carga probatoria.

A la hora de comunicar una alerta, los principales problemas con los que nos podemos encontrar, y que podrían impedir que el análisis sea tenido en cuenta son:

- Las alertas pueden no ser inteligibles, ya que los analistas no están especializados en la comunicación, o no conocen lo suficiente a su cliente como para adaptar el mensaje.
- Los cuellos de botella burocráticos pueden impedir una comunicación rápida y directa.
- Pueden existir desincentivos organizativos o sesgos institucionales, que impiden que se comuniquen puntos de vista que desafíen las políticas prevalecientes en la organización.
- Discordancia entre las conclusiones del análisis y la mentalidad e inclinaciones del receptor del mismo.

---

<sup>37</sup> GRABO, Cynthia M., O. C., p. 15.

Un factor clave es la fiabilidad de la fuente, al que se sumaría la credibilidad de la información, ya que, para el cliente, el analista de inteligencia es una más de las muchas fuentes a las que puede tener acceso. Normalmente, los responsables de tomar decisiones pueden carecer del tiempo, o de la capacidad, para juzgar la credibilidad de las pruebas, pero es que, además, tienden a tener cuidado para evitar ser manipulado por razones políticas.

La forma convencional por la cual las fuentes adquieren fiabilidad es a través de los títulos académicos correspondientes y/o la experiencia sobre el país/región o asunto en cuestión, así como a través de una exitosa trayectoria profesional.

Sin embargo, la evaluación de la fiabilidad de la fuente también será una función del que toma las decisiones, ya que la evaluará como neutral, amistosa u opuesta a sus creencias e ideas. Ser visto como neutral no es el único camino hacia la credibilidad, ya que los mensajes inconvenientes también pueden ser persuasivos, cuando los destinatarios sepan los puntos de vista políticos de la fuente y por lo tanto pueden compensar los sesgos en el contenido del mensaje.

El analista de inteligencia, en muchas ocasiones, tendrá que competir, para tratar de ganar mayor fiabilidad, con otras personas de confianza del cliente, y que por su cercanía, mayor relación y acceso más directo, ejercen una gran influencia sobre él a la hora de tomar decisiones. Cuanto más fiable sea considerado un analista, de mayor credibilidad gozarán sus productos.

En ocasiones, la fiabilidad de la fuente depende de la casualidad; el que se la tenga en cuenta dependerá de las personas de confianza, con el conocimiento suficiente y puntos de vista compatibles, que se encuentran entre el productor del análisis y el cliente, en lugar de basarse en procesos robustos, conocimiento institucional y criterios racionales para juzgar la fiabilidad de la fuente y la credibilidad de la información.

La separación existente entre el analista de inteligencia y el responsable de tomar decisiones, hace que el primero no tenga claro las prioridades del segundo. Hoy en día, en el complejo mundo globalizado en que vivimos, donde los recursos siempre serán insuficientes para detectar la materialización de cualquier amenaza, es necesario que el personal de inteligencia tenga claras cuáles son las prioridades de su cliente.

Ante la detección de la posible materialización de una amenaza y la elaboración de la correspondiente alerta, para apoyar un proceso de toma de decisiones, sería conveniente que esta refleje no solo las consecuencias, sino la importancia de la misma en relación tanto a los intereses de la organización como a otros asuntos que pueden competir por la atención y los mismos recursos.

En el proceso de toma de decisiones la urgencia es clave, ya que el saber cuándo se materializará una amenaza y las consecuencias asociadas, es de-

cisivo a la hora de tomar una decisión u otra. El problema es que, en muchas ocasiones, las alertas son muy vagas en relación a un posible calendario, lo que provoca el descrédito del producto analítico, a lo que se suma la pérdida de fiabilidad del analista.

A la hora de anticipar futuras amenazas, todos los analistas se enfrentan a los mismos desafíos epistemológicos, a la incertidumbre y complejidad de pensar sobre el futuro político, social, militar y del comportamiento humano, que no depende de la organización para la que trabajan, y que podríamos resumir en los siguientes puntos:

- La falta de experiencia de los analistas: en muchas organizaciones, el problema es que no han tenido durante mucho tiempo el análisis de inteligencia como prioridad; por lo tanto, el rendimiento real fue muy dependiente de tener individuos con la capacidad personal y poder de iniciativa para llevar a cabo el análisis.
- Falta de unidades que realicen análisis predictivo: lo que dificulta, por no decir que impide, la identificación de amenazas y riesgos a largo plazo. La inteligencia actual, la del día a día, consume todos los recursos.
- Esfuerzos limitados para realizar un análisis alternativo: es necesario que los analistas y sus clientes, revisen sus asunciones y supuestos, y desarrollen hipótesis alternativas sobre las amenazas y riesgos futuros. La aplicación de técnicas de análisis estructuradas facilitaría y mejoraría la calidad de los productos analíticos.

En el campo de la inteligencia de alertas, uno de los principales problemas es la comunicación de esa alerta al cliente y su comprensión, sobre todo en las primeras fases, cuando las señales sobre una posible amenaza o riesgo futuro son débiles y la incertidumbre muy alta. Algunos factores inherentes, y que afectan en la inteligencia de alertas, son:

- Esquemas mentales: un modo de pensar se puede definir como «el modelo mental de una persona o paradigma de cómo los grupos actúan en un país “X” o en relación a un asunto “Y”; se basa en el conocimiento acumulado de los precedentes anteriores, los actores clave, y los procesos de toma de decisiones»<sup>38</sup>.
- Intereses divergentes: en comparación con otras formas de inteligencia, la de alertas tiene un gran vínculo con la acción, de tal manera que casi siempre interferirá con las políticas actuales o previstas. Cuando una alerta es vista como una oportunidad, por ejemplo, por dirigir hacia una situación deseada, tiene más probabilidad de influir y ser atendida, e influir en la manera de pensar de los clientes, y por supuesto en las po-

<sup>38</sup> DAVIS, Jack (2008). «Why Bad Things Happen to Good Analysts». En: GEORGE, Roger Z. y BRUCE, James B. (eds.), *Analysing Intelligence: Origins, Obstacles and Innovations*. Washington D.C.: Georgetown University Press, p. 160.

sibles decisiones a tomar. Cuando no es el caso, se tiende a realizar una interpretación distorsionada y prestar una atención selectiva.

- Diferentes preferencias sobre las fuentes: un factor clave para determinar el impacto de una alerta es, obviamente, la credibilidad de la información que le da el analista. Sin embargo, los clientes de Inteligencia se apoyan en diferentes fuentes, por lo que, si los analistas tienen un bajo prestigio ante estos, el éxito de sus productos dependerá en la medida en que digan lo mismo que la información proporcionada por la fuente más fiable para su cliente.
- Cultura de alertas negativa: la falta de incentivos para llevar a cabo una correcta alerta temprana, provoca unos efectos secundarios, de tal manera que a los mensajes de alerta se les da un formato muy general. Los clientes no reciben la alerta en su formato original, ya que los analistas tienen la tendencia a esperar a que sus análisis se demuestren más fiables, basados en los acontecimientos, de tal manera que se aseguren que serán tenidos en cuenta. Si esto no es posible y a los analistas se les pide un análisis inmediato, optan por proporcionar uno que no se oponga a ninguna de las inclinaciones cognitivas o visiones de sus clientes.

### *Mejoras del análisis de inteligencia en apoyo a la toma de decisiones*

¿Qué se puede hacer para superar estos obstáculos y mejorar el análisis de inteligencia en apoyo de los procesos de toma de decisiones?

La respuesta común a los fallos en el análisis, en la mayoría de las organizaciones, ha sido llevar a cabo reformas organizativas. A menudo, las investigaciones *post mortem* han proporcionado referencias sobre cómo racionalizar las comunidades de inteligencia, mejorar la cooperación entre agencias, y centralizar la responsabilidad. La historia de la comunidad de inteligencia de los EE.UU. ofrece numerosos ejemplos de esto desde Pearl Harbor al 11-S. Sin embargo, la lección recurrente de estos ejemplos, es que los fracasos de las alertas, en apoyo al proceso de toma de decisiones, siguen ocurriendo a pesar de las reformas.

Es decir, los obstáculos para el éxito no dependen de la estructura, sino más bien de la naturaleza de la inteligencia estimativa y predictiva y la influencia que la psicología y la política tienen sobre la elaboración y comunicación de los análisis de inteligencia.

*Más información no significa un mayor impacto*, dada la incertidumbre inherente y la complejidad del análisis predictivo y estimativo. Inevitablemente, se producirán análisis erróneos, ya que no hay una manera a priori de asegurar el éxito analítico, de tal forma que un análisis correcto tiene las mismas probabilidades de ser tenido en cuenta que uno incorrecto. Como se dijo anteriormente, aquí juega un papel importante la credibilidad que le dé el cliente al producto. El principal problema es que los análisis incorrectos

tiene un mayor impacto y se recuerdan más tiempo, debido a que, normalmente, llevan asociadas consecuencias negativas, de tal manera que pueden tirar por tierra la credibilidad de un analista durante años.

Otro aspecto importante, es la necesidad de reconocer que las alertas no son solo acerca de la precisión, también implican la comprensión del problema de los que toman las decisiones y cómo procesan la información; conocer su modo de pensar y lo que ellos perciben como riesgos.

Por otra parte, se necesita tener identificadas sus inclinaciones e ideas sobre el asunto en cuestión y sus limitaciones, así como –si es posible– lo que se les dice por otras fuentes de su confianza.

Un conocimiento más profundo de las predisposiciones del cliente puede obtenerse a través de:

- El uso de técnicas de análisis estructurados: en los últimos años, con el fin de mejorar el análisis, académicos y profesionales de inteligencia han desarrollado un gran número de técnicas, que los analistas pueden utilizar para revisar su propio pensamiento y supuestos. Algunos de estos métodos (por ejemplo, «Red Hat Analysis» y «Key Assumptions Check») pueden ser modificados y utilizados para estructurar las discusiones sobre las predisposiciones de los clientes. Si estas discusiones se llevan a cabo de forma regular, el personal de inteligencia podría tener un mejor conocimiento de los obstáculos a los que se enfrentan sus productos<sup>39</sup>.
- Promover el intercambio de personal: dejar que los analistas de inteligencia trabajen en el área de planeamiento y viceversa, durante breves periodos de tiempo, así como el asignar un analista a la organización del cliente de una manera más permanente.
- Observación de las reuniones: incluso si no está prevista su participación activa, la asistencia de los analistas a las reuniones donde se toman las decisiones es útil, al poder observar los diferentes puntos de vista.
- Preguntar a los clientes: si la retroalimentación no es proporcionada por el cliente, es importante que los analistas busquen activamente explicaciones de por qué no se aceptan o priorizan sus productos.
- Análisis *post mortem*: la mayor parte de estos ejercicios se centran en cómo se llevó a cabo el análisis. La ampliación a la evaluación explícita del impacto de los productos es muy deseable, y podría determinar cuándo y cómo los productos de inteligencia fracasan o tienen éxito.

Sin cambiar el sentido de las conclusiones del análisis, los analistas deberían ser capaces de adaptar y personalizar el producto a su receptor concreto. Para ello se debería:

---

<sup>39</sup> HEUER Jr., RICHARDS J. y PHERSON, Randolph H. (2011). *Structured Analytic Techniques for Intelligence Analysis*. Washington D. C.: CQ Press, pp. 183-188, 197-200.

- Reforzar y comprobar los supuestos: al elaborar un producto, los analistas deberían tratar de reforzar los supuestos que se consideran correctos, proporcionando las evidencias correspondientes que los apoyen, pero, lo más importante, sería indicar las debilidades del análisis, señalando aquellos hechos que lo refuten. La idea es tratar de influir de manera proactiva, anticipándose a los pensamientos del cliente, para tratar de derribar las barreras a la receptividad por parte del mismo.
- Mostrar asuntos relacionados: si los analistas saben cuáles son los asuntos que el cliente percibe como más importante y urgentes, se puede aumentar el impacto del producto resaltando las relaciones con dichos asuntos. En el complejo mundo actual, raramente se produce un fenómeno aislado, ya que, por ejemplo, una situación de guerra en un país, provoca una oleada de inmigrantes hacia los países vecinos, con la consiguiente influencia en la seguridad.
- Considerar el nivel al que se dirige el producto: no es lo mismo que un producto de inteligencia se dirija al nivel táctico que al nivel estratégico. Las necesidades de inteligencia difieren según el nivel de mando. Por otra parte, también puede ser útil advertir inicialmente a los niveles más bajos en la burocracia, y de esta manera irlos sensibilizando del posible daño, aunque la certeza sobre la predicción en esta etapa sea baja.
- Considerar el nivel de impacto deseado: por último, es importante tener en cuenta qué nivel de impacto se está tratando de lograr. Por ejemplo, si la aspiración es que el cliente tenga en cuenta el producto, un mensaje bastante claro y simple puede atraer su atención y hacer resaltar el producto entre otros muchos. Es recomendable que el analista compare el resultado de su análisis y sus implicaciones con otras amenazas potenciales, y lleve a cabo analogías con incidentes previos similares, de tal manera que pueda mostrar de manera comparativa su importancia al cliente y la necesidad de que se le dé prioridad.

Es útil pensar sobre la forma de aproximarse a las predisposiciones y adelantarse a las diferentes formas de ver el mundo de los analistas y sus clientes, de tal manera que se podría:

- Organizar seminarios conjuntos para discutir temas de análisis: esto permitiría la discusión de las suposiciones en vigor y los diferentes puntos de vista, identificando las divergencias. Esto facilita la comprensión mutua y la identificación de sesgos en la manera de pensar. Las técnicas de análisis estructuradas podrían ser empleadas con este fin.
- Manuales para los clientes: los efectos a largo plazo de las predisposiciones pueden ser mitigados simplemente explicando su influencia a los destinatarios. En los EE.UU., se utilizan mucho, pero su contenido es más bien superficial, ya que la mayoría solo hablan del ciclo de inteligencia, las estructuras de inteligencia y los tipos de producto, dejando de lado otros aspectos clave, como la influencia de los sesgos y prejuicios, no solo en el analista, sino en el cliente cuando recibe el producto.



El debate que existe entre los profesionales y estudiosos de la inteligencia sobre cómo mejorar los productos de inteligencia, para que apoyen un proceso de toma de decisiones y faciliten la identificación de las acciones a llevar a cabo, identifica una serie de prácticas que deberían materializarse:

- Normas comunes para expresar probabilidad: el padre de la inteligencia estadounidense, Sherman Kent, subrayó que los consumidores pueden entender las expresiones de probabilidad de manera muy diferente<sup>40</sup>, por lo que es recomendable el establecimiento de un lenguaje común a la hora de indicar la probabilidad de ocurrencia de un hecho, para evitar malas interpretaciones entre los distintos receptores de un producto.
- Papel activo posterior a la difusión: en caso de que el producto no haya sido tenido en cuenta, el analista debe tratar de repetirlo, pero desde un ángulo diferente. Si los productos son tenidos en cuenta, los analistas pueden contribuir a la planificación y elaboración de las distintas posibilidades de respuesta. Hay técnicas diseñadas para apoyar los procesos de toma de decisiones como el DAFO<sup>41</sup> o el análisis de fuerzas sobre el terreno.

### Influencia de los medios de comunicación

En un entorno dominado por los grandes avances tecnológicos, y que permiten a cualquier persona acceso, prácticamente ilimitado, a cualquier tipo de información desde cualquier lugar del mundo, el analista de inteligencia ha perdido la primacía a la hora de proporcionar información e inteligencia a sus clientes.

Los consumidores de inteligencia no son ajenos a estos avances, y presionados por una opinión pública, cada vez más exigente debido a la información que tiene disponible, se ven obligados a reducir sus ciclos de toma de decisiones, a lo que se une una predisposición natural a realizar sus propias búsquedas de información, y sus propios análisis.

Cuando un cliente recibe hoy en día un producto de inteligencia, en muchas ocasiones con vaguedades e incertidumbres de difícil comprobación, se hace preguntas: ¿Cómo se han llegado a las conclusiones que se muestran? ¿Qué probabilidad hay de que dichas conclusiones sean correctas? ¿Hay que tomar alguna decisión basada en este producto de inteligencia? ¿Cuáles serían

<sup>40</sup> KENT, Sherman (1964). «Words of Estimative Probability» en STEURY, Donald P., ed., (1994), *Sherman Kent and the Board of National Estimates: Collected Essays*. Washington D. C.: Center for the Study of Intelligence, Central Intelligence Agency.

<sup>41</sup> La técnica de análisis DAFO es muy utilizada en todos los ámbitos, por su sencillez, para analizar países, empresas, organizaciones, competidores o adversarios. Las siglas se corresponden en castellano con las palabras: debilidades, amenazas, fortalezas y oportunidades. En inglés, la podemos encontrar denominada como SWOT (strengths, weaknesses, opportunities y threats).

las consecuencias si las conclusiones fueran correctas? ¿Y si no lo fueran? ¿Son mejores las conclusiones del documento que a las que hubiera llegado yo solo?

Si las respuesta que obtiene no le satisfacen, «buscará la información que necesita en cualquier lugar, ya sea en empresas que proporcionan servicios de inteligencia o en los medios de comunicación, tanto los clásicos como los que hoy en día actúan en Internet, los cuales, en la gran mayoría de las ocasiones, pueden proporcionar las respuestas que busca y de una manera más rápida, lo que conlleva la pérdida de relevancia del personal de inteligencia ante su cliente»<sup>42</sup>.

Estas cuestiones son de gran preocupación para el personal de inteligencia, ya que entre otras funciones esta la de apoyar un proceso de toma de decisiones de calidad. La desconfianza del cliente en los productos de inteligencia que recibe, provoca que estos se vuelvan irrelevantes en la mayoría de las ocasiones.

Un actor clave, y que puede alterar o distorsionar el papel de inteligencia en los procesos de toma de decisiones, son los medios de comunicación. Su papel en muchas ocasiones es clave a la hora de alertar y mantener el foco sobre un determinado conflicto o situación de crisis. No hay ningún otro actor no gubernamental que los iguale a la hora de llegar a cualquier tipo de destinatario, ya sea un empresario, un trabajador o un alto cargo político del Estado.

La influencia que pueden ejercer en el discurso político es determinante a la hora de que un Gobierno priorice un asunto sobre otro, ya que tienen la capacidad de determinar cuánto tiempo ese asunto permanecerá expuesto a la opinión pública. Sin embargo, en muchas ocasiones, son criticados por no prestar la suficiente atención a problemas latentes que pueden convertirse en un riesgo, a lo que se une que sus ciclos de atención son, a menudo, erráticos.

A pesar de todas las críticas que reciben, es indudable que hay que tener en cuenta la influencia que los medios de comunicación pueden ejercer en los procesos de toma de decisiones, como se ha visto en diversas ocasiones en el pasado y la competencia que, en muchas ocasiones, mantienen con las estructuras de inteligencia.

Con Internet se ha producido una explosión mediática sin precedentes. Si alguna vez hubo algo así como una única versión de una noticia, hoy en día, los responsables de tomar decisiones se enfrentan a una multitud, a menudo

---

<sup>42</sup> SYMON, Paul B. y TARAPORE, Arzan. *Defense Intelligence Analysis in the Age of Big Data*. Joint Force Quarterly (JFQ) 79, 4th Quarter 2015. Disponible en <http://ndupress.ndu.edu/Media/News/NewsArticleView/tabid/7849/Article/621113/defense-intelligence-analysis-in-the-age-of-big-data.aspx> . Fecha de la consulta 10/12/2015.

confusa, de versiones, especialmente cuando se refiere a una posible crisis o amenaza futura.

### *El papel de los medios de comunicación*

El papel de los medios de comunicación en los procesos de toma de decisiones se puede dividir en cuatro funciones diferentes:

- o Informante.
- o Amplificación.
- o Defensa.
- o Advertencia.

Los últimos años han visto una proliferación sin precedentes de noticias basadas en la web, así como la disponibilidad de información de primera mano que puede ser directamente observada por medio de las redes sociales. Sin embargo, todavía es pronto para afirmar que los medios de comunicación tradicionales han perdido su papel crucial en informar al público, funcionarios y responsables políticos, a pesar de los cambios en el panorama de los medios.

Aunque las nuevas fuentes de información pueden ser más rápidas en la difusión de una noticia, a menudo carecen de la credibilidad de los medios de noticias establecidos, y luchan por que se les tenga en cuenta y se les tome en serio. El problema es que, salvo excepciones, este tipo de fuentes apenas ofrecen el tipo de análisis en profundidad que proporcionan los medios profesionales, en particular la prensa escrita de calidad. Este tipo específico de cobertura de noticias representa un recurso importante de la inteligencia de fuentes abiertas (OSINT). Si la cobertura de una noticia por estas fuentes se produce en las hipotéticas primeras etapas de una crisis, puede servir a los encargados de tomar decisiones como alerta, ya que pondrían de relieve acontecimientos potencialmente dañinos que se avecinan en el horizonte.

La cobertura de los medios de comunicación de los conflictos inminentes puede crear, además, un entorno informativo favorable tanto a la comunicación como a la recepción de alertas dadas por otras fuentes. Si un conflicto latente, o su posible escalada, se convierte en una noticia, su relevancia se eleva, lo que facilita la receptividad de los productos de inteligencia. Aunque los medios de comunicación no informan específicamente sobre alertas, la aparición de una noticia puede tener el impacto de poner un país, una región o un asunto bajo interés por los responsables de tomar las decisiones.

En muchas ocasiones, los medios de comunicación son utilizados por otros actores, como las ONG para difundir su mensaje a una audiencia interesada, a pesar de que muchas organizaciones de este tipo tienen sus propios canales de comunicación. Es decir, se busca la amplificación del mensaje.

Esta diversificación y uso de los medios para dar a conocer su mensaje es importante, ya que:

- Desde el punto de vista de la comunicación, la información no es solo difundida por una fuente, sino que supone una diversificación de los canales de comunicación, lo que incrementa la probabilidad de que el mensaje llegue a quien tiene que llegar.
- Lo más importante es que los medios de comunicación tienen un alcance mayor que la mayoría de las fuentes no gubernamentales. Además, de esta manera, sortean el escepticismo que tienen muchos responsables políticos hacia algunas organizaciones no gubernamentales, al poner en duda su neutralidad y objetividad. Si una información es publicada por un medio de comunicación de calidad, es más fácil que los responsables confíen en la información y se la tomen en serio.
- Por último, los periodistas a veces observan directamente el estallido de una crisis o conflicto, y pueden convertirse en una fuente fiable al proporcionar información de primera mano y su propia evaluación de como considera que la situación podría evolucionar.

### *Problemas y obstáculos*

Desde una perspectiva en la cual una información de los medios sea tenida en cuenta, en un proceso de toma de decisiones, en detrimento de un producto de inteligencia, el principal problema identificado es la falta de fiabilidad, así como lo imprevisible y errática que es, en muchas ocasiones, la cobertura de un determinado asunto.

Hay un aspecto que merece la pena destacar y es la contraposición de la noticia como negocio a la responsabilidad de informar, ya que, como la mayoría de los medios de comunicación son negocios que necesitan obtener beneficios, concentran sus recursos en las áreas donde creen que el interés de la audiencia será grande. Esto nos conduce al asunto de la responsabilidad de los medios de comunicación con la sociedad.

En muchas ocasiones la prensa declara llevar a cabo una tarea de supervisión, apoyada por privilegios legales, de tal manera que la sociedad espera que cumpla con ese papel, estando dispuesta a proporcionarle un estatus especial para que pueda cumplir con esta tarea. Sin embargo, si la noticia se escoge por cuestiones de negocio o audiencia se sale fuera del papel que supuestamente dicen representar.

Es indudable, en base a todo lo anterior, la gran influencia que los medios de comunicación pueden ejercer a la hora de adoptar una decisión u otra, y tienen que ser conscientes de ello tanto los analistas de inteligencia como sus clientes, para no ser dirigidos y manipulados hacia decisiones poco satisfactorias.

Además, esa influencia, apoyada por los avances tecnológicos, que permiten un acceso casi ilimitado a información de todo tipo, provoca que las estructuras de inteligencia se vean abocadas a trabajar sobre los temas de actualidad limitando su capacidad para llevar a cabo análisis a largo plazo, con la intención de identificar amenazas potenciales, lo que provoca que, en muchas ocasiones, se vean sorprendidas y no satisfagan las necesidades de sus clientes.

### Conclusiones

Las organizaciones de inteligencia siguen siendo necesarias, ya que, a pesar de la evolución de la tecnología y los enormes volúmenes de información disponibles para cualquiera que quiera buscarlos, siempre habrá ciertos tipos de información que serán denegados por los competidores o adversarios, y que son necesarios para apoyar un proceso de toma de decisiones.

Además, la necesidad de usar inferencias y supuestos cuando los hechos y evidencias no están disponibles, provoca en muchas ocasiones que los analistas deban llegar a juicios y conclusiones basadas en informaciones incompletas, y es aquí donde el papel del ser humano, representado por el analista de inteligencia, cobra gran importancia, y es, en muchas ocasiones, el punto de fricción con los responsables de tomar decisiones, debido a que estos no son conscientes de cómo los analistas consiguen llegar, desde la información obtenida, hasta las conclusiones que les presentan, y tiene dudas sobre el proceso seguido.

Los clientes tienen que ser conscientes de las limitaciones de las estructuras de inteligencia, pero es que, además, deben en ocasiones involucrarse, sobre todo orientando al analista sobre sus necesidades exactas de información.

Hoy en día, los avances tecnológicos permiten manejar grandes volúmenes de datos y almacenarlos para su posterior manipulación, pero, a pesar de esos avances tecnológicos, el hombre en el sistema es tan importante como siempre, debido a que, aunque la tecnología facilita la manipulación de los datos, al final es el analista de inteligencia entrenado el que es capaz de hacer juicios fundamentados, elaborar conclusiones o extraer significados de los datos obtenidos, y que resulten de utilidad para su cliente.

El desarrollo de la inteligencia necesaria para anticipar, prevenir, interferir o mitigar los efectos de un ataque, una amenaza o un competidor, requiere la elaboración de inteligencia de una manera colaborativa e integrada, donde el cliente tiene un papel clave.

El núcleo central de producción de inteligencia, ya sea para afrontar una amenaza terrorista o más convencional, es la fase de elaboración, y más concretamente el análisis y la síntesis, o en lenguaje más claro, el proceso de descomposición de la información en sus elementos constituyentes, su

procesamiento en componentes manejables, la búsqueda de vínculos con elementos relacionados, ponerlos en contexto y sintetizar los resultados en inteligencia que sea de utilidad para el que tiene que tomar decisiones.

Otro aspecto importante es que, actualmente, las estructuras de inteligencia están dedicadas a trabajar a nivel operacional, táctico o actual. En la mayoría de los casos, se echa en falta un análisis a largo plazo. En otras palabras, la mayoría de los recursos están dedicados al informe de inteligencia, en vez de intentar alcanzar un profundo conocimiento de nuestros adversarios.

Esta situación es debida al complejo entorno de seguridad, la naturaleza de las necesidades de los responsables, las prácticas individuales o de la organización y el éxito de las actividades técnicas de obtención, con unas capacidades actuales inimaginables hace unas décadas. El principal motivo de falta de análisis a largo plazo es debido a que la mayoría de los consumidores de inteligencia es lo que quieren (o, por lo menos, es lo que obtienen, ya que no preguntan por análisis a largo plazo).

Uno de los cambios más importantes que tienen que afrontar las organizaciones de inteligencia hoy en día, es tener la flexibilidad suficiente para adaptarse a trabajar alrededor de un problema o asunto determinados, más que mantener una estructura rígida que dificulte la cooperación, siendo la clave el intercambio de información e inteligencia.

La clave, está en cambiar la manera de trabajar en inteligencia, pasando de una basada en procesos establecidos debido al tipo de información que es obtenida, a otra dirigida por el problema que tiene que ser resuelto. Es decir, cambiar de una inteligencia basada en el análisis de lo que se ha obtenido, a otra basada en el análisis de lo que necesita ser obtenido.

## Bibliografía

- BETTS, Richard K. (2007). *Enemies of Intelligence: Knowledge & Power in American National Security*. New York: Columbia University Press.
- CLARK, R. M. (2010). *Intelligence Analysis: A Target Centric Approach*. Washington: CQ Press.
- CLAUSER, Jerome (2008). *An Introduction to Intelligence Research and Analysis*. Plymouth UK: The Scarecrow Press.
- DAVIS, Jack (2008). «Why Bad Things Happen to Good Analysts». En: GEORGE, Roger Z. y BRUCE, James B. (eds.), *Analysing Intelligence: Origins, Obstacles and Innovations*. Washington D.C.: Georgetown University Press.
- DE FRANCO, Chiara y MEYER, Cristoph O. (2011). *Forecasting, Warning, and Responding to Transnational Risks*. Basingstoke: Palgrave Macmillan.
- DÍAZ-CANEJA GRECIANO, José Manuel (2014). *La Cooperación de Inteligencia en la UE*. Madrid: Instituto Español de Estudios Estratégicos.

- ERDMANN, Drew, y MENDONCA, Lenny (2009). *Focused on foresight: An Interview with the US national intelligence officer for warning*. McKinsey Quarterly.
- GRABO, Cynthia M. (2002). *Anticipating Surprise. Analysis for Strategic Warning*: Washington DC, Joint Military College.
- HALL, W. M., & Citrenbaum, G. (2010). *Intelligence Analysis: How to Think in Complex Environments*. Santa Barbara: Praeger Security International.
- HERMAN, Michael (1996). *Intelligence Power in Peace and War*. Cambridge. Cambridge University Press.
- HEUER Jr., RICHARDS J. y PHERSON, Randolph H. (2011). *Structured Analytic Techniques for Intelligence Analysis*. Washington D. C.: CQ Press.
- JERVIS, Robert (2010). *Why Intelligence Fails: Lessons from the Iranian Revolution and the Iraq War*. Ithaca and London: Cornell University Press.
- KENT, Sherman (1964). «Words of Estimative Probability» en STEURY, Donald P., ed., (1994), *Sherman Kent and the Board of National Estimates: Collected Essays*. Washington D. C.: Center for the Study of Intelligence, Central Intelligence Agency.
- LAHNERMAN, W. J. (2006). *The Future of Intelligence Analysis*. Maryland: University of Maryland, Center for International and Security Studies.
- MEYER, Christoph O., OTTO, Florian, BRANTE, DE FRANCO, Chiara. (2010). *Re-Casting the Warning-Response-Problem: Persuasion and Preventive Policy*. International Studies Review, vol. 12, nº. 4.
- MONTANARO, Lucía y SCHÜNEMANN, Julia (2011). *Walk the Talk. The EU needs an effective Early Warning system to match its ambitions to prevent conflict and promote peace*. Fride & International Alert /Initiative for Peacebuilding-Early Warning,
- SULLIVAN, J. P. (2005). «Terrorism Early Warning and Co-Production of Counterterrorism Intelligence». Montreal, Québec, Canadá.
- SYMON, Paul B. y TARAPORE, Arzan. *Defense Intelligence Analysis in the Age of Big Data*. Joint Force Quarterly (JFQ) 79, 4th Quarter 2015.
- TREVERTON, G. F., & GABBARD, B.C. (2008). *Assesing the Tradecraft of Intelligence Analysis*. Santa Monica: RAND Corporation.
- WALDROP, M. M. (1992). *Complexity: The Emergenging Science at the Edge of Order and Chaos*. New York: Simon & Schuster.





## Capítulo cuarto

### Actores en la producción de inteligencia

Isaac Martín Barbero

#### Resumen

Este capítulo aborda la producción de inteligencia y los actores que intervienen en este proceso y, por ello, ofrece la oportunidad de profundizar en la relación entre productores y consumidores de inteligencia, uno de los principales temas de la inteligencia como campo de estudio y también como práctica.

Inteligencia es mucho más que información estructurada y va mucho más allá que la acumulación de conocimientos. Requiere la identificación de los intereses en juego y la consideración de los retos relevantes y la comprensión de la vinculación entre una organización y su entorno.

Junto a la importancia de la relación entre productores y consumidores de inteligencia, este capítulo recoge dos cuestiones que impregnan la argumentación: el impacto de la tecnología en el proceso de inteligencia y el alcance del proceso de inteligencia en los procesos de toma de decisiones. Con ello, se abordan los principales aspectos transversales a tener en cuenta a la hora de plantearse cualquier proceso de inteligencia destinado a potenciar la calidad de las decisiones.

En la literatura relativa a los procesos de producción de inteligencia, abundan las referencias al llamado ciclo de inteligencia y las aproximaciones, versiones y críticas al mismo. En esta ocasión intentaremos evitar que «el

ciclo de inteligencia» acapare un protagonismo excesivo optando por una visión de la producción más dinámica, acorde con un proceso de producción articulado en fases que presentan solapamientos y que está orientado al objetivo de responder a las necesidades de información de un usuario final.

#### **Palabras clave**

Inteligencia, procesos de producción, conocimiento, ciclo de inteligencia.

#### **Abstract**

This chapter addresses the production of intelligence and the actors, who intervene in this process and which, due to this, offer the opportunity of delving into the relationship between producers and consumers of intelligence, one of the main subjects in intelligence as a field of study and a practical field.

Intelligence is much more than structured information and it goes beyond the acquisition of knowledge. It requires the identification of self-interest and objectives, the main frameworks and the links between an organization and its environment.

Together with the importance of the relationship between intelligence producers and consumers of intelligence this particular chapter addresses two of the main debates of intelligence studies: the impact of the technological revolution in the production of intelligence and in the decision making process. With this, we address the main transversal aspects to take into account when dealing with any intelligence process aimed at improving the quality of the decisions.

In the literature about the intelligence process the references to the so called intelligence cycle are constant. However in this study we choose a different vision and a more dynamic approach based in a production process guide in overlapped phases oriented to answer the information needs of the final consumer.

#### **Keywords**

Intelligence, production process, knowledge, intelligence cycle.

## Inteligencia: actores en busca de guion

El elemento diferenciador de la «inteligencia» no descansa en la aplicación de técnicas de análisis ni de sistemas informáticos altamente sofisticados; lo que hace que la inteligencia sea tal, es su orientación a transformar la información en conocimiento, y el conocimiento en productos que sirvan de ayuda a la toma de decisiones específicas<sup>1</sup>. Inteligencia es mucho más que información estructurada y va mucho más allá que la acumulación de conocimientos. Requiere la identificación de los intereses en juego y la consideración de los retos relevantes y la comprensión de la vinculación entre una organización y su entorno: externo –lo que supone valorar amenazas y oportunidades–; e interno –valorando los puntos fuertes y débiles de la empresa–. Así, cuando el entorno se vuelve volátil, inestable o simplemente poco seguro, los distintos actores (públicos y privados) tienden a centrarse en lo que ocurre fuera y analizan exhaustivamente –para sobrevivir (riesgos y amenazas) y prosperar (oportunidades)– eventos, relaciones entre competidores y tendencias. Esta reacción natural, y en principio razonable, puede tener consecuencias negativas si se pierde de vista la importancia fundamental de la dimensión interna.

La oportunidad de compartir este punto de partida con el lector es particularmente grata en un capítulo que aborda la producción de inteligencia y los actores que intervienen en este proceso y que, por ello, ofrece la oportunidad de profundizar en la relación entre productores y consumidores de inteligencia, uno de los principales temas de la inteligencia como campo de estudio y también como práctica.

Junto a la importancia de la relación entre productores y consumidores de inteligencia, este capítulo recoge dos cuestiones que impregnan la argumentación: el impacto de la tecnología en el proceso de inteligencia y el alcance del proceso de inteligencia en los procesos de toma de decisiones. Con ello se abordan los principales aspectos transversales a tener en cuenta a la hora de plantearse cualquier proceso de inteligencia destinado a potenciar la calidad de las decisiones.

En la literatura relativa a los procesos de producción de inteligencia, abundan las referencias al llamado ciclo de inteligencia y las aproximaciones, versiones y críticas al mismo. En esta ocasión intentaremos evitar que «el ciclo de inteligencia» acapare un protagonismo excesivo optando por una visión de la producción más dinámica, acorde con un proceso de producción articulado en fases que presentan solapamientos y que está orientado al objetivo de responder a las necesidades de información de un usuario final. Este planteamiento se inspira en prácticas propias de la dirección de proyectos tomadas de metodologías tradicionales (en cascada) pero también de

---

<sup>1</sup> Gustavo Díaz Matey: «The use of intelligence in the private sector», *International Journal of Intelligence and Counterintelligence*, n.º. 26, 2014.

«nuevas aproximaciones ágiles» orientadas a dar respuesta a proyectos cuyos requisitos son cambiantes. De esta manera, articularemos la convicción de que los estudios de inteligencia deben actualizar sus procesos bebiendo de metodologías desarrolladas y asentadas en otros campos con resultados satisfactorios y evitar el riesgo de quedar atrapados en conceptos excesivamente academicistas y poco apropiados para abordar situaciones inciertas y cambiantes.

Con todo, desde la aproximación clásica del «ciclo de inteligencia» con las distintas «fases» de los procesos de producción –definición de las necesidades de información, planificación del proyecto, obtención, procesamiento y evaluación de la información, análisis, desarrollo del producto y difusión del mismo– queda claro el papel central de la relación entre productores y consumidores con el que se inicia el proceso y con el que también termina. Quedando de manifiesto que, sin una correcta relación entre los mismos, el proceso no tendrá sentido ni utilidad ya que toda investigación que no sea útil al proceso de toma de decisiones no cumplirá la función para la cual se ha de diseñar todo el proyecto de inteligencia.

Por otro lado, la tecnología ha tenido un impacto importante en el conjunto del proceso de inteligencia y ha supuesto el desarrollo de multitud de herramientas que buscan automatizar partes del trabajo de inteligencia o que aspiran a facilitar el trabajo del analista. Entender de forma correcta qué suponen estas herramientas, cómo se relacionan los analistas con las mismas y cuál es el valor real que aportan en relación a su coste es, a día de hoy, una de las primeras tareas a la hora de implantar una célula de inteligencia en cualquier organización.

Por último, la inteligencia como ya se ha señalado en otros capítulos de este volumen, es una herramienta que ayuda a reducir la incertidumbre inherente al proceso de toma de decisiones<sup>2</sup>. Entender hasta dónde puede llegar la inteligencia, cuáles son los límites de lo que puede conseguir y cuáles son los costes (tangibles e intangibles; explícitos e implícitos) de determinadas actuaciones nos ayudará a entender la forma en que la inteligencia puede ayudar a mejorar la toma de decisiones en una organización, y a ajustar los procesos de inteligencia en el marco concreto de cada organización.

## Entender la inteligencia

En los últimos años, tras el auge del interés por todo lo remotamente relacionado con la «inteligencia», emerge una legítima preocupación por el verdadero valor (si es que no relevancia) de esta, espoleada por sonoros fracasos que, con más o menos razón, suelen atribuírsele. Y se ha escrito

---

<sup>2</sup> Gustavo Díaz Matey: «Hacia una definición inclusiva de inteligencia», *Revista de inteligencia y prospectiva* 4, 2008.

mucho sobre la relación entre inteligencia y mejora del desempeño de una organización en la consecución de aquellos objetivos considerados estratégicos. Pero ante todo, conviene no empezar por pedir peras al olmo<sup>3</sup>.

Aún asumiendo que una buena inteligencia es necesaria para una estrategia óptima, de poco nos servirá sin una idea clara de hacia dónde se dirige nuestra organización o, según el caso, de cuales son por ejemplo, los intereses de seguridad nacional de nuestro Estado. Como señala, Ben Gilad, «si bien una buena estrategia con una mala inteligencia producirá resultados mediocres; una mala estrategia con buena inteligencia es garantía absoluta de fracaso».

Por lo tanto, la estrategia es una condición necesaria de todas las organizaciones (públicas y privadas), independientemente de su mayor o menor importancia, que tengan interés en su propia supervivencia... y a ese objetivo es al que ha de estar orientada la inteligencia. Una supervivencia sostenida y sostenible depende de la capacidad de evaluar un desarrollo dado, de anticipar y de explorar el potencial de diferentes elecciones y así poder decidir de entre esas posibilidades considerando los objetivos y las reacciones potenciales de otros agentes hacia nuestras propias acciones.

Las actividades de inteligencia en el ámbito de la seguridad pública no pueden reducirse a meras labores de espionaje y acciones encubiertas. Ningún Estado u organización puede dirigir sus actividades de inteligencia exclusivamente contra las amenazas directas. La inteligencia aplicada a entornos empresariales no puede basarse únicamente en actividades tales como la búsqueda de competidores y la evaluación de su competitividad. Debe contemplar también la identificación de puntos de apoyo o proveedores potenciales; evaluación de situación financiera de clientes; seguimiento de la regulación de los nuevos mercados y captación de nuevas oportunidades empresariales. Sin embargo, la pertinencia de estos ámbitos viene dada por su impacto potencial sobre la capacidad de la organización de lograr su propósito fundamental: el afianzamiento de su capacidad sostenible de sobrevivir y prosperar.

En este sentido, la inteligencia no solo ayuda a evaluar amenazas, también está íntimamente relacionada con la reducción del riesgo, la reducción de la incertidumbre y el correcto entendimiento del entorno, algo aplicable al sector público y que, en el marco del sector privado, se denominaría inteligencia estratégica en la empresa o inteligencia empresarial. Por el contrario, es necesario «un entendimiento claro» del entorno y de la situación general. Lo que en último término se traduce en identificar no solo riesgos y amenazas, sino también oportunidades.

---

<sup>3</sup> Mario Esteban Navarro: «¿Por qué debo usar inteligencia competitiva en mi empresa?», *Revista de Inteligencia y Seguridad* 7, diciembre de 2009 – mayo de 2010; Jorge Postigo: «La inteligencia competitiva en España: una encuesta sobre su utilización por parte de las empresas exportadoras», *El Profesional de la Información* 10, nº. 10, 2001.

Pero a pesar de todo su enorme potencial, es importante destacar que la inteligencia ayuda fundamentalmente a reducir la incertidumbre, a ampliar el arco de opciones a nuestra disposición y a situarnos en mejor disposición de asumir desenlaces contrarios a nuestras aspiraciones. Asumir plenamente este planteamiento contribuirá a evitar que la inteligencia se convierta en un instrumento para justificar decisiones ya tomadas, que se emplee para facilitar el seguir la estela de terceros o que se utilice para dar por finalizada la necesaria labor de actualización permanente del rumbo de las organizaciones. La inteligencia, por el contrario, debería ser un faro que alumbré los procesos de toma de decisiones. Decisiones que posteriormente, a la luz de los acontecimientos, se antojarán afortunadas o desafortunadas, pero que serán buenas o malas por la forma en la que se adopten, con independencia de sus resultados. Para ello, es necesario que los encargados de tomar decisiones (los usuarios de la inteligencia) sean conscientes de sus beneficios potenciales, y también de sus limitaciones, e incorporen ambos aspectos plenamente a sus procesos específicos de toma de decisiones.

### **Necesidades de información: atinar es cosa de dos, fallar puede hacerse solo**

De entre los mayores obstáculos a superar a la hora de construir soluciones en inteligencia destacan las carencias de los consumidores de inteligencia en la comprensión y articulación de sus propias necesidades. Abundan las falsas concepciones sobre los principales problemas a los que se enfrentan, que dificultan la plasmación de las necesidades de información del usuario final en una petición informativa específica. Por diversos motivos, los encargados de tomar decisiones, en la mayoría de las ocasiones, no transmiten de forma acertada sus verdaderas necesidades de información. Aquellas que justificarían en primera instancia el trabajo de inteligencia y que, posteriormente, deberían ser traducidas en un planteamiento de inteligencia. Las razones son diversas.

En ocasiones es el propio desconocimiento de cómo llegar hasta las verdaderas preguntas cuyas respuestas ayudarían a reducir la incertidumbre de su proceso de toma de decisiones. En otras ocasiones, «el cliente» simplemente no quiere poner encima de la mesa las vulnerabilidades de su propia organización o incluso lo que él percibe como sus propias carencias. Por cierto, que esta tendencia se ve severamente afectada por la relación entre el consumidor de inteligencia y el responsable de proporcionarla. Según el contexto, el carácter externo o interno de la célula de inteligencia puede ser una condición suficiente para condenar el proyecto al fracaso más rotundo.

Para contrarrestar esta situación, es clave que los encargados de tomar decisiones entiendan e interioricen para qué sirve la inteligencia y cuáles son las limitaciones de esta herramienta. Ya que, un uso efectivo de la inteligencia, supondrá importantes mejoras en los procesos de toma de decisiones

y en la capacidad de identificar y reducir el grado de incertidumbre, siendo, en definitiva, una pieza clave en el incremento de la competitividad o de la posición relativa de un Estado. Para ello, será clave conseguir homogeneizar el lenguaje relativo a los temas de inteligencia. La claridad conceptual ayudará, sin duda, a que los encargados de tomar decisiones dejen de percibir estos asuntos como cuestiones oscuras relacionadas con temas de espionaje y prácticas poco éticas, para conseguir vislumbrar la verdadera utilidad de la inteligencia en sus estructuras. Si los gestores principales no están muy seguros en cuanto al papel de la inteligencia en los procesos de toma de decisiones de sus propias organizaciones (públicas o privadas), no estarán muy dispuestos a invertir tiempo y dinero en dotarse de una capacidad significativa. Pero, la confianza en el potencial de la herramienta debe verse complementada por la confianza en los agentes de inteligencia con los que el consumidor interactúe y, en su defecto, con la certeza de que la franqueza a la hora de expresar sus limitaciones y demandas no podrá perjudicarle ni a él ni a su organización.

En un campo aparentemente ajeno a la seguridad nacional, pero con tanto potencial para la introducción de este tipo de aproximaciones como es la inteligencia empresarial en el tejido de la pequeña y mediana empresa, el proyecto CITEX –financiado por la Comisión Europea y en el que participó ICEX España, Exportación e Inversiones en 2012– estaba orientado a la creación de un itinerario formativo en materias de inteligencia con el fin de mejorar la competitividad de las empresas europeas y apuntaba estas dos líneas de trabajo (la formación, para la concienciación de los encargados de tomar decisiones, y la claridad conceptual) como fundamentales para una mejora de la implantación de la inteligencia en las empresas europeas<sup>4</sup>. Este argumento es válido también en el ámbito de la inteligencia en materia de seguridad pública, donde una correcta percepción del para qué vale la inteligencia y cómo esta puede ayudar a reducir la incertidumbre en los procesos de toma de decisiones es clave para un correcto funcionamiento de los procesos de inteligencia en primera instancia, tal y como refleja la atención dedicada a este asunto por parte de los estudios de inteligencia. Para tal fin, será necesario avanzar hacia unos estándares comunes que nos permitan poder hablar de formación en materias de inteligencia. De una verdadera profesión en materias de inteligencia con cursos e itinerarios formativos para tal fin. Al fin y al cabo, si entendemos la inteligencia como una herramienta de ayuda al proceso de toma de decisiones, de cualquier proceso de decisiones estratégicas, nos encontramos con la imperiosa necesidad de contar con profesionales formados en temas de inteligencia para mejorar la competitividad de nuestras empresas y la posición relativa de nuestras instituciones.

---

<sup>4</sup> Proyecto CITEX, Competitive Intelligence in Trade and Export, en [http://www.citexproject.eu/index.php?option=com\\_content&task=blogsection&id=4&Itemid=90&PHPSESSID=0011930bc6e5e9fac877a511989e77d5&mylang=spanish&PHPSESSID=0011930bc6e5e9fac877a511989e77d5](http://www.citexproject.eu/index.php?option=com_content&task=blogsection&id=4&Itemid=90&PHPSESSID=0011930bc6e5e9fac877a511989e77d5&mylang=spanish&PHPSESSID=0011930bc6e5e9fac877a511989e77d5).

Es en el desarrollo de esta futura profesión y en la concreción de sus desempeños, competencias y límites donde se enmarca la correcta relación entre productores y consumidores de inteligencia.

Aunque no existe una fórmula única para la relación entre productores y consumidores de inteligencia, está fuera de cuestión que se requiere la implicación de ambos en el proceso de definición de las necesidades para lograr una máxima efectividad. Michael Herman, en su estudio de referencia sobre la inteligencia en seguridad pública, aboga a favor de una relación dinámica y «emprendedora», de acuerdo con la comprensión de Peter Drucker de este concepto: la reasignación permanente de recursos desde áreas de bajo rendimiento hacia otras de alto rendimiento. Así, los productores de inteligencia presentan su producto a los responsables de tomar decisiones y buscan una retro-alimentación para identificar los aspectos de mayor utilidad de acuerdo con los consumidores que revisan los resultados con la voluntad de ejercer una crítica constructiva que permita su mejora continua a la luz de la experiencia y con la vista puesta en los cambios que se producen en el entorno.

Entender, plasmar y priorizar las necesidades de información del encargado de tomar decisiones será una tarea tan importante en cualquier proceso de inteligencia que condicionará el resto del proceso, ya que orientará los esfuerzos de obtención, priorizando la búsqueda de unas informaciones sobre otras, lo que tendrá un impacto posterior en el resto de fases. En definitiva, si las necesidades del cliente se identifican mal, el resto del trabajo de inteligencia estará herido de muerte.

### **De las necesidades de información a los requerimientos de inteligencia. Planificando el trabajo y trabajando el plan**

Una vez determinadas las necesidades de información que plantean los consumidores de inteligencia, estas deben convertirse en un conjunto de requisitos específicos sobre los que trabajar. Este conjunto de requisitos conforma el plan de trabajo destinado a cubrir esas necesidades de información y orientar los esfuerzos de obtención y el posterior análisis. Este punto concreto tiene unas implicaciones muy importantes sobre el conjunto del proceso de producción. Es aquí donde se determina si el resultado del trabajo de inteligencia irá orientado a la potenciación del proceso de toma de decisiones dirigido a conducir a una acción o no acción y, por tanto, será en este punto donde se determinará si el trabajo de inteligencia está alineado con los objetivos de la organización. Cuando esto no ocurre, se producen desviaciones y, si estas persisten en el tiempo, se adquieren «vicios», viéndose socavada la efectividad del trabajo y la sostenibilidad de las propias capacidades de inteligencia a medio y largo plazo. Debe prestarse especial atención a evitar que la necesaria proximidad de los responsables de las tareas de inteligencia a los encargados de tomar decisiones se traduzca en



una contaminación del trabajo de los primeros a través de una preconfiguración de las conclusiones conforme a las aspiraciones y deseos de los líderes de la organización. En este empeño, es muy útil ser muy consciente de las relaciones estructurales e informales en el seno de la propia estructura, así como de las agendas de los encargados de tomar decisiones.

Para el correcto desarrollo de este plan de trabajo, la figura del gestor de inteligencia es clave para salvaguardar el equilibrio entre necesidades, capacidades y recursos disponibles. Para ello, el gestor deberá establecer los costes del trabajo planteado en relación a los requerimientos. Una vez identificados los costes del trabajo, y con el fin de desarrollar un plan de trabajo adecuado centrado en los requerimientos de inteligencia, el gestor deberá, con el soporte de un marco teórico adecuado, encontrar y entender las características principales y componentes de las distintas cuestiones planteadas.

Lo que se sabe hasta el momento es un punto de partida básico a la hora de delimitar los contornos básicos del problema. El gestor deberá ser consciente de las premisas de partida (modelos conceptuales o marcos de referencia) así como de las imágenes mentales preexistentes acerca de un fenómeno. Estas imágenes son los referentes básicos con los que se explica lo que es, cómo funciona, quién está involucrado y por qué existe. El marco teórico, en definitiva, nos proporciona una guía muy importante para hacernos las preguntas adecuadas, a fin de que, a través de las mismas, el producto resultante tenga sentido, ofrezca un relato y permita aflorar relaciones no obvias entre sucesos dispersos.

Estos marcos son, con todo, generalizaciones; eso sí, necesarias para establecer las condiciones sobre las que se basará nuestra investigación. La teoría, en definitiva, da sentido a numerosas piezas de información, explicando o anticipando relaciones y clarificando qué causas son básicas para explicar distintos efectos/sucesos y cuáles son periféricas. Cuando se trabaja conforme a este plan de trabajo se ponen encima de la mesa las premisas de partida y el marco teórico sobre el que se basará la posterior investigación. Como ha escrito Putnam: «... La importancia primordial de las ideas es que guían la práctica, que estructuran formas completas de vida...». En definitiva, los marcos teóricos nos guían en el discernimiento de qué datos son importantes y hacia dónde tenemos que orientar, primero, la mirada y la obtención, después. Es importante conservar la humildad de saber que la anticipación, a menudo, no supone la capacidad de predecir. Afirma Kristan J. Wheaton (2014): «Just as we cannot predict black swan events, we cannot predict which precise grain of sand will bring the whole sandpile down». Es muy difícil saber cuál es el elemento concreto que desencadenará el colapso de un equilibrio altamente inestable aunque, a menudo, lo importante, lo sustancial, lo más valioso es apuntar la inminencia del desencadenamiento del colapso.

En este mismo sentido, en el plan de trabajo, se han de desarrollar indicadores claves que permitan seguir la evolución de un suceso o el cambio en las

propiedades de una entidad, al tiempo que se desarrollan hipótesis de trabajo –alternativa posible basada en asunciones claras, en datos, en el entendimiento y en la especulación–. Estas hipótesis, basadas en el marco teórico desarrollado previamente, nos permitirán constatar qué aspectos guardan semejanza y cuando ciertas suposiciones pueden acercarse a ser certezas.

Posteriormente, el gestor de inteligencia con las necesidades de información encima de la mesa y el marco teórico será capaz de definir las tareas y asignar los roles necesarios para cumplirlas. Este punto se concretará de una u otra forma en función de la metodología empleada y de la estructura de la propia organización. En un contexto en el que el tiempo disponible para tomar decisiones se ha reducido enormemente, la carga de la prueba se inclina en favor de metodologías ágiles que doten a estos procesos de flexibilidad y permitan adecuar la fuerza de trabajo a requerimientos cambiantes.

En conclusión, el plan de trabajo ha de definir los requerimientos de inteligencia, acotar el trabajo de inteligencia, establecer fronteras nítidas y limitar el alcance del trabajo a realizar hasta constituir un punto de partida para los posteriores procesos de obtención y análisis de información.

### **Tecnología y factor humano: una muy falsa disyuntiva en tiempos de cambio**

La revolución de las comunicaciones y la proliferación de información en la web han supuesto un incremento exponencial de la información disponible sobre cuestiones antes inaccesibles. De hecho, hoy en día, Internet se sitúa como el principal soporte de búsqueda y recuperación de información –tanto a nivel profesional como de usuario– y aunque no ha cambiado ni la naturaleza ni la necesidad de las actividades de vigilancia e inteligencia, estas se han visto profundamente afectadas por la irrupción, primero, y la consolidación y extensión, después, del fenómeno de Internet. A día de hoy, con las metodologías y herramientas adecuadas, Internet permite desarrollar parte del proceso de obtención de información en menos tiempo y a costes más reducidos (aspiradores, metamotores, herramientas de visualización, herramientas de análisis semántico y agentes inteligentes).

Por otro lado, debido a la progresiva digitalización de nuestra vida, asistimos a la emergencia de un nuevo potencial de *conocimiento* derivado de un mayor uso de la información. Así, se ha incrementado la interdependencia, y las organizaciones (tanto públicas como privadas) están más imbricadas con su entorno y sus competidores. Al tiempo que el correcto entendimiento y la comprensión del entorno se convierten en una actividad decisiva y diferenciadora, este no deja de complicarse. La globalización ha sacudido las antiguas reglas económicas y la revolución en las comunicaciones y tecnologías acelera el ritmo de estos cambios, por lo que se acaban imponiendo nuevos

condicionantes. El cambio tecnológico no solo continúa acelerándose, sino que adquiere características nuevas que nos conducen a un tipo de sociedad distinto, en el que el papel de las organizaciones se transforma.

«Las actividades que ocupan la posición central en una empresa no son ya aquellas dedicadas a producir y distribuir objetos, sino aquellas que producen y distribuyen información y conocimientos»<sup>5</sup>.

Hoy en día existen nuevas tecnologías de información –nuevos procesos, nuevos productos– y el requerimiento de satisfacer nuevas necesidades; lo que, en último término, supone que el periodo de respuesta es mucho más corto y las ventanas de oportunidad también. En definitiva, asistimos a un entorno con mucha más incertidumbre y con un elenco de riesgos y amenazas nuevo o con nuevas manifestaciones de amenazas tradicionales, todo lo cual impone un conjunto de respuestas adaptativas sin precedentes, tanto en el sector público como en el privado<sup>6</sup>.

De igual modo, la tecnología ha tenido un impacto directo en el propio trabajo de inteligencia, con el desarrollo de multitud de herramientas informáticas que ayudan a automatizar partes del proceso y otorgan agilidad al mismo. A la luz de estos desarrollos, cada organización debe de ser consciente de qué partes del proceso necesita automatizar y a qué coste. No todas las empresas necesitan todas las herramientas, ni todas las herramientas existentes se ajustan a todas las organizaciones. En este sentido, la tecnología y la llamada «revolución de las fuentes abiertas», son armas de doble filo ya que pueden generar expectativas inapropiadas y conducir al menosprecio de la importancia de las inversiones en análisis y el papel de los analistas y, en general, a que se subestimen las capacidades humanas, sobrevalorando los productos con un alto componente técnico. Conviene tener muy presente que, a pesar del desarrollo de la tecnología, esta no ha sido capaz de reemplazar la labor humana en los procesos de inteligencia. Incluso con el desarrollo del *Big Data*, el cómo analizar la información y sacar inferencias adecuadas seguirá siendo la clave y el elemento diferencial del trabajo de inteligencia en cualquier organización.

La evolución descrita, lejos de relativizar su papel, refuerza la importancia de la figura del gestor de inteligencia, que ha de facilitar un puente entre el equipo de inteligencia y los consumidores de la misma. Es el propio gestor quién debe entender los flujos existentes dentro de la propia organización y quién, en última instancia, ha de coordinar con los usuarios de inteligencia no solo los productos de inteligencia necesarios sino también elegir las herramientas más eficaces en cada caso para conseguir una mayor agilidad y un mayor impacto de su trabajo.

<sup>5</sup> Peter Drucker: «The Rise of the Knowledge Society», *Wilson Quarterly* 17, n.º. 2, 1993.

<sup>6</sup> Gustavo Díaz Matey: *Los servicios de Inteligencia ante el siglo XXI*, Madrid. Chavin, 2012.

**Más es mejor, en ocasiones; y más accesible, a menudo, también es mejor**

Una vez entendidas las necesidades de los consumidores de inteligencia, y bajo la dirección de un plan de trabajo claro, procede obtener información. En esta fase, es útil tomar como premisa de partida que la materia prima para realizar este trabajo –la información– es parcial, incompleta, sesgada hasta que se demuestre lo contrario. Por lo que la verificación debe tenerse como objetivo desde el inicio del proceso de captación u obtención de información. Las fuentes deben de ser: creíbles, fiables, relevantes y, *a priori*, susceptibles de ser confirmadas. En términos generales, la información se capta en función del plan de obtención de información que está asentado en las necesidades del cliente y contenido en el tiempo disponible para la realización del proyecto. De este modo, lo importante no es solo, cómo se pensaba en los años 90 del siglo XX, la cantidad de información que se posea. Resulta clave el momento en el que se posee esa información. Hoy, la información tiene un ciclo de vida más corto en el tiempo, y ello tiene implicaciones también en aspectos como el secreto de las informaciones, que juega un papel distinto al que desempeñaba, por ejemplo, durante la Guerra Fría.

Al tratar de la obtención de información y de los actores que intervienen en esta fase, y en especial tras citar el fenómeno de «el secreto», debe hacerse especial referencia al impacto de las llamadas fuentes abiertas en el trabajo de inteligencia. Estas fuentes abiertas (OSINT), a pesar de ser uno de los más significativos fenómenos de este comienzo del siglo XXI, no son algo nuevo, pues, desde siempre, se ha tenido conciencia del potencial de los viajeros, de la observación directa, de los libros y de las lecturas estructuradas. Y a pesar de que no es algo nuevo, sigue envuelto en un halo de confusión.

La revolución de la información no supone, ni mucho menos, que toda la información necesaria esté o se pueda encontrar en la web. Se repite que actualmente hasta el 80% de la información usada por la inteligencia estatal estadounidense se deriva de las fuentes abiertas (OSINT). Pero este dato se malinterpreta con facilidad. Cuando Robert Steel afirma que el 80% de lo que el usuario de inteligencia necesita no está *online*, podría pensarse que ambas afirmaciones son contradictorias. No lo son. La información publicada en Internet, representa solo una ínfima parte de lo que constituyen las llamadas OSINT<sup>7</sup>.

En este punto, a pesar de los beneficios que producen las fuentes abiertas, es necesario tener en cuenta sus limitaciones en cuanto a su utilidad y aplicación. La más fácilmente apreciable es la sobreabundancia de información y el nivel de ruido que esta produce, lo que supone que, si los esfuerzos no se orientan correctamente, lejos de ahorrarse tiempo se consumirá más

---

<sup>7</sup> Álvaro Cremades y Gustavo Díaz: «Información e Inteligencia: una reflexión interdisciplinar», *Revista de Estudios en Seguridad Internacional* 1, n.º. 2, 2015.

del necesario. Otra de las principales limitaciones inherentes a las fuentes abiertas se refiere a su precisión y rigor, ya que, en general, este tipo de fuentes son difíciles de validar y en ellas se agudiza la dificultad para discernir entre aquellas sobre las que se han aplicado medidas de desinformación de aquellas otras sobre las que no. Ni toda la información disponible es útil, como tampoco es necesario poseer toda la información disponible; la ventaja informativa –en su caso, susceptible de convertirse en ventaja competitiva– reside en disponer de aquella información relevante para la toma de decisiones. Nada más y nada menos.

Como ya se ha apuntado, una vez que comienza el proceso de obtención, es necesario que la información se clasifique y se verifique de forma correcta, con el fin de facilitar el posterior análisis de la misma y evitar trasladar a los analistas información repetida, irrelevante o confusa. Para ello, es necesario procesar la información, registrarla e indexarla. En términos generales, el procesamiento consiste en «traducir» a un lenguaje comprensible los datos recogidos, agrupándolos en piezas de información que puedan ser interpretadas en la siguiente fase del proceso. Partiendo de esta premisa, a través de este proceso de evaluación de la información, se pone de manifiesto la veracidad de la información y su exactitud.

Existe un código muy útil para determinar la exactitud de la información obtenida que proviene de la inteligencia militar, pero que puede ser extrapolado a cualquier situación. El Código OTAN o Código del Almirantazgo es efectivo para analizar la evolución de la información vertida por una fuente durante un periodo de tiempo, con el fin de terminar evaluando no solo la información sino la fuente que la vierte, evaluando su exactitud y su fiabilidad. Otra forma de evaluar la calidad es a través de la triangulación de la información con otras fuentes. Sin embargo, el hecho de que algo lo diga eventualmente «todo el mundo» no significa que necesariamente sea verdad.

### **Análisis: en pugna con todos los enemigos internos y externos**

Analizar consiste en establecer la presencia de una relación consistente y convincente entre los datos disponibles y la conclusión a la que se llega a través de esos datos. Esta relación –inferencia– supone que, por medio de procesos de análisis, se crean nuevos conocimientos a partir de lo previamente conocido. Así, se define el término análisis como el proceso por el cual se pasa de un conjunto de información acumulada (evidencias) a la creación de conocimiento. Analizar es «una operación lógica referida a proposiciones admitidas como verdaderas (premisas) y que concluye en la verdad de una nueva proposición en virtud de su vinculación con las primeras. Es decir, establecer una relación de dependencia convincente, llamada inferencia, entre los datos disponibles y la conclusión». Para ello es necesario entender cómo la totalidad de la entidad a estudio y sus partes están constituidas, funcionan y se relacionan entre sí. El objetivo principal de esta fase y de los actores

que intervienen en ella es obtener evidencias con el fin de contrastar las hipótesis planteadas.

Por medio del análisis, somos capaces de ver la tendencia y estar alerta ante cualquier cambio en los distintos escenarios<sup>8</sup>. Así, en esta fase los analistas de información completan los vacíos y la falta de información con inferencias calculadas a través de principios o leyes generales; se establecen «verdades» basadas en regularidades observadas, teniendo muy en cuenta las asunciones de partida y los factores generales que enmarcan la pregunta de investigación, sin perder de vista la necesidad de prevenir.

Para realizar correctamente su trabajo, los analistas de inteligencia deben relacionarse correctamente con las herramientas que tienen disponibles para realizar su trabajo, internas (procesos mentales y sesgos cognitivos) y externas (técnicas de análisis y herramientas de visualización y automatización)<sup>9</sup>.

En resumen, el trabajo de los analistas de información se ha de basar en el llamado método científico, el cual nos lleva a analizar y sistematizar realidades determinadas, permitiéndonos llegar a explicaciones lógicas y coherentes<sup>10</sup>. En esta fase, por tanto, los analistas interpretan toda la información obtenida convirtiéndola en un producto consumible por los encargados de tomar decisiones.

Esto quiere decir que, al analizar, se separa el problema en sus elementos constitutivos con el fin de interpretar la información disponible. Analizar no es describir. La inteligencia basada en el método científico explica a través de hipótesis y teorías. Porque, el conocimiento científico trasciende los hechos observados, los infiere, los interpreta, los conceptúa de forma inductiva, deductiva o abductiva, algo clave en todo proceso de inteligencia. Tomar conciencia de la relación de la inteligencia con la racionalidad científica nos sitúa en una mejor posición para enfrentarnos tanto a puzles como a misterios.

A la hora de presentar esta parte del trabajo de inteligencia, la parte dedicada a los actores involucrados en el análisis, es importante tener claro qué significa, cómo funciona esta parte y, sobre todo, cómo se relaciona con el proceso posterior de emitir conclusiones y cómo depende del proceso anterior de obtención de información. Así, la relación de los analistas con el gestor de inteligencia será fundamental para llegar a conclusiones válidas, pero también para reorientar los procesos de obtención iterativamente, a la luz de los nuevos análisis. Por tanto, en este punto, vemos una vez más que

---

<sup>8</sup> Gregory Treverton: *Assessing the Tradecraft of Intelligence Analysis*, Santa Monica, CA, RAND Corp., 2008.

<sup>9</sup> H. Hazlitt: *Thinking as a science*, New York, E.P. Dutton & company, 1999.

<sup>10</sup> Thomas Kunt: *La estructura de las revoluciones científicas*, México, Fondo de Cultura Económica, 1971.

el proceso de producción de inteligencia, no es, ni mucho menos, lineal y que, en ocasiones, los requerimientos cambian, y no solo por las necesidades de los consumidores, sino también como consecuencia de la propia evolución del plan de inteligencia.

Este argumento implica que el análisis de información depende tanto de técnicas estructuradas no científicas, tomadas en préstamo de otras disciplinas, como de una correcta definición de los procesos de obtención de información, y del correcto diseño y despliegue del plan de trabajo en todo el ciclo de producción.

La literatura sobre inteligencia relacionada con el análisis es abundante pero, con frecuencia, estos trabajos ofrecen una aproximación descriptiva, errónea o incompleta, y buena parte de las cuestiones clave del «análisis» no reciben ni la atención necesaria ni son tratadas con la profundidad debida.

En resumen, aún hoy, los trabajos sobre cómo debería funcionar el análisis de inteligencia en distintas organizaciones son notas puntuales y anecdóticas, en trabajos bibliográficos o históricos, y no presentan una idea clara del proceso completo del trabajo del analista, de las similitudes y diferencias con los trabajos de investigación en otras disciplinas, ni un estudio crítico de la validez de las metodologías aplicadas en relación a los objetivos a conseguir. Esto lastra la superación de estas limitaciones, tanto a través de la incorporación de avances técnicos, como a través de la necesaria renovación doctrinal orientada a adecuar el trabajo de la inteligencia a la nueva situación que el siglo XXI impone, tanto para organizaciones privadas como para las tradicionales entidades estatales.

### *Herramientas internas del analista de información. Procesos mentales y sesgos cognitivos*

Antes de entrar de lleno en los métodos para realizar un análisis estructurado, debemos tener en cuenta dos factores clave. En primer lugar, es importante reflexionar sobre la forma en que pensamos y cuáles son las principales limitaciones a las que debemos hacer frente a la hora de enfrentarnos a un análisis. En segundo lugar, debemos tener en cuenta que, a pesar de la revolución en el acceso a la información, de la proliferación de escritos de todo tipo y de la globalización de las comunicaciones, el desarrollo de los procesos de pensamiento no ha mejorado al mismo ritmo. No existe una relación directa entre la mejora de los procesos de pensamiento y el acceso a un mayor volumen de información. En última instancia, no se piensa mejor y, por tanto, no se toman mejores decisiones por tener acceso a un mayor volumen de información.

Con respecto al primer factor, uno de los problemas más evidentes en el análisis de inteligencia se deriva de cómo los seres humanos procesamos información y realizamos juicios ante información ambigua e incompleta.

Por tanto, a la hora de realizar análisis de información hay que tener en cuenta las limitaciones cognitivas, los prejuicios, y los errores mentales causados por estrategias mentales de simplificación. Estas limitaciones no son fruto de ninguna predisposición emocional o intelectual ante un juicio; más bien, son procesos subconscientes del procesamiento de la información, debidos a que vemos el mundo en patrones y estereotipos basados en la experiencia, la percepción y la memoria; de manera que, tanto asunciones como prejuicios, asaltan al ser humano instintivamente.

Por otro lado, pero relacionado con lo anterior, el analista debe entender que, en cualquier campo de las ciencias sociales, existen consecuencias de acciones humanas que están más allá de la comprensión de los agentes implicados y que estas consecuencias están en relación directa tanto con las cadenas deductivas como con las cadenas causales. Esto repercute, en última instancia, en los sistemas de predicción de los acontecimientos. La mera existencia de consecuencias no intencionales, no previsibles, constituyen elementos que incidirán sobre el futuro desarrollo de la realidad en un sentido que la desviará de las predicciones del analista formuladas con anterioridad al desencadenamiento de los factores en los que cabe buscar el origen de las consecuencias no intencionales. En general, cuanto más complejo es un problema, más propiedades emergentes se generan, las cuales no estaban (o no podían estar) contempladas. Así, extrapolando este argumento al análisis de inteligencia, podemos inferir que ni la información es lineal ni el ambiente es una constante, por lo que no podemos perder de vista que es muy difícil evaluar el potencial de la información que nos falta, ya que desconocemos el valor de lo que no sabemos.

### *Herramientas externas del analista de información. Técnicas de análisis*

De igual modo, el analista debe de conocer y manejar, de una forma correcta, las diferentes técnicas de análisis con el fin de incrementar la calidad de su producto y salir airoso, de forma más efectiva, de los principales problemas a los que se ha de enfrentar<sup>11</sup>.

En definitiva, cuando se habla de técnicas de análisis estructurado, se hace referencia a mecanismos a través de los cuales procesos internos de pensamiento son externalizados de forma sistemática y transparente a fin de poder ser compartidos, entendidos y criticados por otros. El análisis estructurado comprende una serie de técnicas que guían al analista a través de un problema, más que aportarle una solución definitiva al mismo.

---

<sup>11</sup> Richard Heuer y Randy Pherson: *Structured analytic techniques for intelligence analysis*, Washington, D. C., CQ Press, 2001, p. 4; traducido al español en 2015 por Plaza y Valdés.



Existen distintas técnicas estructuradas de análisis, que ni se limitan al uso de la inteligencia, ni le son propias. El análisis en profundidad de algunas de ellas y su aplicación al campo de inteligencia ha sido abordados por otros autores como Richard J. Heuer Jr. y Randolph H. Petherson, y a ello se han dirigido los esfuerzos de empresas como Mindtools o el Laboratorio francés de Investigación en Prospectiva Estratégica y Organización (Lipsor). Técnicas de análisis hay muchas; formas de aplicarlas innumerables. En muchas ocasiones, diversas técnicas responden a formas específicas de otras más generales como el uso de matrices o el *Brainstorming*, por poner algunos ejemplos. De igual modo, diferentes técnicas estructuradas sirven a un mismo propósito, ya sea la toma de decisiones, el razonamiento y comprensión de un problema, las relaciones entre eventos, la estadística, o visualización de datos, entre otras. En general, el tipo de herramientas usadas dependerá de los objetivos de la investigación y de las fuentes disponibles, comenzando por la propia distinción entre técnicas cuantitativas y cualitativas.

En primer lugar, al estudiar la ontología de las técnicas de análisis estructuradas hay que diferenciar entre técnicas de análisis científicas y no científicas, más que entre cuantitativas y cualitativas, ya que las técnicas cuantitativas y las cualitativas son, en buena medida, extensiones unas de otras. Con frecuencia, en inteligencia lo que puede ser cuantificado es también una cualidad y la cuantificación es un método que expresa la cualidad con una mayor precisión.

Posteriormente conviene clasificar en función del método y en función de su utilidad. Es importante señalar, una vez más, que esta fase está íntimamente relacionada con el proceso de obtención de información anterior, ya que, de lo contrario, por muchas técnicas disponibles que existan, el analista será incapaz de realizar bien su trabajo.

Antes de entrar de lleno en esta cuestión se hace necesario puntualizar que estructurar no es sinónimo, ni sustituto, de pensar. Así, las técnicas para estructurar no son técnicas para analizar. Estructurar implica agrupar, clasificar, comparar, relacionar, centrar. Analizar es algo más que una suma de procesos visuales o técnicas para la solución de problemas. Tampoco es cierto que las mejoras técnicas mejoren las formas analíticas. Analizar es algo más que aplicar estadísticas, es algo más que una suma de datos. Como bien afirma Edward E. Bono: «Los hechos en sí mismos, nunca son más importantes que su uso. La verdad no está tan íntimamente relacionada con los hechos como la gente parece imaginar»<sup>12</sup>.

De este modo, la clasificación elegida en este trabajo para encuadrar las técnicas estructuradas de análisis sigue una doble línea. En primer lugar, tiene en cuenta el objetivo del análisis, distinguiendo entre análisis descriptivos y análisis predictivos. Por otro lado, las técnicas susceptibles de ser usadas en

---

<sup>12</sup> Edward De Bono: *Six thinking hats*, Boston, Little, Brown and Company, 1985, p.11.

análisis se presentan agrupadas en tres niveles distintos: Por la información buscada (descriptiva y predictiva), por la materia de trabajo que usan las técnicas (datos, información, metáforas, estrategias) y por las características de las técnicas (diagramas, árboles, tablas, técnicas específicas).

En general, en todos los casos, para mejorar la calidad del análisis de inteligencia es requisito previo indispensable la revisión periódica de la calidad de la información y de las asunciones propias que nos conducen a los juicios establecidos, lo que se denomina, *pre-mortem assessment*. De ese mismo modo, es importante descubrir si la información disponible ha estado (o sigue estando) sujeta al engaño (*deception*) con anterioridad a la aplicación de las técnicas; en la propia naturaleza del término inteligencia, se encuentra el principio de la ocultación de información propia de los esfuerzos de obtención de «otros» y, en muchas ocasiones, la información se vierte deliberadamente con fines muy distintos al de informar.

### De la predicción a la anticipación: la criticidad del criterio

Desde el inicio del desarrollo de la disciplina de la inteligencia, Sherman Kent aconsejaba la aplicación de las técnicas consideradas «científicas» en el estudio de los acontecimientos presentes y pasados, con el fin de analizar situaciones complejas en marcha y estimaciones sobre sucesos futuros. Así, Robert Gates contribuyó al desarrollo del campo de estudio de la inteligencia con la distinción entre lo que el analista sabía y lo que creía, es decir, entre manifestar claramente cuál era el hecho y cuál era la opinión del analista. Estas ideas serían usadas posteriormente por Douglas MacEachin para desarrollar lo que la comunidad de inteligencia estadounidense (CI) denominaría los *standards* del analista desde el pensamiento crítico. De este modo, abogar por un mayor énfasis del método científico y del pensamiento crítico en el análisis de inteligencia tiene implicaciones profundas. No estamos hablando de *training* de oficiales de inteligencia, sino de reeducación. En el desarrollo de esta educación es donde los estudios de inteligencia juegan un papel crucial.

En el punto anterior hemos puesto de manifiesto la importancia, para el analista de información, de ser consciente de los procesos de razonamiento, de sus limitaciones y conocer las distintas técnicas de análisis y el impacto de las nuevas tecnologías sobre el análisis. Es necesario ir más allá frente a un futuro incierto, y el recurso al pensamiento crítico es más que importante.

El uso del pensamiento crítico es un proceso, una orientación mental, que incluye tanto procesos cognitivos como dominios de razonamiento efectivo. Su aplicación permite mejorar el análisis en cuestiones complejas donde la información es incompleta, ambigua y en ocasiones distorsionada.

Por *pensamiento crítico* se entenderá el proceso intelectual disciplinado que conceptualiza, aplica, analiza, sintetiza y evalúa de forma activa la informa-

ción obtenida mediante observación, experiencia, reflexión, razonamiento y comunicación, como guía para la acción; «el pensamiento crítico, es un examen activo, persistente y cuidadoso de una creencia o supuesto de los conocimientos a la luz de las bases que lo sustentan y de las conclusiones que derivan de los mismos»<sup>13</sup>.

El pensamiento crítico es esencialmente un proceso activo con uno mismo, más que aprender de las enseñanzas de otros; es decir, es una habilidad cognitiva complementada por conocimientos y actitudes, donde se tiene en cuenta la capacidad de imaginar, de explorar alternativas poco probables, de entender correctamente el entorno o de revisar profundamente los argumentos usados. De este modo, el pensamiento crítico supone estar continuamente cuestionando las asunciones que damos por sentado que están bien o que están mal. El pensamiento crítico entrena la mente del analista y le facilita el aproximarse a los problemas, ayudando a mitigar los efectos de los prejuicios y limitaciones mentales del analista. Es un camino para entender las cosas, no es un objetivo en sí mismo, va más allá de resolver problemas. Aplicar herramientas de pensamiento crítico en el analista requiere:

1. Capacidad para interpretar, lo cual significa mejorar la habilidad para establecer categorías y marcos que permitan encuadrar la información, aumentando así la capacidad de descripción. Ello lleva a una mejor conceptualización de términos mejorando la capacidad de codificación del lenguaje (verbal y no verbal) y su significado.
2. Capacidad de análisis. Detectar y analizar los propios argumentos que sostienen las ideas por medio de las relaciones directas e indirectas entre términos, ideas, expresiones y argumentos, las conclusiones principales, las premisas y razonamientos que sustentan esas conclusiones, elementos adicionales que explican las conclusiones (como orientaciones políticas, creencias, asunciones, etc.).
3. Evaluar la credibilidad de lo expresado. Reconocer los factores relevantes que condicionan la credibilidad de la fuente de información, los contextos, las preguntas, los principios aplicados, los juicios, las opiniones y las creencias y los argumentos, la aceptación y el nivel de verificación y verdad en lo que se razona. Para ello, se evalúan las evidencias y se tiene en cuenta que las informaciones disponibles en ocasiones son ambiguas y contradictorias, a lo que hay que añadir los esfuerzos de contrainteligencia y engaño de los adversarios. La pregunta final que lo resumiese sería: ¿Qué grado de credibilidad tiene esta fuente?
4. Inferir reconociendo premisas y elementos que nos permitan establecer alternativas y conclusiones. La pregunta esta vez sería: ¿Están las inferencias basadas en las evidencias? ¿Llevan estas inferencias a nuevas evidencias?

---

<sup>13</sup> J. Dewey: *Democracy and Education*, New York, McMillan, 1916.

5. Explicar los resultados obtenidos en términos de evidencias, conceptos, metodologías, criterios y consideraciones contextuales; establecer resultados, justificar los procedimientos, presentar argumentos dando razones de por qué se acepta o no algo.

En definitiva, practicar la autocrítica y estar abierto a nuevas posibilidades más allá de nuestras propias creencias y asunciones.

**Si no está orientada a la acción, no tiene consecuencias operativas y no llega a tiempo; no es inteligencia**

Una vez que se ha analizado toda la información y se han extraído las conclusiones pertinentes, hay que configurar el producto final. Existen multitud de productos de inteligencia, y la elección de uno u otro vendrá determinada por las necesidades y las preferencias del consumidor de inteligencia. Antes de presentar cualquier producto de inteligencia, es necesario revisar la consistencia de los argumentos utilizados, contrastar las inferencias realizadas y sopesar la solidez de las conclusiones alcanzadas.

El mensaje que aporta la inteligencia tiene que ser relevante para las necesidades del cliente (con el fin de conseguir credibilidad y aceptación). Es clave estructurar bien la información, presentando correctamente los argumentos utilizados y presentando especial atención a la forma. De igual manera, cualquier producto de inteligencia tiene que ser consistente con el tiempo disponible (siempre escaso), por lo que debe de ser claro, preciso y conciso.

En este punto, el gestor de inteligencia ha de velar para que cualquier producto de inteligencia cumpla con los siguientes requisitos:

- *Exactitud*: todos los datos y fuentes deben ser evaluados para evitar la posibilidad de un error técnico, mala percepción o esfuerzos hostiles dirigidos a confundir.
- *Objetividad*: todos los juicios deben ser evaluados frente a la posibilidad de manipulaciones guiadas por el interés propio o debidas a distorsiones involuntarias.
- *Utilidad*: todas las comunicaciones de inteligencia han de estar hechas de una forma que se facilite la buena comprensión y la aplicabilidad inmediata. Los productos de inteligencia deben de ser compatibles con las capacidades del consumidor para recibir, manipular, proteger y almacenar el producto.
- *Relevancia*: la información ha de estar seleccionada y organizada conforme los requerimientos del consumidor, sin perder de vista sus consecuencias potenciales, y buscando significados suficientemente explícitos conforme a las circunstancias del consumidor.
- *Oportunidad*: la inteligencia tiene que dar respuesta a las necesidades de los consumidores. En este sentido, se refuerza la idea de que la inteligencia está orientada a la acción, ya que la inteligencia tiene que di-

fundirse mientras el contenido todavía es útil por las circunstancias del consumidor.

### **El consumo de inteligencia como objetivo final y punto de partida del proceso**

En términos generales, cualquier producto de inteligencia tiene como misión ayudar a reducir la incertidumbre inherente al proceso de toma de decisiones. El contenido de los productos de inteligencia debe de ser relevante, pero también es clave el «cuándo» está disponible el producto y en qué momento se entrega el mismo<sup>14</sup>. Para que los productos de inteligencia cumplan su función, estos deben de contener un relato contundente, expresado con máxima rotundidad y objetividad, sin emplear más tiempo y extensión que la estrictamente necesaria. La utilidad de la inteligencia exige compatibilidad con las capacidades del destinatario para recibir en tiempo y forma, manipular, proteger y clasificar el producto. Se entenderá objetivo lo basado en datos evaluados y contrastados. A la hora de presentar un producto de inteligencia, el gestor de inteligencia encargado de hacerlo debe de tener en cuenta que un buen análisis de inteligencia debe de ser explicado y contextualizado. La correcta explicación y presentación es necesaria, no solo para mejorar la utilidad del producto sino también para poder calibrar las reacciones de los consumidores, a fin de que el gestor de inteligencia pueda obtener el *feed-back* necesario para mejorar en el futuro y retroalimentar el proceso.

#### 10.1. Suma y sigue.

A pesar de la revolución tecnológica y su repercusión, tanto en la multiplicación de canales como en el número de fuentes de información disponibles, siempre habrá informaciones ocultas, y cierto tipo de información seguirá teniendo la vocación de permanecer oculta. Existirá, por largo tiempo, información a la espera de ser descubierta en un mundo que nunca deja de envolver nuevos puzzles y misterios. Pero, el secreto no es condición ni necesaria ni suficiente de incertidumbre en un mundo en el que, cada vez más, las decisiones de un actor afecta las posiciones de otros. Los procesos de inteligencia juegan un papel importante a la hora de mitigar esta incertidumbre. Sin embargo, no existen fórmulas mágicas que eliminen la incertidumbre existente en todo proceso de toma de decisiones. La inteligencia, bien implementada, es simplemente una herramienta tremendamente útil a ese propósito.

Para ilustrar nuestros argumentos, en este capítulo, hemos intentado realizar una aproximación al campo de la inteligencia desde perspectivas tan-

---

<sup>14</sup> Bruce Berkowitz y Allan Goodman: *Best truth: Intelligence in the Information Age*, New Haven, Yale University Press, 2000, p. 69.

to teóricas como prácticas en vez de hacerlo desde los clásicos puntos de vista estructurales y organizacionales normalmente empleados para explicarla. Se ha optado por la deconstrucción del llamado ciclo de inteligencia para presentar cada una de sus fases, la relación entre ellas, y los actores implicados en las mismas desde el punto de vista de su necesaria imbricación, y también con el propósito práctico de poder abogar por la introducción de la inteligencia –su uso y su puesta en práctica en cualquier marco conceptual– para toda organización, independientemente de su tamaño.

Tal y como apunta Michael Warner, poco se ha hecho hasta el momento para fijar una taxonomía de la inteligencia y explicar su relación con otras disciplinas. Este trabajo es una modesta contribución en ese sentido, que reclama que el campo de estudio de la inteligencia pueda conseguir un marco teórico suficiente que le permita constituirse como una disciplina aceptada e integrada en el marco de las ciencias sociales.

Por último, no querríamos terminar sin subrayar las principales conclusiones que hemos extraído del análisis de las distintas partes del ciclo de producción de inteligencia.

En primer lugar que, inteligencia es algo más que mera información; hablar de inteligencia es hacerlo de información analizada, sintetizada y orientada para su uso como herramienta específica en la toma de decisiones. Pero, inteligencia es también algo más que un mero producto, pues, en buena medida, viene definida por los procesos por los que es transformada en aras a su consumo/utilización.

La inteligencia, también, es algo más que información secreta. Su relación con el secreto es circunstancial y no esencial. Tal y como el Ministerio Británico de Defensa puso de manifiesto en su publicación *Understanding and Intelligence Support to Joint Operations* (JDP 2-00), la obtención de información no se reduce únicamente a métodos secretos y clandestinos. Extrapolada al sector privado, encontramos que tal afirmación está en perfecta sintonía con la realidad, pues casi toda la información es extraída de fuentes abiertas o por lo menos semiabiertas.

Por último, la inteligencia debe estar alineada con la estrategia de la organización, ya que la inteligencia ha de ir guiada por la búsqueda de la capacidad sostenida y sostenible de la organización para prosperar y para progresar en el cumplimiento de su propósito fundamental. Es clave que la inteligencia encuentre su justo lugar en el seno de cada organización y sepa acomodarse a las necesidades específicas de la misma.

## Bibliografía

- ACKOFF R. y GUPTA S. *Scientific method: Optimizing applied research decisions*. New York: Wiley & Sons, 1965.
- AMBROSINI, V., SCHOLLES, K. y JOHNSON, G. *Exploring techniques of analysis and evaluation in strategic management*. Harlow: Prentice Hall, Europe, 2000.
- ANSOFF, H. I. *Corporate strategy: An analytic approach to business policy for growth and expansion*. New York: McGraw-Hill, 1965.
- ARROYO R. *Inteligencia competitiva: Una herramienta clave en la estrategia empresarial*. Madrid: Ediciones Pirámide, grupo Anaya, 2005.
- ASHTON, W. B. «Technical intelligence in business: understanding technology threats and opportunities». *International Journal of Technology Management* 10. Nº. 1 (1995).
- ATTAWAY M. «A review of issues related to gathering and assessing competitive intelligence». *American Business Review* 16. Nº. 1 (1998).
- BARNDT, W. D. *User-directed competitive intelligence: Closing the gap between supply and demand*. Westport: Quorum Books, 1994.
- BAUMARD, Philippe. «Stratégie et surveillance des environnements concurrentiels». Paris: Masson, 1991.
- BERKOWITZ, B. D. y GOODMAN, A. E. *Best truth: Intelligence in the Information Age*. New Haven: Yale University Press, 2000.
- BERMHARDT, D. *Competitive intelligence: how to acquire and use corporate intelligence and counter-intelligence*. London: Prentice Hall, 2003.
- BESSON, B. y POSSIN, J.C. *Du Renseignement à l'intelligence économique*. Paris, Dunod, 1996.
- BETTS Richard. «Intelligence for Policymaking». *The Washington Quarterly* 3. Nº. 3, (1980).
- BETTS, Richard. «Policy-Makers and Intelligence Analysts: Love, Hate or Indifference?». *Intelligence and National Security* 3. Nº. 1, (January 1988).
- BOOKFIELD, S. *Developing Critical Thinkers*. San Francisco, CA: Josie Bass, 1987.
- BOUTHILLER, F. y SHEARER, K. *Assessing competitive intelligence software: A guide to evaluating CI technology*. Medford, N. J.: Information Today, 2003.
- BOWEN W. «Open Source Intelligence». *Janes Intelligence Review* 11. Nº. 11 (Nov. 1999).
- BUNGE, M. *La investigación científica. Su estrategia y filosofía*. La Habana: ciencias sociales, 1991.
- CALOF, J. L. «Competitive Intelligence - For King and Country... and Company». *Business Quarterly* 61. Nº. 3 (1997).
- CARAYON, B. *Patriotisme économique: De la guerre à la paix économique*. Monaco: Editions du Rocher, 2006.

- CARAYON, B. *Intelligence économique, compétitivité et cohésion sociale, Rapport au Premier Ministre*. Paris: La Documentation Française, 2003.
- CHAMPION, B. «A Review of Selected Cases of Industrial Espionage and Economic Spying, 1568-1945». *Intelligence and National Security* 13. Nº. 2, (1998).
- CLAUSER, J. y GOLDAMN, J. *An introduction to Intelligence research and analysis*. Lanham, Md., Scarecrow Press, 2008.
- COBURN, M. *Competitive technical intelligence: A guide to design, analysis, and action*. New York: Oxford University Press, 2004.
- COMAI, A., y PRESCOOT, J. E. *Workbook: Establishing a world-class competitive intelligence function*. Barcelona: EMECOM Editions, 2007.
- COMMISSARIAT général au plan. *Intelligence économique et stratégie des entreprises, rapport présidé par Henri Martre*. Paris: La Documentation Française, 1994.
- CREMADES, A. y DÍAZ MATEY, G. «Información e Inteligencia: una reflexión interdisciplinar». *Revista de Estudios en Seguridad Internacional* 1. Nº. 2, (2015).
- DE BONO, E. *Six thinking hats*. Boston: Little, Brown, 1985.
- DECONCINI, D. «The Role of U.S. Intelligence in Promoting Economic Interests», *Journal of International Affairs* 48. Nº. 1 (1994).
- DEWEY, J. *Democracy and Education*. New York: McMillan, 1916.
- DEWITT, M. *Competitive intelligence, competitive advantage*. Grand Rapids. Mich: Abacus, 1997.
- DÍAZ MATEY, G. *Inteligencia Teórica*. Madrid: La Torre Literaria, 2009.
- DÍAZ MATEY, G. *Los Servicios de inteligencia ante el siglo XXI*. Madrid: Chavin, La torre Literaria, 2010.
- DRUCKER, P. F. «The Rise of the Knowledge Society». *Wilson Quarterly* 17. Nº. 2 (1993).
- DUTKA, Alan F. *Competitive Intelligence for the Competitive Edge*. Lincolnwood, IL: NTC Business Books, 1999.
- ESCORSA, P. y MASPONS, R. *De la vigilancia tecnológica a la inteligencia competitiva*. Madrid: Prentice Hall, 2001.
- ETTORRE, B. «Managing Competitive Intelligence». *Management Review* 84. Nº. 10 (1995).
- FEDORIV, D. «How competitors learn your company's secrets». *Competitive Intelligence Review* 1. Nº. 2 (December 07, 1990).
- FIALKA, J. J. *War by other means: economic espionage in America*. New York: Norton, 1997.
- FLESISHER, C. S. «Using open source data in developing competitive and marketing intelligence». *European Journal of Marketing* 42. Nº. 7-8 (2008).



- FLESHER, C. S. y BLENKHORN, D. L. *Controversies in competitive intelligence: The enduring issues*. Westport, Conn: Praeger, 2003.
- FLESHER, C. S. y BLENKHORN, D. L. *Managing frontiers in competitive intelligence*. Westport, Conn: Quorum Books, 2001.
- FLESHER, C. S. *Business and competitive analysis methods: Effective application of new and classic methods*. Indianapolis: Financial Times Prentice Hall, 2007.
- FULD, L. M. *The new competitor intelligence: The complete resource for finding, analyzing, and using information about your competitors*. New York: J. Wiley, 1995.
- FULD, L. M. *The secret language of competitive intelligence: How to see through and stay ahead of business disruptions, distortions, rumors, and smoke screens*. New York, Crown Business, 2006.
- GARZA RAMOS, A. *Teoría, métodos y técnicas en la investigación social*. México: Ediciones de Cultura Popular, 1974.
- GENTRY, J. A. *Lost promise: How CIA analysis misses the nation; an intelligence assessment*. Lanham, Md.: University Press of America, 1993.
- GIBBONS, P. T. y PRESCOOT, J. E. «Parallel competitive intelligence processes in organizations». *International Journal of Technology Management* 11. N°. 1-2 (1996).
- GILAD, B. *Business war games: How large, small, and new companies can vastly improve their strategies and outmaneuver the competition*. Franklin Lakes, N.J.: Career Press 2009.
- GILAD, B. *Early warning using competitive intelligence to anticipate market shifts, control risk, and create powerful strategies*. New York, N.Y.: American Management Association, 2004.
- GILAD, B. *Business blind spots: Replacing your company's entrenched and outdated myths, beliefs, and assumptions with the realities of today's markets* Chicago, Ill: Probus, 1994.
- HALL, W. M. y CITREBAUM, G. *Intelligence analysis: How to think in complex environments*. Santa Barbara, Calif.: Praeger Security International, 2010.
- HANSEN, J. H. *Japanese intelligence: The competitive edge*. Washington, D.C.: National Intelligence Book Centre, 1996.
- HARDING, R. N. *Corporate intelligence awareness: Securing the competitive edge*. Lakefield, Ont.: Multi-Media Publications, 2006.
- HAZLITT, H. *Thinking as a science*. New York: E. P. Dutton & company, 1969.
- HERMAN, M. *Intelligence Power in Peace and War*. Cambridge: Cambridge University Press, 1996.
- HEUER, Jr. y PHERSON Randolph H. (2010). *Structured Analytic Techniques for Intelligence Analysis*. Washington, D. C.: Congressional Quarterly Press, 2010.

- HEUER, Jr. y PHERSON Randolph H. *Structured analytic techniques for intelligence analysis*. Washington, D.C., CQ Press, 2011.
- HOCK, R. *The extreme searcher's Internet handbook: A guide for the serious searcher*. Medford, N.J.: CyberAge Books, 2007.
- HORN, Robert V. *Statistical indicators for the economic and social sciences*. Cambridge; Hong Kong Cambridge, University Press, 1993.
- HULNICK, Arthur. «The Intelligence Producer-Policy Consumer Linkage: A Theoretical Approach». *Intelligence and National Security* 1, N° 2 (May 1986).
- HUSSEY, D. E. y JENSTER, P. V. *Competitive intelligence and analysis: Turning analysis into success*. Chichester, John Wiley and Sons, 1999.
- JAKOBIAK, François. *L'intelligence économique*. Paris: Editions d'Organisation, 2004.
- JERVIS, Robert. «What's Wrong with the Intelligence Process?». *International Journal of Intelligence and Counterintelligence* 1. N° 1, (1986).
- JUILLET, A. «Du renseignement à l'intelligence économique». *Revue Défense Nationale*. N° 12 (2004).
- JULLIET, A. «Principios y aplicación de la inteligencia económica». *Inteligencia y Seguridad: Revista de análisis y prospectiva*. N° 1 (2006).
- KAHANER, L. *Competitive intelligence: How to gather, analyze, and use information to move your business to the top*. New York: Simon & Schuster, 1997.
- KERKINGER F. *Investigación del comportamiento, técnicas y metodología*. México: Interamericana, 1975.
- KILTZ, L. «Developing Critical Thinking Skills in Homeland Security and Emergency Management Courses». *Journal of Homeland Security and Emergency Management* 6. N° 1 (2009).
- KUHN, T. S. *La estructura de las revoluciones científicas*. México: Fondo de Cultura Económica, 1971.
- LEFEBVRE, S. «A Look at Intelligence Analysis». *International Journal of Intelligence and Counterintelligence* 17. N° 2 (2004).
- LOWENTHAL, M. M. y OSS Academy. *Open source intelligence: Executive overview*. Oakton, Va: OSS Academy, 1998.
- LOWENTHAL, M. M.: *Intelligence: From secrets to policy*. Washington, D.C.: CQ Press, 2009.
- LUX, C. *Competitive Intelligence und Wirtschaftsspionage*. Analyse, Praxis, Strategie, Wiesbaden: Gabler, 2002.
- MARRIN, Stephen, «Intelligence Analysis Theory: Explaining and Predicting Analytic Responsibilities» *Intelligence and National Security* 22. N° 6 (2007).
- MARTIN A. y WILSON P. «The value of non-government intelligence widening the field». *Intelligence and National Security* 23. N° 6 (December 2008).

- MASPONS, R. *Inteligencia competitiva*. Barcelona: Universitat Oberta de Catalunya, Barcelona UOC, 2002.
- MEYER, H. E. *Real-world intelligence: Organized information for executives*. New York: Weidenfeld & Nicolson, 1987.
- MICHAELI, R. *Competitive intelligence: Competitive advantage through analysis of competition, markets and technologies*. Berlin: Springer, 1998.
- MILLÁN, T. y COMAI Alessandro. *Inteligencia Competitiva y Vigilancia Tecnológica, experiencias de implantación en España y Latinoamérica*. Barcelona: Emecom, 2006.
- MILLÁN, T. y COMAI Alessandro. «El desarrollo de la Inteligencia Competitiva en España: un recorrido bibliográfico». *Puzzle - Revista Hispana de la Inteligencia Competitiva*. Nº. 16 (2005).
- MILLÁN, T. y COMAI Alessandro. «Los propósitos de la inteligencia en la empresa: competidora, cooperativa, neutral e individual». *El profesional de la información* 10. Nº. 5 (2001).
- MILLER, J. *Millennium intelligence: Understanding and conducting competitive intelligence in the digital age*. Medford, N. J.: Cyber Age Books, 2000.
- MINISTERIO DE DEFENSA del Reino Unido. Joint Doctrine and Concepts Centre: Joint Warfare Publication 2-00 Intelligence Support to Joint Operations, UK: 2001.
- MINTZBERG, H. *Tracking strategies: Toward a general theory*. Oxford: Oxford University Press, 2007.
- Muller, M. L. *Managing competitive intelligence*. Randburg: Knowledge Resources, 2002.
- MURPHY, C. *Competitive intelligence: Gathering, analysing, and putting it to work*. Aldershot, Hants: Gower, 2005.
- NASHERI, H. *Economic espionage and industrial spying*. Cambridge, UK: Cambridge University Press, 2005.
- PALOP, F. *Vigilancia tecnológica e inteligencia competitiva: su potencial para la empresa española*. Madrid: COTEC, 1999.
- PORTER, M. E. *Cases in competitive strategy*. New York: Free Press, 1983.
- PORTER, M. E. *Competitive strategy: Techniques for analyzing industries and competitors*. New York: Free Press, 1980.
- POSTIGO, J. «La inteligencia competitiva en España: una encuesta sobre su utilización por parte de las empresas exportadoras». *El profesional de la información* 10. Nº. 10 (2001).
- POTTER, E. H. *Economic intelligence and national security*. Ottawa: Carleton University Press, 1998.
- PRESCOTT, J. E. y GIBBONS, P. T. *Global perspectives on competitive intelligence*. Alexandria, Society of Competitive Intelligence Professionals, 1993.

- PRESCOTT, J. E. y MILLER, S. H. (eds.): *Proven Strategies in Competitive Intelligence: Lessons from the Trenches*. New York: John Wiley and Sons, 2001.
- PRESCOTT, J. E. «The Evolution of Competitive Intelligence». *International Review of Strategic Management* 6 (1995).
- PRESCOTT, J. E. *Advances in competitive intelligence*. Vienna, Va.: Society of Competitor Intelligence Professionals, (SCIP), 1989.
- PRUNCKUN, H. *Handbook of scientific methods of inquiry for intelligence analysis*. Lanham: Scarecrow Press, 2010.
- QUIGGIN, T. *Risk assessment and horizon scanning: National and economic security intelligence in an uncertain age*. Hackensack, N. J.: World Scientific, 2007.
- RAFALOWSKI, M. «Competitive Analysis and Strategic Planning for Clinical Research Sites». *Journal of clinical research and drug development* 8. N°. 4 (1994).
- RAGIN, C. C. *The Comparative Method, Moving Beyond Qualitative and Quantitative Strategies*. London: University of California Press, 1987.
- RANDOM, R. A. «Intelligence as a Science», *Studies on Intelligence CIA* (22 September 1993).
- RICCARDI, R., RODRIGUES, L. C. y COLOMBO, P. *Inteligencia competitiva en los negocios y en las organizaciones*. Buenos Aires, Argentina: Ediciones Macchi, 2003.
- ROUACH, D. *La veille technologique et l'intelligence économique*. Paris: Presses Universitaires de France, 1996.
- RUIZ NAVARRO, J. y CARMELO ORDAZ, C. «Competitividad regional y recursos intangibles: un análisis comparado Andalucía-España,». Universidad de Cádiz: Servicio de Publicaciones, 2000.
- SALLES, M. «Decision-making for SMEs and Information Requirements for Competitive Intelligence». *Production Planning and Control* 17. N°. 3 (2006).
- SHARP, S. *Competitive Intelligence Advantage How to Minimize Risk, Avoid Surprises, and Grow Your Business in a Changing World*. Epub Edition, New York, John Wiley y Sons, 2009.
- SPULBER, D. F. *Global competitive strategy*, Cambridge: Cambridge University Press, 2007.
- STEWART, T. A. *Intellectual capital: The new wealth of organizations*. London: Nicholas Brealey, 1997.
- UK Ministry of Defence, Development, Concepts and Doctrine Centre. *Joint Doctrine Publication 2-00: Understanding and Intelligence Support to Joint Operations*. London, 2011.
- UNITED STATES OF AMERICA. *Department of Defense dictionary of military and associated terms*. Washington, D.C.: Joint Chiefs of Staff, 1972.

- VERGARA, J. C.; COMAI, A. y TENA Millán, J. *Software para la inteligencia tecnológica de patentes: evaluación de aplicativos informáticos y necesidades de inteligencia tecnológica*. Barcelona: EMECOM, Puzzle, 2006.
- VIBERT, C. (2004). *Competitive intelligence: A framework for web-based analysis and decision making*. Mason, Ohio: Thomson/South-Western.
- VIBERT, C. *An introduction to online competitive intelligence research: Search strategies, research case study, research problems, and data source evaluations and reviews*. Mason, Ohio: Thomson/Texere, 2004.
- VRIENS, D. *Information and communications technology for competitive intelligence*. Hershey, P.A.: Idea Group Publishing Inc., 2003.
- WALKER, G. *Modern competitive strategy*. Boston: McGraw-Hill/Irwin, 2004.
- WALTZ, E. *Knowledge Management in the Intelligence Enterprise*. Boston: Artech House, 2003.
- WARNER M. «Wanted: A Definition of Intelligence» *Studies in Intelligence* 46. N° 3 (2002).
- WATERS, T. J. *Hyperformance: Using competitive intelligence for better strategy and execution*. San Francisco: Jossey-Bass, 2010.
- WEST, C. *Competitive intelligence*. Houndmills, Basingstoke, Hampshire: Palgrave, 2001.
- WESTPHAL, C. R. *Data mining for intelligence, fraud, & criminal detection: Advanced analytics & information sharing technologies*. Boca Raton: CRC Press, 2009.
- WRIGHT, Jeffrey W. «Intelligence and Economic Security», *International Journal of Intelligence and Counterintelligence* 5. N° 2 (Summer 1991).
- ZANASI, A. «Competitive Intelligence through Data Mining Public Sources». *Competitive Intelligence Review* 9. N° 1 (1998).
- ZANASI, A. «Text Mining and Its Applications to Intelligence, CRM, and Knowledge Management». *Advances in management information series*. vol. 2, Southampton, UK: WIT Press, (2005).



## Capítulo quinto

### Beneficios de la inteligencia en apoyo de la política/ estrategia de una organización

Valentín Martínez Valero

#### Resumen

La situación de seguridad actual, tanto a nivel nacional como internacional, es, con mucho, más difícil que lo ha sido en el pasado.

En un entorno tan peligroso e imprevisible, donde se constata que la incertidumbre es muy superior a la vivida en épocas pretéritas, la necesidad de una alerta temprana se convierte en vital e imperativa. De ahí, la urgente necesidad de reforzar las capacidades de los diferentes servicios de inteligencia estatales y, muy especialmente, de asegurar un funcionamiento sincronizado/coordinado del conjunto de todos ellos, a nivel nacional, y de establecer una fuerte y estrecha colaboración entre los mismos, a nivel internacional.

Por otro lado, la inteligencia es muy necesaria también en muchos sectores de la actividad privada, tanto en el campo empresarial como en el financiero, sanitario, etc., en los que, representa un elemento imprescindible en el apoyo a las personas que deben tomar las necesarias decisiones en cada momento.

Con la finalidad de proporcionar a los potenciales usuarios de inteligencia un buen entendimiento de la materia, se introducen y explican los conceptos básicos, la tipología y las diferencias entre las diferentes clases presentadas, así como el significado de las diferentes acepciones del término: como

producto, como proceso y como servicio, llevando al lector el claro mensaje de aquello que el usuario puede, y no puede, esperar de la inteligencia.

#### **Palabras clave**

Inteligencia, servicios de inteligencia, apoyo a la toma de decisiones, tipos de inteligencia, inteligencia como producto, inteligencia como proceso, inteligencia como servicio, comunidad de inteligencia.

#### **Abstract**

The current security situation, both at national and international levels, is by far more difficult than ever.

In such a dangerous and unpredictable environment, where uncertainty is much higher than in the past, the need for early warning becomes vital and imperative. Hence the pressing need for reinforcing the capabilities of the various national intelligence services, and above everything, to ensure the synchronized /coordinated work of all of them at national level, as well as to establish a strong and close collaboration among them at the international one.

On the other hand, intelligence is also very much required in many sectors of the private activity, both in the business world and in the financial, medical, etc. where it is indispensable to support the decision-makers any time.

With the aim of providing the potential users with a good knowledge on the matter, intelligence basic concepts, types and the differences between them, as well as the diverse meanings of it: as a product, a process or a service, are presented and explained, conveying to the user the clear message of both what he can, and cannot, expect from intelligence.

#### **Keywords**

Intelligence, Intelligence services, Support to Decision-makers, Types of Intelligence, Intelligence as a product, Intelligence as a process, Intelligence as a service, Intelligence Community.



## Introducción

«Debemos esperar lo inesperado» (*We must expect the unexpected*), es frase que el editorial «Britain Begins to Rearm», correspondiente a los días 28-29 del pasado mes de noviembre, del rotativo *The Wall Street Journal* pone en boca del primer ministro inglés, David Cameron, haciendo referencia a la situación de seguridad mundial, y en concreto de su país y de los llamados países occidentales.

Los trágicos atentados terroristas de índole yihadista perpetrados en París el 13 de noviembre han hecho saltar todas las alarmas en casi todos los países; en respuesta a ello, el mismo editorial proporciona información muy significativa acerca de las medidas con las que el Reino Unido planea afrontar los nuevos retos y amenazas. Con un monto total estimado en 2 billones de libras esterlinas (£) dedicados a la adquisición de armas adicionales para sus fuerzas especiales, 20 nuevos drones Reaper de largo alcance, 9 aviones P8 Poseidon, así como nuevas escuadrillas de aviones Eurofighter Typhoon basados en tierra, y F-35 basados en la mar, se incluye así mismo la contratación de 1.900 nuevos agentes de inteligencia, tanto nacionales como extranjeros. Y todo ello para, como el propio *premier* aclara: «estar seguros de que tenemos la versatilidad y los medios para responder a nuevos retos y amenazas a nuestra seguridad».

Después de reseñar las variaciones sufridas por el presupuesto de defensa del Reino Unido desde la desaparición del Pacto de Varsovia hasta nuestros días, y de identificar los problemas que acarrearán las reducciones aplicadas, en la creencia de que el mundo permanecerá pacífico sin la existencia de una fuerte y creíble capacidad de disuasión, el editorial concluye con una frase categórica que merece ser resaltada en tanto en cuanto afecta de manera directa a nuestro país: «Mr. Cameron ha dado un muy positivo paso adelante, y sus aliados de la OTAN deberían seguir su ejemplo».

La información comentada facilita significativamente el poner en contexto, tanto la materia que nos ocupa en este documento, la disciplina denominada inteligencia, como su importancia para una organización; en este caso, un Estado. Como se puede apreciar, y es una manifestación más de lo que ya ha ocurrido en otros países, como Francia, las nuevas amenazas y retos a la seguridad han motivado un incremento de sus respectivas capacidades de inteligencia, amén de otras medidas de variado signo. Sin embargo, en un entorno tan peligroso e imprevisible, donde se constata que la incertidumbre es muy superior a la vivida en épocas pretéritas, la necesidad de prevenir, en la medida de lo posible, se convierte en vital e imperativa. De ahí, la consecuente necesidad de reforzar las capacidades de los diferentes servicios de inteligencia y, muy especialmente, de asegurar un funcionamiento sincronizado/coordinado del conjunto de todos ellos; lo que en muchos de estos países se conoce como su «comunidad de inteligencia».

En la publicación *Intelligence Community–Consumer’s Guide*, de 2009, dirigida fundamentalmente a los miembros de la comunidad de inteligencia norteamericana, David R. Shedd, subdirector para Policy, Plans, and Requirements de Inteligencia Nacional, de la Oficina del Director Nacional de Inteligencia, decía:

*«Dear Colleagues: No single person or organization can protect our Nation from the many and varied threats we face today. These threats, from looming terrorist plots, to pandemic disease, to the proliferation of weapons of mass destruction, require that we, as a government, work together.*

*As we have articulated in the Intelligence Community (IC)’s Vision 2015, we must partner with intelligence consumers to meet the need for more timely and unique intelligence. In order to enhance our relationships, it is important for consumers to understand the mission, background, opportunities, and challenges facing the IC. We have published this handbook with this very thought in mind—to broaden your understanding of our work and to help us become stronger partners in protecting our Nation».*

Los párrafos anteriores son muy importantes para dar sentido a este documento, puesto que, ciertamente, la labor de los diferentes servicios y órganos dedicados a elaborar la inteligencia que un país u organización necesita, resulta una labor baldía si los destinatarios de la misma no son conscientes de los múltiples aspectos inherentes a la misma; de lo que inteligencia puede, y también de lo que no es capaz de hacer por dichas organizaciones; de sus capacidades y de sus limitaciones; de los medios mínimos necesarios para desempeñar sus cometidos; de su campo de actuación, y de los plazos de tiempo en que las actividades deberán tener lugar según los objetivos que, en cada caso, se pretendan alcanzar.

Así, pues, a modo de introducción de los objetivos de este capítulo, creemos conveniente y apropiado recoger tanto los conceptos como el orden de exposición que se realiza en el antes citado documento, por considerarlos perfectamente ajustados a la finalidad perseguida en esta publicación.

Empezaremos, por tanto, recogiendo lo que, la comunidad de inteligencia norteamericana, entiende por inteligencia:

*«Conforme a la Ley “Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA)”, Inteligencia Nacional y el término “Inteligencia relacionada con la seguridad nacional” se refieren a todo tipo de inteligencia, cualquiera que sea la fuente de la que se obtenga, incluyendo la información obtenida dentro y fuera de los Estados Unidos, que, concierna, siempre que sea consistente con cualquier directiva emanada del presidente, a más de una agencia gubernamental, y que implique:*

*Amenazas a los Estados Unidos, su población, propiedades o intereses; El desarrollo, proliferación o empleo de armas de destrucción masiva; o Cualquier otro asunto relacionado con la seguridad nacional interior (del territorio de los EE.UU.)».*

## Beneficios de la inteligencia en apoyo de la política...

De igual manera, resulta muy interesante la descripción del empleo que el Gobierno norteamericano hace de dicha inteligencia:

*«El Gobierno USA emplea la inteligencia para entender y mejorar las consecuencias de sus decisiones en seguridad nacional. La inteligencia ayuda a la toma de decisiones políticas, acciones militares, negociaciones internacionales, e interacciones con los contactos en otros países al nivel de ejecución. En algunas circunstancias, puede ayudar también a los responsables y elementos de reacción inmediata en el ámbito de la seguridad interior [en el ámbito del territorio de los EE.UU.]».*

Al igual que cuando se trata de cualquier otra herramienta o servicio, y aunque pudiera resultar obvio repetirlo, la inteligencia alcanza su mayor utilidad cuando los usuarios/destinatarios de la misma comprenden perfectamente lo que pueden y no pueden razonablemente esperar de ella. Mientras las leyes, capacidades, políticas, y estándares están en continuo cambio, el entender claramente esa diferencia permitirá al usuario de la inteligencia el obtener el máximo rendimiento de este recurso.

Es por ello que, en el citado documento, se manifiesta de forma explícita y sin ambigüedad que el usuario norteamericano puede esperar de la inteligencia servicios como los siguientes:

- Proporcionar ventaja en la toma de decisiones, mejorando el proceso de la toma de decisión de consumidores y socios, a la vez que se niega a los enemigos.
- Alertar de potenciales amenazas.
- Entender mejor los acontecimientos clave actuales.
- Conocimiento de la situación.
- Valoraciones estratégicas de largo plazo sobre asuntos de permanente interés.
- Ayuda en la preparación de reuniones de alto nivel, que incluyan temas relacionados con la seguridad nacional.
- Entrevistas y apoyos de seguridad previos a desplazamientos/viajes.
- Informes sobre temas concretos, bien como parte de informes regulares o a petición, cuando se trate de necesidades a corto plazo.
- Recopilación del conocimiento en los Estados Unidos acerca de personas buscadas (de interés). En este ámbito, los Estados Unidos disponen de dos potentes fuentes de información: TIDE (Terrorist Identities Datamart Environment), repositorio centralizado de información clasificada en el que se encuentran los datos de los terroristas extranjeros conocidos o sospechosos; y la TSDB (Terrorist Screening Database), base de datos no clasificada operada por el FBI, en la que se encuentran almacenados los nombres de todos los terroristas conocidos o sospechosos acerca de los que tiene información el Gobierno de los EE.UU. A esta base de datos tienen acceso los agentes de la ley a todos los niveles del gobierno, y también todas las organizaciones del Gobierno Federal (tales como el

Ministerio de Exteriores), que tengan necesidad de realizar la comprobación del nombre de algún individuo.

Puesto que las expectativas del usuario han de estar basadas en la realidad, si importante es que este sea muy consciente de lo que la inteligencia puede proporcionarle, es igualmente importante que sea conocedor de aquellas otras facetas en las que la actividad de inteligencia nunca le va a poder ser de utilidad. El referido documento lo explicita diciendo que la inteligencia NO puede:

- Predecir el futuro. Inteligencia puede proporcionar una valoración o un juicio sobre posibles escenarios o evoluciones, pero no puede en forma alguna predecir con certeza lo que ocurrirá.
- Violar las leyes o la Constitución de los EE.UU.

### Ámbitos de aplicación de la inteligencia

Habiendo partido de un entorno y un problema que a cualquier ciudadano de cualquier país le resulta de interés y le es más o menos familiar; es decir, definido el marco de reflexión, es posible dar un paso más y entrar en materia, empezando por considerar, de una forma resumida, los campos en los que la disciplina inteligencia es de aplicación, para, más adelante, y en la medida de lo posible, profundizar en aquellos otros que, a nuestro juicio, tienen una mayor relevancia en el contexto actual.

Para ello, nada mejor que tomar como referencia la Ley 11/2002, de 6 de mayo, reguladora del Centro Nacional de Inteligencia, al que se encomienda como misión principal la de proporcionar al Gobierno la información e inteligencia necesarias para prevenir y evitar cualquier riesgo o amenaza que afecte a la independencia e integridad de España, los intereses nacionales y la estabilidad del Estado de derecho y sus instituciones. Y ello, llevando a cabo las actividades conducentes 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» (artículo 4a de la citada Ley).

Exceptuando el ámbito militar, del que, se puede deducir por lo anterior, el responsable exclusivo sería el Centro de Inteligencia de las Fuerzas Armadas (CIFAS), los campos de actividad del Centro Nacional de Inteligencia que resultan de interés para satisfacer la finalidad perseguida por el Gobierno de la nación, especificados en el citado artículo, abarcan prácticamente todos aquellos que también pudieran ser de interés parcial o total para cualquier otro tipo de organización.

Dado que la Ley contempla que el CNI pueda llevar a cabo sus actividades tanto fuera como dentro del territorio nacional, parece lógico deducir que, en este ámbito, deberán existir procedimientos que contemplan/regulen la

necesaria coordinación de aquellas con las que realizan los organismos de información/inteligencia de los cuerpos y fuerzas de seguridad del Estado.

Como se ha expresado anteriormente, la Ley 11/2002 asigna al Centro Nacional de Inteligencia la misión de «proporcionar al Gobierno la información e inteligencia necesarias para prevenir y evitar cualquier riesgo o amenaza que afecte a la independencia e integridad de España, los intereses nacionales y la estabilidad del Estado de derecho y sus instituciones». Ante lo cual, el lector puede razonablemente preguntarse en qué consistirá esa «inteligencia» que se cita; y es el artículo 1 de la propia Ley el que aporta una primera idea del significado, al expresar que «El Centro Nacional de Inteligencia es el organismo público responsable de facilitar al presidente del Gobierno y al Gobierno de la nación las informaciones, análisis, estudios o propuestas que permitan prevenir y evitar cualquier peligro, amenaza o agresión contra la independencia o integridad territorial de España, los intereses nacionales y la estabilidad del Estado de derecho y sus instituciones».

Como paso previo a la exposición de inteligencia como producto, proceso y organización, proponemos al lector considerar la redacción del artículo anterior desde un punto de vista lo más amplio posible, lo que nos llevaría a interpretar la actividad de inteligencia como un «servicio» realizado por organizaciones específicas, que llevan a cabo una serie de actividades propias de su campo de especialización, con la finalidad de apoyar la toma de decisiones por parte de un usuario (persona física u organización).

Entremos pues, en materia, empezando por conocer lo que se entiende por inteligencia. Aunque es posible encontrar bastantes definiciones diferenciadas en detalles más o menos importantes, proponemos emplear aquí una que, en su día, recogía el manual *AAP-6, NATO Glossary of Terms and Definitions (edición de 2012)*<sup>1</sup>, en razón a su más amplia perspectiva. En dicho documento se define inteligencia como «el “producto” resultante del procesamiento de información referente a naciones extranjeras, fuerzas o elementos hostiles o potencialmente hostiles, o áreas de operaciones actuales o futuras. El término se aplica también a la “actividad”, que genera el producto, y a la “organización” responsable de dicha actividad»<sup>2</sup> (NATO AAP-6).

Es, por ello, muy conveniente tener muy presente el contexto en que se emplee la palabra para no caer en error, ya que, dependiendo de este, podremos

<sup>1</sup> En febrero de 2015 se ha publicado el manual *Informal interorganizational military glossary of abbreviations, terms and definitions related to Conflict Prevention (CP) and Defence and related security Capacity Building (DCB)*, en el que se recogen términos y definiciones en los ámbitos OTAN, UE y ONU. En aras del consenso, la definición de inteligencia en esta más reciente publicación, es ligeramente diferente a la utilizada en este capítulo.

<sup>2</sup> Intelligence is the product resulting from the processing of information concerning foreign nations, hostile or potentially hostile forces or elements, or areas of actual or potential operations. The term is also applied to the activity, which results in the product and to the organization engaged in such an activity.

estar refiriéndonos al producto, al proceso, e incluso a la organización que lo genera, sin que, a veces, sea fácil distinguir o separar una acepción de otra.

### La inteligencia como producto

A los fines que nos ocupan, el producto tiene una importancia extrema, por cuanto es, mediante su utilización en el proceso de la toma de decisiones, cuando la disciplina inteligencia adquiere su auténtico valor. Por ello, el que el usuario de ese producto tenga perfectamente claro tanto el valor intrínseco asociado al mencionado producto, como la compleja actividad que lo hace posible, resulta de una importancia extrema a los fines pretendidos con este documento. En consecuencia, se inicia este recorrido por el mundo de la inteligencia exponiendo los aspectos más significativos en lo que a dicho producto se refiere para, seguidamente, presentar, con una extensión adecuada, el proceso y actividades necesarias para la generación de inteligencia, y finalizar considerando la importancia y aspectos relevantes acerca de la organizaciones dedicadas al desempeño de dicha disciplina, haciendo especial mención a los profesionales de la misma, componente esencial del sistema.

Hacer llegar al lector la idea de que inteligencia no es información, sino el resultado de un proceso que, perfectamente estructurado y rigurosamente realizado, permite extraer conocimiento de toda la información disponible relacionada con el problema de que se trate, es esencial para llegar a comprender su valor y sus limitaciones. Sin embargo, confundir inteligencia con información es un error excesivamente presente en muchos campos de aplicación, en los que se concede poca o ninguna importancia a la rigurosa aplicación de las metodologías que permiten llegar a ver lo que está presente en la información, pero que no todos son capaces de detectar.

En palabras de William S. Brei<sup>3</sup>, «Inteligencia es más que información. Es conocimiento que ha sido especialmente preparado para las circunstancias específicas de un usuario. La palabra conocimiento resalta la necesidad de la participación humana. Los sistemas de obtención de información producen [...] datos, no inteligencia; solo la mente humana puede proporcionar ese toque especial que da sentido a los datos según las diferentes necesidades de los usuarios. El proceso especial que define parcialmente la inteligencia es la continua obtención, verificación, y análisis de información que permite comprender el problema o situación de forma clara y adaptar seguidamente el producto al contexto de las circunstancias del usuario. Si falta cualquiera de esos atributos esenciales, el producto sigue siendo información en vez de inteligencia».

---

<sup>3</sup> Captain William S. Brei. «Getting Intelligence Right: The Power of Logical Procedure», *Occasional Paper Number Two* (Washington, D. C.: Joint Military Intelligence College, January 1996).

Hablar de inteligencia en abstracto resulta un tanto frustrante. Inteligencia, como producto empleado para reducir la omnipresente incertidumbre asociada al proceso de toma de decisiones, está íntimamente ligada al problema a que se enfrenta la persona que ha de decidir, y, por ello, resulta estar también asociada a la planificación estratégica de la organización apoyada, cuando esta actividad se lleve a cabo, de forma más o menos organizada, en la misma. Y esto es así porque, en la mayoría si no en todos los casos, las decisiones se adoptan con la finalidad de alcanzar los objetivos de la organización, cualquiera que sea el nivel en que estos se encuentren.

Como dice muy acertadamente Michel Porter: «... Las empresas [las organizaciones] que no tengan una "estrategia", sean grandes o pequeñas, son muy vulnerables y serán derribadas por los vientos de la competencia en el corto plazo...». En suma, incluso en las organizaciones pequeñas, es posible contemplar diferentes niveles (o aspectos) que requieren adoptar las decisiones más apropiadas para la consecución de los objetivos pretendidos. En cualquiera de esos casos/niveles, la toma de una decisión implica, dicho de una forma sencilla, definir la forma en que se pretende alcanzar dichos objetivos y los recursos que, para ello, se dedicarán. Habitualmente, la propia dinámica de la organización implica la necesidad de adoptar decisiones cuyos efectos se manifestarán en plazos de tiempo más o menos dilatados, lo que conllevará la necesidad de tener en cuenta aquellos factores que configuren esos escenarios de futuro a más corto o largo plazo.

Esencialmente, lo anteriormente descrito hace que se contemplen diferentes niveles en la toma de decisiones, que, tradicionalmente, se suelen reducir a tres: estratégico, operacional y táctico; en ese orden, de más largo a más corto plazo, en el ámbito militar, mientras que, en el ámbito empresarial, suelen invertirse los dos últimos. Sin embargo, a este respecto, es preciso aclarar que «operacional» y «operativo» no son términos intercambiables, por cuanto, aunque sean adjetivos similares, su significado es completamente diferente. A la hora de diferenciar dichos niveles, es preciso contemplar los objetivos, plazos, necesidades, y factores a considerar en el estudio de la situación o análisis del problema a que se enfrenta quien decide.

Nos encontraremos en el nivel estratégico cuando la decisión se ha de tomar al máximo nivel de la organización, implica la realización de actividades cuyos objetivos se deberán alcanzar después de periodos de tiempo significativamente largos, así como disponer de amplios plazos de tiempo; y, en el análisis del problema, habrán de ser tenidos en cuenta una muy amplia variedad de factores (políticos, geográficos, históricos, económicos, tecnológicos, sociológicos, etc.) según cada caso.

En el nivel táctico, por el contrario, las decisiones se toman, en muchos casos, en los estratos inferiores de la organización; sus objetivos se encuentran materialmente al alcance de la mano, y requieren prácticamente actuaciones inmediatas o en tiempo real; el problema es el adversario, al que se

disputa el objetivo a alcanzar en el entorno (geográfico, económico, tecnológico, sociológico, etc.) inmediato de que se trate, que habitualmente será bien conocido por ambas partes.

El nivel operacional es el responsable de organizar convenientemente las actuaciones del nivel táctico, de forma que, como consecuencia de los resultados de estas, la organización alcance los objetivos fijados en la decisión tomada en el nivel estratégico.

El denominador común en todos los referidos niveles es que, con plazos de tiempo más largos o más cortos, considerando más o menos factores, etcétera, en todos ellos se adoptan decisiones. Y es precisamente por ello, en todos y cada uno de esos niveles, las personas que deban tomarlas habrán de disponer de la inteligencia necesaria para reducir la incertidumbre a la que se enfrentan.

Pero, como se ha expresado anteriormente, y es muy importante no perder la perspectiva, la inteligencia se extrae (se «destila») de la información disponible relacionada con el problema de que se trate y, resulta casi innecesario decir que, siendo único el problema al que se enfrenta la organización en una determinada situación, será igualmente único el producto inteligencia, aunque estará disponible para todos los niveles. Sin embargo, no lo será la aplicación que, de ese producto, se hará en cada nivel: tendrán un carácter y una finalidad predictiva cuando se aplique al nivel estratégico (lo que permitirá establecer directivas y planes corporativos y/o departamentales a largo plazo), mientras que, al nivel operacional, deberá considerarse como de naturaleza estimativa (para facilitar la concepción, planeamiento y conducción de las operaciones departamentales), y finalmente, al nivel táctico, su naturaleza será meramente descriptiva (para permitir el planeamiento y conducción de las operaciones de las unidades de negocio, cuya actuación tiene lugar en tiempo real). Es por ello que, aunque de forma impropia, porque, como queda dicho, el proceso de elaboración de inteligencia arroja un único producto que procede de un único conjunto de información, se suele hablar de inteligencia estratégica, operacional y táctica, asociando cada una de ellas al respectivo nivel de decisión.

Antes de pasar a exponer otros aspectos de inteligencia, procede traer a colación en este punto un término que suele ser motivo de confusión para las personas poco familiarizadas con dicha disciplina. En ocasiones, incluso por parte de algún ensayista, se ha cometido el error de confundir dos voces aparentemente intercambiables: inteligencia estratégica e inteligencia a largo plazo. El factor tiempo está, efectivamente, presente en ambos casos, y precisamente es el motivo de la confusión, porque la inteligencia necesaria para la toma de decisiones estratégicas (vulgo, inteligencia estratégica) se refiere a aquella necesaria para alcanzar objetivos (consecuencias) en el largo plazo, mientras que la inteligencia a largo plazo es aquella que se consigue elaborar a partir de información que se va obteniendo a lo largo de



amplios periodos de tiempo, a fin de responder a una necesidad de carácter permanente de un usuario a lo largo de un extenso periodo de tiempo, con independencia del nivel de decisión (estratégico, operacional o táctico) en que este se encuentre. El ejemplo típico es la inteligencia asociada a actividades que requieren muy largos periodos para su materialización (p. e. el programa nuclear de un país; el desarrollo de nuevas armas, etc.) y, por ello, según el caso de que se trate, puede tener carácter estratégico o no, pero, en cualquier caso, ambos términos no son, como queda expuesto, intercambiables.

Por otro lado, se distinguen tres tipos de inteligencia: básica, actual y de alertas. La primera es la que se precisa sobre cualquier asunto para poder ser utilizada de referencia material en la formulación de planes y en la elaboración de la información posterior, tiene cierto carácter de permanencia, se conserva en bases de datos y se actualiza continuamente. Se emplea principalmente para establecer el escenario inicial y cubrir las necesidades de inteligencia (NI) relativas a elementos de carácter permanente en el tiempo. Incluye los antecedentes e historia reciente del área y/o asunto en cuestión y, en su elaboración, se deben tomar en consideración todos los factores, tanto del entorno como del adversario/competidor, que influyen o pueden influir en la evolución de la situación.

Por su parte, la «inteligencia actual» es la que refleja la situación del momento, tanto a nivel estratégico como operacional o táctico. Se refiere a la situación actual y los acontecimientos en curso, y proporciona una evaluación en tiempo real de las capacidades e intenciones de cualquier adversario/competidor que posea un potencial susceptible de constituir una amenaza.

Finalmente, la «inteligencia de alertas» valida escenarios (hipótesis) que predicen hechos futuros; proporciona alertas a la dirección de nivel estratégico y se basa en «indicadores críticos», que son hechos que prueban o eliminan una hipótesis.

Por otro lado, según la naturaleza de la fuente o del órgano de obtención que la explota, se diferencian un significativo número de disciplinas cuya denominación hace referencia a los mencionados orígenes. Son las denominadas «INT»<sup>4 5</sup>:

---

<sup>4</sup> HUMINT, o inteligencia de fuentes humanas; IMINT, o inteligencia de imágenes; OSINT, o inteligencia de fuentes abiertas; TECHINT, o inteligencia técnica; MASINT, o inteligencia de medición y firma; ACINT, o inteligencia acústica; MEDINT, o inteligencia sanitaria; RADINT, o inteligencia de [radiaciones] radar; y SIGINT, o inteligencia de señales (en la que, habitualmente, se diferencian dos ramas: COMINT, o inteligencia de comunicaciones; y ELINT, o inteligencia electrónica).

<sup>5</sup> Aunque en su día fue una disciplina independiente, en la actualidad, IMINT se considera incluida en el término GEOINT: *the exploitation and analysis of imagery and geospatial information to describe, assess, and visually depict physical features and geographically referenced activities on the Earth. GEOINT consists of imagery, imagery intelligence [IMINT], and geospatial information.*



Figura 5-1. Clases de inteligencia según la fuente o el órgano de obtención

Existen otras formas de clasificar la inteligencia, que no han sido muy conocidas durante años fuera del ámbito estricto de los profesionales de la disciplina, pero las especiales circunstancias y el dinamismo que ha supuesto la globalización en el mundo actual, han hecho que algunas de ellas hayan adquirido una creciente notoriedad e importancia para la vida de las empresas y de los Estados. Así, por ejemplo, según la temática, se pueden considerar la inteligencia biográfica; económica; geográfica; militar; política; sociológica; científica y técnica; de transporte y comunicaciones.

Otra forma que se puede considerar para clasificar el producto inteligencia es según el uso que se dé a la misma; así se puede hablar de inteligencia actual estimativa, operacional, de investigación; científica y técnica, o de alertas<sup>6</sup>.

A partir de los conceptos y métodos aplicados principalmente en el ámbito militar, en el mundo empresarial se han desarrollado una serie de disciplinas que, con el transcurso de los años, han adquirido carta de naturaleza y, como queda dicho anteriormente, una indiscutible y creciente importancia. Entre ellas, merecen destacarse:

La inteligencia de negocios (Business Intelligence), que incluye las metodologías, herramientas y sistemas utilizados en el proceso de planificación estratégica de la organización de que se trate, facilitando la captura, almacenamiento, acceso y análisis de los datos corporativos para ayudar en la toma de decisiones.

La inteligencia competitiva, que incluye la obtención ética y legal de información acerca de organizaciones (empresas) competidoras, así como el análisis de la misma en lo que se refiere a capacidades, vulnerabilidades e inten-

<sup>6</sup> Lisa Krizan. *Intelligence Essentials for Everyone*.

ciones de estas<sup>7</sup>. En algunos ámbitos, este tipo de inteligencia se denomina también «de competidores», mientras que, por inteligencia competitiva (o mejor, inteligencia para competir), se entiende el conjunto de acciones que incluyen la definición, obtención, análisis y difusión de inteligencia acerca de productos, clientes o usuarios, competidores y cualquier otro aspecto del entorno, necesarios para apoyar la toma de decisiones al nivel estratégico de la organización/empresa de que se trate.

Inteligencia tecnológica, conjunto de estrategias y herramientas enfocadas a la administración y creación de conocimiento mediante el análisis de datos (de carácter técnico) existentes en una organización o empresa, y fuera de ella. Relacionada con ella, la vigilancia tecnológica consiste en el conjunto de acciones sistemáticas y coordinadas de búsqueda, tratamiento, análisis y difusión de toda información (técnica), útil para una organización en el proceso de toma de decisiones y definición de su política estratégica.

Inteligencia de mercado, consiste en información principalmente externa, obtenida y analizada por una empresa acerca de mercados en los que pretende participar, con la intención de utilizarla en su toma de decisiones. La inteligencia de mercado se puede utilizar para evaluar oportunidades de entrada en un mercado, y para formular planes de desarrollo de mercado y estrategias de penetración.

Inteligencia económica, entendida como el esfuerzo coordinado de obtención, tratamiento y difusión, con propósitos de explotación, de información útil para los operadores económicos, incluyéndose en este esfuerzo la protección de la información considerada sensible para las compañías interesadas (Comisión Europea), o como una actividad que consiste en obtener, analizar, valorar, difundir y proteger la información económica estratégica, a fin de reforzar la competitividad de un Estado, de una empresa o de un organismo de investigación (Delegado Interministerial para la Inteligencia Económica [D2iE], Francia).

### La inteligencia como proceso: el ciclo de inteligencia

Analizado, aunque de forma bastante somera, el producto inteligencia, consideramos conveniente introducirnos en el proceso que permite generarla: el denominado ciclo de inteligencia. El término procede del ámbito militar, donde ha sido utilizado durante décadas sin modificaciones sensibles, pasando a ser adoptado, primero, por organizaciones gubernamentales del ámbito policial y, posteriormente, por organizaciones civiles, tanto en el mundo empresarial, como en el académico y en las dedicadas a labores de consultoría, entre otras muchas.

---

<sup>7</sup> SCIP: Strategic and Competitive Intelligence Professionals.

El ciclo de inteligencia consiste en un conjunto de pasos repetidos e interrelacionados, mediante los cuales se añade valor a las entradas originales (generalmente, información) y se genera un producto sustancialmente diferente, transformado y mejorado. Esta transformación o mejora es lo que distingue al Ciclo de inteligencia de una actividad simplemente cíclica.

En este punto, y para que el ciclo de inteligencia encuentre su encaje correcto, debemos recuperar lo expuesto anteriormente acerca del proceso de toma de decisiones en el ámbito de la planificación estratégica de las organizaciones.

La adopción de una decisión se realiza mediante el denominado estudio o análisis de la situación, en el que se consideran tanto los factores externos a la persona/organización que decide como los de carácter externo, entre los que se incluirán tanto los posibles adversarios como aquellos aspectos del entorno que resulten de aplicación a la situación de que se trate. La decisión inicial adoptada como consecuencia de dicho análisis suele estar compuesta de tres planes: de acción u operaciones, logístico y de inteligencia. Este último se desarrolla como consecuencia de las «lagunas» o faltas de conocimiento que hayan sido identificadas en el proceso de la toma de la decisión y, por ello, recogerá las hipótesis de actuación del adversario o adversarios, las necesidades de inteligencia de la(s) persona(s) que decide(n), y los plazos en que se necesita disponer de dicha inteligencia a fin de adoptar la decisión definitiva. Lógicamente, dicha decisión nunca será «definitiva» porque, con toda seguridad, los factores que intervienen en la situación son de carácter dinámico y, por otro lado, será sumamente extraño llegar a conocerlos en la medida de lo necesario para que los planes preparados no sufran modificación alguna a lo largo de la acción

La aprobación del plan de inteligencia, representa el «disparo de salida» o inicio del ciclo de inteligencia, cuya finalidad única es la satisfacción de las necesidades de inteligencia del usuario. En consecuencia, es muy importante que el ciclo de inteligencia no se contemple como una «foto fija», en el que cada una de sus fases haya de ser seguida necesariamente y en todos los casos por la que se presenta en el modelo que seguidamente se expondrá. Por el contrario, el lector deberá tener siempre presente que se trata de un proceso metódico, cíclico, multidimensional, multidireccional y, lo que es más importante, interactivo e iterativo, en el que existirá siempre la posibilidad de volver a cualquiera de las fases precedentes, sin que ello conlleve la ruptura del proceso sino todo lo contrario. Puesto que lo que se pretende con el proceso es «comprender el problema o situación de forma clara y adaptar seguidamente el producto al contexto de las circunstancias del usuario», siempre que, de la evaluación de los resultados que se estén obteniendo, se considere que, por ejemplo, no se dispone de suficiente información para llegar a ese conocimiento, habrá que «retroceder en el ciclo» para resolver dicha deficiencia.

Dependiendo del ámbito de aplicación, se considera que el ciclo de inteligencia se desarrolla en cuatro o cinco pasos, referidos casi siempre como fases. En el ámbito militar y gubernamental, dichas fases se denominan típicamente dirección, obtención, elaboración y difusión; en el ámbito civil, académico y empresarial, a estas, se suele añadir una quinta fase denominada realimentación.



Figura 5.2. El ciclo de inteligencia y sus fases

### Ciclo de inteligencia. Fase de dirección

Dado que, como ya se ha expresado anteriormente, la inteligencia solo tiene sentido cuando sirve para satisfacer oportunamente las necesidades concretas de un usuario determinado en unas circunstancias concretas, la primera de estas fases, la de dirección, deberá acometer, en una primera subfase, la definición del «problema de inteligencia»; dicho de otra forma, como punto de partida de toda la actividad posterior, deberá permitir la identificación sin ambigüedad de las necesidades de inteligencia del usuario.

Es decir, el personal dedicado a elaborar la inteligencia que la organización necesite para apoyar la toma de decisiones de aquel o aquellos a los que corresponda hacerlo, deberá comprender claramente todos los matices del problema. Ante lo cual, debemos advertir al lector no apercibido de que se trata de todo menos de una cuestión baladí. Y ello es así porque, aparte y además de diferencias bastante comunes de nivel jerárquico, cultura, responsabilidad y perspectiva entre unos y otros, hay que añadir circunstancias tales como tiempo, urgencia y trabas burocráticas, que hacen que el entendimiento entre quien decide y aquellos que tienen que apoyarle, proporcionándole oportunamente la inteligencia adecuada, no sea, casi en ningún caso, un camino de rosas.

Es evidente que esto no debiera ser así, y, sin embargo, es mucho más frecuente de lo que se pueda pensar, que el usuario no sabe exactamente lo que necesita, y, cuando lo sabe, no es capaz de exponerlo de forma que su interlocutor alcance a comprenderlo con el detalle suficiente (¡y ya se sabe, que el diablo está en los detalles!). Por otro lado, en la inmensa mayoría de los

casos, la organización de inteligencia, tanto si es propia como contratada, no tiene relación directa con el usuario, sino que las necesidades de este se le comunican por medio de terceras personas, lo cual únicamente potencia la falta de entendimiento entre ambos actores. Lo razonable, para la buena marcha de una empresa de esta naturaleza, sería que el responsable de inteligencia recibiera el «encargo» directamente del usuario en una entrevista, durante la cual el primero pudiera hacer a su «cliente» las preguntas pertinentes para estar seguro de que, con su trabajo, le podría ayudar a despejar la mayoría de las dudas a las que se enfrenta. Pero, como se dice, casi nunca es así; en el mejor de los casos, el responsable de inteligencia recibe por escrito la(s) necesidad(es), pero, en muchos otros, el «encargo» es verbal y sin concreción alguna.

No se escapará al lector lo indeseable de una situación como la descrita, no solo por lo absurdo que resulta llevar a cabo un trabajo sin estar seguro de que, con él, se dará respuesta a una necesidad, sino también por el mal empleo que se hará de los medios humanos y materiales empeñados en el mismo. Es por ello que, cuando la organización de inteligencia reciba una misión en circunstancias similares a la descrita, y siempre que sea posible, deberá solicitar y recabar la información aclaratoria que precise, mediante un formulario adecuado a cada caso. Es un clásico en este aspecto, referirse a las famosas 5W+H<sup>8</sup> como forma de dar respuesta, si quiera aproximada, al denominado «problema de inteligencia». Las respuestas del usuario a esas preguntas permitirían al personal de inteligencia tener una idea más aproximada al problema real de aquel.

Porque, una vez entendido el problema, el personal de inteligencia debe transformar esas peticiones o necesidades de inteligencia del usuario (que se denominan, de forma genérica, necesidades de inteligencia (NI)<sup>9</sup> en necesidades de información (NINFO). Seguidamente, el órgano directivo de inteligencia de la organización ha de transformar dichas NINFO en misiones informativas (MI), o tareas a asignar a los órganos/medios de obtención con que se cuente, para que estos procedan a adquirir la información que se necesita procesar para llegar a disponer del conocimiento/inteligencia necesaria para apoyar oportuna y eficazmente al usuario.

Resulta casi innecesario insistir en la necesidad de que el usuario sea consciente de las capacidades de la organización de inteligencia que le apoya,

---

<sup>8</sup> *Who, What, When, Where y Why, más How (quién, qué, cuándo, dónde y por qué, además de cómo).*

<sup>9</sup> De entre las NI, se deberán identificar las necesidades críticas de inteligencia (NCI), y de estas, la organización de inteligencia deducirá las denominadas necesidades prioritarias de inteligencia (NPI). Por otro lado, es preciso considerar también otras necesidades de inteligencia (ONI). La organización de inteligencia confecciona las NINFO a partir de las NPI y ONI. No se considera imprescindible, a los fines de este documento, entrar en detalle en cada una de estas categorías cuyo título refleja, por sí solo, su importancia relativa.

así como, en consecuencia, de lo que puede esperar de la misma. Y yendo un poco más allá, para evitar desencuentros y malas interpretaciones en lo referente al producto esperado versus el recibido, debería existir un acuerdo entre ambos actores en cuanto a lo referente a, al menos, los siguientes parámetros o valores:

<b>Parámetros (valores) de inteligencia</b>
Fuente: Brei (Intelligence Essentials, Lisa Krizan)
<b>Precisión:</b> Se deberán evaluar todas las fuentes y datos ante la posibilidad de que existan errores técnicos, percepciones equivocadas o acciones hostiles para provocar equivocaciones.
<b>Objetividad:</b> Todos los juicios deberán ser evaluados ante la posibilidad de distorsiones intencionadas y manipulaciones por interés propio.
<b>Usabilidad:</b> Todas las comunicaciones de inteligencia deben realizarse en un formato que facilite su fácil comprensión e inmediata aplicación. Los productos de inteligencia deben ser siempre compatibles con las capacidades de que disponga el usuario para recibir, manipular, proteger y almacenar el producto.
<b>Relevancia:</b> Se debe seleccionar y organizar la información, o su aplicabilidad a las necesidades del usuario, conforme a sus potenciales consecuencias y al significado de la información respecto a las circunstancias de este.
<b>Disponibilidad:</b> Los sistemas/organizaciones de inteligencia deben ser capaces de responder a las actuales y futuras necesidades de los usuarios a todos los niveles de mando/decisión.
<b>Oportunidad:</b> La inteligencia debe ser entregada cuando, en sus circunstancias, el usuario pueda todavía aprovecharla.

En este punto es esencial hacer llegar al lector una importante diferencia en el desarrollo del ciclo según en qué entorno se desarrolle. Cuando se trata de una organización que dispone de sus propios medios de obtención y análisis con los que producir inteligencia para sus propias necesidades, el usuario debe ser consciente de las capacidades y de las limitaciones de dicha organización, para no esperar de ella más de lo razonablemente posible. Si, por el contrario, la organización de inteligencia es ajena a la del usuario, para evitar problemas sobrevenidos, el proveedor del servicio deberá especificar en cada caso el alcance y la precisión de sus productos, y el contratante del servicio debe, a su vez, ser consciente de dichas circunstancias.

Una vez identificadas con la mayor precisión posible las necesidades de inteligencia, y deducidas de estas las necesidades de información (NINFO), se generan, como se expresaba anteriormente, las correspondientes misiones informativas (MI), que no son sino la expresión de la forma en que se pretende obtener la información necesaria para, procesada según la secuencia del

propio ciclo de inteligencia, elaborar la inteligencia que el usuario precisa para dar respuesta al problema al que se enfrenta. Dichas misiones informativas son, en efecto, tareas que se encomienda realizar a alguien (bien sea una persona física o una organización). Asociando a cada MI el órgano responsable de obtener la información correspondiente, así como los plazos para ello (y, en cualquier caso, la fecha límite para proporcionarla), se entra en la subfase denominada «gestión de la obtención», en la cual se confecciona el denominado programa de obtención (PROB), o Intelligence Collection Plan (ICP), que no es más que un «plan» para recopilar información de todas las fuentes disponibles para dar respuesta las necesidades de inteligencia, mediante la transformación de dichas necesidades en órdenes y peticiones a los órganos y/o medios de obtención apropiados.

El propio carácter del ciclo de inteligencia hace imprescindible que exista una íntima relación entre la actividad de análisis y la de obtención, ya que la calidad y oportunidad del producto final dependerá en gran medida de una buena coordinación entre ambos campos. Es por ello que, para la confección del programa de obtención, el área de análisis debe proporcionar las necesidades de inteligencia (NI), priorizadas; su desglose en necesidades de información (NINFO); y los indicios<sup>10</sup> que se derivan de dichas NINFO. A partir de estos es posible desarrollar las misiones informativas (MI), que permiten, en primer lugar, seleccionar los órganos y medios de obtención apropiados (CON QUÉ buscar) para, seguidamente, asignar a estos la correspondiente MI, que contendrá QUÉ obtener, CUÁNDO y DÓNDE. Es absolutamente imprescindible que el PROB especifique expresamente el tiempo límite y el lugar/organización a la que se deberá remitir la información, así como la necesidad de, en su caso, comunicar la imposibilidad de proporcionar la información solicitada.

En resumen, la gestión de la obtención, segunda subfase de la fase de dirección del ciclo de inteligencia, es un proceso analítico mediante el cual se convierten las NI en misiones informativas, se asignan estas a los medios/órganos de obtención, se realiza un seguimiento de los resultados, y si es necesario, se vuelven a asignar misiones informativas. Aunque su nombre suele llevar a confusión a los no iniciados en la terminología, en esta subfase no se realiza obtención alguna, sino que se organiza la misma. Es decir, se desarrolla una actividad organizativa que corresponde al nivel directivo del órgano de inteligencia, por lo que se identifica claramente como perteneciente a la fase de dirección.

La selección del medio/órgano de obtención más apropiado para llevar a cabo un determinada MI se realiza mediante un meticuloso proceso, en el que se tienen en cuenta, por un lado, la capacidad y disponibilidad de to-

---

<sup>10</sup> Los «indicios» son elementos de información que reflejan el propósito o la capacidad de un adversario para adoptar o rechazar un determinado tipo de acción; se basan en las capacidades y en la forma de actuar del adversario, así como en el entorno exterior.



dos y cada uno de los órganos/medios propios y contratados, considerando aquellos que ya tienen misiones asignadas o solicitadas (según sean propios o ajenos), y la necesidad de distribuir convenientemente la carga de trabajo entre estos. Pero, además, dependiendo de la misión a desarrollar, para cada medio, será preciso evaluar su alcance, sus características técnicas, la influencia que el entorno y el adversario puedan tener sobre él, y como factor muy importante y en ocasiones decisivo, su oportunidad; es decir, su capacidad para proporcionar la información solicitada en el plazo requerido. De la confrontación de las capacidades del medio con la localización y características del objetivo, la amenaza representada por el adversario y el entorno en general, y el tiempo disponible, se llegará a la identificación del medio que mejor sea capaz de cumplir la misión de que se trate. En aquellos casos en que la organización de inteligencia disponga de sus propios medios/órganos de obtención, las MI se traducirán en «órdenes» para estos en el PROB, mientras que, cuando se trate de órganos ajenos a la organización, el plan las recogerá como «peticiones».

### Ciclo de inteligencia. Fase de obtención

Durante la fase de obtención, se llevan a cabo las actividades de búsqueda y recogida de la información precisa para responder a las NI. de la persona que ha de decidir. Se inicia con la puesta en marcha por parte de los órganos de obtención de las acciones necesarias para el oportuno cumplimiento de las misiones informativas asignadas en el PROB a cada uno de ellos. Los «órganos» de obtención son organizaciones dotadas de medios humanos y materiales que trabajan en la obtención y el tratamiento de la información; pertenecen a la propia organización de inteligencia, y vienen definidos por su naturaleza. Los «medios» de obtención son personas o sistemas que obtiene información de las «fuentes», que son personas o cosas de las que se puede obtener información. Así, de forma resumida, se puede decir que «las fuentes proporcionan datos e información, que son adquiridos por los *órganos* de obtención a través de sus medios».

Así, extrapolando lo dicho, resulta de forma genérica que «obtención» equivale a «explotación de fuentes»; sin obtención (o lo que es lo mismo, sin fuentes por explotar) no es posible disponer de información y, sin información, es imposible producir inteligencia. En otras palabras, la actividad de obtención y las fuentes asociadas a dicha actividad tienen una importancia capital en el proceso denominado ciclo de inteligencia. Una fuente (persona o cosa de la que se puede obtener información) proporciona información accidentalmente, consciente o inconscientemente con su presencia, actividad o ausencia de esta. Dicho de otra forma, una fuente es una persona, hecho, actividad o falta de ella, o lo que puede ser noticia por acción u omisión.

Las fuentes pueden ser controladas o incontroladas; a las primeras se les asignan misiones, si son propias, o se les envían peticiones de información,

si son ajenas, pero siempre en el entendimiento de que proporcionarán lo esperado; las segundas, por el contrario, no tienen relación de dependencia o colaboración alguna con el órgano de inteligencia u obtención, y proporcionan la información que desean en la cantidad, detalle, forma y momento que les resulta más conveniente para ellas mismas.

Atendiendo a la relación entre la fuente y la información que proporciona, se suelen clasificar aquellas como fuentes primarias o secundarias. Aproximadamente un 90% de los datos útiles para una organización o empresa está publicado en medios abiertos: se trata de la información «formal». Con el desarrollo de las nuevas tecnologías, la cantidad de datos disponibles ha alcanzado una enorme magnitud, y continúa creciendo día a día. La tarea de localizar la información relevante entre semejante volumen de datos requiere el uso de herramientas informáticas especializadas. Las fuentes de las que procede esa información formal o abierta, se denominan «secundarias», ya que dicha información, en la mayoría sino en todos los casos, ha sido generada por terceras partes; en este grupo cabe mencionar Internet, prensa, servicios on-line, y otros similares. Sin perjuicio de lo anterior, la pequeña proporción de información (menos del 10% restante) que no está disponible en medios «abiertos» suele ser la que tiene un mayor valor. Normalmente es posible conseguir estos datos, dentro de un marco legal y deontológico, a través de redes de contactos, del «trabajo sobre el terreno» (por ejemplo en conferencias, ferias y otros eventos profesionales) y del seguimiento constante de nuevas fuentes de información potencialmente útiles; las fuentes (personas –mediante entrevistas, encuestas, y cuestionarios–, documentos inéditos, y la observación) de las que procede directamente dicha información se suelen denominar fuentes primarias. Estas fuentes proporcionan detalles que no están disponibles en bases de datos, bibliotecas o Internet; exigen tiempo, pero es tiempo siempre bien empleado.

Una de las formas de clasificar el producto inteligencia, introducida en páginas precedentes, consistía en denominarla en razón al origen de la información en base a la cual se generaba: eran las famosas «INT». El siguiente cuadro recoge tanto las fuentes que las caracterizan como el uso analítico que se puede hacer de cada una de ellas<sup>11</sup>.

Resulta casi innecesario decir que, aunque, en su origen, muchas de estas fuentes han representado capacidades disponibles fundamentalmente en el ámbito gubernamental, y en muchos casos, casi exclusivamente dedicadas a la obtención de información con fines militares, la realidad actual dista mucho de ese paradigma. Por un lado, las nuevas tecnologías han puesto a disposición de un número muy importante de usuarios capacidades cuya consecución en tiempos pretéritos implicaba desembolsos económicos que solo los Estados estaban en condiciones de realizar; por otro, la cultura de inteligencia ha empezado a instalarse en el mundo empresarial, y muchas

---

<sup>11</sup> Fuente: Adaptado de Clauser y Weir (*Intelligence Essentials*, Lisa Krizan).

## Beneficios de la inteligencia en apoyo de la política...

Fuente	Técnica(s) de Obtención relacionada(s) y Atributos de la Fuente	Uso analítico
Personas	<b>HUMINT:</b> expertos en la materia, investigadores, especialistas en información, testigos o participantes.	Transferencia de conocimiento de primera mano; referencia a otras fuentes.
Objetos	<b>IMINT:</b> características físicas de equipos, materiales o productos, tales como textura, forma, tamaño o marcas específicas.	Base para informes objetivos sobre composición, estado, origen o posible empleo.
Emanaciones	<b>MASINT, SIGINT:</b> fenómenos detectables emitidos por objetos naturales o artificiales; energía electromagnética, calor, sonido, huellas, pisadas, y residuos químicos o materiales.	Análisis técnicos y científicos.
Registros	<b>IMINT, SIGINT:</b> simbólicos (informes escritos u orales, tablas numéricas) y no simbólicos (imágenes, grabaciones de datos electromagnéticos).	Investigación, información básica, traducción, conversión a forma utilizable.

Tabla 5-1. Técnicas de obtención, atributos de la fuente

corporaciones han identificado las importantes ventajas competitivas que pueden alcanzar merced a información que, con un esfuerzo económico razonable, pueden llegar a conseguir. El siguiente cuadro<sup>12</sup> muestra sencillos ejemplos del «uso dual» de la información procedente de fuentes de diversa naturaleza en los referidos ámbitos gubernamental y empresarial.

Fuente	Información proporcionada	Gubernamental	Negocios
Personas	Revelación inadvertida o intencionada por una persona en un encuentro casual, reunión oficial o en su papel de informador	Un diplomático extranjero	Un participante en una feria
Objetos	Características físicas y funcionales del objeto, descubiertas mediante su examen físico o visual	Equipo militar	Productos o componentes
Emanaciones	Indicios acerca de la identidad y actividades del originador	Comunicaciones interceptadas	Rastros químicos en los vertidos de una fábrica
Registros	Evidencia de la existencia y características de las entidades objetivo	Imágenes, telemetría, documentos	Publicaciones varias

Tabla 5-2. La información según el ámbito de trabajo

<sup>12</sup> Fuente: *Intelligence Essentials*, Lisa Krizan.

Las técnicas y medios empleados en cada una de las INT vienen, como no podía ser de otra forma, muy condicionados por su propia naturaleza. En un significativo número de casos es preciso realizar una «normalización» previa del producto original obtenido, ya que su explotación con fines de inteligencia resulta imposible para cualquier experto en análisis como consecuencia de que los formatos en que se obtiene dicha información, de carácter técnico, precisa de los conocimientos de un experto en la correspondiente materia (es el caso de la explotación de imágenes espaciales ópticas, infrarrojas o radar; o el de las emisiones radioeléctricas; o el de la información asociada a una pandemia; etc.). Es decir, entendemos por «normalización», la transformación de los datos obtenidos por el medio, o sensor, en información inteligible, volcándola en formatos normalizados, en forma tal que dicha información pueda ser explotada convenientemente durante las siguientes fases del ciclo de inteligencia.

A modo de ejemplo, y sin carácter exhaustivo, en el cuadro siguiente se presentan de forma sencilla algunas de las técnicas y medios empleados en las INT. Téngase en cuenta, respecto a IMINT, lo ya referido anteriormente: en USA, IMINT es una componente de la denominada GEOINT (inteligencia geoespacial).

**HUMINT:** Enlaces de inteligencia, entrevistas, asesoramiento de expertos, vigilancia pasiva, reconocimiento móvil y operaciones de fuentes.

**IMINT:** Sensores fotográficos y de video, electroópticos, IR, radares, etc., en plataformas terrestres, marítimas, aéreas o aeroespaciales.

**SIGINT:** Equipos dedicados a escucha, detección y localización, en plataformas terrestres marítimas, aéreas o aeroespaciales.

**OSINT:** Prensa y medios de comunicación social impresos, radio y televisión, empresas de noticias, discursos, organizaciones, Internet...

**ACINT:** Sensores por sonido dedicados a detección y localización, en plataformas terrestres marítimas, aéreas o aeroespaciales.

**MASINT:** Sensores técnicos que identifican características de fuente emisora y facilita posterior identificación y localización.

**TECHINT:** Explotación del estudio de los materiales de interés localizados en el entorno o en las fábricas.

**MEDINT:** Estudio de las condiciones médico-sanitarias del entorno.

De todas ellas, OSINT (Open Source Intelligence, o inteligencia de fuentes abiertas) es la disciplina que, con la aparición de las nuevas tecnologías y, muy especialmente, debido al crecimiento exponencial de Internet y de los inimaginables volúmenes de datos e información que pone al alcance de la mano del usuario, ha adquirido una mayor importancia hoy en día. El fenómeno *Big Data*, que, en buena medida se basa en esa capacidad y en la

natural evolución de la misma al haberse incrementado con los datos e información de la denominada Internet de «las cosas y de las redes sociales», hacen que, en la actualidad, muchas de las demás técnicas y metodologías de obtención de información vayan quedando, si no obsoletas, muy relegadas a aplicaciones muy especializadas en la esfera gubernamental.

Es importante señalar que la información obtenida por fuentes humanas o personas (HUMINT) es materia de muy alta sensibilidad por diferentes y variados motivos. Por un lado, es la más apreciada, porque el ser humano es capaz de captar detalles que escapan habitualmente a cualquier otro sensor. Pero, por otro, es también una de las que, con mayor frecuencia, puede resultar influenciada/engañada por acciones intencionadas de un adversario y/o por sus propios prejuicios. Es por ello, que, aparte de otros elementos de evaluación que se verán más adelante, la información proporcionada por una fuente humana deberá incluir, en todos los casos, una primera valoración, tal y como se puede ver en el siguiente cuadro, que no precisa explicación alguna.

CLAVE	SIGNIFICADO
AC / BO	Asunto Conocido / Buena Observación
AC / PO	Asunto Conocido / Poca Observación
APC / BO	Asunto Poco Conocido / Buena Observación
APC / PO	Asunto Poco Conocido / Poca Observación
AD / PI	Asunto Desconocido / Posible Interés

**Tabla 5-3. Clasificación «personal» en cuanto a conocimiento y capacidad de observación**

Cualquiera que sea el campo en el que se actúe, y la fuente que se utilice para obtener la información, es preciso tener siempre presente el principio de oportunidad: la información que se entrega fuera de plazo, no resulta útil, y es, por ello, superflua.

Identificados los diferentes INT en que se vaya a trabajar, y las correspondientes fuentes mediante las que se va a obtener la información, es preciso referir siquiera de forma rápida los diferentes procedimientos que se pueden emplear, y que serán más o menos apropiados según de qué INT se trate. Los tradicionales son reconocimiento, vigilancia, adquisición de objetivos e inteligencia (o explotación de personas, documentos o materiales).

Por «reconocimiento» se entiende la acción o conjunto de acciones encaminadas a obtener, mediante la observación visual u otros métodos de igual

naturaleza, información acerca de las actividades y medios del adversario/competidor actual o potencial, o para confirmar los datos relativos a otros factores del entorno. Normalmente, dichas acciones estarán referidas a un lugar concreto y a un momento preciso, y se realizan con importantes limitaciones en tiempo y espacio.

La observación sistemática del entorno (lugares, personas o cosas) por medios electrónicos, fotográficos o acústicos se conoce como «vigilancia», e incluye la vigilancia pasiva de amplios espacios y actividades, o la activa de espacios y actividades más concretas, así como la contravigilancia. Habitualmente, se lleva a cabo durante amplios periodos de tiempo.

La «adquisición de objetivos», de origen y aplicación típicamente militar, (aunque el concepto resulta aplicable en otros ámbitos con la necesaria adaptación) consiste en la detección, identificación y localización de objetivos con detalle y precisión suficiente para poder actuar con eficacia contra ellos, y evaluar los efectos. Esta actividad pretende facilitar todo tipo de acciones permitidas sobre los mismos, tanto a nivel táctico como operacional o estratégico.

Los procedimientos para la adquisición de objetivos y el reconocimiento se utilizan para investigar actividades o zonas con más detalle. La vigilancia necesita de una actividad, o ausencia de la misma, del adversario/competidor que permita descubrirle.

Finalmente, la adquisición de información mediante el examen material de productos de la competencia, o de información en cualquier soporte, así como por la actividad de fuentes humanas sobre otras personas (mediante entrevistas u otras), se conoce por el nombre genérico de inteligencia.

Como se comentaba anteriormente, es particularmente en el caso de la obtención por fuentes humanas (HUMINT) donde se presenta con más intensidad el dilema entre la necesidad de obtener la información deseada y el estricto cumplimiento de la legalidad. Si, por el contrario, las limitaciones que se plantean a la obtención se refieren más a razones de tipo ético que a consideraciones legales, el problema es de muy difícil solución. En el primero de los considerandos, hay factores, como por ejemplo, el entorno normativo regulatorio o legal, que difiere o puede diferir de manera notable entre zonas culturales y/o países, o incluso entre gobiernos locales o regionales; la fuente tratará de cumplir con su misión utilizando cualquier procedimiento que considere ajustado a la legalidad (o la interpretación que él pueda hacer de la misma). Cuando se trata de ética, el problema es realmente de imposible solución, ya que, aunque ha habido innumerables intentos de llegar a un acuerdo encaminado a definir unos principios éticos de aplicación universal, la realidad es que, por ejemplo, las diferencias culturales representan barreras infranqueables para hacer de ello una realidad.

Es por ello, que el mayor reto en las actividades de obtención consiste en no vulnerar, intencionadamente o no, las normas éticas y legales existentes en el entorno, que determinan la accesibilidad a la información. Los casos de Wikileaks y Snowden, tan recientes, escandalosos e impactantes en las relaciones entre países considerados amigos y aliados durante tantos años, han puesto este problema encima de la mesa. Pero no es nada nuevo. Desde hace muchos años, organizaciones de todo tipo, gubernamentales o no, han procedido a clasificar la información que han considerado importante para la vida de las mismas y de las personas que en ellas trabajan (a fin de proteger adecuadamente a ambas).

El esquema es sencillo, tal y como se puede ver a continuación:



Figura 5-3. Clasificación de la información

Sin embargo, cuando el propósito de proteger no se corresponde con las capacidades necesarias para que esa protección resulte efectiva, cualquier agente avisado puede encontrar la forma de acceder a esa «información de interés» que, clasificada por la organización a la que pertenece en razón a la importancia que tiene para esta, puede tener gran valor para sus adversarios/competidores. Como muy bien, dice Goodden<sup>13</sup>: «A medida que la información está llegando a ser cada vez más un factor de producción, de valor intangible por sí misma, el valor del especial conocimiento que representa la esencia de la inteligencia adquirirá un precio en el mercado global de la era de la información mayor que el del conocimiento disponible con carácter general. En ello se basa el más antiguo y, a la vez, el más moderno desafío en el futuro de la inteligencia: protegerla».

Como muestra de la preocupación que el asunto de la accesibilidad de la información representa, en Francia se elaboró el esquema que seguidamente se muestra, en el que es posible identificar casi toda la casuística que se pueda dar en este tema:

<sup>13</sup> Dearth and Goodden, 415.

	Información Blanca	Información Gris	Información Negra
Código de Color	Zona Blanca La que cualquiera puede ver y obtener	Zona Gris <ul style="list-style-type: none"> <li>• La que resulta de «escuchar los espíritus»</li> <li>• Del tratamiento de confidencias</li> <li>• Por la habilidad del que escucha</li> <li>• La que puede ser inmoral sin llegar a ser ilegal</li> </ul>	La que está protegida por ley o contrato y reservada a personas autorizadas
Calificación	Información abierta (90% del total) Pública	Información sensible (% en aumento) Abierta o cerrada	Información cerrada (10% del total) Secreta
Calificación jurídica de las infracciones	Ninguna ilegalidad: <ul style="list-style-type: none"> <li>• Obtención lícita</li> <li>• Propiedad intelectual</li> </ul> Puede haber ilegalidad en su empleo	Según jurisprudencia: <ul style="list-style-type: none"> <li>• ¿Litigio de concurrencia?</li> <li>• ¿Deserción de directivos?</li> <li>• ¿Atenta contra el secreto profesional?</li> </ul>	Infracción de leyes civiles o comerciales: <ul style="list-style-type: none"> <li>• Atentado contra los intereses fundamentales de la nación</li> <li>• Atentado contra la administración</li> <li>• Atentado contra la personalidad</li> <li>• Atentado contra los intereses de la empresa</li> <li>• Infracción de leyes o reglamentos</li> </ul>
Fuentes	<ul style="list-style-type: none"> <li>• Medios de comunicación</li> <li>• Reuniones públicas</li> <li>• BD y centros de documentación</li> <li>• Organismos públicos</li> <li>• Archivos de los tribunales de comercio</li> </ul>	<ul style="list-style-type: none"> <li>• Documentación reservada a la empresa</li> <li>• Personal de la empresa</li> <li>• Cualquier información no pública obtenida de manera no ilegal</li> </ul>	<ul style="list-style-type: none"> <li>• Fuentes consultadas legalmente sin autorización oficial o privada</li> <li>• Fuentes ilegales (Interceptaciones técnicas)</li> <li>• Fuentes humanas actuando de forma ilegal</li> </ul>

Tabla 5-4. Clasificación para protección de la información



Expuestos de este modo los aspectos que se han considerado más relevantes de la fase de obtención, y antes de pasar a la siguiente, es conveniente finalizar la misma identificando, de entre los principios básicos que se aplican en la actividad de inteligencia, aquellos que tienen una especial y específica aplicación en la referida fase de obtención. La figura siguiente recoge, de forma muy sencilla, el conjunto de los mencionados principios.



Figura 5-4. Principios de aplicación en la fase de obtención

De todos ellos, adquieren en la obtención una importancia especial los de dirección centralizada, explotación sistemática, oportunidad y protección de la fuente.

Con el fin de evitar duplicidades injustificadas e interferencias entre órganos, el esfuerzo de inteligencia tiene que coordinarse, mediante una dirección centralizada, para lograr apoyo mutuo y asegurar un empleo eficaz y rentable de todos los recursos disponibles.

La explotación sistemática garantiza que las fuentes sean explotadas de manera continua, por los órganos de obtención, mediante la asignación metódica de misiones a las mismas, sin esperar pasivamente la llegada de información.

El principio de «oportunidad» establece de forma nítida que la información o inteligencia más precisa y fiable no tiene ningún valor si se dispone de ella demasiado tarde. Por ello, el procedimiento de asignación de misiones de obtención debe ser capaz de responder, sin retraso, a cualquier cambio significativo de la situación, para asegurar que la información se proporciona no más tarde del límite temporal establecido.

Todas las fuentes de información deberán estar protegidas adecuadamente para, por un lado, garantizar su propia seguridad, y, por otro, para asegurar la continuidad de su explotación en el tiempo. El principio de «protección de la fuente» tiene carácter «crítico» para el buen desarrollo de la obtención.

Los órganos y medios de obtención se emplean siguiendo unos procedimientos que, de forma general, se pueden resumir en cuatro: Acolamiento o secuenciación (Cueing), redundancia, mezcla y reasignación (retasking), que se pueden emplear de forma independiente o, mejor, combinándolos adecuadamente según la situación.

Cueing consiste en el empleo de varios órganos/medios diferentes, de forma consecutiva, en forma tal que la obtención realizada por uno dirige a la del otro. Con este procedimiento se obtiene una rentabilidad máxima de los medios.

Cuando la probabilidad de éxito inicial es baja, se recurre al empleo de medios de la misma clase de INT (redundancia) para cubrir el mismo objetivo. Implica el empleo de más recursos.

Cuando se emplean órganos/medios pertenecientes a diversas clases de INT se está utilizando el procedimiento de mezcla, con el que se busca obtener complementariedad e informes más ricos en datos, mientras, además, se reduce la posibilidad de sufrir «decepción» (resultado de las posibles acciones de engaño llevadas a cabo por un adversario).

Por último, la integración, reasignación o retasking consiste en integrar las nuevas tareas de obtención en las misiones planeadas o que se están ejecutando.

Finalizaremos la fase de obtención con una idea clave a retener respecto a la misma, y es que las capacidades de obtención no se consiguen solo con maravilloso, sofisticado, moderno, costoso y potentísimo *software* o *hardware*, sino, y muy especialmente, con recursos humanos, organizados y dotados convenientemente. El componente humano es el recurso clave y siempre crítico de la actividad inteligencia, y particularmente de la obtención de información.

La oportuna y correcta entrega de la información recogida durante la fase de obtención da inicio a la fase de elaboración: etapa del ciclo de inteligencia constituida por una secuencia estructurada de acciones que tienen por objeto la producción de inteligencia a partir de la información disponible; su finalidad es la determinación de las posibilidades, y estimación de las posibles intenciones, del adversario o competidor.

### Ciclo de inteligencia. Fase elaboración

Para entender de una forma más sencilla en qué consiste la fase de elaboración, nos parece oportuno traer al lector la siguiente frase: [Elaboración es] «El proceso de evaluar la fiabilidad, validez y relevancia de los datos, integrándolos y analizándolos, y convirtiendo el resultado de este esfuerzo en un todo coherente, que incluye la valoración de los acontecimientos y las implicaciones de la información obtenida»<sup>14</sup>.

<sup>14</sup> Johnson, 2005.

Esta fase se subdivide en las siguientes subfases: Compilación, evaluación, análisis, integración e interpretación, que recorreremos seguidamente resaltando su significado y las tareas más importantes que, en cada una de ellas, se llevan a cabo.

La primera subfase, compilación<sup>15</sup>, es el paso en el que se agrupan los elementos de información o de inteligencia relacionados entre sí, y se registran, facilitando su posterior procesamiento. Tiene como finalidad clasificar adecuadamente los datos e informes recibidos, facilitar el acceso fácil y rápido a ellos, identificar «vacíos de información», y poder realizar la difusión de la información a los elementos de análisis conforme a la importancia de la misma. No consiste simplemente en reunir físicamente la información obtenida, sino en organizarla de forma tal que sea utilizable, añadiéndole valor donde no sea evidente en el original. Por un lado, como queda dicho anteriormente, puede revelar «vacíos» de información; lo que, en principio, puede conducir a más actividades de obtención y/o análisis, y, por otro, proporciona el marco adecuado para seleccionar y organizar información posterior. Durante la compilación se realiza una primera comprobación de la calidad de la información recibida analizándola bajo los aspectos recogidos en la siguiente figura, en cuya exposición no se considera necesario entrar puesto que son prácticamente todos autoexplicativos:

	ASPECTOS		
RELEVANCIA DE LA FUENTE	<i>Fiabilidad</i>	<i>Proximidad</i>	<i>Capacidad</i>
APLICABILIDAD DE LA INFORMACIÓN	<i>Verosimilitud</i>	<i>Previsibilidad</i>	<i>Respaldo</i>

Tabla 5-5. Parámetros para comprobar la calidad de la información

La información compilada y convenientemente organizada durante la subfase anterior pasa seguidamente a la de evaluación, durante la cual se lleva a cabo «la calificación de todos y cada uno de los elementos de información en relación con la fiabilidad de la fuente y con la credibilidad de la información»<sup>16</sup>, lo que, en otras palabras, representa una medida de la calidad de cada pieza informativa.

Siguiendo lo establecido en el manual *NATO AJP-2.1(A) Intelligence Procedures*, se aplica a cada elemento de información un código compuesto por dos caracteres: el primero, alfabético, que identifica la fiabilidad de la fuente; y el segundo, numérico, que hace lo mismo en lo que se refiere a la credibilidad de la información, según se puede observar en el siguiente cuadro:

<sup>15</sup> *Collation*, en inglés.

<sup>16</sup> NATO APP6.

Fiabilidad de la Fuente		Credibilidad de la Información	
A	Totalmente fiable	1	Confirmada por otras fuentes
B	Normalmente fiable	2	Probablemente cierta
C	Bastante fiable	3	Posiblemente cierta
D	Normalmente no fiable	4	Dudosa
E	No fiable	5	Improbable
F	No se sabe si es fiable	6	No se sabe si es cierta

Tabla 5-6. Evaluación de la información

Así pues, la evaluación es la calificación otorgada a un elemento de información en base a la fiabilidad de la fuente que lo proporciona y la credibilidad de su contenido, unidos a un criterio previo de utilidad. Se efectúa por comparación con la información disponible (BD INFO); representa un importante antídoto contra las acciones de decepción que pueda intentar un adversario, y, además, permite suprimir toda la «paja» que hace difícil las fases posteriores de la elaboración. Los criterios por los que se asignan las calificaciones anteriores a la fuente y a la información son independientes entre sí, y una vez que han sido asignados, pasan a formar parte consustancial con el resto del documento.

El análisis, tercera de las subfases de la elaboración, «consiste en la descomposición de un problema grande en un número de problemas más pequeños, y llevar a cabo operaciones mentales con los datos a fin de llegar a una conclusión o a una generalización. Implica un examen riguroso de los elementos de información que guardan relación para determinar en qué medida confirman, complementan o se contradicen entre sí y establecer las correspondientes probabilidades y relaciones.<sup>17</sup>

En el análisis, la información o inteligencia se somete a revisión y estudio, con objeto de identificar los hechos más significativos. Posteriormente se relacionan y comparan con otros hechos conocidos y se hacen deducciones.

Es posible que una información estimada importante en etapas anteriores no lo sea tanto al analizarla o, al revés, que un elemento de información considerado de poca o dudosa utilidad inicialmente revele una importancia grande al ponerlo en contexto; es decir, no se puede ni debe desechar nada, salvo que no exista la más mínima duda de su falta de interés.

Toda la información obtenida debe alimentar el banco o base de datos.

Cada elemento analizado debe serlo desde todos los puntos de vista que resulten relevantes en el problema de que se trate: políticos, económicos, militares, etc.

<sup>17</sup> Mathams, 88.

El proceso consiste, básicamente, en la realización de las siguientes acciones:

1. Formulación de hipótesis.
2. Identificación de indicadores que confirmen/denieguen las hipótesis.
3. Identificación de hechos significativos en la información disponible.
4. Comparación.
5. Confirmación/denegación de hipótesis (conclusiones).

El análisis, que implica «anticipación», pero no es nunca «predicción» ni «profecía», tiene una importancia extrema en el proceso del ciclo de inteligencia, ya que es durante el mismo cuando se añade valor a la información disponible al determinar en qué medida la información y los datos disponibles acerca del problema considerado confirman, complementan o se contradicen entre sí y permiten establecer las correspondientes probabilidades y relaciones, así como las posibles consecuencias. Aunque el análisis se refiere habitualmente a hechos concretos y actuales, el analista deberá considerar, siempre que lo estime necesario o conveniente, los antecedentes, que deberán estar disponibles y actualizados en todo momento.

El análisis no orienta acerca de posibles soluciones, solo anticipa, en base a lo conocido, la posible evolución de la situación; por ello, no elimina la responsabilidad del que decide, puesto que sus deducciones solo permiten reducir la incertidumbre a la que este se enfrenta. El producto (informe, nota, etc.) debe estar disponible en tiempo oportuno y, lo primero que se deberá exponer en él serán las conclusiones.

La figura del analista, que adquiere una importancia extrema en esta y en las siguientes subfases, ha sido motivo de extensos (y, en ocasiones, acalorados) estudios de todo tipo, incluso psicológicos, dada la influencia que la experiencia y el juicio del mismo, así como los posibles sesgos de su personalidad puedan tener en el producto que genere. Remitimos al lector interesado a consultar la extensa bibliografía disponible al respecto. Precisamente, por la importancia, en ocasiones decisiva, del factor subjetividad, se han potenciado mucho en los últimos años la aplicación de técnicas de análisis estructuradas, que, por un lado, permiten racionalizar y pautar esta subfase, mientras, por otra, facilita la enseñanza de nuevos analistas. No obstante, los buenos y experimentados analistas representan el mayor valor de que puede estar dotada cualquier organización de inteligencia.

Para que el análisis sea completo debe estar basado en el conjunto constituido por toda la información obtenida de todas las fuentes disponibles con relación al asunto o problema que se esté considerando.

Toda la información y datos reunidos hasta este momento se canalizan hacia el siguiente paso, la integración, pero, al mismo tiempo, como se dice anteriormente, tienen que ir alimentando y actualizando la BD.

En la práctica, el análisis (3ª subfase) se «funde» con la cuarta, la integración, por cuanto, en esta, se selecciona y combina la información/inteligencia anteriormente obtenida y analizada, para formar un modelo que ha de ser posteriormente interpretado. En otras palabras, con la integración se produce la imagen resultante de las deducciones del análisis y se busca un modelo coherente de inteligencia, un modelo de amenaza.

Este aspecto del proceso es casi totalmente intelectual y es el punto crítico en el ciclo de inteligencia. Está totalmente basado en los conocimientos, experiencia y juicio del analista, para los cuales, como se ha expresado ya, no se dispone, hasta la fecha, de ningún sustituto que proporcione idénticas capacidades.

La integración nos lleva a identificar la amenaza, que no es solamente una cuestión de identificar el problema planteado por el adversario, sino de llegar a determinar su entidad y naturaleza, y qué actividad realiza para, en consecuencia, poder deducir sus acciones posteriores.

Después de considerar la «identificación» y «actividad», cualquier conclusión debe relacionarse con los indicios confirmados, ya que, al obtener sus deducciones, los analistas deben tener en cuenta que cualquier adversario necesita la sorpresa, por lo que pueden haberse generado indicios que lleven a una conclusión errónea, y, por ello, deberán buscar constantemente una confirmación fiable sobre cualquier modelo aparente de los acontecimientos. Es decir, todo lo logrado hasta ahora debe estar en permanente revisión.

El paso o subfase final de la elaboración se denomina interpretación, en la que se valora la importancia de la información o inteligencia extraída en los pasos anteriores en relación con el conjunto actual de conocimientos, extrayendo conclusiones y presentando una panorámica general de la situación, incluyendo habitualmente, previsiones de futuro. La Interpretación no es fácil, lleva tiempo y requiere experiencia. Sus resultados se incluirán normalmente en los «juicios de inteligencia», o en las sucesivas actualizaciones de los mismos, que el analista de inteligencia presenta a su jefe o al usuario, en su caso. Las respuestas a las cuestiones de «identificación», «actividad» y «relevancia», situadas adecuadamente en la perspectiva del problema en estudio, conducirán a deducciones y conclusiones; estas últimas pueden ser tratadas como hipótesis, sujetas a confirmación o rechazo a la luz de la información/inteligencia recibida posteriormente. La necesaria y conveniente revisión permanente de las conclusiones alcanzadas es lo que proporciona su característica cíclica al proceso (ciclo) de inteligencia.

Finalizada la fase de elaboración, puede decirse que el órgano de inteligencia dispone de la respuesta que el usuario necesita para enfrentarse al problema que le preocupa, pero no deja de ser un atrevimiento el pensar así puesto que, salvo en muy contadas ocasiones, esa situación no será la normal sin todo lo contrario. En general, la respuesta a las necesidades de inteligencia

del usuario de que se dispondrá será limitada; sin embargo, y dado que lo normal será poder aportar un limitado conocimiento de la solución al problema, será preciso poner un punto final al proceso en un momento dado. Por ello, creemos necesario recordar que, uno de los parámetros que contenía el plan de inteligencia, era la fecha límite para que la persona que decide recibiera la inteligencia que diera respuesta, en mayor o menor medida, a sus NI. Y es por ello también que, en ocasiones, se entiende que «inteligencia es información que ha sido analizada hasta el punto en que puede emplearse para apoyar la toma de una decisión»<sup>18</sup>.

### Ciclo de inteligencia. Fase de difusión

Elaborada, pues, la inteligencia es preciso hacerla llegar al usuario o persona que decide, lo cual se realiza durante la siguiente fase del ciclo, la de difusión, que consiste en la oportuna entrega del producto inteligencia al usuario, en la forma y por el medio adecuado.

Como idea general a retener, la inteligencia es sensible al tiempo; es decir, pierde valor con el paso del tiempo y, al igual que ocurre con la información en el caso de la fase de obtención, es inútil cuando llega tarde al usuario. Por ello, es imperativo hacerla llegar al usuario lo antes posible y, en cualquier caso, con tiempo suficiente para que sea tenida en cuenta en el proceso de la toma de decisiones. En ello consiste el principio de la oportunidad, fundamental en esta fase.

Otro principio importante en la difusión es el de adecuación, que consiste en que la inteligencia que se difunda deba responder a las necesidades del usuario, estar redactada en un lenguaje preciso, proporcionarse en un formato adecuado, y difundirse por un sistema común al remitente y al destinatario.

La difusión puede ser oral y escrita. Cuando se trata de esta última, y dependiendo mucho del entorno (gubernamental o no) podrá hacerse utilizando formatos normalizados o no, y de forma regular o periódica, o a petición. Por su parte, la difusión oral podrá ser presencial o a distancia, e igualmente con periodicidad fija o no. Las ventajas asociadas a cada una de estas modalidades son ampliamente conocidas y no merecen más comentarios.

Como se indicó al inicio del estudio del ciclo como proceso, lo habitual (al menos en el ámbito gubernamental) es que el mismo concluya con la entrega del producto inteligencia al usuario.

Sin embargo, incluso en este caso, pero sobre todo cuando el demandante de la inteligencia y el órgano productor no pertenecen a la misma organización, se hace necesaria una mínima realimentación, que permita, por un

---

<sup>18</sup> *Millennium Intelligence* (J. Miller).

lado, conocer el nivel de satisfacción del primero y que, por otro, facilite al segundo realizar un juicio crítico (o valoración) del producto generado. Si el reconocimiento y aprecio del producto es fundamental para que la actividad de inteligencia tenga sentido, el que el órgano productor de inteligencia pueda identificar, mediante la fase de realimentación, tanto los aspectos de la NI que no han quedado resueltos (y reanudar, consecuentemente el ciclo de inteligencia), como los posibles fallos o deficiencias en que ha incurrido durante el proceso anterior, son de capital importancia para llevar a cabo el análisis interno que conduzca a la permanente mejora del servicio que debe proporcionar. Son las mismas dificultades de relación que se señalaban en la subfase de identificación de las necesidades de inteligencia (NI) las que, aunque parezca mentira, hacen muy difícil, y en ocasiones imposible, que se produzca una mínima realimentación, incluso cuando ambos interlocutores pertenecen a la misma organización.

No se ha querido profundizar en más detalles de los necesarios en la presentación del proceso para no cansar al lector, pero la extensión con que se ha hecho ha sido considerada la necesaria para que aquellos que no estén familiarizados con el mismo perciban con la suficiente claridad la complejidad de los problemas, y la meticulosidad y rigurosidad que se aplican durante el mismo. La persona que no es consciente de que, en la producción de inteligencia, se aplica una metodología de estas características puede pensar que, a la hora de decidir, sería lo mismo apoyarse en el conocimiento que le ofrece inteligencia como el hacerlo en la información que puede extraer de, pongamos, Internet o un periódico especializado. En muchas ocasiones, la persona que decide, por ignorancia del proceso o por prejuicios, concede incluso menos importancia a la primera.

### **La inteligencia como organización: servicios y comunidad de inteligencia**

Es pues momento de, antes de poner el punto final a este capítulo, hacer un breve recorrido por la tercera acepción de inteligencia contenida en la definición del manual AAP-6: la de entender como tal a la organización en que se lleva a cabo la actividad, y se elabora el producto (ver página 7), así como las implicaciones que ello conlleva.

Para no exponer en abstracto, y dado que este documento está dirigido a lectores españoles, pensamos que nada más razonable que hacer un sencillo estudio del tema, restringiéndolo precisamente al ámbito nacional.

Retomaremos, a tal fin, la ya mencionada Ley 11/2002, reguladora del Centro Nacional de Inteligencia, cuyo artículo 6.1, introduce la novedad de la Comisión Delegada del Gobierno para Asuntos de Inteligencia (CDGAI), que, según el mismo, «velará por la adecuada coordinación de todos los servicios de información e inteligencia del Estado para la formación de una comuni-



dad de inteligencia», siendo responsable, según detalla más adelante en el mismo artículo (art. 6.4 c) de «velar por la coordinación del Centro Nacional de Inteligencia, de los servicios de información de los Cuerpos y Fuerzas de Seguridad del Estado y los órganos de la Administración civil y militar».

A los fines que nos ocupan, hay dos aspectos en el párrafo anterior que merecen destacarse. El primero, la indefinición de los servicios (órganos de inteligencia o información) considerados, ya que, aparte de englobar las organizaciones especializadas en Inteligencia/Información de la Guardia Civil y de la Policía Nacional en un genérico bloque referido como de los «Cuerpos y Fuerzas de Seguridad del Estado», es mucho más ambigua todavía cuando se refiere a los restantes que pudieran existir. Y el asunto es importante porque, precisamente, afecta de lleno al segundo aspecto que se quería resaltar: el de la comunidad de inteligencia. El legislador no parece estar en condiciones de citar sus componentes, y, por ello, no debe resultar tampoco extraño el que, a pesar de ser citada en esta Ley, la mencionada comunidad de inteligencia no haya existido más que en el papel, mientras la CDGAI ha venido cumpliendo regularmente lo que se expresa en la Ley en lo que refiere al Centro Nacional de Inteligencia.

Contrasta esta situación con lo expresado en el documento de la Oficina del Director Nacional de Inteligencia norteamericano (ver página 2): «*No single person or organization can protect our Nation from the many and varied threats we face today*»; y esto lo manifiesta la organización que dirige la Comunidad de Inteligencia norteamericana, constituida por nada más ni nada menos que las 16 agencias del país especializadas en inteligencia, que, consecuente con esa idea, reclama que todas ellas, como órganos del gobierno, trabajen conjuntamente. Pero, la declaración va incluso más allá cuando entiende como de capital importancia la colaboración de toda la comunidad con los usuarios de inteligencia, y concede similar importancia a que dichos usuarios entiendan la misión, antecedentes, oportunidades y desafíos a los que se enfrenta la misma. Para que sus clientes amplíen su conocimiento del trabajo que realiza la comunidad de inteligencia, y le ayuden, publica regularmente el documento que se cita.

Cabe preguntarse en este punto si, dejando aparte el tamaño de ambas naciones y de sus respectivas organizaciones, agencias o servicios, de inteligencia, la situación de España es, desde el punto de vista de la seguridad, muy diferente de la de Estados Unidos. Dicho de otro modo, no se entiende bien que, transcurridos más de trece años desde la promulgación de la Ley 11/2002, los sucesivos gobiernos hayan pasado «de puntillas» sobre un asunto de tanta importancia para la seguridad nacional, y la Comunidad Nacional de Inteligencia siga siendo una figura meramente literaria.

La sinergia que se conseguiría con la estrecha coordinación de todas las capacidades de inteligencia existentes en la nación (del Estado, como señala la Ley, y no solo las de nivel gubernamental, como, pese a ello, se expresa a

continuación en el mismo artículo), es de enorme importancia para la seguridad nacional. Sin embargo, entendemos que la CDGAI, órgano colegiado no permanente, no es la solución más adecuada para llevar a cabo una eficaz y fuerte coordinación de las actividades de los diferentes organismos que se integraran en la citada Comunidad de Inteligencia. Nos parecería mucho más razonable adoptar modelos probados, como el norteamericano, en el que exista una figura externa a todas ellas que, situada en el nivel orgánico adecuado e investida de la necesaria autoridad de coordinación, y dotada de los recursos humanos y materiales para llevarla a cabo, actúe como director de Inteligencia a nivel nacional, y sea responsable único en la materia ante los poderes del Estado.

Por otra parte, el funcionamiento sincronizado de los diferentes servicios necesitará que el sistema, en su conjunto, trabaje con comunidad de doctrina y de procedimientos, por lo que será preciso desarrollar una educación y cultura de inteligencia comunes para todos ellos, sobre la cual cada uno aplicará sus características diferenciales a nivel de ejecución. En consecuencia, se cree que sería necesaria la existencia de una universidad o academia nacional de inteligencia, en la que formar al recurso más importante de todos los existentes en las organizaciones a las que nos hemos venido refiriendo en esta presentación: las personas; en todos sus niveles, tanto los cuadros directivos como los elementos ejecutivos de la comunidad. Pero, además de ello, dicho centro podría llevar a cabo la muy necesaria divulgación de la disciplina para crear una conciencia nacional al respecto que impulsara la creación de una fuerte «reserva de inteligencia» en el tejido social de la nación.

Es innecesario señalar al lector que la implantación de un modelo de comunidad de inteligencia como el dibujado esquemáticamente en las líneas precedentes representa un fuerte desafío organizativo y regulatorio, pero, se considera, con toda seguridad, que es perfectamente realizable. Las organizaciones ya existen, y la necesidad de coordinarlas está incluso recogida en la Ley, con lo que lo único que se precisa es la decisión de adoptar las medidas oportunas para garantizar que el cliente (la nación) está bien servida. Para ello, existen todas las organizaciones que producen inteligencia en los diferentes ámbitos del Estado, desde el nivel gubernamental hasta, en algunos casos, el autonómico. Las capacidades existen; las sinergias que se alcanzarían mediante su correcta racionalización, coordinación y dirección hay que crearlas mediante la adopción de las oportunas decisiones al máximo nivel del Estado.

Parafraseando a John F. Kennedy<sup>19</sup>, «no preguntes qué puede hacer inteligencia por ti, [lector a quién va dirigido este documento], sino qué puedes hacer tú por la inteligencia y, en definitiva, por España».

---

<sup>19</sup> «No preguntes qué es lo que tu país puede hacer por ti; pregunta qué es lo que tú puedes hacer por tu país», del discurso inaugural como presidente de los Estados Unidos, pronunciado el día 20 de enero de 1961.

## Bibliografía

- BREI William S., Captain. *Getting Intelligence Right: The Power of Logical Procedure*. Joint Military Intelligence College (USA), Occasional Paper Number Two, 1996.
- EJÉRCITO DE TIERRA ESPAÑOL, Mando de Adiestramiento y Doctrina. *D02-010 Doctrina Inteligencia*. Edición 2003.
- KRIZAN, Lisa. *Intelligence Essentials*. Joint Military Intelligence College (USA), Occasional Paper Number Six, 1999.
- Ley 11/2002, de 6 de mayo, reguladora del Centro Nacional de Inteligencia.
- MILLER, Jerry P. (et al.). *Millenium Intelligence, Understanding and Conducting Competitive Intelligence in the Digital Age*, 2000.
- OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE (USA). *National Intelligence: A Consumer's Guide*, 2009.



## Conclusiones

---

A lo largo de las páginas precedentes, y desde puntos de vista complementarios, los cinco ponentes han tratado de trasladar al lector su forma de entender no solo lo que, para cada uno, significa inteligencia sino también su finalidad, sus campos de aplicación, los actores y recursos que en ella intervienen y la hacen posible, así como los beneficios que, con su correcto empleo, pueden alcanzar las organizaciones de todo tipo. Se han presentado las diferentes acepciones del término para que el lector, ya avisado, entienda correctamente en el futuro la materia a que pudiera tener que enfrentarse en algún momento.

Creemos que, de entre los muy documentados y bien presentados trabajos aquí recogidos, es recomendable apuntar algunas ideas fuerza, que consideramos conveniente retener. La primera, es la imprescindible diferenciación que el lector ha debido aprehender entre información e inteligencia, magistralmente expresada por W.S. Brei:

*«Inteligencia es más que información. Es conocimiento que ha sido especialmente preparado para las circunstancias específicas de un usuario. La palabra conocimiento resalta la necesidad de la participación humana. Los sistemas de obtención de información producen [...] datos, no inteligencia; solo la mente humana puede proporcionar ese toque especial que da sentido a los datos según las diferentes necesidades de los usuarios. El proceso especial que define parcialmente la inteligencia es la continua obtención, verificación, y análisis de información que permite comprender*

*el problema o situación de forma clara y adaptar seguidamente el producto al contexto de las circunstancias del usuario. Si falta cualquiera de esos atributos esenciales, el producto sigue siendo información en vez de inteligencia».*

La segunda, igualmente trascendente, se refiere a la necesidad de situar inteligencia en contexto. La expresa muy bien uno de los autores cuando coloca inteligencia en el marco del apoyo a la toma de decisiones en el proceso de la planificación estratégica y en la implantación y desarrollo de la correspondiente estrategia, tomando la cita de B. Gilad para sentenciar que: «si bien una buena estrategia con una mala inteligencia producirá resultados mediocres; una mala estrategia con buena inteligencia es garantía absoluta de fracaso»; en otras palabras, la inteligencia *per se* no es garantía de nada, a menos que sea correctamente aplicada en decisiones que tengan sentido de cara a la consecución de los objetivos de la organización apoyada.

Los avances tecnológicos producidos en los últimos años y los enormes volúmenes de información disponibles, hacen que, actualmente, se preste atención únicamente a la inteligencia actual, dejando de lado el análisis en profundidad (estratégico y a largo plazo) en apoyo de la planificación estratégica. Es en este tipo de análisis donde el papel del analista es crucial, ya que se necesita tener personal formado en múltiples campos, además de en inteligencia, para poder llevar a cabo, por ejemplo, estudios prospectivos. Pensamos que es un error dar primacía o casi exclusividad al análisis cuantitativo, apoyado en fuertes capacidades tecnológicas, sino que, por el contrario, creemos esencial fomentar e impulsar el análisis cualitativo, imposible de realizar sin analistas formados y con experiencia. A este respecto, consideramos crucial que los usuarios últimos de la inteligencia tengan un perfecto conocimiento de las capacidades reales de su organización en dicha materia, para lo cual resulta ineludible una correcta labor de difusión que conduzca a que sean perfectamente conscientes de lo que inteligencia puede, y no puede hacer, en su beneficio.

En otro orden de cosas, deseamos trasladar al lector la preocupación manifestada, más o menos explícitamente, por casi todos los autores, respecto a la necesidad de que se desarrollen e implanten en España tanto una buena y fuerte cultura de inteligencia, como una robusta reserva de inteligencia, así como que se establezca una academia/universidad o centro docente equivalente dedicado a la formación del recurso más importante, con mucho, de todos los dedicados a esta disciplina: el personal de inteligencia, desde su nivel directivo hasta los de más baja cualificación. Este es, con absoluta seguridad, el componente más importante en cualquier organización dedicada a elaborar inteligencia; es por ello que, especialmente en el ámbito público, entendemos imprescindible la existencia de un completo y bien estructurado programa de formación y un perfil de carrera claramente definido, lo que ayudaría a que tuvieran la deseable continuidad. En cualquier caso y organización, se entiende como necesario y muy recomendable que, al me-

nos, el responsable de inteligencia se encuentre jerárquicamente muy cerca del nivel de decisión, a fin de evitar las distorsiones que inevitablemente se producen cuando el producto tiene que pasar por elementos interpuestos.

Finalmente, y por encima de todo ello, se propugna y recomienda como la más urgente e importante acción el que se desarrolle e implante una fuerte y cohesionada comunidad de inteligencia española, siguiendo los principios que están claramente recogidos en la *Estrategia Española de Seguridad*, en particular el de unidad de acción, que supone la implicación, coordinación y armonización de todos los actores y los recursos del Estado bajo la dirección del presidente del Gobierno, así como la colaboración público-privada y la implicación de la sociedad en general. Creemos que, de ello, solo pueden derivarse beneficios para la sociedad española, en términos de seguridad.





## Composición del grupo de trabajo

- Coordinador y ponente:* **D. Valentín Martínez Valero**  
General de División del Ejército de Tierra (retirado).
- Secretario y ponente:* **D. José Manuel Díaz-Caneja Greciano**  
Teniente coronel de Infantería.
- Ponentes:*
- D. Valentín Díaz Blanco**  
Coronel (guardia civil).
  - D. Isaac Martín Barbero**  
Director general del ICEX.
  - D. Juan Bautista Sánchez Gamboa**  
General de brigada del ET (reserva).



## Relación de Monografías del CESEDEN

1. Clausewitz y su entorno intelectual. Kant, Guibert, Fichte, Moltke, Schlieffen, Lenin
2. Las Conversaciones de Desarme Convencional (CFE)
3. Disuasión convencional y conducción de conflictos: el caso de Israel y Siria en el Líbano
4. Cinco sociólogos de interés militar
5. Primeras Jornadas de Defensa Nacional
6. Prospectiva sobre cambios políticos en la antigua URSS. Escuela de Estados Mayores Conjuntos. XXIV Curso 91/92
7. Cuatro aspectos de la defensa nacional. (Una visión universitaria)
8. Segundas Jornadas de Defensa Nacional
9. IX y X Jornadas CESEDEN-IDN de Lisboa
10. XI y XII Jornadas CESEDEN-IDN de Lisboa
11. Anthology of the essays
12. XIII Jornadas CESEDEN-IDN de Portugal. La seguridad de la Europa Central y la Alianza Atlántica
13. Terceras Jornadas de Defensa Nacional
14. II Jornadas de Historia Militar. La presencia militar española en Cuba (1868-1895)

15. La crisis de los Balcanes
16. La Política Europea de Seguridad Común (PESC) y la Defensa
17. Second anthology of the essays
18. Las misiones de paz de la ONU
19. III Jornadas de Historia Militar. Melilla en la historia militar española
20. Cuartas Jornadas de Defensa Nacional
21. La Conferencia Intergubernamental y de la Seguridad Común Europea
22. IV Jornadas de Historia Militar. El Ejército y la Armada de Felipe II, ante el IV centenario de su muerte
23. Quintas Jornadas de Defensa Nacional
24. Altos estudios militares ante las nuevas misiones para las Fuerzas Armadas
25. Utilización de la estructura del transporte para facilitar el cumplimiento de las misiones de las Fuerzas Armadas
26. Valoración estratégica del estrecho de Gibraltar
27. La convergencia de intereses de seguridad y defensa entre las Comunidades Europeas y Atlánticas
28. Europa y el Mediterráneo en el umbral del siglo XXI
29. I Congreso Internacional de Historia Militar. El Ejército y la Armada en 1898: Cuba, Puerto Rico y Filipinas
30. Un estudio sobre el futuro de la no-proliferación
31. El islam: presente y futuro
32. Comunidad Iberoamericana en el ámbito de la Defensa
33. La Unión Europea Occidental tras Ámsterdam y Madrid
34. Iberoamérica, un reto para España y la Unión Europea en la próxima década
35. La seguridad en el Mediterráneo. Coloquios C-4/1999
36. Marco normativo en que se desarrollan las operaciones militares
37. Aproximación estratégica española a la última frontera: la Antártida
38. Modelo de seguridad y defensa en Europa en el próximo siglo
39. V Jornadas de Historia Militar. La aviación en la guerra española
40. Retos a la seguridad en el cambio de siglo. (Armas, migraciones y comunicaciones)
41. La convivencia en el Mediterráneo Occidental en el siglo XXI
42. La seguridad en el Mediterráneo. Coloquios C-4/2000
43. Rusia: conflictos y perspectivas
44. Medidas de confianza para la convivencia en el Mediterráneo Occidental

45. La cooperación Fuerzas de Seguridad-Fuerzas Armadas frente a los riesgos emergentes
46. La ética en las nuevas misiones de las Fuerzas Armadas
47. VI Jornadas de Historia Militar. Operaciones anfibias de Gallípoli a las Malvinas
48. La Unión Europea: logros y desafíos
49. La seguridad en el Mediterráneo. Coloquios C-4/2001
50. Un nuevo concepto de la defensa para el siglo XXI
51. Influencia rusa en su entorno geopolítico
52. Inmigración y seguridad en el Mediterráneo: el caso español
53. Cooperación con Iberoamérica en el ámbito militar
54. Retos a la consolidación de la Unión Europea
55. Revisión de la Defensa Nacional
56. Investigación, Desarrollo e innovación (I+D+i) en la Seguridad y la Defensa
57. VII Jornadas de Historia Militar. De la Paz de París a Trafalgar (1763-1805). Génesis de la España contemporánea
58. La seguridad en el Mediterráneo. Coloquios C-4/2002
59. El Mediterráneo: Proceso de Barcelona y su entorno después del 11 de septiembre
60. La industria de defensa: el desfase tecnológico entre la Unión Europea y Estados Unidos de América
61. La seguridad europea y las incertidumbres del 11 de septiembre
62. Medio ambiente y Defensa
63. Pensamiento y pensadores militares iberoamericanos del siglo XX y su influencia en la Comunidad Iberoamericana
64. Estudio preliminar de la operación: Libertad para Irak
65. Adecuación de la defensa a los últimos retos
66. VIII Jornadas de Historia Militar. De la Paz de París a Trafalgar (1763-1805). La organización de la defensa de la Monarquía
67. Fundamentos de la estrategia para el siglo XXI
68. Las fronteras del mundo iberoamericano
69. Occidente y el Mediterráneo: una nueva visión para una nueva época
70. IX Jornadas de Historia Militar. De la Paz de París a Trafalgar (1763-1805). Las bases de la potencia hispana
71. Un concepto estratégico para la Unión Europea
72. El vínculo transatlántico
73. Aproximación a las cuestiones de seguridad en el continente americano
74. Defensa y Sociedad Civil

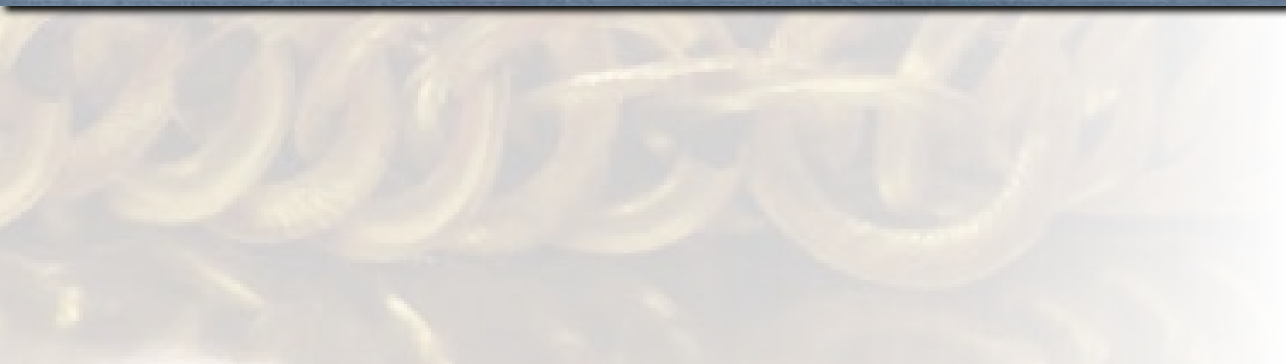
75. Las organizaciones internacionales y la lucha contra el terrorismo
76. El esfuerzo de defensa. Racionalización y optimización
77. El vínculo transatlántico en la guerra de Irak
78. Mujer, Fuerzas Armadas y conflictos bélicos. Una visión panorámica
79. Terrorismo internacional: enfoques y percepciones
80. X Jornadas de Historia Militar. De la Paz de París a Trafalgar (1763-1805). El acontecer bélico y sus protagonistas
81. Opinión pública y Defensa Nacional en Iberoamérica
82. Consecuencias de la guerra de Irak en el Mediterráneo Occidental
83. La seguridad en el Mediterráneo. Coloquio C-4/2004-2005
84. Hacia una política de cooperación en Seguridad y Defensa con Iberoamérica
85. Futuro de la Política Europea de Seguridad y Defensa
86. Una década del Proceso de Barcelona: evolución y futuro
87. El conflicto árabe-israelí: nuevas expectativas
88. Avances en tecnologías de la información y de las comunicaciones para la Seguridad y la Defensa
89. La seguridad en el Mediterráneo. Coloquio C-4/2006
90. La externalización en las Fuerzas Armadas: equilibrio entre el apoyo logístico propio y el externalizado
91. La adhesión de Turquía a la Unión Europea
92. La seguridad en el Mediterráneo: complejidad y multidimensionalidad
93. La situación de seguridad en Irán: repercusión en el escenario regional y en el entorno mundial
94. Tecnología y Fuerzas Armadas
95. Integración de extranjeros en las Fuerzas Armadas españolas
96. El mundo iberoamericano ante los actuales retos estratégicos
97. XI Jornadas de Historia Militar. La enseñanza de la historia militar en las Fuerzas Armadas
98. La energía y su relación con la Seguridad y Defensa
99. Prospectiva de Seguridad y Defensa: viabilidad de una unidad de prospectiva en el CESEDEN
100. Repercusión del actual reto energético en la situación de seguridad mundial
101. La evolución de la Seguridad y Defensa en la Comunidad Iberoamericana
102. El Oriente Próximo tras la crisis de El Líbano
103. Los estudios de posgrado en las Fuerzas Armadas
104. Las fronteras exteriores de la Unión Europea

105. La industria y la tecnología en la Política Europea de Seguridad y Defensa
106. De la milicia concejil al reservista. Una historia de generosidad
107. La Agencia Europea de Defensa: pasado, presente y futuro
108. China en el sistema de seguridad global del siglo XXI
109. Naciones Unidas como principal elemento del multilateralismo del siglo XXI
110. Las relaciones de poder entre las grandes potencias y las organizaciones internacionales
111. Las nuevas guerras y la polemología
112. La violencia del siglo XXI. Nuevas dimensiones de la guerra
113. Influencia de la nueva Rusia en el actual sistema de seguridad
114. La nueva geopolítica de la energía
115. Evolución del concepto de interés nacional
116. Sesenta años de la OTAN ¿Hacia una nueva estrategia?
117. La importancia geoestratégica del África Subsahariana
118. El Mediterráneo: cruce de intereses estratégicos
119. Seguridad Nacional y estrategias energéticas de España y Portugal
120. Las armas NBQ-R como armas de terror
121. El futuro de las relaciones Latinoamérica-Estados Unidos
122. La influencia social del islam en la Unión Europea
123. África ¿nuevo escenario de confrontación?
124. Las nuevas guerras: globalización y sociedad
125. El impacto de la crisis económica en el área de la Seguridad y la Defensa
126. El ciberespacio. Nuevo escenario de confrontación
127. En una sociedad posheroica: la transformación del paradigma militar
128. Los ámbitos no terrestres en la guerra futura: espacio
129. Valores y conflictos. Las claves culturales en el conflicto del siglo XXI
130. Análisis prospectivo de las operaciones de multipolaridad
131. Nuevas guerras. Nuevas paces
132. Valores y conflictos. Aproximación a la crisis
133. Análisis y evaluación de la estabilidad del Magreb
134. África: riesgos y oportunidades en el horizonte de 2035
135. Enfoque integral de la seguridad en el espacio marítimo español
136. El liderazgo en las Fuerzas Armadas del siglo XXI
137. Necesidad de una conciencia nacional de ciberseguridad. La ciberdefensa: un reto prioritario

## Relación de Monografías del CESEDEN

138. Racionalización de las estructuras de las Fuerzas Armadas. Hacia una organización conjunta
139. África futuro escenario de operaciones militares
140. Capacidades futuras de las Fuerzas Armadas
141. Recursos vitales y recursos energéticos. Implicaciones para la seguridad
- 141-B. Vital resources and energy resources. Repercussions for security
142. Nanociencia, nanotecnología y defensa
143. La piratería emergente en el Golfo de Guinea. Estrategia de la UE para el Golfo de Guinea
144. África
145. Nuestra frontera más avanzada entre el Sahara Occidental y Senegal
146. La industria de defensa en España tras los consejos europeos de diciembre de 2013 y junio de 2015
147. La geopolítica líquida del siglo XXI





SECRETARÍA  
GENERAL  
TÉCNICA

SUBDIRECCIÓN GENERAL  
DE PUBLICACIONES  
Y PATRIMONIO CULTURAL

