

CENTRO SUPERIOR DE ESTUDIOS DE LA DEFENSA NACIONAL



**MONOGRAFÍAS
del
CESEDEN**

40

**RETOS A LA SEGURIDAD
EN EL CAMBIO DE SIGLO**
(Armas, migraciones y comunicaciones)

**ABSTRACT
IN ENGLISH**

MINISTERIO DE DEFENSA



CENTRO SUPERIOR DE ESTUDIOS DE LA DEFENSA NACIONAL



**MONOGRAFÍAS
del
CESEDEN**

40

**RETOS A LA SEGURIDAD
EN EL CAMBIO DE SIGLO**

(Armas, migraciones y comunicaciones)

Noviembre, 2000



FICHA CATALOGRÁFICA DEL CENTRO DE PUBLICACIONES

RETOS a la seguridad en el cambio de siglo : armas, migraciones y comunicaciones. — [Madrid] : Ministerio de Defensa, Secretaría General Técnica, 2000. — 204 p. ; 24 cm — (Monografías del CESEDEN ; 40). — Precede al tit.: Centro Superior de Estudios de la Defensa Nacional.

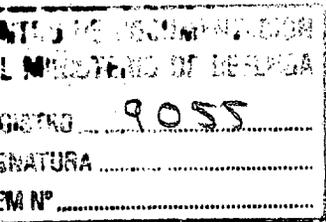
NIPO: 076-00-111-5. — D.L. M. 888-2001

ISBN: 84-7823-785-2

I. Centro Superior de Estudios de la Defensa Nacional (España). II. España. Ministerio de Defensa. Secretaría General Técnica, ed. III. Serie.

Tráfico de Armas / Armamento / Armas biológicas / Armas nucleares / Armas químicas / Misiles / Seguridad internacional / Migración / Sistemas de información / Sistemas de comunicación / S. XXI

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



Edita:



MINISTERIO
DE DEFENSA

SECRETARÍA
GENERAL
TÉCNICA

NIPO: 076-00-111-5

ISBN: 84-7823-785-2

Depósito Legal: M-888-2001

Imprime: Imprenta Ministerio de Defensa

Tirada: 1.250 ejemplares

Fecha de edición: diciembre 2000

RETOS A LA SEGURIDAD EN EL CAMBIO DE SIGLO
(Armas, migraciones y comunicaciones)

SUMARIO

	<u>Página</u>
INTRODUCCIÓN.....	9
<i>Capítulo primero</i>	
TRÁFICOS ILÍCITOS DE ARMAS.....	15
• TRÁFICOS ILÍCITOS DE ARMAS: ARMAMENTO CONVENCIONAL	17
<i>Por Dionisio García Flórez</i>	
• ARMAMENTO NUCLEAR, QUÍMICO Y BIOLÓGICO.....	43
<i>Por Vicente Garrido Rebolledo</i>	
• TRÁFICO DE MISILES Y DE TECNOLOGÍAS EN EL MARCO DE UN NUEVO CONCEPTO DE SEGURIDAD.....	77
<i>Por Belén Lara Fernández</i>	
<i>Capítulo segundo</i>	
MOVIMIENTOS MIGRATORIOS Y SEGURIDAD INTERNACIONAL....	109
<i>Por Jesús A. Núñez Villaverde</i>	
<i>Capítulo tercero</i>	
SISTEMAS DE INFORMACIÓN Y AMENAZAS A LA SEGURIDAD.....	129
• LOS SISTEMAS DE INFORMACIÓN Y LAS TECNOLOGÍAS DE LA INFORMACIÓN EN EL SIGLO XXI.....	131
<i>Por Alejandro Klecker de Elizalde</i>	

- LA UTILIZACIÓN DE LAS COMUNICACIONES Y SISTEMAS DE INFORMACIÓN COMO AMENAZAS A LA SEGURIDAD ACTUAL..... 151
Por Ricardo Martínez Isidoro

Capítulo cuarto

- AMENAZAS Y RIESGOS DE CARÁCTER MILITAR..... 173
Por Gonzalo Parente Rodríguez

- COMPOSICIÓN DEL GRUPO DE TRABAJO..... 193

- ABSTRACT..... 195

- ÍNDICE..... 197

INTRODUCCIÓN

INTRODUCCIÓN

El trabajo se ha dividido en dos áreas creadas en el seno del grupo, la de «Tráficos ilícitos» (coordinada por el doctor don Vicente Garrido Rebolledo), que junto con el área de «Sistemas de información» (coordinada por el general don Ricardo Martínez Isidoro) y dos ponencias adicionales, una de balance prospectivo, sobre la «Amenazas y riesgos de carácter militar» (a cargo del coronel don Gonzalo Parente Rodríguez) y otra, sobre los «Movimientos migratorios y seguridad internacional» (a cargo de don Jesús A. Núñez Villaverde), han conformado el objeto de este grupo de trabajo.

No se ha pretendido fijar una fecha concreta de cara a afrontar los retos que pueden afectar a la seguridad en el nuevo siglo, sino más bien, hacer una evaluación y balance prospectivo de los cambios a los que se ha visto sometido el orden de seguridad en el que nos ha tocado convivir, debido a una serie de factores externos, con influencia directa en los conflictos de fin de siglo y quizás los del próximo. Un futuro que el coronel Parente ha situado en el inmediato horizonte del año 2010, en el que los retos se funden con la amenaza militar, consecuencia directa de la globalización de intereses, pero también de la globalización de la propia seguridad. El coronel Parente ha dedicado especial atención a la relación entre los nuevos retos a la seguridad en un tiempo de cambio y la morfología actual del conflicto, así como el papel de las organizaciones de seguridad y defensa y el de las Fuerzas Armadas, en relación a la guerra del siglo XXI.

Nuestra modesta aportación a la identificación de los retos para la seguridad (unas veces clásicos y otras de nueva dimensión) tampoco ha pretendido ser global. Se ha optado por la identificación de tres áreas bási-

cas, para entender la dimensión futura de los conflictos, sean éstos armados, sociales y hasta culturales. De aquí que se haya preferido aislar tres de los grandes retos, ya mencionados, a la seguridad en el cambio de siglo: la inestabilidad política y social a través de los flujos migratorios masivos, los tráficos ilícitos de armamentos y por último, los sistemas de información como amenaza a la seguridad.

La inclusión de los movimientos masivos de población dentro de la agenda de la seguridad viene dada por la constatación de que estos flujos, aunque responden a motivaciones muy diversas, presentan como rasgo común un considerable potencial desestabilizador a escala nacional, regional e internacional. Por lo tanto si se asume que la mejor manera de garantizar la estabilidad es prevenir que se desaten los conflictos en sus primeras etapas, se entiende la conveniencia de estudiar las causas de esos flujos, así como su evolución y las posibles vías de solución para desactivar sus mecanismos de desarrollo y reducir la posibilidad de un estallido que obligue a adoptar otras medidas. Todo ello ha sido analizado por don Jesús A. Nuñez Villaverde.

La parte correspondiente al análisis de los tráficos ilícitos de armamentos ha sido dividida en tres subáreas: armamento convencional —especialmente el tráfico ilícito de armas ligeras y sus municiones—, misiles balísticos y su tecnología y por último, las armas Nucleares, Químicas y Biológicas (NBQ).

El estudio realizado por el doctor don Dionisio García Flórez ha puesto de manifiesto las enormes dificultades que entraña el control del tráfico ilegal de armas ligeras, que sin ser directamente la causa de los conflictos armados, sí son en cambio responsables de hacer éste más letal. En los más de 49 conflictos armados, contabilizados en el mundo en el año 1977, las armas ligeras estaban presentes en todos ellos y en 46 de éstos, eran de hecho las únicas armas utilizadas, algo fácilmente comprensible si se tiene en cuenta su fácil transporte y manejo por cualquier persona de más de diez años. Además, dichas armas pasan fácilmente de un conflicto, cuando éste ya ha finalizado, a otro. No existe un enfoque único a dicho problema, como tampoco soluciones universales que permitan poner fin a dichos tráficos ilícitos. Lo que sí es cierto es que a nivel regional, organizaciones como la Unión Europea, la Organización de Estados Americanos (OEA), la Organización para la Seguridad y Cooperación en Europa (OSCE) o la Organización del Tratado del Atlántico Norte (OTAN), ya han tomado conciencia del problema adoptando algunas medidas concretas,

como el Código de Conducta en el ámbito de los 15 Estados miembros de la Unión Europea.

El tráfico de misiles y su tecnología supone también un factor de inestabilidad para la seguridad, como ha sido puesto de manifiesto por la doctora doña Belén Lara Fernández, a través de un minucioso estudio sobre los posibles canales de distribución, así como la posible utilización de armas de destrucción masiva por grupos terroristas. El estudio ha incluido también el análisis de los instrumentos de control en el marco de los foros internacionales, así como el diálogo y la cooperación entre Estados Unidos y Rusia.

Finalmente, el doctor don Vicente Garrido Rebolledo ha cerrado esta segunda aproximación a los futuros retos a la seguridad ocupándose del control de los tráficos ilícitos de materiales nucleares, agentes y sustancias químicas y biológicas, así como los productos y las tecnologías de doble uso, susceptibles de ser utilizadas para la fabricación de armas de destrucción masiva. El asunto se ha convertido a lo largo de los últimos años en una de las prioridades de política internacional, no sólo por los posibles riesgos que entrañaría para las poblaciones y el medio ambiente un lanzamiento, intencionado o accidental, de este tipo de sustancias, sino sobre todo, porque incide de forma directa en la seguridad de los Estados y en la proliferación de armamento, NBQ. No obstante, la principal dificultad a la hora de controlar dichos componentes y agentes, es su doble naturaleza, civil y militar, lo que ocasiona innumerables problemas de verificación, como se está poniendo de manifiesto en la actualidad con la negociación del Protocolo de Verificación de la Convención de Armas Biológicas (CAB).

El análisis de los sistemas de información y de la amenaza potencial de la agresión informática para la seguridad ha sido también subdividido en dos estudios. Don Alejandro Klecker de Elizalde, se ha ocupado de describir en detalle el entramado de los sistemas y las tecnologías de información en el siglo XXI, teniendo en cuenta que las telecomunicaciones son al mismo tiempo factor de desarrollo y dependencia. Las amenazas a la seguridad se podrían concretar en la posibilidad de ser agredido por un tercero, desde el interior o desde puntos lejanos al propio Estado o centro que pudiera sufrir la agresión, o bien, ante la imposibilidad de detectar en la mayoría de los casos el origen de esa agresión.

Esas dos nuevas amenazas potenciales a la seguridad, concretadas en la que podríamos denominar como ciberguerra o guerra de la información,

ha sido desarrollada por el general don Ricardo Martínez Isidoro, quién nos ha descrito además cuales serían los efectos de los ataques a los sistemas de información, los actores de la amenaza y las respuestas y las estrategias para hacer frente a esa amenaza, que exige la participación de todos los gobiernos.

Sería muy ambicioso, por nuestra parte, pensar que este estudio pueda servir para evitar los conflictos del nuevo siglo, a través de la simple identificación de unos cuantos, de entre los tantos retos a la seguridad a corto y medio plazo. Nos daremos sin embargo, por satisfechos sí, una vez publicada esta Monografía, nuestras reflexiones contribuyen a aunar las conciencias y pensamientos colectivos en torno a la definición de un nuevo marco de seguridad y defensa, por otra parte, en continuo cambio.

CAPÍTULO PRIMERO

TRÁFICOS ILÍCITOS DE ARMAS

TRÁFICOS ILÍCITOS DE ARMAS: ARMAMENTO CONVENCIONAL

Por DIONISIO GARCÍA FLÓREZ

Introducción

*Tráfico de armas y crimen organizado
en el nuevo concepto de seguridad*

El concepto de seguridad se ha ampliado considerablemente desde el fin de la guerra fría, abarcando hoy en día aspectos económicos, políticos, sociales, medioambientales, etc. El tráfico ilegal de armas no es un concepto ni un hecho nuevo y existe desde muy antiguo; y su relación con la seguridad entendida en el ámbito global, tampoco. Durante la guerra fría el tráfico ilegal de armas estaba sometido, como la mayoría de las cuestiones de seguridad, a la rivalidad militar de ambas potencias, y oculto por la seguridad militar e intereses políticos, por lo que era difícil discernir entre lo que era un auténtico «mercado negro» de armamento y aquel que era «protegido» o «esponsorizado» por cada una de las superpotencias. El escenario geoestratégico y de seguridad cambió bruscamente tras el fin de la guerra fría y la desaparición del bloque comunista. La globalización de la sociedad internacional en todos los campos ha sido acompañada por un dramático incremento del crimen transnacional en todas sus facetas: tráfico de drogas, armas, seres humanos, nuevas tecnologías, etc. A su vez, el combate contra los tráfico ilícitos se hace más difícil y es necesaria la cooperación en el ámbito internacional si se quieren obtener unos mínimos resultados en la lucha.

Tales crímenes, en su conjunto, suponen un riesgo, y en muchos casos una verdadera amenaza, a la estabilidad de países y determinadas regiones del mundo. Dichos tráficos ilícitos son un reto global que pueden minar, y de hecho lo hacen, las bases económicas y democráticas de cualquier país mediante la introducción de dinero ilegal o blanqueo del mismo, generando una gran corrupción a todos los niveles, que conlleva el consiguiente debilitamiento de las instituciones públicas y privadas y la pérdida de confianza en dichas instituciones y en el imperio de la ley por parte de la población, que es la base de todo Estado democrático. A su vez, y ya en un aspecto más relacionado con la seguridad militar de los países, el tráfico ilegal de armas provoca un incremento de la inestabilidad en las zonas de conflicto o proclives a él. Debido a este motivo, el tráfico ilegal de armas aumenta los riesgos de escalada y posterior intervención militar en determinadas zonas del planeta, por lo que los países occidentales pueden ver un serio riesgo en la proliferación de dichos tráficos ilegales de armas.

En determinados casos dichos tráficos ilegales de armas influyen directamente en la propia seguridad de varios países aliados en la Organización del Tratado del Atlántico Norte (OTAN). Aquellos que tienen problemas de terrorismo interior han percibido siempre el riesgo grave de inestabilidad, y en ocasiones de agresión directa a su seguridad, que supone la existencia de dicho tráfico. En el mes de julio de 1999, mientras en Irlanda del Norte se negociaba el asentamiento definitivo del acuerdo de paz, a la negativa del Ejército Republicano Irlandés (IRA) a entregar las armas había que añadir las detenciones de varios traficantes de armas que estaban ayudando a incrementar los arsenales de las partes en conflicto, añadiendo de ese modo más violencia e inestabilidad a un proceso ya de por sí difícil.

La globalización de la sociedad internacional ya mencionada, junto con las realidades de integración social y lo permeables y difusas en que se han convertido las fronteras actuales, hace que sea difícil establecer la distinción entre crimen y conflicto. El ejemplo más claro lo tenemos en las revueltas que tuvieron lugar durante el mes de abril de 1997 en Albania, en la guerra de Chechenia, y más recientemente en el caso de los ataques armados en Daguestán, o en la situación en Somalia, donde resulta difícil distinguir que partes eran facciones políticas, fuerzas públicas, grupos terroristas o simplemente bandas mafiosas. Dicho caldo de cultivo, países donde no existe un poder central fuerte al que se puedan exigir responsabilidades por los tráficos ilegales, o que al menos tenga algún tipo de control sobre los mismos, especialmente de armamentos, permite que los «mercados negros» funcionen sin, prácticamente, barrera alguna.

El tráfico ilegal de armas se alimenta en muchas de las ocasiones de la militarización que suele producir en la sociedad civil tras el fin de los conflictos armados, cuando, de no producirse un completo y verificable desarme de las partes en conflicto, se produce una introducción y venta de armas en la sociedad civil de dicho país, lo que unido a la permeabilidad de las fronteras, permite su pase y transferencia a las zonas y países limítrofes. Este flujo de armamento ilegal, y por lo tanto incontrolado, influye enormemente en las tasas de criminalidad de las sociedades tras los conflictos. Así, en países como El Salvador o Suráfrica, el fin de los conflictos propios o de países vecinos, ha disparado los índices de asesinatos y de violencia en general debido a la gran cantidad de armas incontroladas en poder de los civiles.

Tras las guerras, las armas ligeras incontroladas son usadas también como moneda de canje. A menudo, si no se ha producido una adecuada desmovilización, los soldados o guerrilleros desmovilizados se ven abocados al paro y su único bien material es, en numerosas ocasiones, sus armas. Éstas son a menudo vendidas en el «mercado negro» para conseguir dinero o, en una gran parte de los casos, usadas para el crimen y bandidaje, lo que genera a su vez más inestabilidad y más problemas para la superación del anterior conflicto. Es muy difícil, una vez que el conflicto en sí ha terminado, tomar el control de las armas en él usadas

Las armas ligeras y sus problemas

Cuando hablamos de tráfico ilegal de armamento convencional nos estamos refiriendo principalmente a la cuestión de las armas ligeras. Existe, indudablemente, tráfico ilegal de armas pesadas, pero éste supone un porcentaje muy pequeño con respecto al de armas ligeras. Aunque cuando hablamos de armas ligeras todo el mundo tienen en mente lo que son, aún no se ha dado una definición aceptada internacionalmente sobre lo que se entiende por «arma ligera». Independientemente de su peso, se suele hablar de armamento ligero en función del calibre del arma, considerándose la categoría de «ligera» para un arma de fuego cuyo calibre es inferior a 20 milímetros. Aunque debemos hacer aquí la salvedad de armas como los morteros, lanzagranadas y lanzacohetes, que aún siendo de mayor calibre, su manejabilidad los hace ser considerados también como armas ligeras.

Aunque las armas no son la causa de la violencia, si son responsables en gran medida de hacer que el crimen sea más violento y el conflicto más

letal. Está demostrado que la mayor cantidad de armamento ilegal en una zona hace aumentar las violaciones de los derechos humanos, e impide en gran medida un desarrollo económico y social sostenible y, en muchos casos, una solución pacífica a los conflictos. Hay un dato que debe hacer reflexionar: de los 49 conflictos armados contabilizados en el mundo en el año 1997, las armas ligeras eran usadas en todos ellos, y en 46 de ellos eran las únicas armas utilizadas.

El porqué de estas abrumadoras cifras es fácil de comprender: las armas ligeras son las principales porque son baratas, duraderas, sin necesidad apenas de repuestos y fáciles de entretener y transportar por cualquier persona desde un niño de 10 años en adelante. Son también las armas preferidas de los traficantes de armamentos por esas mismas razones, ya que son las más fáciles de transportar y las que más demanda tienen, lo que redundará en mayores beneficios.

En la actualidad la tendencia del tráfico ilegal de armas es su recirculación de un conflicto a otro. Al no existir un control y una desmovilización completa y comprobable tras los conflictos armados, las armas sobrantes ya para ese conflicto son recicladas por los traficantes ilegales para su uso y venta en cualquier otro conflicto del mundo, y de ahí, gran parte de ellas pasa a la sociedad civil. Ejemplos de esto lo tenemos en el conflicto de Kosovo, donde gran parte del armamento del Ejército de Liberación de Kosovo (ELK) procedía de Bosnia y de los *stocks* robados en Albania durante las revueltas de abril del año 1997. Igualmente, el recrudecimiento del conflicto en Angola y en el Congo se debe a la gran afluencia de armas procedentes de otros conflictos ya finalizados como el de Mozambique o Namibia.

Las cifras son elocuentes, el tráfico ilegal de armas ligeras supone más del 50% del comercio global de armas ligeras en el mundo. Es decir, por cada arma vendida legalmente, existe al menos un arma en situación de ilegalidad. España tampoco escapa a esta dinámica. Según algunos reportajes periodísticos, en nuestro país pueden existir hasta 350.000 armas no controladas.

Las líneas de abastecimiento que se utilizan para el tráfico ilegal de armas ligeras son muy largas, ya que como hemos indicado, van reciclándose de un conflicto a otro, lo que hace que su seguimiento por parte de las autoridades nacionales e internacionales sea sumamente complicado. A menudo, como veremos más adelante, uno de los pasos de esta cadena es «legal» y este es uno de los factores que hacen que la frontera entre el comercio legal y el tráfico ilegal sea muy difusa.

Tráfico de armas

Historia

Como indicamos en la introducción, el tráfico de armamentos ha existido prácticamente desde siempre. Pero centrándonos en el problema de hoy en día, debemos arrancar analizando las diferentes fases por las que ha pasado desde el final de la Segunda Guerra Mundial. El tráfico ilegal de armas desde la Segunda Guerra Mundial ha vivido dos grandes épocas doradas:

— La primera etapa abarca desde los años cincuenta hasta los setenta. En dicha etapa existían grandes *stocks* de armamentos sobrantes de la Segunda Guerra Mundial y fue un periodo caracterizado por un gran número de conflictos en el mundo, particularmente en África y Asia: guerras anticoloniales y movimientos guerrilleros.

Durante la guerra fría cada bloque militar vendía armas a sus Estados o movimientos irregulares de de clientes. El bloque occidental vendía armas más como negocio y se cuidaba mucho de que dichas armas no fuesen reexportadas a un tercer país, con el fin de que la tecnología armamentística no pasase al bloque comunista. La política de ventas de los países comunistas era bastante distinta, primando lo ideológico sobre la cuestión de mercado. En ocasiones, los países del Pacto de Varsovia se limitaban a regalar las armas a movimientos de liberación y guerrillas afines. Al regalar el armamento los comunistas a beneficiarios no gubernamentales y no imitarles los occidentales, es donde entraba en escena el traficante de armas para llenar ese hueco. Por lo tanto, durante la guerra fría, el traficante ilegal de armas de alimentaba y se movía, principalmente, en el mundo occidental.

El traficante debía estar en íntima relación con las autoridades de su país que la mayoría de las veces era su abastecedor. Éste era el caso de las grandes compañías que por dinero, hacían de intermediarios entre los países vendedores y los compradores a los que oficialmente no se quería o, de cara a la opinión pública, estaba mal visto vender. Tras estas grandes empresas estaban los meros *brokers* o intermediarios, cuya función era poner de acuerdo a la empresa vendedora y al comprador, que generalmente no solía ser un Estado, sino otra clase de organización o grupo. Los menos importantes entre los traficantes eran los que tenían sus propios *stocks* de armas y operaban directamente en el «mercado negro».

- La segunda etapa abarca desde el año 1989 hasta nuestros días. Se caracteriza por la desaparición del bloque comunista y la reducción de armamentos generalizada en todos los países europeos. Dichas circunstancias generan grandes *stocks* de armamentos sobrantes que coinciden con el resurgimiento de gran número de conflictos nacionalistas y guerrillas por todo el planeta.

En la actualidad, al no existir regalos de armas por parte de los antiguos países del bloque comunista, los traficantes ilegales de armas no encuentran «competidores», por lo que las redes de tráfico ilegal de armas han florecido y han ampliado sus mercados.

Las retransferencias de los *stocks* existentes, producto de conflictos finalizados, es lo que define el mercado en la actualidad. Ya hemos comentado que hoy en día la recirculación de las armas de un conflicto a otro es la norma, por lo que tampoco hacen falta nuevos *stocks* procedentes del mercado «legal» para que el «mercado negro» siga funcionando, ya que se retroalimenta él solo. En varios de los antiguos países del Pacto de Varsovia y antiguas repúblicas soviéticas han proliferado los «mercados negros» de armas. Anteriormente los embarques eran hechos por el propio Estado o el partido dirigente, pero en la actualidad se puede encontrar, en algunos países, todo tipo de transferencias: transferencias del gobierno, transferencias semioficiales, embarques de armas hechos por miembros de las Fuerzas Armadas, contratos hechos por traficantes de armas, robos de armas hechos por el crimen organizado, «mercado negro», etc.

Como ejemplo de cómo el mercado ilegal de armas funciona, y afecta enormemente a la propia seguridad europea, recientemente salieron a la luz noticias sobre los contactos que el ELK mantuvo con la organización terrorista ETA para aprovisionarse de armamento. Dichos contactos entre grupos armados y transferencias de unos a otros también se dan en ocasiones sin necesidad de intermediarios, aunque no suele ser lo más frecuente debido al riesgo que para ambas partes supone.

Funcionamiento del tráfico de armas

LEGISLACIONES

El paso de un arma del mercado legal al ilegal se da a través de las lagunas que en sus legislaciones mantienen los países vendedores, o directamente a través de la comisión de un delito como puede ser el robo directo

o la falsificación de la documentación necesaria para comprar dicha arma. El «mercado negro» de armas se aprovecha en gran medida de la disparidad en materia legislativa entre las diferentes naciones. En el ámbito occidental en el cual se mueve España, los países de la OTAN y de la Unión Europea intentan homogeneizar sus políticas de venta de armamento así como sus legislaciones al respecto. Como veremos más adelante, la Unión Europea ha dado un gran paso al emitir una serie de criterios para que unifiquen los de cada Estado miembro a la hora de exportar armamento.

Las legislaciones de los países de la Unión Europea en materia de venta de armamento convencional son muy similares como consecuencia de estas medidas. La mayoría de las legislaciones establecen unos mecanismos de control, tanto en el ámbito industrial, político como legislativo, para asegurar que la venta de dicho armamento no incrementará el «mercado negro» o no irá a parar a una tercera parte no deseada.

Vamos a repasar brevemente la legislación española en materia de exportación de armamento y, a través de ella, ver como se puede producir el paso de legal a ilegal en la venta de un arma.

En España, la exportación de armamento se halla regulada actualmente a través del Real Decreto 491/1998, de 27 de marzo, por el que se aprueba el *Reglamento del comercio exterior de material de defensa y doble uso*. En España, para que una empresa pueda exportar armas, debe estar registrada en el Registro Especial de Exportadores de Material de Defensa y Doble Uso y pasar el informe preceptivo de la Junta Interministerial Reguladora del Comercio Exterior de Material de Defensa y Doble Uso (JIMDDU).

El registro tiene como objeto conocer al comercial que va a exportar materiales de defensa. Este requisito es indispensable y previo a la solicitud de cualquier tipo de operación de exportación y reexportación

La JIMDDU está compuesta por aquellas unidades de la Administración que están directamente implicadas en el control del comercio exterior de material de defensa y doble uso. En la actualidad está compuesta por: un presidente que es el secretario de Estado de Comercio, Turismo y Pequeñas y Medianas Empresas (PYME); un vicepresidente que es el subsecretario del Ministerio de Asuntos Exteriores; y siete vocales que son el director general del Centro Superior de Investigación de la Defensa (CESID), el director general de Armamento y Material del Ministerio de Defensa, el

director general de Comercio Exterior, el director general de la Guardia Civil, el director general de la Policía, el secretario general técnico del Ministerio de Industria y el director del Departamento de Aduanas. La más relevante de sus funciones es la de informar con carácter preceptivo y vinculante sobre las autorizaciones administrativas y acuerdos previos tanto de materiales de defensa como de productos de doble uso que se soliciten. Las actas de dicha junta son secretas, pero están a disposición del Parlamento siguiendo los cauces propios de dicho organismo para el tratamiento de materias así consideradas. La JIMDDU tiene facultades para eximir al exportador de determinados documentos o bien solicitar otros añadidos que considere oportunos al margen de los contemplados en el Reglamento.

Estos organismos emiten una serie de autorizaciones administrativas de exportación-expedición de material de defensa y doble uso y su solicitud. Aparte de estas autorizaciones, existen una serie de documentos de control que permitan asegurar al país vendedor que dichos materiales no van a ser reexportados sin autorización previa.

Dentro de estos documentos vamos a estudiar detenidamente dos de ellos: la Declaración de Último Destino y el Certificado de Último Destino

En la utilización de estos dos documentos es donde se produce en su gran mayoría el paso de un arma del mercado «legal» al «ilegal».

DECLARACIÓN DE ÚLTIMO DESTINO (DUD)

Es una declaración en la que figura el compromiso del destinatario de efectuar la importación del material señalado y de no reexportar el material en cuestión sin la autorización de las autoridades del país exportador.

CERTIFICADO DE ÚLTIMO DESTINO (CUD)

Es un documento en el que el país comprador se compromete ante las autoridades del país exportador a controlar el destino final del material importado y a no reexportarlo a una tercera parte sin autorización previa de la parte vendedora.

El mal uso o la falsificación directa de ambos documentos permite el paso de una mercancía al mercado ilegal de armamentos. Se pueden dar varias circunstancias:

- El DUD y el CUD son auténticos y expedidos por autoridades oficiales. En este caso si el país exportador no vigila y controla el uso de dicho

material periódicamente, la parte compradora podrá desviarlo de su uso inicial sin que nadie se dé cuenta.

- El DUD y el CUD son auténticos pero la instancia que los firma es falsa. En este caso, de nuevo, si la parte compradora no verifica que dicha solicitud está respaldada por un destinatario claramente identificado, el material puede de nuevo ser desviado de su uso inicial.
- El DUD y el CUD son falsos. Aquí se da la falsificación directa de todo, los documentos y la instancia que los remite. De nuevo, si el país exportador no verifica y comprueba los mismos, el material será desviado.

El problema con ambos documentos es que no se hallan estandarizados en el ámbito internacional ni existe un organismo internacional que vigile su uso y su cumplimiento, por eso queda a voluntad de la parte exportadora su comprobación y seguimiento, así como también mirar hacia otro lado cuando se da su incumplimiento en caso de detectarlo. Los traficantes de armas internacionales aprovechan dicha laxitud en los controles internacionales para negociar con las partes interesadas dichas transferencias, las cuales se pueden hacer con la aquiescencia de ambas partes o bien mediante el engaño a la parte exportadora.

Como vemos, la cuestión fundamental está en falsificar el CUD y las cláusulas de no reexportación. En la mayoría de los casos se utilizan lo que se conoce como «países pantallas». Este término se refiere a países cuyas autoridades, por un buen precio, ponen su sello al CUD haciéndolo pasar por legal y auténtico sin que después se preocupen del destino final del armamento. Durante la guerra fría, varios países del Este y, sobre todo, países africanos donde la corrupción era la norma, eran famosos por ejercer como países pantalla. Aún hoy en día existe dicho tipo de países. Recordemos que son muchos los casos en los que países conocidos de todos transfieren directamente armamento a grupos terroristas o guerrilleros.

El incumplimiento de las legislaciones nacionales en vigor, como es lógico, acarrea su pena correspondiente, pero al estar la mayoría de las personas que intervienen en dichos acuerdos fuera del territorio del país exportador, su persecución por las autoridades nacionales es muy difícil, de ahí que los traficantes de armas internacionales se muevan con cierta libertad por el mundo y su procesamiento sea sumamente difícil en caso de que no exista cooperación internacional.

En la legislación española, concretamente en la Ley Orgánica 12/1995 de Represión del Contrabando, se tipifica el delito de contrabando de armas como:

«Los que exporten material de defensa o de doble uso sin autorización o habiéndole obtenido mediante declaración falsa o incompleta en relación con la naturaleza o destino último de los mismos o de cualquier otro modo ilícito.»

Esta definición, en opinión del autor, posee algunas lagunas, ya que tipifica el delito de contrabando cuando exista exportación ilegal de armamento, pero no se menciona la importación ilegal del mismo.

En el ámbito internacional encontramos una definición más completa en uno de los pocos documentos internacionales firmados contra el tráfico ilegal de armas y que más adelante mencionaremos. En la Convención Interamericana contra el Tráfico y Fabricación Ilícitos de Armas de la Organización de Estados Americanos (OEA) se define «tráfico ilícito» como:

«La importación, exportación, adquisición, venta, entrega, movimiento o transferencia de armas de fuego, munición, explosivos y otros materiales relacionados desde o a través del territorio de un Estado-Parte a otro, sin autorización.»

También aquí se encuentran lagunas pues tipifica el tráfico ilegal de armas entre países, pero no menciona tráfico interno en los propios países.

TRAFICANTES

La figura del traficante ilegal de armas se ha visto rodeada de un cierto halo romántico durante muchos años, tal vez fruto de las novelas de aventuras o de las películas de cine. Muchos piensan en ellos como mercenarios o aventureros que desembarcan las armas de noche desde un viejo barco en un punto escondido de la costa. Esta imagen se aleja bastante de la realidad en lo que se refiere a los grandes traficantes. La mayoría de las veces, el traficante de armas no es más que un mero intermediario o *broker* que se limita a poner en contacto a las partes interesadas en comprar y en vender, eso sí, cobrando por ello en la medida de que, con su dinero e influencia lima, todas las barreras legales que se puedan interponer en el negocio. Aunque para el traslados de un lugar a otro también se utilizan en determinadas ocasiones buques, no es menos cierto que con una buena cobertura legal, los envíos de armas pueden ser enviados directamente por avión, y a través de canales normales. De hecho, no son pocas las veces que las autoridades de aduanas de los diversos países han aprendido cargamentos de armas en vuelos comerciales.

Una de las imágenes populares acerca del tráfico internacional de armas es aquella que imagina grandes almacenes escondidos con enormes cantidades de armas. Sin embargo, según se sabe, apenas existen grandes *stocks* almacenados de armas y tan sólo se pueden contar un par de personas con la suficiente capacidad para mantenerlos seguros. Dado que la tendencia actual es la retransferencia de los *stocks* de armas de un conflicto a otro, no es necesario la existencia de dichos *stocks* almacenados, pues la demanda actual supera en muchas ocasiones la oferta que de armamento ilegal existe. Dichos grandes almacenes sí se dieron en la etapa posterior a la Segunda Guerra Mundial. Donde la gran abundancia de material sobrante sobrepasaba con creces la escasa demanda.

El mercado ilegal de armas, contrariamente a lo que pudiera pensarse visto lo lucrativo del negocio, es un mercado muy restringido donde sólo participan muy determinados personajes, muchos de los cuales son de actualidad permanente en las páginas sobre casos judiciales. La necesidad de grandes sumas de dinero, así como de contactos a todos los niveles, hace que el tráfico internacional de armas sea cuestión de unos pocos, que en la mayoría de las ocasiones tienen sus sedes en paraísos fiscales o en territorios o países donde sus autoridades los protegen, para evadir la persecución fiscal y judicial internacional.

La tendencia actual, con la globalización del crimen a todos los niveles, apunta hacia las grandes organizaciones de crimen organizado y mafiosas como las de Rusia, Chechenia o Italia, que, dentro de sus negocios globales, participan abiertamente en el contrabando de armas. Las relaciones entre los tráficoos ilegales (narcotráfico, armas e inmigración ilegal) son cada día más estrechas y globalizadas y las grandes organizaciones criminales se están haciendo poco a poco con el control de todos estos flujos.

Lazos entre las transferencias legales e ilegales de armas

Como hemos visto anteriormente, hoy en día es muy difícil distinguir una exportación legal de una ilegal. El «mercado negro» se alimenta de los agujeros existentes en las legislaciones nacionales (y la total ausencia de legislación internacional), tales como ausencia de control sobre transferencias a terceras partes, inadecuado o negligente uso del certificado de destino final o gobiernos que miran hacia otro lado en transacciones cuestionables. Esta barrera difusa entre lo legal e ilegal es uno de los puntos que deben aclarar las instancias internacionales para combatir el tráfico de armas.

Dado que las resoluciones y acuerdos internacionales sólo son aplicables a aquellos países que los firman y se adhieren a ello, y que apenas existen mecanismos internacionales judiciales para dirimir su incumplimiento, es muy difícil la creación de un acuerdo internacional para la limitación o erradicación del tráfico ilegal de armas. Un ejemplo claro lo tenemos en algunas recientes resoluciones del Consejo de Seguridad de Naciones Unidas estableciendo embargos de armas a países en conflicto. A pesar de dicho decreto, son muchos los países que siguen vendiendo armas a las partes en conflicto, por lo que según el Derecho Internacional emanado de Naciones Unidas dicha venta de armas sería ilegal, aunque fuese legal según la legislación interna del país exportador. Pero, de nuevo, nos encontramos en la falta de mecanismos internacionales para perseguir y sancionar dichas faltas.

Otra cuestión muy importante para identificar las transferencias legales de las ilegales es el uso de intermediarios. Los grandes traficantes, en su propio nombre o a través de empresas pantalla o «fantasmas», la mayoría de las veces con sede en paraísos fiscales, utilizan este método para traficar con armas. En este caso la venta de armamento no se hace a un sujeto gubernamental o un país, sino a una empresa que posteriormente lo vende a un tercero.

Varios casos recientes avalan la hipótesis de que ésta es la más peligrosa de las tendencias. En 1998 se hizo una importante venta de armas a través de una empresa intermediaria a los partidarios del derrocado presidente de Sierra Leona, meses después estalló una cruenta guerra civil. Caso similar ocurrió en Ruanda meses antes del genocidio del año 1994, de nuevo una empresa intermediaria fue la encargada de realizar importantes transferencias de armas al Gobierno hutu.

Arsenal de Europa Oriental: controlando los flujos de armas a zonas de conflictos

Una de las cuestiones que más preocupa a Occidente en relación con la extensión y proliferación de las transferencias ilegales de armas es la situación de los antiguos países del Pacto de Varsovia y de las ex repúblicas soviéticas. Existen enormes arsenales de armas ligeras en estos países que han quedado en desuso ante la reducción de efectivos militares o ante la modernización que algunos de ellos están haciendo para estandarizar sus armamentos con los de los países de la OTAN. La situa-

ción de dichos arsenales es, en algunos casos, sumamente preocupante debido a la relajación de los controles que el Estado y las Fuerzas Armadas mantienen sobre ellos. Así, por ejemplo, las tropas rusas abandonaron importantes arsenales en el Cáucaso tras su retirada de Repúblicas como Armenia, Georgia o Azerbaiyán, contribuyendo con ello a la militarización de la zona y a alimentar los conflictos entre ellos. A ello hay que sumar la alta demanda de dicho tipo de armamento debida a los conflictos que han estallado por todo el mundo tras el fin de la guerra fría.

Hay algunos datos que deben llevar a la reflexión. En el año 1995, Rusia poseía el 40% del mercado de armas ligeras en el mundo, bastante por encima de Estados Unidos. El arma insignia de dicho mercado, y casi ya un referente universal, es el legendario fusil de asalto *Kalashnikov AK-47* y sus variantes. De este arma se han producido casi 70 millones de ejemplares en todo el mundo y todavía se fabrica bajo licencia en nueve países. Su dureza, fiabilidad y bajo coste le hacen ser el arma preferida de los grupos guerrilleros e insurgentes

Durante la guerra fría, los países del Pacto de Varsovia vendieron armas a más de 50 países y numerosos grupos guerrilleros de toda condición. Dicha tendencia se redujo tras la desaparición del Pacto de Varsovia y de la Unión Soviética, pero aún se mantiene ese importante mercado para algunos países.

La pérdida de poder y de control del gobierno central en varios de dichos Estados hizo que muchos de estos arsenales desaparecieran en manos del crimen organizado y mafias locales. Para contribuir a ello fueron caldo de cultivo la inestabilidad política vivida en la mayoría de estos países y las luchas civiles internas en el Cáucaso y guerras como en Chechenia y los Balcanes.

Algunas de las medidas adoptadas por estos países produjeron en ocasiones el efecto contrario al deseado. En Rusia se intentó acabar con el monopolio de la empresa pública para la venta de armamentos, Rozvoorzheniye, dando licencias a otras 12 empresas privadas, pero dicha medida tuvo que anularse ante los escándalos en la venta de armamentos realizados por varias de estas empresas el Estado tuvo que volver a controlar la cuestión de la venta de armamentos.

Han aparecido en numerosos medios de comunicación denuncias sobre el lamentable estado en que se encuentran los depósitos de munición en muchos de estos países, que en mucho casos están sin vigilar y descuidados.

Durante las revueltas ocurridas en Albania en abril del año 1997 numerosos arsenales del Estado fueron saqueados centenares de depósitos de munición y arsenales. Algunas fuentes estiman que cerca de un millón de armas ligeras y más de 1.500 millones de disparos de munición fueron extraídos de allí. Muchas de esas armas podrían estar ahora en manos del ELK y circulando incluso por muchos de los países de la OTAN y la Unión Europea.

Semejante cantidad de armamento en el mercado negro provoca situaciones tan asombrosas en países como Mozambique o Angola, donde un fusil de asalto *Kalashnikov* AK-47 con dos cargadores se puede adquirir solamente por 15 dólares.

Soluciones

Hasta aquí hemos planteado la gravedad del problema que supone la existencia del tráfico ilegal de armas en el ámbito internacional y lo que representa para la seguridad y la estabilidad internacional. Ahora debemos analizar cuales son las medidas a adoptar para combatirlo. Las medidas en el ámbito nacional hemos visto que son del todo insuficientes ya que el tráfico ilegal de armas se mueve precisamente entre las lagunas legislativas que existen en la comunidad internacional, por lo tanto, para combatir esta amenaza la cooperación internacional es indispensable.

Si hemos de definir en dos palabras cuales han sido las medidas en el ámbito internacional adoptadas hasta el momento para resolver este problema la respuesta sería: absolutamente nada.

Tan sólo en los últimos años varias organizaciones internacionales se han planteado seriamente este problema y están estudiando ciertas medidas para combatirlo. Son muchas personas las que opinan que este tipo de tráficos ilegales, en particular el de armas y el de la droga, son casi imposibles de erradicar en función de que aportan mucho dinero con mínimo esfuerzo y que nunca faltarán clientes para ellos. A pesar de esto, si su erradicación completa es casi imposible, si se deben establecer una serie de mecanismos y controles para mantenerlos bajo control y evitar que la inestabilidad que la existencia de dichos tráficos conlleva se extienda en el terreno internacional.

Vamos a repasar, organización por organización, las medidas que se están adoptando y el estado de la cuestión en cada una de ellas.

Organización de Naciones Unidas (ONU)

Las Naciones Unidas como principal foro de discusión internacional y generador de Derecho Internacional, debe ser el foro central en el cual se abarque en el ámbito global el problema del tráfico ilegal de armas. Curiosamente, la cuestión del tráfico ilegal de armas no se aborda en el Consejo de Seguridad ni en ninguno de los varios foros que sobre desarme tiene la ONU, a pesar de que al comenzar las negociaciones sobre desarme en Ginebra se incluyó en uno de sus puntos la cuestión de los armamentos convencionales, que posteriormente se olvidó, centrándose en la cuestión nuclear y química. La cuestión del tráfico ilegal de armas se trata en el Consejo Económico y Social (ECOSOC), en concreto en la Comisión sobre Prevención del Crimen y Justicia Criminal.

En abril del año 1998 esta Comisión del ECOSOC aprobó una resolución orientada a crear una convención internacional sobre tráfico ilegal de armas para ser establecida en la Asamblea General. Dicha resolución fue firmada por 54 países. Los principales puntos abordados en dicha resolución son:

1. El tráfico ilegal y el uso criminal de las armas de fuego dañan la seguridad de todos y cada uno de los Estados y pone en peligro el bienestar de los pueblos y su desarrollo económico y social.
2. La apreciación del papel de organizaciones regionales como la OEA y su Convención Interamericana contra la Fabricación Ilícita de Armas de Fuego, Munición, Explosivos y otros Materiales Relacionados.
3. El establecimiento de regulaciones modelo para el control del movimiento internacional de armas de fuego, así como sus partes y componentes, incluyendo además los explosivos.
4. Tener en cuenta algunas medidas adoptadas por foros como la Unión Europea y la Directiva del Consejo Europeo sobre regulación de armas de fuego Directiva 91/477/CEE de 18 junio 1991.
5. El establecimiento de grupos de trabajo sobre regulación de armas de fuego de Europa, África, América y Asia.

El principal objetivo del ECOSOC con esta resolución era elaborar un instrumento internacional para combatir la fabricación y tráfico ilícitos de armas de fuego, partes componentes y munición, así como métodos para identificar y hacer el seguimiento de dichas armas, y proponer la creación de un régimen para la exportación e importación de dichas armas que impida su canalización a otros usos ilegales.

El Grupo de los ocho (G-8)

Los G-8, el antiguo G-7 más Rusia, fue uno de los primeros foros en los cuales se empezó a tratar la cuestión del tráfico ilegal de armas. Ello es sumamente significativo pues debemos tener en cuenta que los países miembros de dicho foro son, a su vez, los principales vendedores de armamentos en el mundo, por lo que sus resoluciones podrían tener más efectividad práctica que las adoptadas incluso en Naciones Unidas.

La primera vez que se trató el tema del tráfico ilegal de armas fue en la Cumbre de Halifax en 1994. Posteriormente se volvería a ello en la Cumbre mantenida en Denver en 1997, donde se tomó la decisión de considerar la creación de un nuevo instrumento internacional y un régimen más fuerte para el control del tráfico ilegal de armas. Se tuvieron en cuenta las medidas adoptadas por la OEA

En la Cumbre sostenida ese mismo año en Washington, los G-8 dieron 40 recomendaciones para la lucha contra el crimen organizado en el ámbito global, englobando entre sus actividades, lógicamente, el tráfico ilegal de armas. Los principales puntos hablaban de la necesidad de fortalecer la cooperación con la ONU, la Unión Europea y otros foros que ya han adoptado medidas para la lucha contra dicho tipo de crimen. Se apoya la idea de negociar en los próximos dos años una convención la ONU contra el crimen organizado para proporcionar herramientas a las autoridades nacionales para luchar contra él. Entre dichas medidas, los G-8 aprobaron un plan de 10 puntos y 10 principios contra el crimen de «alta tecnología», de manera que se alcance un acuerdo para crear un trasfondo legal con el objetivo de obtener, presentar y preservar datos electrónicos como evidencia para su posible persecución judicial. También se estudió el impacto de las nuevas tecnologías en dicho tipo de crimen, y se estudió controlar el abuso de Internet y otras tecnologías para combatirlo.

En la siguiente reunión mantenida en Birmingham los días 15-17 de mayo de 1998 se volvieron a reiterar las medidas anteriormente contra el tráfico de armas.

En el año 1999 se espera mantener en Moscú una reunión ministerial para combatir el crimen transnacional. Entre las nuevas propuestas a presentar se incluye el establecimiento de nuevas Unidades de Inteligencia Financiera (FIU) *Fiscal Intelligence Unit*, para recoger, procesar y analizar la información sobre blanqueo de dinero llevado a cabo por dichos grupos, así como aumentar la colaboración con otras agencias, de manera que se

puede detener y confiscar los bienes de aquellos que lo practican, aunque sea en otros países.

Los países del G-8 aprobaron la idea de crear una convención internacional sobre el crimen organizado en el marco de la ONU y suscribieron la convención global contra el tráfico de armas creada por el ECOSOC. Sin embargo, a pesar de la importancia de la adhesión de los países del G-8, limitan su utilidad en función de que, al ser tratado el tema en el ECOSOC esta declaración se dirige solamente a la proliferación de armas pequeñas y su transferencia a los criminales no al conjunto global del tráfico internacional de armas. Las fronteras entre crimen y conflicto son muy difusas y tomar el problema sólo como una cuestión de prevenir el crimen sólo puede tener un éxito limitado. Hay que reexaminar las políticas interiores y de exportación de los países y sus responsabilidades como productores, vendedores y receptores de armas ligeras.

Los aspectos a debatir en futuras reuniones deberán ser la relación entre crimen y conflicto, la creación de fondos necesarios para controlar el tráfico ilegal de armas y los lazos entre el tráfico legal e ilegal de armas

Unión Europea

INICIATIVAS PARA IMPEDIR Y CONTROLAR EL TRÁFICO DE ARMAS

La Unión Europea fue una de las primeras organizaciones en llevar a cabo medidas concretas para el tráfico ilegal de armas, tanto en el ámbito de los países miembros, como en la relación de éstos de cara al exterior. Las primeras referencias a este tema las encontramos en las conclusiones del Consejo Europeo de Luxemburgo, *Boletín* 6-1991, punto 1.47 y en las conclusiones del Consejo Europeo de Lisboa, *Boletín* 6-1992, punto 1.28, en las cuales ya se habla del establecimiento de medidas para evitar la proliferación y controlar las exportaciones de armamento de los países miembros.

El siguiente paso se dio en junio de 1997 cuando la Unión Europea acordó un «Programa para la Prevención y Combate del Tráfico Ilícito de Armas Convencionales». Dicho Programa fue firmado por los 15 Estados miembros. El Programa combina una serie de medidas para combatir el tráfico ilegal de armas en los países miembros a través de la asistencia y mejora de las capacidades de los países para combatirlo y así como establecer medidas para la retirada de armamentos de la sociedad en regiones de conflicto.

El paso más importante dado por la Unión Europea en materia de control de armamentos se llevó a cabo entre enero y junio de 1998, cuando en la Unión Europea se discutió la creación de un Código de Conducta para las exportaciones de armamento de los países miembros. La importancia de este paso se refleja en el interés que el Congreso de Estados Unidos y una comisión de Premios Nobel han expresado en dicho Código para crear códigos similares para Estados Unidos y toda la comunidad internacional. Naciones Unidas, como ya hemos visto, abogaba por un código similar.

El Código de Conducta sobre exportación de armas se aprobó mediante un acuerdo político del Consejo de Asuntos Generales, el día 25 de mayo de 1998. Este Código, basado en los criterios establecidos por los Consejos Europeos de Luxemburgo y Lisboa de 1991 y 1992 en materia de no-proliferación y exportación de armas, establece una serie de disposiciones operativas para garantizar la aplicación de dichos criterios.

Los criterios que los países miembros deberán tener en cuenta a la hora de exportar armamento deberán ser:

1. Respeto de los compromisos internacionales de los Estados miembros de la Unión Europea, en particular las sanciones decretadas por el Consejo de Seguridad de Naciones Unidas y las decretadas por la Comunidad, los acuerdos de no-proliferación y otros temas, así como otras obligaciones internacionales.
2. Respeto de los derechos humanos por parte del destinatario final. No se expedirá una licencia de exportación cuando exista un riesgo manifiesto de que la exportación propuesta pueda utilizarse con fines de represión interna y se ponderará con especial detenimiento, caso por caso, y según la naturaleza de los equipos, a países en los que los organismos competentes de Naciones Unidas, el Consejo de Europa o la Unión Europea hayan constatado graves violaciones de los derechos humanos
3. Situación interna del país destinatario final, en términos de la existencia de tensiones o conflictos armados.
4. Mantenimiento de la paz, la seguridad y la estabilidad regional. Se tendrá en cuenta la existencia o probabilidad de un conflicto armado entre el país receptor y otro país, la reivindicación de territorio de un país vecino que el receptor haya intentado imponer o haya amenazado con obtener por la fuerza en el pasado, la probabilidad de que el equipo sea utilizado con fines distintos de la seguridad nacional y la legítima defensa del receptor, y la necesidad de no perjudicar de forma importante la estabilidad regional.

5. Seguridad nacional de los Estados miembros, de los países amigos o aliados y de los territorios cuyas relaciones exteriores dependan de un Estado miembro.
6. Comportamiento del país comprador respecto de la comunidad internacional, en especial a su actitud frente al terrorismo, la naturaleza de sus alianzas y el respeto al Derecho Internacional.
7. Existencia del riesgo de desvío interno o de reexportación no deseada.
8. Compatibilidad de la exportación de armas con la capacidad técnica y económica del país receptor, teniendo en cuenta la conveniencia de que los Estados satisfagan sus necesidades legítimas de seguridad y defensa con el mínimo desvío de recursos humanos y económicos para armamentos. El Código prevé una serie de disposiciones prácticas para la verificación del cumplimiento de este código de conducta.
9. Se cotejarán una por una las solicitudes de licencia de exportación con los criterios del Código de Conducta.
10. El criterio no va en menoscabo de aplicar por parte de los Estados miembros normas más estrictas.
11. Los Estados miembros difundirán por cauces diplomáticos los datos de las licencias denegadas en virtud del Código de Conducta junto con la motivación de la misma.
12. Se mantendrá la confidencialidad de las consultas y denegaciones y no se usarán para fines comerciales.
13. Se llevará a cabo la adopción de una lista común de equipo militar.
14. Se reforzará en el marco de la Política Exterior de Seguridad Común (PESC) la cooperación y la convergencia en el ámbito de la exportación de armas convencionales.
15. Cada país miembro distribuirá anualmente un informe anual confidencial sobre sus exportaciones de armas y su aplicación del Código.

Organización de Estados Americanos (OEA)

La OEA, al igual que ocurriera en el año 1968 con la firma del Tratado de Tlatelolco y la creación de la primera zona libre de armas nucleares en el mundo, adelantándose a todas las demás organizaciones internacionales, también se ha adelantado ahora a todas las demás en la lucha contra el tráfico ilegal de armas mediante la firma en el mes de noviembre de 1997 de la Convención Interamericana contra la Fabricación y Tráfico Ilegales de Armas de Fuego, Munición, Explosivos y otros Materiales Relacionados.

Dicha Convención supone un gran salto cualitativo en el ámbito internacional para la lucha contra el tráfico ilegal de armas, tal como lo han reconocido la ONU y los países del G-8. Dicha Convención es, para muchos, junto con el código de conducta de la Unión Europea, la base sobre la que se debe desarrollar un futuro código internacional contra el tráfico ilegal de armas.

La firma de dicha Convención nace de la preocupación por el incremento en el ámbito internacional de la fabricación y el tráfico ilícito de armas, municiones y explosivos y los perniciosos efectos que tiene esta actividad sobre la seguridad de cada Estado y su influencia en el desarrollo económico y social y el bienestar de los pueblos

La Convención tiene como base un informe que el Consejo Permanente de la OEA elaboró sobre el tema —AGH/doc.6 (XXIV-E/97)/rev.1—, fruto del interés de algunos Estados ya expresado en la Cumbre de las Américas celebrada en Miami en el año 1994 y del comunicado del Grupo de Río a instancias de México elaborado el día 4 de septiembre de 1996.

La Convención detalla en primer lugar el significado de cada uno de los términos empleados y establece su objetivo que es prevenir, combatir y erradicar la fabricación y el tráfico ilícito de armas de fuego, munición, explosivos y otros materiales relacionados, así como promover y facilitar la cooperación e intercambio de información y experiencia entre los Estados firmantes para dicho fin.

Entre las medidas: marcado de las armas en el punto de fabricación y de importación, armonización de los procedimientos de licencias e intercambio de información y experiencia.

OTAN-Organización para la Seguridad y Cooperación en Europa (OSCE)

La OSCE es más adecuada para acuerdos políticos, mientras que la OTAN serviría para forzar altos el fuego, embargos de armas y destrucción y entrega de las mismas. Ambos deben desarrollar programas de control de armas ligeras en Europa, junto con la Comunidad de Estados Independientes (GEI) y G-8.

Entre las medidas que ambos podrían adoptar se halla el control de armas sobrantes, destrucción de *stocks*, la restricción de los flujos a áreas de tensión y la extensión del Código de Conducta de la Unión Europea a todos los Estados OSCE, así como el control de las propias industrias de armamento.

La cooperación de ambas Organizaciones puede ser vital para complementar las medidas de lucha contra el «mercado negro», bien compartiendo información o desarrollando los contactos de inteligencia, desarrollando las legislaciones nacionales o estableciendo una convención de la OSCE sobre control de tráfico ilícito de armas.

La OSCE podría llevar a cabo también programas de microdesarme en regiones localizadas. Esta Organización debe ampliar su gestión diplomática de conflictos e incluir aspectos como el del tráfico de armas.

La OTAN tiene necesidad de establecer una política coherente para el control de armamentos (tanto legales como ilegales) a través de la Asociación para la Paz (APP) con los países de centro y este de Europa. En los Acuerdos de Dayton para finalizar la guerra en la antigua Yugoslavia no se estableció una destrucción de armamento ligero. En vez de eso, Estados Unidos ha introducido en el Ejército bosnio 41.000 fusiles de asalto M-16, 2.000 ametralladoras y 21 millones de disparos de munición, sin retirar antes las armas que poseían los bosnios, gran parte de esas armas han ido a parar al «mercado negro» y de ahí a la guerrilla kosovar.

En los actuales ejercicios y entrenamientos que la OTAN realiza para futuras operaciones de paz, sí se están introduciendo medidas para retirar las armas de circulación y evitar la extensión del conflicto. La experiencia adquirida en Bosnia, y últimamente en Kosovo, parece haber calado en los mandos OTAN y es previsible que en adelante, en todos los despliegues militares de la Alianza Atlántica, se tenga en cuenta la necesidad de destruir el armamento sobrante y controlar el destino de las armas desmovilizadas en las partes enfrentadas

Algunos aspectos que tanto la OSCE (como Organización en el ámbito político), como la OTAN (como Organización más del ámbito militar) deberían tratar al abordar la cuestión del control del tráfico ilegal de armas son:

PROGRAMAS DE CONTROL EN LA OTAN

— Introducir el aspecto del tráfico ilegal de armas en los foros de debate de ambas Organizaciones, tal como el Consejo de Cooperación Euroatlántico (CCEA) y la APP.

PROGRAMAS DE CONTROL EN LA OSCE

La OSCE en un aspecto más político, debería:

- Crear un sistema de seguimiento y una base de datos para los *stocks* y transferencias de armas, tanto en tiempos de paz, como en las zonas de conflicto.
- Programas de microdesarme, llevados a cabo a nivel local o regional.
- Medidas de Creación de Confianza (CBM) que permitan una mayor transparencia y cooperación en la lucha contra el tráfico ilegal.

DESTRUCCIÓN DE ARMAS SOBRANTES

Impedir el reciclaje de armamentos retirados de los arsenales o desmovilizados en conflictos:

- Programas de destrucción de armas en misiones de pacificación.
- Destrucción del armamento obsoleto sustituido por otro nuevo.
- Apoyo financiero a los Estados que lleven a cabo programas de desarme.
- Apoyo financiero a las organizaciones, estatales o no, que lleven a cabo programas de microdesarme.
- Ofrecer incentivos económicos y financieros (y en su caso políticos), así como garantías de seguridad, a los Estados a cambio de la destrucción de los *stocks* de armas sobrantes.
- Destrucción de los propios *stocks* de la OTAN como CBM y ejemplo. Por ejemplo, el ministro holandés de Defensa ha anunciado que, incapaz de encontrar compradores que satisfagan los criterios del Código de Conducta de la Unión Europea para exportación de armamentos, se destruirán la mayoría de las armas sobrantes.

CONTROLAR LOS TRÁFICOS ILEGALES DE ARMAS A LAS REGIONES EN CONFLICTO

- Programas de microdesarme llevados a cabo por Organizaciones No Gubernamentales (ONG).
- Legislación internacional y marcos para tratar con traficantes y *brokers*.
- Registros regionales de armas ligeras.

MEDIDAS RESTRICTIVAS

- Promover medidas para impedir los flujos de armas a regiones en conflicto desde o a través de los Estados OSCE.
- Extender Código de Conducta de la Unión Europea a todos los países miembros de OSCE.
- Adoptar los criterios de la OSCE y de la Unión Europea en la CEI y vigilar su cumplimiento.

CONTROL DE LA INDUSTRIA DE ARMAMENTOS

- Controlar en sus orígenes la fabricación de armamentos.
- Aplicación estricta del Código de Conducta de la Unión Europea a los fabricantes.
- Controles sobre exportaciones e importaciones

Conclusiones

Como principales conclusiones de este estudio, encaminadas a controlar y perseguir el tráfico ilegal de armamentos, hemos llegado a las siguientes:

1. Es necesario incorporar programas de recolección y destrucción de armas en las misiones de pacificación de la ONU. Recientemente en la misión de las Fuerzas de Estabilización (SFOR) llevada a cabo en Bosnia por la OTAN bajo mandato de Naciones Unidas se comenzó a llevar a cabo una recogida de armas ligeras, denominada operación *Harvest* (cosecha).
2. Son necesarias medidas en foros como G-8, Unión Europea, CEI o la Asociación de Naciones del Sureste Asiático (ASEAN) aporten fondos y reorienten la ayuda hacia el control de armas ligeras.
3. Reconocimiento de los lazos entre la seguridad y estabilidad y desarrollo a largo plazo. Sin embargo, los programas para impulsar el control interno en regiones proclives a conflictos apenas dispone de fondos.
4. El Código de Conducta de la Unión Europea debe ser el punto de salida para crear un código internacional verdaderamente restrictivo para impedir la venta de armas a regímenes represivos, que no respetan los derechos humanos y a zonas en conflicto.
5. Combatir el tráfico ilegal de armas del «mercado negro» a través de medidas como: persecución de los traficantes y crimen organizado que trafican con armas en conjunción con las luchas contra el terrorismo y la droga. La Oficina Europea de Policía (EUROPOL) podría tener competencias para ello, y beneficiarse de la experiencia de la Comisión Internacional de Policía Criminal (INTERPOL) y su IWETS (*Interpol Weapons and Explosives Tracking System*). La única base de datos internacional para armas robadas, IWETS puede facilitar el seguimiento.
6. Establecer unas medidas de seguridad mayores en torno a las armas, tanto en su fabricación como en su circulación.
7. Fomentar una mayor cooperación en cuestiones de inteligencia e información sobre traficantes, mafias y crimen organizado y su relación con el tráfico ilegal de armamentos.

8. Reforzar las legislaciones nacionales sobre posesión de armas por particulares y controlar su uso y distribución.

Munición y conflicto armado

En los círculos de seguridad y diferentes centros de análisis de conflictos, se ha comenzado a abordar un tema, cuando menos novedoso, sobre un aspecto hasta ahora prácticamente olvidado de la lucha contra el tráfico ilegal de armas: el control de la munición como método para combatir el tráfico de armas.

Un antiguo adagio dice que un fusil sin munición es un palo de metal, por lo tanto sería lógico pensar que si no podemos controlar el fusil, tal vez si se podría controlar la munición.

La munición sigue las mismas rutas que las armas en su camino hacia el «mercado negro», y a cada gran venta de armamento le suele acompañar una venta mayor aún de munición. La mayor parte de la munición procede de Estados Unidos actualmente, pero Rusia y los países del Este, gracias a sus precios más bajos, comienzan a arrebatarse el liderazgo en determinadas zonas y tipos de armamento.

La idea de controlar la munición, podría parecer, por lo que hemos descrito anteriormente, tan difícil de aplicar como la del control del armamento propiamente dicho, pero tiene algunos aspectos que podrían hacer más factible un control más estricto sobre los envíos de munición.

La munición consiste básicamente en cuatro partes: bala, casquillo, propelente e iniciador. Pues bien, mientras que la bala y el casquillo pueden ser fácilmente fabricados en cualquier taller mínimamente equipado, la pólvora ya es más difícil de fabricar. En cuanto al fulminante o iniciador, normalmente compuesto por nitrato de mercurio, solamente existen en el mundo unas 150 compañías capaces de fabricarlo. Es decir, sólo 150 compañías en el mundo reúnen las características para fabricar los cuatro componentes de la munición.

Por lo tanto, a la hora de controlar la munición y el armamento desde el origen, será siempre más fácil hacerlo con la munición ya que sólo 150 compañías en el mundo pueden fabricar los cuatro componentes en conjunto. Igualmente, a la hora de introducir métodos de control sobre armas y municiones, la menor existencia de fabricantes de munición permitiría homogeneizar y poner en marcha dichas medidas.

Recomendaciones

Las recomendaciones para el control y lucha contra el tráfico ilegal de municiones son, lógicamente, las mismas que para el control de armamentos.

Podríamos incidir de nuevo sobre la destrucción de los excedentes de munición, establecer el control de munición unido al control de armamentos, promover y controlar una mayor transparencia en la producción de munición, crear nuevos métodos para identificar y marcar la munición y, examinar las rutas de comercio, transferencias, equipos de abastecimiento, precios y acuerdos tarifarios a nivel internacional que faciliten la labor de control.

ARMAMENTO NUCLEAR, QUÍMICO Y BIOLÓGICO

Por VICENTE GARRIDO REBOLLEDO

Algunos problemas relacionados con el control de las armas de destrucción masiva

Cuando nos referimos al control de las armas de destrucción masiva o NBQ (Nucleares, Biológicas y Químicas, respectivamente) se nos escapa el hecho que como tal, el «control» es un concepto político con infinidad de problemas técnicos. El control de armas de destrucción masiva trata de evitar la proliferación horizontal, es decir, la que se produce entre Estados que no teniendo armas NBQ acceden a ellas por vez primera. Por su parte, el desarme persigue la dimensión vertical de la proliferación con el objetivo de eliminar totalmente los arsenales de aquellos Estados que ya disponen de ese tipo de armas (1).

Por lo tanto, aunque «control» y «desarme» comparten en sí la misma filosofía, si se tiene en cuenta que el objetivo final no es el mismo (la reducción de las armas, o por lo menos, su no incremento, hasta un límite aceptable, en el caso del control o bien, su total eliminación, en el caso del desarme), conviene también considerar por separado las medidas con las que cuentan ambos ámbitos para frenar su proliferación. Además,

(1) A este respecto véase, GARRIDO REBOLLEDO, V.: «La agenda de las negociaciones sobre no-proliferación y desarme» en «Un estudio sobre el futuro de la no-proliferación», *Monografías del CESEDEN*, número 30, pp. 19-49. Centro Superior de Estudios de la Defensa Nacional, Ministerio de Defensa. Madrid, marzo 1999.

como medida específica de no-proliferación habría que considerar la cuestión de los tráficos ilícitos, ya no sólo de armas de destrucción masiva, sino de sustancias e incluso, del conocimiento científico necesario para su fabricación.

Es en este último punto en donde comienza el primero de lo que podríamos denominar problemas técnicos del control: cómo saber *a priori* que un material o sustancia NBQ va a ser utilizada expresamente para la fabricación de armamento de destrucción masiva. La cuestión acerca de cómo evitar que un material o tecnología inicialmente declarado con finalidad civil pueda, amparándose en el doble uso, civil y/o militar, ser finalmente destinado a una actividad no pacífica ha sido objeto a partir de 1995 de una gran atención por parte de los regímenes de no-proliferación. Ello ha conducido en algunos casos concretos a la adopción de políticas multilaterales, como la de la Unión Europea que, cómo analizaremos, ya ha dado sus primeros frutos.

El segundo de los problemas está relacionado con la definición y naturaleza del «riesgo», muy distinta dependiendo del ámbito al que nos refiramos. En el nuclear, desaparecida la amenaza militar procedente de los países del Este, tras la desintegración política de la Unión Soviética, el objeto de preocupación se centró casi de forma inmediata en el futuro de las cerca de 30.000 armas nucleares en manos de Rusia y las nuevas Repúblicas nucleares soviéticas (Bielorrusia, Ucrania y Kazajstán). Estas tres últimas renunciaron al derecho de conservar su estatus nuclear en virtud del Protocolo de Lisboa del Tratado START I, suscribiendo el Tratado de No-Proliferación de Armas Nucleares (TNP) entre los años 1993 y 1994. No obstante, dicha decisión, aunque histórica, no evitó que se produjesen los primeros casos preocupantes de tráfico ilícito de sustancias y materiales del antiguo arsenal nuclear soviético, unido a la llamada fuga de cerebros o científicos nucleares a terceros Estados en el «umbral nuclear».

La nueva situación puso de manifiesto que el riesgo nuclear de final de siglo estaría centrado en cómo evitar que terceros Estados sacasen partido del debilitamiento de los sistemas de control a la exportación de muchas industrias nucleares soviéticas (especialmente, desde la desaparición del monopolio estatal de exportación de materiales nucleares, Technabexport) o simplemente, que colectivos que asistían impotentes a la pérdida de su poder adquisitivo, por el impago de salarios (como el Ejército) o se le retiraban los privilegios de los que gozaban bajo la Unión Soviética, por ejemplo, los físicos nucleares, se sintiesen tentados a acu-

dir a un floreciente «mercado negro» o bien ofrecer sus servicios a terceros Estados con dudosas ambiciones nucleares (2).

El caso iraquí puso el dedo en la llaga (3). Denotó no sólo la falta de controles efectivos a la exportación de materiales y componentes esenciales para la fabricación de armamento nuclear (y ello, pese a que Irak era un Estado-Parte en el TNP desde 1970) sino sobre todo, la necesidad de intensificar dichos controles, no poniendo en marcha nuevas instituciones, sino reforzando los mecanismos ya existentes. Esa fue precisamente la filosofía del programa reforzado de salvaguardias del Organismo Internacional de la Energía Atómica (OIEA) conocido con el nombre «93+2» (4). El modelo de Protocolo Adicional (INFCIR/540) que desarrolla el sistema de salvaguardias a aplicar por el OIEA a todo el conjunto de instalaciones y actividades del ciclo combustible nuclear, fue adoptado por el Organismo el 15 de mayo de 1997. El día 1 de octubre de 1999, fecha de conclusión de la XLIII Asamblea General del OIEA, 45 Estados habían suscrito ya acuerdos de salvaguardias adicionales con el Organismo (5).

Hoy día el riesgo nuclear se sigue definiendo en términos de proliferación horizontal. Además de las cinco potencias nucleares *de iure* (Estados Unidos, Rusia, Reino Unido, Francia y China, por orden cronológico de acceso al arma nuclear), existen dos Estados nucleares *de facto*, India y Pakistán, tras la realización de pruebas nucleares en mayo de 1998 (6)

(2) Véase GARRIDO REBOLLEDO, V.: «El futuro del arsenal nuclear soviético» en *Anuario 1991-1992*, pp. 125-138, Centro de Investigación para la Paz (CIP). Icaria. Barcelona, 1992. «Problemas Nucleares en la CEI: ¿Un futuro incierto?» en *Cuadernos del Este*, número 8, pp. 79-86. Editorial Complutense. Madrid, abril 1993.

(3) Para un análisis completo acerca del origen y evolución del programa nuclear iraquí véase, GARRIDO REBOLLEDO, V.: «El programa nuclear iraquí: el juego del escondite» en *Tiempo de Paz*, número 23, pp. 90-97. Madrid, 1992.

(4) El Programa «93+2» consta de dos partes. La aplicación de la primera, que se refiere al refuerzo de las medidas de verificación bajo el acuerdo de 1972 denominado INFCIRC/153, y que todo Estado-Parte en el TNP está obligado a concluir con el OIEA, se puso en marcha en el año 1995. Por lo que respecta a la segunda parte, el Organismo decidió adoptar un conjunto de medidas de refuerzo de las salvaguardias mediante la adopción de un protocolo adicional, que sería aplicado a los Estados que ya tuviesen suscrito un acuerdo de salvaguardias totales con el OIEA. Para más información sobre el programa véase, GARRIDO, V., MUELLER, H. y MARQUINA, A. (eds.): «The implications of the 1995 NPT Review and Extension Conference: A Spanish point of view», en *Unisci Papers*, número 7. Madrid, 1996.

(5) Documento del OIEA GC (43)/L.13.

(6) Sobre los programas nucleares de ambos Estados y el análisis de la situación tras los ensayos, véase GARRIDO REBOLLEDO, V.: «India, Pakistán y el Régimen de No-Proliferación Nuclear», en *Política Exterior*, número 64, pp. 99-107. Julio-agosto de 1998; «India y Pakistán: ¿dos nuevas potencias nucleares?», en *Revista Española de Defensa*, pp. 72-77. Julio-agosto de 1998 y «Locura nuclear asiática», en *Tiempo de Paz*, número 49, pp. 53-63. 1998.

junto con Israel, único Estado nuclear no reconocido como tal. Al margen de los citados, la capacidad nuclear del resto de los Estados, aunque en muchos casos muy avanzada, pasa necesariamente por la ayuda de un tercer país para poder fabricar un arma nuclear. En definitiva, ello significa que el control de la proliferación nuclear comienza por el del tráfico ilícito de materiales fisibles, como el plutonio 239 (Pu-239) o el uranio altamente enriquecido.

Del año 1993 a 1995 el OIEA detectó 227 casos considerados como «tráficos ilícitos de materiales radiactivos» y otros 106 sospechosos, pese a que las cantidades confiscadas a particulares, sin ninguna conexión con redes internacionales o mafias nucleares, siempre fueron relativamente pequeñas. Pese a que las cifras han disminuido considerablemente, sobre todo, a raíz de la creación de un banco de datos del organismo sobre tráfico ilícito, de los 33 casos de tráfico con sustancias radiactivas, nueve se consideraron operaciones ilícitas. El día 31 de diciembre de 1998, el número acumulado de casos de tráfico ilícito de materiales nucleares contabilizados por el OIEA ascendía a 304, de los cuales, 237 habían sido confirmados por los propios Estados (7).

Cuestión diferente a la de los tráfico ilícitos sucede en el caso de que cualquiera de los ocho países mencionados decidiese suministrar armas nucleares «listas para su lanzamiento» a terceros Estados que no las poseyesen, algo que por otra parte, iría en contra del artículo I del TNP, se verá más adelante.

Pese a todo, el riesgo nuclear no se acaba con la posibilidad de que los materiales radiactivos puedan ser transferidos a un tercer Estado para fabricar un arma nuclear. No hay que olvidar los riesgos medioambientales derivados de la posible contaminación por la manipulación de los mismos. La fabricación de una bomba atómica exige grandes conocimientos científicos y técnicos, cuyo conjunto parece estar fuera del alcance de individuos e incluso de grupos terroristas, pese a que las novelas de ciencia ficción se esfuerzan por demostrarnos lo contrario.

Sin embargo, pese a que el tráfico de materiales nucleares para la fabricación de armamentos disminuya, no significa que los riesgos de robo de sustancias utilizadas en medicina y en la industria y por lo tanto, fáciles de encontrar, sea nulo. A título de ejemplo, el plutonio 238 se utiliza en los

(7) *The IAEA Annual Report for 1998.*

análisis por fluorescencia de rayos X o el iridio 192 (de alta intensidad) para la radioterapia. Ello quiere decir que si bien las armas nucleares parecen hoy día bajo control de unos pocos Estados, no sucede lo mismo con las fuentes o los desechos radiactivos, muchas veces olvidados y a merced que puedan ser robados. El incidente del año 1997 en Lilo, cerca de Tbilisi (Georgia), en el que 11 soldados resultaron severamente irradiados por cápsulas de cesio 137 abandonadas en una antigua base del Ejército Rojo (transformada posteriormente en Centro de Formación de Guardias Fronterizos), representa sólo la punta del iceberg de un problema en el que tanto el OIEA como la Comisión Internacional de Policía Criminal (INTERPOL) ya trabajan conjuntamente (8).

Por lo que respecta a los ámbitos biológico y químico la definición del riesgo es mucho más compleja. En primer lugar, los controles sobre la producción de armas biológicas y/o químicas han sido hasta ahora prácticamente inexistentes, debido a la falta de mecanismos de verificación. La Convención para la Prohibición de las Armas Químicas (CAQ) entró en vigor hace tan sólo dos años, el día 29 de abril de 1997 y su mecanismo de verificación no contempla ningún sistema internacional de vigilancia de modo que, los datos que sobre ese tipo de armas se puedan obtener proceden de la denuncia de un Estado-Parte en la Convención Acerca de las Actividades Ilícitas de otro Estado o de las propias declaraciones que realice el Estado en cuestión (9). Por lo que respecta al ámbito biológico, aún no se ha adoptado ni siquiera un protocolo de verificación, con lo que los mecanismos de control de la Convención para la Prohibición de las Armas Biológicas (CAB), que entró en vigor en 1975, son totalmente ineficaces, mientras que dicho protocolo, que desde 1995 se está negociando por un Grupo *Ad-Hoc* especial, no sea firmado por los Estados-Partes en la Convención.

En segundo lugar, no resulta tampoco tan fácil controlar las posibles transferencias de sustancias químicas, debido a su mayor diseminación. Se estima que existen alrededor de 20 Estados con programas químicos operativos con finalidad militar. Sólo se sabe que tres de ellos (Estados

(8) Conviene recordar que en septiembre del año 1998 tuvo lugar en Dijon (Francia) el I Congreso Internacional sobre Control y Prevención de Accidentes con Dispositivos Nucleares y «fuentes huérfanas», patrocinado por ambos Organismos. A él asistieron policía, cuerpo de aduanas y expertos de 83 Estados.

(9) Sobre el funcionamiento y aplicación de la CAQ tras su entrada en vigor véase KELLE, A.: «Assessing the First Year of the Chemical Weapons Convention» en *The Nonproliferation Review*, pp. 27-35. Primavera-verano, 1998.

Unidos, Rusia e Irak) poseen arsenales químicos (los dos `primeros porque así lo han declarado mientras que el iraquí fue descubierto a raíz de las inspecciones internacionales). Sin embargo, existen sospechas que otros muchos Estados están desarrollando en la actualidad programas químicos con finalidad militar.

En relación con las armas biológicas, la situación es mucho más ambigua debido a que, con la única excepción de Estados Unidos, que admitió haber puesto fin en 1969 a su programa de armas biológicas, ningún otro Estado ha reconocido oficialmente haberlas fabricado ni siquiera, haber investigado y experimentado en animales con ellas (10).

En tercer lugar, porque a diferencia de las armas nucleares, lo importante de las armas químicas y biológicas no es su número, sino su posesión efectiva, dado que su multiplicación en laboratorios es más sencilla y rápida y tampoco exigen grandes inversiones. De ahí que frecuentemente se hable de la «bomba de los pobres» para referirse a este tipo de armas, porque se pueden utilizar para su producción las mismas infraestructuras e instalaciones que las industrias civiles (química y farmacéutica). A menudo se emplea también la expresión proliferación cualitativa para referirse a las armas químicas y biológicas ya que, este tipo de armas, constituyen hoy día una amenaza más política que militar y resultan mucho más efectivas como medida de chantaje o amenaza ante su eventual utilización.

En cuarto lugar, tampoco se necesitan sofisticados sistemas de expulsión para su lanzamiento (como demostró el atentado en «el metro» de Tokio en mayo del año 1995), ni grandes contenedores para su transporte. Pueden ser fácilmente ocultadas y por lo tanto los tráfico ilícitos con estas sustancias de difícil detección.

Por otra parte, una peculiaridad añadida de las armas biológicas con respecto a las químicas consiste en que mientras estas últimas deben fabricarse en grandes plantas o laboratorios para que tengan una aplicación militar, los agentes biológicos, como el ántrax, se producen a pequeña escala y son mucho más efectivos con una sola unidad (se escoge sólo

(10) Acerca del programa de armas biológicas de algunos Estados, resulta de especial interés el estudio de RICHARDSON, B.: «The Threat of Chemical and Biological Proliferation». BAYLEY, K. y RUDNEY, R. (eds.): *Proliferation and Export Controls*, University Press of America-National Institute for Public Policy. Lanham, 1993. Respecto al programa de Estados Unidos, véanse las pp. 14-18.

unos pocos kilogramos de bacteria de ántrax seco para producir un arma letal efectiva).

No obstante, en relación con tema que nos ocupa, hay que tener en cuenta que los tráficos son lícitos o ilícitos dependiendo de la finalidad última de la sustancia NBQ transferida. En el ámbito nuclear se puede admitir la prohibición de transferir agua pesada, uranio altamente enriquecido o plutonio pero en cambio, no se puede prohibir en un régimen de control de sustancias biológicas la producción de una vacuna o un antibiótico, que a su vez puede servir para producir un virus. Este último podría ya ser utilizado como arma biológica. Y lo mismo sucede con respecto a un agente químico que sea la base de un pesticida, de utilidad para la agricultura pero susceptible de ser también utilizado como un arma binaria.

Además, como está poniendo de manifiesto la negociación del Protocolo de Verificación de la CAB, los Estados se muestran especialmente escépticos con respecto a los controles que podría imponer la CAB a sus actividades en el ámbito civil. Muchos Estados pretenden limitar las inspecciones (término sustituido por el menos sospechoso y agresivo de «investigaciones») a las instalaciones estrictamente militares que por otra parte, casi ningún Estado reconoce poseer. Aunque no se declare abiertamente, la industria farmacológica de los Estados más desarrollados se muestra también sumamente recelosa con respecto al sistema de investigaciones que pretende instaurar la Convención y al que considera podría dar lugar al intrusismo poniendo en peligro los secretos industriales. En otros casos las mismas industrias consideran que el nuevo Protocolo podría suponer una forma sencilla y nada sospechosa para poder acusar a una empresa de estar fabricando armamento biológico con la única finalidad de impedir que siga investigando o produciendo un producto que entre en competencia directa con otros laboratorios. Todos esos recelos tendrán que ser superados si se pretende conseguir la aplicación uniforme de un régimen eficaz de verificación de los agentes biológicos.

Breve clasificación de las armas químicas y biológicas y de sus efectos

Teniendo en cuenta la doble finalidad de las armas químicas y biológicas a la que nos venimos refiriendo, es necesario establecer una clasificación, si quiera de forma breve, de las sustancias químicas y biológicas, así

como los riesgos que ocasionaría para el hombre y su medio natural, su posible utilización como armas de destrucción masiva, bien en un conflicto, acción terrorista o accidente. Sólo de ese modo puede entenderse la magnitud del problema y las consecuencias que puede tener la ausencia de controles capaces de prevenir la utilización y especialmente, el tráfico ilícito de sustancias fácilmente alterables.

Armas químicas

Existen dos escenarios en los que las armas químicas pueden ser emitidas al medio ambiente. El primero, en un ataque contra una factoría de armas químicas. El segundo, por el uso directo de las armas en un ataque militar. Los efectos de las emisiones accidentales de los agentes químicos que pueden estar presentes en un conflicto serían diferentes en función del tipo de gas utilizado: nervioso, vesicante o asfixiante. Además, existen otros gases no letales pero nocivos para la salud y el medio humano. Pasamos a describirlos brevemente (11):

- Agentes nerviosos. Se trata de compuestos organofosforados diseñados para penetrar en el cuerpo humano a través de la piel o por inhalación. Su efecto (anticolinesterasado) inhibe la actividad del sistema nervioso, causando parálisis y finalmente la muerte por supresión del sistema respiratorio. Los agentes más importantes de este tipo son el GA (tabun), el GB (sarín), el soman y el VX. Todos ellos son líquidos a temperaturas normales y pueden ser lanzados en las cabezas de los misiles o fumigados desde tanques, pasando aerosoles. Se puede asumir que Irak tiene una capacidad similar a la de Estados Unidos para introducir algunos de dichos gases en proyectiles (un kilogramo en los M360, 105 gramos en la bomba MK-116 o 615 kilogramos en el tanque fumigador TMU-28/B). Los gases nerviosos son los más letales. Como ejemplo, una concentración de sarín de 100 mg por metro cúbico de aire respirado durante un minuto, puede causar la muerte o bien 200 mg en medio minuto.
- Gases vesicantes. Son venenos celulares que destruyen las células en determinados tejidos. Se dividen en dos grandes grupos: «gas mos-

(11) La clasificación de los agentes así como la descripción de los programas de los Estados que han desarrollado programas de armas químicas puede encontrarse en *The Arms Control Reporter (ACR)*, fichas con la entrada 704. También constituye una buena base para ver la evolución de las negociaciones bilaterales y multilaterales relativas a su destrucción (CAQ). Este dato puede ser también consultado en la página web de la Organización para la Prohibición de las Armas Químicas: www.opcw.nl.

taza» y otros vesicantes (principalmente el lawisite que con una sola dosis de 13 mg/kg puede llegar a provocar cáncer de piel o dañar el hígado y/o el riñón). El «gas mostaza» puede presentarse en forma de mostaza destilada o mostaza nitrogenada. Las indicaciones de artillería señalan que están diseñados para ser lanzados en una gran variedad de proyectiles. Es menos tóxico que los agentes nerviosos pero no obstante las células sometidas a «gas mostaza» son destruidas por la reacción del compuesto químico con proteínas celulares, encimas y ácidos nucleicos. Su mayor riesgo no es el efecto inmediato (irritación de piel, ojos y aparato respiratorio, principalmente), sino el hecho que a largo plazo pueda provocar ceguera, bronquitis crónica o cáncer de pulmón y piel. Respecto a las dosis nocivas para el hombre varían entre 12 y 70 mg por minuto y metro cúbico.

- Gases asfixiantes. Los más conocidos son el cianuro de hidrógeno (afecta a la cadena celular por inhalación, por aire respirado durante 60 minutos 120 mg/kg), el cloro y el fosgeno. El primero se utilizó en la Primera Guerra Mundial. El cloro es un agente irritante que ataca a los pulmones (en un ataque aliado realizado del día 22 de abril de 1915 se emitieron 168 toneladas de cloro en un frente de siete kilómetros; el resultado fue el de un 20% de muertes producidas entre un total de 27.000 soldados afectados. El fosgeno, también utilizado durante la Gran Guerra, tiene un determinado periodo de latencia entre su exposición y la aparición de resultados. También se utilizó en la Primera Guerra Mundial.
- Gases no letales. Se pueden clasificar en gases paralizantes (BZ, este último en forma de vapor no visible y sin olor); gases irritantes sensoriales (lacrimógenos o los que actúan causando un picor en la piel, CS, CN y CR), vomitivos (la adamsita) y por último los psicoquímicos (como el LSD). La mayoría de ellos hacen efecto tras haber sido inhalados.

Aparte de los riesgos directos para el hombre a los que nos hemos referido, como consecuencia de un lanzamiento voluntario o accidental de agentes químicos, existen otros riesgos generales para el medio ambiente que se pueden manifestar a largo plazo.

Afectan principalmente al medio acuático y terrestre con efectos variables, dependiendo sobre todo de las condiciones climatológicas (temperaturas, dirección e intensidad de los vientos), densidad de población (que posibilita también cuanto más grandes sean los núcleos de población su propagación por contacto), entre otras.

Además de los casos citados de utilización durante la Primera Guerra Mundial, varios Estados han sido acusados abiertamente (incluso, ante la Asamblea General de Naciones Unidas) de haber hecho uso de ellos utilizado en conflictos armados. Existen denuncias contra Libia (en el Chad), Rusia (en Afganistán) o mutuas, como en la guerra irano-iraquí, en donde después de un procedimiento especial de investigación, el día 21 de marzo de 1985 el Consejo de Seguridad condenó el empleo de armas químicas por tropas iraquíes. La mayoría de las denuncias se han realizado con base en el Protocolo de Ginebra de 1925, que prohíbe expresamente el uso de las armas químicas y biológicas en dichos conflictos, incluyendo los gases asfixiantes, los venenosos y similares, así como todos los líquidos, materias o procedimientos análogos. No obstante, aparte de Estados Unidos, Francia y Rusia, prácticamente ningún Estado reconoce en la actualidad haber desarrollado o estar desarrollando armas químicas, aunque son muchos los que desean su adquisición y/o fabricación, de forma directa o indirecta. De ahí la importancia de someter a control, en el marco de la CAQ de 1997, los tráfico ilícitos futuros.

Armas biológicas

La posible utilización de microbios o agentes biológicos como armas en combinación con algún sistema de lanzamiento ha sido considerada hasta la fecha como una hipótesis extraída de una novela de ciencia ficción. En este caso, la ciencia ficción ha servido sin embargo para adoptar algunas medidas específicas en el terreno político y militar destinadas a evitar los riesgos de un posible ataque con armamento biológico. No en vano, el presidente norteamericano, Bill Clinton, se ha basado en las hipótesis planteadas por Richard Preston en su novela *The Cobra Event*, en la que la ciudad de Nueva York se ve sometida al terror de un ataque con armas biológicas, para convencer al Congreso acerca de la necesidad de destinar cerca de 400.000 millones de pesetas al año para defender a Estados Unidos del riesgo potencial de un ataque con armas biológicas o químicas.

Debido sobre todo a la doble finalidad, civil y militar, que en la mayoría de los casos caracteriza a los agentes biológicas, es mucho más difícil establecer una definición de lo que se entiende por arma biológica. Desde el punto de vista de la CAB de 1975, un arma biológica es un «microbio u otro agente biológico». Pero si se tiene en cuenta que la Convención no define el término agente (que normalmente se refiere a organismos o material infectado o bien, su equivalente sintético, obtenido de aquéllos y

que se multiplica dentro de un organismo humano, animal o planta atacada), la ambigüedad en este sentido es muy amplia. De igual modo, la Convención tampoco define el término toxina, es decir, toda sustancia que actúa como los agentes químicos descritos, pero que es obtenida a partir de procesos biológicos o microbianos (12).

Las armas biológicas son de naturaleza muy diferente a las químicas. Un arma química es un veneno que se convierte en letal al entrar en contacto con la piel. Las armas biológicas son microorganismos, bacterias o virus que invaden el cuerpo, se multiplican dentro de él y lo destruyen. Se pueden utilizar como armas estratégicas (de ahí su enorme potencial destructor). Pueden matar a un número enorme de personas y sus efectos no se limitan a un lugar u objetivo pequeño. Por el contrario, las armas químicas sólo tienen un uso táctico. Es prácticamente imposible poner suficiente cantidad de una sustancia química en el aire, con una concentración suficientemente elevada para matar a un elevado número de personas en un territorio extenso.

Existen dos tipos básicos de armas biológicas, las contagiosas y las que no lo son. El ántrax, pese a su enorme poder devastador no lo es y sí lo es en cambio el virus de la viruela, que se extiende con rapidez y crece, por lo que provoca la mortandad a gran escala. Una de las variedades de este virus es el *Variola Major*, sumamente contagioso, ya que por cada nuevo caso se puede contagiar a 20 personas (13).

Son muchos los países que han desarrollado o incluso realizado experimentos relacionados con las aplicaciones militares con armas biológicas y ello, pese a que la CAB está en vigor desde el año 1975. Aunque de forma oficial nunca ha sido reconocido, se sospecha que el Reino Unido utilizó la isla de Gruinard, frente a la costa de Iverness, para experimentar el potencial del ántrax como instrumento de lucha biológica, en el año 1941. En el año 1943, cuando se hizo evidente que ni los japoneses ni los alemanes contaban con ese material, el programa fue definitivamente cancelado, al igual que hizo Estados Unidos (14).

(12) KELLE, A.: «Developing Control Regimes for Chemical and Biological Weapons» en *International Spectator*, volumen XXXII, número 3-4, pp. 137-139. Julio-diciembre, 1997.

(13) Para la clasificación y los efectos de los agentes biológicos véase *ACR-1999*, fichas 701.E.7.a y 701.E.12.

(14) Aunque algunos análisis apuntan a que las investigaciones se prorrogaron hasta el año 1977. Véase *The Bulletin of the Atomic Scientists*. Enero-febrero, 1987.

Otros Estados han sido también acusados de haber desarrollado o estar desarrollando programas de armamento biológico. El propio presidente de la República Francesa, François Mitterrand, anunció en 1988 haber destruido en el año 1972 todas sus armas biológicas (15). Existen otros casos en los que los programas de armas biológicas siguen su curso. Irak fue acusada en 1994 de poseer tularemia —una bacteria que causa un tipo de neumonía— y ántrax. Recientemente, los inspectores de la Misión Especial de Naciones Unidas encargada de verificar la destrucción de las armas de destrucción masiva en Irak, acusaron a este país de haber realizado experimentos con armas químicas y biológicas con prisioneros políticos (16). Libia nunca ha ocultado su deseo por poseer armas químicas y biológicas. Otros Estados bajo sospecha internacional son Corea del Norte, Irán o Sudán (17).

Estados Unidos declaró en 1975 haber destruido totalmente su arsenal biológico. El embajador de Corea del Norte ante Naciones Unidas acusó a Estados Unidos (a través de una carta enviada el día 9 de marzo de 1999 al Consejo de Seguridad) de haber utilizado armamento biológico durante la guerra de Corea, hipótesis que también ha sido manejada por varios especialistas (18).

Finalmente, existen más dudas acerca del programa de armas biológicas ruso (el más amplio de todos), rodeado aún hoy en día de un gran hermetismo. Gran parte de la información respecto al mismo (en lo que se refiere a tipos de agentes y cantidades producidas) se conoce a través de las declaraciones realizadas a diferentes medios por el científico ruso Ken Alibek (conocido por el nombre de doctor Anatjan Alibekov, subdirector de investigación y producción del programa de armas biológicas de la Unión Soviética), que emigró a Estados Unidos en 1992. Según éste, las instalaciones biológicas rusas de Biopreparat «El Sistema» estaban repartidas por toda la Unión Soviética y en ellas estaban empleados 60.000 científicos, de ellos, 2.000 expertos dedicados exclusiva-

(15) Declaración de François Mitterrand recogidas en *Jane's NATO Report*, 29 de noviembre de 1988.

(16) Según el informe de 31 de enero de 1999 de la UNSCOM. Véase ACR-1999, ficha 701.B.223. Véase también el artículo de AL VENTER, «UNSCOM Odyssey: The Search for Saddam Hussein's Biological Arsenal» en *Jane's Intelligence Review*. Marzo, 1998.

(17) Acerca de los programas de estos países véanse las denuncias realizadas por Estados Unidos en ACR-1999, fichas 701.B.223 a 701.B.226.

(18) Entre otros, un estudio de la Universidad de York en Canadá titulado, *The United States and Biological Warfare: Secrets from the Early Cold War and Korea*. Marzo, 1999. Véase también al respecto ACR-1999, fichas 701.B.229 y 701.B.231.

mente al ántrax (19). Todo ello da muestras del enorme potencial ruso en el ámbito biológico.

Proliferación de armas NBQ y tráficos ilícitos de materiales nucleares y agentes químicos y biológicos

En muchas ocasiones, los Estados que no poseen armas nucleares, más susceptibles de ser controladas bajo el régimen de no-proliferación existente, justifican la posesión y desarrollo de armas químicas como derecho legítimo a su autodefensa. En otras, la justificación viene del lado de la disuasión, frente a un posible ataque del enemigo, país vecino o no, con armas de destrucción masiva. Por último, como medida de presión para forzar la desnuclearización de una determinada zona o por razones de prestigio regional o internacional. Ésa sería la situación en Oriente Medio y especialmente los argumentos esgrimidos por Irak, Libia o Egipto, que sí son Estados-Partes en el TNP pero que no han suscrito en cambio la CAQ, frente a Israel, que sí lo es Estado-Parte en esta última pero no es signatario del TNP y está considerado el único Estado nuclear no declarado de la región. Con ello, el posible desarrollo de armas químicas en esos países, por citar sólo algunos ejemplos, pasa de tener unas consecuencias estrictamente regionales a una dimensión internacional ya que, a nivel político, afecta a la eficacia de los regímenes internacionales de no proliferación, que por otra parte, ahora más que nunca están fuertemente interrelacionados (20).

En otro orden de cosas, el deseo de esos países por dotarse con este tipo de tecnología afecta directamente al tráfico ilícito de componentes nucleares y agentes químicos y biológicos. Es bien conocido el caso iraquí, en el que varias empresas de países occidentales se vieron involucradas en el suministro de sustancias como el thiodiglycol, que como es conocido,

(19) Las revelaciones de Alibek acerca del programa de armas biológicas de la Unión Soviética, en el que trabajó desde 1975 hasta 1992, han sido publicadas en su libro *Biohazard: The Chilling True Story of the largest Covert Biological Weapons Program in the World*. Random House, 1999. Además de este, Alibek ha concedido un gran número de entrevistas a diferentes medios de comunicación occidentales explicando los propósitos, orígenes y evolución de dicho programa (entre ellas a la *Jane's Defense Weekly* o una más reciente en *The Non-Proliferation Review*, volumen 6, número 3, pp. 1-10. Primavera-verano, 1999. Center for Non-Proliferation Studies, Monterey Institute for International Studies. Un esquema-mapa acerca de la distribución de dichas las armas biológicas de «El Sistema» aparece reproducido en el artículo «Planning a Plague?» en *Newsweek*, pp. 20-22. 1 de febrero, 1993.

(20) Acerca de la convergencia de regímenes internacionales de no-proliferación véase MÜLLER, H.: *Europe and Nuclear Disarmament*. European Interuniversity Press. Bruselas, 1998.

constituye un elemento básico para fabricar «gas mostaza». Además, en esos momentos Irak estaba acusada de estar realizando experimentos con armas químicas en sus instalaciones de Samarrá (21). Igualmente problemáticas son las instalaciones de Libia en Rabta.

El problema de los agentes químicos y sobre todo los biológicos es su versatilidad. Ello hace prácticamente imposible demostrar *a priori* su finalidad militar en el momento que un Estado o empresa nacional realiza una transferencia de una sustancia química a un tercero. Además, a ello se une una dificultad añadida: un agente químico se convierte en un arma química cuando la sustancia ya ha sido manipulada como bomba binaria. Las «bombas binarias» incluyen dos componentes que no son letales por separado pero que una vez combinados en una bomba u artefacto similar (por ejemplo una cápsula de un proyectil de 155 milímetros) los convierten en agentes letales. Los gases contenidos en dichas bombas se encuentran normalmente en estado líquido. En la mayoría de los casos los dispositivos son giratorios con el fin de que se mezclen bien sus elementos químicos. El impacto sobre el objetivo abre la cápsula y el agente, ya letal, sale disparado, normalmente como aerosol.

Por lo que respecta a las armas biológicas, la relación entre proliferación horizontal y tráfico ilícito de agentes biológicos no es tan preocupante como la posibilidad de que personas con conocimientos científicos suficientes sobre los agentes biológicos, puedan emigrar a terceros países interesados en reproducir virus y bacterias a gran escala para su aplicación militar. La hipótesis se ha visto especialmente reforzada a raíz de la desintegración política de la Unión Soviética. Algunos científicos rusos que trabajaron largo tiempo en el programa de armas biológicas de la antigua Unión Soviética, como el ya mencionado doctor Anatjan Alibekov (al que se le debe, entre otras cosas, la invención del ántrax ruso, mucho más potente y letal que el ántrax convencional) señalan que con la reducción de los salarios de los científicos (17 dólares mensuales) muchos de ellos emigraron no sólo a Estados Unidos y Reino Unido, sino también a China, Irán, Irak, Libia y Siria (22).

En el año 1991, justo antes de la llegada de Gorbachov al poder, la Unión Soviética tenía capacidad para fabricar la variante U del virus de *Marburg*

(21) AL VENTER, *UNSCOM Odyssey...*, obra citada.

(22) Además de las declaraciones del propio Alibek, véase también el artículo «Científicos en el infierno» en *El Mundo*. 20 de febrero, 1998.

(parecido al virus del *Ébola* y enormemente letal), muy potente al aire, ya que bastan cinco partículas microscópicas en los pulmones de un mono para conseguir que el animal muera (23). Como análisis comparativo, el ántrax convencional, necesita 8.000 esporas alojadas en los pulmones para garantizar la infección y la muerte. La peculiaridad adicional de dicho virus es que podría ser cargado en las cabezas de los MIRV, con unos sistemas especiales de enfriamiento en cada una de las 10 cabezas cónicas que mantendría el virus con vida durante el calor de la entrada en la atmósfera terrestre. Se dejaría caer sobre un objetivo preelegido utilizando unos paracaídas, liberando una nube de biopartículas que se harían rápidamente invisibles.

El dato anterior, meramente ilustrativo, pone no obstante de manifiesto la importancia del problema y la fatídica relación que pudiera tener proliferación de agentes químicos y biológicos con el riesgo incontrolado de ese tipo de sustancias. La variante U del virus de *Marburg* nunca formó parte del arsenal biológico soviético, que sí estaba en cambio compuesto por alrededor de 20 toneladas de viruela seca de uso bélico, almacenada en bunkers y del ántrax de Alibekov. Sin embargo, uno de los máximos peligros puesto de manifiesto por el que trabajara durante 18 años en «El Sistema» es la posibilidad que al menos 10 de sus colegas pudieran haberse llevado consigo antes de emigrar a los países mencionados la variante U del virus congelado y que hasta ahora sólo ha sido probado en monos.

Finalmente, otro de los riesgos vinculados con las sustancias químicas y biológicas, es su gran atractivo para grupos terroristas (como demostró en el atentado en «el metro» de Tokio por parte de una secta religiosa en 1995) con lo que la problemática de su proliferación a nivel internacional adquiere con ello una nueva dimensión, más preocupante si cabe y que pasa obligatoriamente por la necesidad de reforzar los controles internacionales.

Medidas políticas y diplomáticas para controlar los tráfico ilícitos de armamento NBQ y las transferencias de productos y tecnologías de doble uso

Pese a que la tendencia actual se incline por la convergencia de los regímenes de no-prolifерación de armas de destrucción masiva y el control de

(23) «The Breeding of Death» en *Time*. 16 de febrero, 1998.

las exportaciones de productos y tecnologías de doble uso, no significa que exista el enfoque para abordar dicho problema sea único. Ello es debido a que los regímenes de control no tienen la misma antigüedad en lo que respecta a su establecimiento y funcionamiento. Así, mientras que en el ámbito nuclear el TNP ha desarrollado desde el año 1970 un conjunto de medidas destinadas a asegurar la no transferencia de materiales nucleares (incluyendo después también los de doble uso) a países al margen del régimen o que no ofrezcan garantías suficientes sobre su uso final, los compromisos en los ámbitos químico y biológico se han realizado durante largo tiempo sobre una base no convencional. Ello se debe a que hasta fecha reciente (29 de abril de 1997) no entró en vigor el principal instrumento jurídico de control de las armas químicas (la CAQ), sin que existiese por lo tanto mecanismos adecuados de verificación de los compromisos estatales de no fabricación y destrucción de ese tipo de armas por parte de los Estados. Y por lo que respecta al ámbito biológico, el Protocolo de Verificación de la CAB, aunque avanzado en su redacción, aún no ha sido adoptado, como ya señalamos. En consecuencia, la intensidad de los controles y la tradición en la aplicación de las medidas de verificación ha sido, hasta la fecha, mucho mayor en el ámbito nuclear que en el químico o biológico.

*Controles con base convencional:
tratados internacionales y medidas de verificación*

Se trata de instrumentos de no-proliferación de armas de destrucción masiva que afecta de forma indirecta al tráfico ilícito de productos y tecnologías de doble uso, al establecer una prohibición sobre su transferencia si la finalidad última de su uso es militar.

ÁMBITO NUCLEAR: TNP

Cuenta con 188 Estados-Partes (sólo permanecen al margen del mismo Cuba, India, Israel, Niue y Pakistán). Constituye el TNP internacional (y desde el año 1995 también de control de armamentos y desarme) más universal (24).

(24) Para una mayor información sobre el contenido del Tratado y las modificaciones introducidas durante la Conferencia de Revisión y Prórroga del mismo del año 1995 véase GARRIDO REBOLLEDO, V.: «La Conferencia de Revisión y Prórroga del TNP: el debate entre consenso o mayoría» en *Meridiano Ceri*, número 3, Centro Español de Relaciones Internacionales. Madrid, 1995. «Después de Nueva York: la fragilidad de la no-proliferación nuclear», en *Papeles*, número 55, CIP. Madrid, 1995. Para un análisis histórico de la cuestión se puede consultar: «El futuro del TNP: apuntes para el debate» en *Anuario 1994-1995*, pp. 289-299, CIP. Icaria. Barcelona, 1995.

Los principales compromisos del TNP con respecto a la no transferencia de armamento nuclear se encuentran contenidos en los artículos I, II y III.2 del Tratado. En concreto, el artículo I se refiere al compromiso al que se someten las potencias nucleares (a efectos del Tratado sólo Estados Unidos, Rusia, Gran Bretaña, Francia y China) de:

«No traspasar a nadie armas nucleares u otros dispositivos nucleares explosivos ni el control sobre tales armas o dispositivos explosivos, sea directa o indirectamente; y a no ayudar, alentar o inducir en forma alguna a ningún Estado no poseedor de armas nucleares a fabricar o adquirir de otra manera armas nucleares u otros dispositivos nucleares explosivos, ni el control sobre tales armas o dispositivos explosivos.»

Pese a que los dos primeros artículos del TNP pueden ser considerados el «corazón que hace funcionar el Tratado», las críticas con respecto a ambos han sido una constante desde que éste entrase en vigor en 1970. Efectivamente, el artículo I no prohíbe el traspaso de armas y tecnología nucleares entre Estados ya nucleares, sino sólo a aquellos no nucleares. Desde ese punto de vista, la ayuda nuclear de Estados Unidos a Gran Bretaña y a Francia para el desarrollo de sus programas nucleares y la cooperación nuclear anglo-norteamericana, no constituye, por paradójico que pueda resultar, una violación de los compromisos del TNP.

No obstante, hasta el momento no se ha podido demostrar que un Estado poseedor de armas nucleares haya traspasado armas nucleares a un Estado no nuclear. Lo que es más difícil de verificar es la exigencia del artículo I de «no ayudar, alentar o inducir a adquirir armas nucleares» por parte de un Estado nuclear a otro no nuclear. Esta exigencia resulta más difícil de verificar si tenemos en cuenta que ninguna disposición del TNP prohíbe que un Estado no nuclear, Parte en el Tratado, ayude a otro Estado no poseedor de armas nucleares, no signatario del mismo, a fabricar este tipo de armamento. Si el país receptor fuese Parte en el TNP, estaría sujeto a las obligaciones del artículo II, es decir, no aceptar dicha ayuda. Por su parte, el Estado suministrador, no poseedor de armamento nuclear, no podría transferir a ningún otro Estado (Parte o no en el TNP) ningún material o equipo de los enumerados en el artículo III.2 del Tratado (otros distintos que los destinados a fines pacíficos), a no ser que estén sometidos a salvaguardias del OIEA. En definitiva, si un Estado no nuclear, Parte en el TNP ayuda a otro Estado no nuclear, no Parte en el Tratado a adquirir armamento nuclear, suministrándole materiales no sometidos al control del OIEA, aunque se declare que la finalidad última de éstos sea pacífica, el hecho será considerado como una violación del Tratado.

No obstante, en la década de los setenta, algunos Estados consideraron que el suministro de material nuclear sometido a salvaguardias del OIEA entre Estados no nucleares no constituía una violación del TNP, alegando para ello la finalidad pacífica del material exportado. Así nos encontramos con suministros importantes de uranio enriquecido de Alemania a Pakistán, así como reactores de reprocesamiento a Brasil (bajo salvaguardias del OIEA) o bien, el caso de un acuerdo para la construcción de una planta de enriquecimiento de uranio en Almelo (Holanda) por parte de la República Federal Alemana y Gran Bretaña. Este tipo de cooperación nuclear, aún con base en los fines pacíficos de la energía nuclear, ha dado lugar a lo se denomina como «proliferación nuclear oblicua».

Sin embargo, la cuestión no termina aquí. La interpretación que hay que hacer del artículo III.2, en conexión con el primero, sólo se refiere a los materiales nucleares con fines pacíficos suministrados por Estados no nucleares Partes en el Tratado a los Estados no nucleares no signatarios del TNP. En el caso de que dichos materiales tuvieran una finalidad militar, no entrarían en el supuesto del artículo III.2. Este aparente vacío legal ha intentado ser cubierto tanto por Estados Unidos como por la antigua Unión Soviética, que ya en 1968 manifestaron que la ayuda de un Estado no nuclear Parte en el Tratado a otro Estado no nuclear que no lo fuera, con independencia de su finalidad, sería considerada una violación grave del TNP, al presuponerse que el Estado destinatario de dicha ayuda estaba tratando de adquirir armas nucleares para sí mismo. La cuestión acerca de las limitaciones en la aplicación de las salvaguardas del OIEA fue tratada durante la celebración de la primera y tercera conferencias de revisión del TNP de los años 1975 y 1985 respectivamente y fue la base de la revisión del sistema de salvaguardas del Organismo, dando lugar al mecanismo reforzado conocido con el nombre de «93+2», al que ya nos hemos referido.

El problema de las transferencias de armamentos materiales nucleares es que, mientras los Estados han intentado, con mayor o menor éxito, establecer controles a las exportaciones de productos y tecnologías de doble uso en los que no estuviese garantizada la finalidad civil última del material suministrado, muchas empresas se han guiado por un criterio puramente comercial para inclinar la balanza a favor de la proliferación nuclear, sobre todo, si tenemos en cuenta que mientras las políticas son públicas, la mayoría de las empresas son privadas.

Por otra parte, hay que señalar que mientras el artículo II del TNP (aplicable al resto de los Estados «no nucleares») (25) prohíbe a cualquier Estado

no nuclear Parte en el Tratado adquirir armas nucleares, en cambio no existe prohibición expresa para un Estado «no poseedor de armas nucleares» posea ese tipo de armas, lo que constituye una nueva paradoja del Tratado. Esta omisión aparente ya fue objeto de debate durante el periodo de negociación del Tratado entre 1965 y 1968. Se puso de manifiesto que ningún otro Estado, aparte de las cinco potencias ya nucleares, tenía derecho a poseer armas nucleares y por lo tanto, se prohibía a otros Estados su fabricación. La idea nacía vinculada al deseo de mantenimiento por parte de las cinco potencias nucleares su *statu quo* nuclear.

La violación del artículo II por parte de Irak reabrió el debate sobre la función del TNP. El caso iraquí puso de manifiesto que un Estado no nuclear que fuese Parte en el Tratado podía desarrollar su propio programa nuclear de forma ilegal teniendo además como ventaja añadida su propia pertenencia al Tratado para obtener tecnología nuclear de suministradores extranjeros, apoyándose en el artículo IV del TNP (derecho de todas las Partes a utilizar la energía nuclear con fines pacíficos) (26). Irak era signataria del TNP desde 1969 y los inspectores del OIEA habían visitado el país dos veces al año sin llegar a detectar, desde la década de los años setenta hasta 1991, ningún signo alarmante que les hiciese suponer la existencia de un programa nuclear militar clandestino (27). Pero sobre todo, el caso iraquí puso de manifiesto el fracaso de los controles a la exportación de materiales de doble uso susceptibles de ser utilizados para la fabricación de armamentos nucleares.

Por último, nos debemos referir al sistema de verificación del Tratado: las salvaguardas del OIEA. Las medidas están enunciadas en el artículo III.2 del TNP, que establece las condiciones en las que debe de ser realizado el comercio nuclear (28).

(25) Dicho artículo establece un compromiso de los Estados no nucleares de «no recibir de nadie ningún traspaso de armas nucleares u otros dispositivos nucleares explosivos ni el control sobre tales armas o dispositivos explosivos, sea directa o indirectamente; a no fabricar ni adquirir de otra manera armas nucleares u otros dispositivos nucleares explosivos; y a no recabar ni recibir ayuda alguna para la fabricación de armas nucleares u otros dispositivos nucleares explosivos».

(26) BARNABY, F.: «Strengths and Weaknesses of the Non-Proliferation Treaty: and is it Worth Extending in 1995? en *Strengthening the Non-Proliferation Regime: 1995 and Beyond*», en *Current Decisions Report*, número 13, pp. 3-4. Oxford Research Group. Diciembre, 1993.

(27) GARRIDO REBOLLEDO, V.: *El programa nuclear iraquí...*, pp. 90-97, obra citada.

(28) «Cada Estado-Parte en el Tratado se compromete a no proporcionar: a) materiales básicos o materiales fisibles especiales; b) equipo o materiales especialmente concebidos o preparados para el tratamiento, utilización o producción de materiales fisibles especiales, a ningún Estado no poseedor de armas nucleares, para fines pacíficos, a menos que estos materiales básicos o materiales fisibles sean sometidos a las salvaguardias exigidas por el presente artículo».

Resulta también paradójico que la aplicación dicho artículo haya resultado hasta la fecha a veces más favorable para los no signatarios del Tratado que para los que sí lo son. Ello se debe a que hasta la reforma del sistema de salvaguardas del OIEA en 1995 (Documento INFCIRC/540, aún no en vigor para todos los Estados) las Partes en el Tratado se veían obligadas a someter a salvaguardas el total de sus actividades nucleares (de ahí que se conozcan con el nombre de salvaguardas plenas o totales), incluyendo las relacionadas con el uso pacífico de la energía nuclear, mientras que los que no eran Parte en él sólo tenían que declarar los *ítems* importados (instalaciones individuales o materiales). De ese modo, muchos exportadores nucleares, conscientes de los peligros de proliferación nuclear que entrañaba la distinción entre tecnologías nacionales e importadas, comenzaron a exigir también a los Estados no signatarios la aceptación de salvaguardas totales como extensión de las exigidas por el TNP a los Estados-Partes (29). Algunos Estados exportadores se mostraron al principio reticentes a modificar las condiciones de sus exportaciones ante el temor a perder mercados nucleares internacionales. Sin embargo, el caso iraquí primero, y el norcoreano después pusieron de manifiesto la necesidad de reforzar el régimen de control de las exportaciones de materiales nucleares y doble uso.

ÁMBITO QUÍMICO: CAQ

La CAQ entró en vigor el 29 de abril de 1997. A 31 de octubre de 1999 había sido firmada por 169 Estados y de éstos, ratificada por 126.

La CAQ tiene como órgano de verificación de los compromisos asumidos por los Estados en virtud de la Convención la Organización para la Prohibición de las Armas Químicas (OPAQ), con sede en La Haya. Las Autoridades Nacionales para la Prohibición de las Armas Químicas (ANPAQ) se encargan de aplicar en el ámbito estatal las disposiciones de la Convención así como de transmitir la información que reciben periódicamente sobre las actividades de las empresas del sector a la OPAQ. Con ello se mejora considerablemente el mecanismo de verificación, hasta hace muy poco, inexistente en este ámbito.

No obstante, el principal problema de carácter estructural de la CAQ es que, como ya señalamos no prevé ningún Sistema Internacional de Vigi-

(29) GOLDBLAT, J.: «The Non-Proliferation Treaty: Status of Implementation and Threatening Developments» en FRY, M.; KEATINGE, P. y ROTBLAT, J. (eds.): *Nuclear Non-Proliferation and the Non-Proliferation Treaty*, p. 4. Springer Verlag, Berlín y Heidelberg, 1990.

lancia de modo que ante discrepancias con los datos transmitidos por las ANPAQ sólo puede actuar en un supuesto de denuncia por parte de otro Estado, iniciando así un procedimiento de investigación.

La Convención consta de 24 artículos y tres anexos, (que se refieren a las sustancias químicas, la aplicación de la verificación y la protección de la información confidencial, respectivamente). El primer anexo divide las sustancias químicas en tres listas diferentes, en función de su grado de peligrosidad. Para cada una de ellas se establecen una serie de limitaciones en lo relativo a las cantidades máximas de producción permitidas, venta de componentes o transferencias. En este último apartado, que es el que directamente está relacionado con los tráficó ilcítos, se limita la capacidad de exportación de productos químicos dependiendo de si la sustancia está o no contenida en una de las tres listas citadas y que el Estado en cuestión sea o no Parte en la Convención. Como regla general, se admite que ningún Estado-Parte transferirá o empleará sustancias químicas de ninguna de las tres listas fuera de su territorio, salvo a otro Estado-Parte en la Convención, a menos que se realice una declaración detallada de último destino y se garantice su utilización exclusivamente con finalidad pacífica y la no retransferencia. Los Estados-Partes se comprometen por su parte a adaptar sus legislaciones internas sobre exportación a las disposiciones de la Convención (30).

ÁMBITO BIOLÓGICO: CAB

La CAB está en vigor desde el año 1975. Sin embargo, como ya señalamos, su eficacia se ha visto limitada por la ausencia de un Protocolo de Verificación de las disposiciones contempladas en la misma.

Con respecto al Protocolo de Verificación, ahora, tras cuatro años de negociaciones (que dieron comienzo en 1995) y 16 reuniones del Grupo *Ad-Hoc* de la CAB (la última celebrada del 13 de septiembre al día 8 de octubre) se empieza a ver los progresos realizados en el texto. El borrador de Protocolo consta de un preámbulo, 13 artículos, siete anexos y un apéndice. Las tres secciones principales del Protocolo son el artículo III (que es el más avanzado y que con los anexos correspondientes, tiene 100 páginas), que se refiere a las medidas relacionadas con el cumpli-

30) El texto íntegro de la Convención en español fue publicado en el *Boletín Oficial del Estado*, número 300, pp. 37.090-37.150, de fecha 13 de diciembre de 1996 (corrección de errores en el *Boletín Oficial del Estado*, número 63, pp. 21.090-21.092 de 9 de julio de 1997).

miento de la Convención; el artículo VII que se refiere a la cooperación técnica y el artículo II, el menos avanzado y más problemático, ya que se refiere a las definiciones. Existe cierto optimismo por parte de los negociadores para que el Protocolo pueda quedar adoptado en el verano del 2000 (31).

El Protocolo y sus anexos, tratan de establecer, a semejanza de la CAQ con respecto a las armas químicas, una listas de productos y sustancias que se permite producir (siempre en función de su finalidad), así como las garantías para su transferencia entre Estados-Partes en la Convención. Una vez comience aplicarse el Protocolo de la CAB, se crearán en cada uno de los Estados-Partes las respectivas autoridades nacionales que, entre otras cosas, se encargarán de aplicar a nivel de interno las disposiciones del Protocolo de Verificación.

Muchos Estados, especialmente aquellos pertenecientes al grupo de países no-alineados (incluyendo Brasil, India, Irán y Pakistán), han manifestado su oposición a que se establezcan controles adicionales al comercio de determinados sustancias biológicas, especialmente aquellas empleadas en la industria farmacéutica. Para ello, esgrimen el argumento que dichos controles son redundantes y discriminatorios. Sin embargo, detrás de esas críticas subyace su deseo de reemplazar los controles que se llevan a cabo en el seno del Grupo Australiano (al que más adelante nos referiremos) por el nuevo régimen que instaure el Protocolo de la CAB, de tal modo que sólo se le pueda denegar a un Estado el acceso a determinados productos o tecnologías caso de no cumplir las disposiciones de la CAB (32). Hasta ahora, la base para denegar la exportación de dichas sustancias es el artículo III de la CAB, que establece una obligación genérica de no transferir a ningún Estado cualquier agente, toxina o arma biológica prohibida por la Convención.

El día 31 de octubre de 1999 un total de 141 Estados habían ratificado la CAB. La falta de un mecanismo efectivo de verificación se ha venido sustituyendo hasta la fecha por un conjunto de medidas de confianza (política pero no jurídicamente vinculantes) adoptadas solamente con el apoyo de

(31) Así lo pone de manifiesto uno de los especialistas que más ha contribuido hasta la fecha a la redacción del Protocolo, Graham S: Pearson. La estructura provisional del Protocolo es la que sugiere este experto. Véase entre otros su artículo «The BTWC Protocol Enters the Endgame» en *Disarmament Diplomacy*, número 39, pp. 6-14. Julio-agosto, 1999.

(32) TUCKNER, Jonathan, «Strengthening the BWC: Moving Toward a Compliance Protocol» en *Arms Control Today*, volumen 28, número 1, pp. 20-27. Enero-febrero de 1998.

la mitad de los Estados signatarios. Éstas se centran en el fomento del intercambio de información entre los Estados, a través de la realización de una serie de declaraciones anuales voluntarias acerca de las actividades de sus centros de investigación y laboratorios, brotes de infecciones causadas por toxinas y vacunas, así como las cantidades producidas. Sin embargo, durante el primer semestre del año 1999 sólo 34 de los 141 Estados signatarios de la Convención habían enviado al Departamento de Asuntos de Desarme de Naciones Unidas dichas declaraciones y de éstos, sólo ocho lo habían hecho en la fecha prevista (15 de abril de 1998) (33). Además, hay que tener en cuenta que, en el supuesto que se detecte alguna violación de las disposiciones de la Convención sólo cabe informar al Consejo de Seguridad de Naciones Unidas, que tras recibir las denuncias realizadas por otro Estado se encarga de investigarlas, de conformidad con la Carta, lo que hace al sistema altamente vulnerable.

Foros internacionales de control de comercio exterior de productos y tecnologías de doble uso

Al igual que los regímenes convencionales, los acuerdos destinados a evitar los tráficos ilícitos de productos y tecnologías de doble uso pueden agruparse por una parte, en aquellos que se ocupan específicamente de los materiales nucleares y los que se ocupan de los agentes y sustancias químicas y biológicas, por otra. Existe un mecanismo común a los dos regímenes, el Acuerdo Wassenaar y otro específicamente diseñado para evitar la proliferación y los tráficos ilícitos de misiles balísticos, el Régimen de Control de Tecnología de Misiles (MTCR) y del que apenas nos vamos a ocupar por ser objeto de estudio en otro de los capítulos de esta *Mono-grafía*.

ÁMBITO NUCLEAR

Como ya hemos señalado, el TNP proporciona sólo una base a partir de la cual se interpretan los compromisos de los Estados en materia de no transferencia de materiales nucleares con finalidad militar al margen de los cinco Estados ya nucleares. Sin embargo, en ningún caso define lo que son «materiales básicos o materiales fisibles especiales» o «equipo o materiales especialmente concebidos o preparados para el tratamiento, utilización o producción de materiales fisibles especiales». Por este mo-

(33) Véase ACR-1999, ficha 701.B.236.

tivo, las explicaciones y especificaciones de todos esos términos fueron encargadas al Comité Zangger o (Comité de Exportadores Nucleares), un grupo de naturaleza informal fundado en el año 1971. Los resultados alcanzados por el Grupo fueron publicados en 1974 por el OIEA (a petición de los entonces 15 Estados miembros del Comité) en el Documento INF-CIRC/209. Este Documento contenía lo que se conoce como *Trigger List* del Comité Zangger, dividida en dos memorandos, para materiales básicos y fisibles especiales siguiendo la definición establecida en el artículo XX del Estatuto del OIEA (Memorando A) y para las exportaciones de equipos y materiales no nucleares (Memorando B). Desde entonces, la *Trigger List* del Comité Zangger ha sido actualizada en varias ocasiones con el fin de incluir nuevas tecnologías sobre el enriquecimiento del uranio, avances tecnológicos o bien plantas para la producción de agua pesada.

El Comité Zangger se reúne en Viena dos veces al año (en mayo y octubre), y sus encuentros son informales y confidenciales. En la actualidad, 36 Estados, entre los que se encuentra España desde 1993, son miembros del mismo.

Los compromisos más importantes del Comité Zangger a la hora de exportar equipos o materiales incluidos en la lista crítica o *Trigger List* son:

- Que dichos equipos o materiales no sean utilizados para fabricar explosivos nucleares.
- Que estén sometidos a salvaguardias del OIEA en el Estado no nuclear que recibe el equipo o material nuclear.
- Que el equipo o material exportado no sea reexportado a menos que esté sometido a salvaguardias en el nuevo Estado que lo reciba.

Un grupo más informal, pero de más relevancia que el primero (que en definitiva refuerza los compromisos del artículo III del TNP) es el Grupo de Suministradores Nucleares (GSN). Fundado inicialmente en el año 1975 bajo el nombre de «Club de Londres», tras la primera explosión nuclear india del año 1974 por los entonces siete suministradores nucleares más importantes, cuenta en la actualidad con 35 Estados miembros aunque en el plenario de 1999 acordó considerar favorablemente las candidaturas como Estados adheridos al Grupo de Bielorrusia, Chipre, Eslovenia, Kazajstán y Turquía.

El GSN se creó con el propósito principal de adoptar una serie de nuevas directrices a la exportación de materiales nucleares con el fin de que ese tipo de exportaciones fuesen realizadas exclusivamente a aquellos Estados que previamente hubiesen aceptado las salvaguardas del OIEA. Las

directrices (o *guidelines*) originales fueron publicadas en 1978 por el OIEA en el Documento INFCIRC/254. Los productos sometidos a control eran aquellos que habían sido previamente identificados por el Comité Zangger, pero añadiendo a su vez un nuevo ítem a la lista: las «instalaciones para la producción de agua pesada, el deuterio y sus componentes, así como el equipo especialmente concebido para dicho fin». Uno de los principales propósitos del «Club de Londres» era lograr la inclusión de Francia, suministrador nuclear de primer orden y que por entonces, no era Parte en el TNP ni miembro del Comité Zangger.

Las directrices del «Club de Londres» fueron totalmente modificadas en el año 1991 durante un encuentro celebrado en La Haya, en dónde se decidió también su cambio de nombre por el de GSN. Se adoptaron también nuevas directrices para exportaciones nucleares especiales o que pudiesen tener un posible uso nuclear, civil y militar, con independencia de que el Estado fuese o no Parte en el TNP. Algunos países como India, Pakistán o Brasil se mostraron contrarios a los controles establecidos por estos dos grupos, argumentando que dichos controles ya se venían realizando con efectividad por parte del OIEA (34).

En abril de 1992, en el encuentro del GSN de Varsovia se acordó aplicar y exigir por primera vez salvaguardas totales a los productos exportados (es decir, no sólo a los materiales nucleares, sino también a los productos y tecnologías de doble uso). Desde entonces la cuestión ha sido muy polémica ya que no existe un consenso generalizado, incluso en el seno de los Estados miembros del Grupo a la hora de exigir la aplicación de dichas salvaguardas. Algunos Estados consideran que la aplicación de las salvaguardas totales va mucho más allá de lo que exige el propio artículo III.2 del TNP. Sin embargo, hoy día dichas salvaguardas constituyen para la inmensa mayoría la piedra angular del régimen de no-proliferación de armas nucleares, como se puso una vez más de manifiesto durante la celebración del III Comité Preparatorio de la Conferencia de Revisión del TNP del año 2000 (celebrado en Nueva York del 10-21 de mayo de 1999).

En el mes de julio de 1992 el OIEA publicó a petición del GSN las «Directrices para la transferencia de equipo, material y tecnologías de doble uso», que incluía con un total de 65 productos divididos en ocho catego-

(34) Resulta de interés el estudio sobre los diferentes regímenes de exportación de armas NBQ y de misiles balísticos ya que establece un cuadro comparativo entre todos ellos: Advisory Council on Peace and Security, *Towards a Multifaceted Non-Proliferation Policy*. La Haya, diciembre 1992.

rías. Esta lista entró en vigor en enero de 1993 (INFCIRC/254/Rev.1/Part 2). La condición para exportar un producto o tecnología de los contenidos en la lista es que el importador acepte previamente la aplicación de las salvaguardas totales del OIEA. Desde entonces, las directrices del GSN han sido modificadas en varias ocasiones con el fin de armonizar las listas del grupo a las del Comité Zangger, que pese a establecer controles muy parecidos a los del GSN y tener una estructura de miembros muy similar (la única excepción es China que no pertenece al GSN y sí en cambio al Comité Zangger) siguen funcionando de forma separada. Mientras que el primero está más centrado en la actualidad en interpretar los compromisos contenidos en el artículo III.2 del TNP el GSN ha volcado sus esfuerzos en el control de las tecnologías de doble uso.

Por último señalar que además del sistema de verificación casi universal del OIEA (reforzado a partir de la adopción del Protocolo Adicional al que ya nos hemos referido, existe un sistema de salvaguardias regionales específico para los miembros de la Unión Europea, a cargo de la Comisión Europea para la Energía Atómica (EURATOM).

Para evitar posibles conflictos en lo que se refiere a la aplicación de las salvaguardias a los miembros de la Unión Europea, existen mecanismos específicos de cooperación (como el acuerdo entre la Comisión Europea y los 15 Estados miembros de la Unión Europea con el OIEA del día 22 de septiembre de 1998).

ÁMBITOS QUÍMICO Y BIOLÓGICO

El único foro multilateral encargado de armonizar las políticas de sus Estados miembros en materia de controles a la exportación de sustancias químicas y agentes biológicos susceptibles de utilizados para producir armas químicas y/o biológicas es el Grupo Australiano. Se trata de un Grupo informal intergubernamental creado ha iniciativa de Australia en 1985 ante las consecuencias de utilización de armas químicas durante la guerra irano-iraquí y desde entonces, se reúne una vez al año. Ha alcanzado ya los 30 Estados miembros, junto con la Comisión Europea, que participa en calidad de observadora. España se adhirió al mismo en 1985.

El Grupo Australiano se centró en un principio en controlar exclusivamente las exportaciones de 54 precursores químicos incluidos en una lista de base o *Core List*, ampliándola posteriormente a los equipos y tecnología químicas y, en el año 1994, también a los agentes, la tecnología y los equipos biológicos patógenos para el hombre, los animales o las plantas.

No existe en cambio un organismo multilateral de consulta, sino una serie de compromisos nacionales acordados por los miembros del Grupo. En diciembre de 1994 los Estados miembros establecieron una serie de criterios a la exportación con vistas a la concesión de licencias. Para ello, se elaboraron listados de productos divididos en: precursores químicos; equipos y tecnología químicos y biológicos; agentes patógenos; microorganismos genéticamente modificados (humanos y animales) y por último, toxinas que afectan al ser humano. Para poder exportar un producto de cualquiera de dichas listas es necesario obtener previamente una licencia de exportación y demostrar que el producto va a dedicarse exclusivamente a una aplicación civil. La cantidad de producto a exportar es también determinante, así como su posible doble uso.

Los miembros del Grupo, aparte de la armonización de sus legislaciones, intercambian información sobre los potenciales químicos y biológicos de aquellos países no miembros bajo sospecha de estar desarrollando programas de armas químicas y/o biológicas. Además se encarga de distribuir a las industrias, en colaboración con las ANPAQ, una lista no oficial de alerta de productos y tecnologías de doble uso.

ACUERDOS QUE AFECTAN A VARIOS REGÍMENES

El problema inicial que plantea la desaparición formal del Comité de Control Multilateral de las Exportaciones Tecnológicas hacia los Países del COMECON (COCOM) el día 31 de marzo de 1994 y en consecuencia de los controles a cargo de este en materia de exportación de materiales sensibles y muy sensibles, fue subsanado con la creación de un nuevo foro: el Acuerdo Wassenaar (así llamado en honor a la ciudad danesa donde se concluyó el acuerdo fundacional el 18 de diciembre de 1995). El día 2 de abril de 1996 se reunieron en Viena 31 Estados para inaugurar la aplicación del Acuerdo destinado, a controlar y evitar las transferencias de armas convencionales y tecnologías de doble uso a Estados considerados «expansionistas y que pudiesen amenazar y/o tener intención de adquirir armas de destrucción masiva». En la actualidad son miembros del Acuerdo Wassenaar 33 Estados que adoptaron las directrices por las que se rige el Grupo (llamadas «Elementos iniciales») en el mes de julio de 1996.

El nuevo régimen sustituye las antiguas listas del COCOM, simplificando todos los controles de los productos y tecnologías en dos grupos: la lista de productos y tecnologías de doble uso (que se subdivide a su vez en dos anexos, el primero relativo a productos sensibles y el segundo a los

muy sensibles) y la lista de municiones (equivalente a la lista industrial y militar del COCOM). Ambas listas se revisan periódicamente. Por lo que se refiere a la antigua lista atómica del COCOM desaparece dentro del Acuerdo Wassenaar incorporándose los controles que se establecían sobre los productos nucleares en las listas del GSN.

Para exportar un producto contenido en las listas a un Estado no Parte del Acuerdo Wassenaar es necesario solicitar autorización previa. Lo realmente importante no es el producto en sí, sino su finalidad, civil o militar.

La participación en el Wassenaar es voluntaria y todas las decisiones se adoptan por consenso (no existe tampoco ningún mecanismo de aplicación coercitiva o forzosa de sus decisiones). Sus miembros se reúnen cada seis meses para intercambiar información sobre transferencias y denegaciones de licencias a la exportación de materiales sometidos a control que tengan como destino un Estado no miembro del Acuerdo.

Por último, y aunque como hemos señalado, su análisis será objeto de estudio en otra parte de esta *Monografía*, mencionar el MTCR es un Grupo también informal y no un tratado internacional en sí. El principal objetivo del MTCR es controlar las exportaciones de sistemas y tecnologías que puedan contribuir a la proliferación de misiles capaces de portar una carga nuclear. El régimen se centra en los materiales y las tecnologías destinadas a la fabricación de misiles balísticos y por lo tanto, no establece prohibición alguna en cuanto a la fabricación, posesión o uso de dicho armamento. En la actualidad forman parte del MTCR 32 Estados, entre los que se encuentra España, que decidió adherirse al régimen en marzo del año 1989. La aplicación de las directrices específicas del MTCR queda al arbitrio de cada uno de los Estados miembros y eso es lo que determina también la pertenencia al Grupo como miembro o simplemente su adhesión al mismo.

Políticas de control adoptadas en el seno de organizaciones internacionales

Para completar el cuadro genérico de controles a la exportación de productos y tecnologías que eventualmente podrían utilizarse para la fabricación de armas de destrucción masiva, pasamos a describir los esfuerzos normativos de la Unión Europea y en menor medida, el de la Organización de Naciones Unidas (ONU) en materia de represión de tráfico ilícitos de productos y tecnologías de doble uso.

De forma intencionada dejamos al margen a la Organización del Tratado del Atlántico Norte (OTAN). Si bien es cierto que entre las preocupaciones de la Alianza Atlántica está la lucha contra la proliferación de armas de destrucción masiva, siendo además una de sus prioridades, (como ha puesto una vez más de manifiesto el Documento titulado «Una alianza para el siglo XXI» adoptado el 24 de abril de 1999 por los jefes de Estado y de gobierno de los países miembros de la Organización en la Cumbre de Washington), no persigue sin embargo, atacar de forma directa la cuestión de los tráfico «ilícitos». Además, las medidas que la Alianza Atlántica pone en marcha para combatir el problema de la proliferación son exclusivamente de tipo militar (entrarían dentro de lo que se ha venido denominando desde el año 1993 como «contraproliferación»), si bien es cierto que viene apoyando todos los esfuerzos políticos y diplomáticos que se llevan a cabo dentro de los foros internacionales de no-proliferación.

LA UNIÓN EUROPEA

La Unión Europea ha venido realizado un esfuerzo importante en materia de armonización de las políticas de sus Estados miembros en materia de comercio exterior de productos y tecnologías de doble uso y especialmente, la de aquellos materiales susceptibles de poder ser utilizados para la fabricación de armamento de destrucción masiva. Aunque no es el objeto específico de nuestro estudio consideramos conveniente resumir cuál ha sido la evolución y principales resultados alcanzados (35).

En el año 1993 la Unión Europea introdujo el Mercado Único Europeo, por el que como es sabido, quedaban eliminados, entre otras cosas, la casi totalidad de las barreras a los intercambios comerciales entre sus miembros. Sin embargo, y tal como señala el artículo 223 del Tratado de Roma (actual 296, tras la nueva numeración introducida en virtud del Tratado de Amsterdam), las cuestiones que afectan a la seguridad de los Estados miembros de la Unión Europea no son competencia comunitaria. De este modo, los productos y tecnologías de doble uso, al no ser específicamente militares, podrían haber quedado sometidos a un régimen de libre

(35) Para un análisis detallado de la cuestión, así como la política española al respecto véase GARRIDO REBOLLEDO, V.: «Spain Nuclear Export Control Policy» en MUELLER, H. (ed.): *Nuclear Export Controls in Europe*, Press Interuniversitaires Europeennes-Peace Research Institute Frankfurt, Bruselas, octubre de 1995, pp. 121-144 y «Nuclear and Dual-Use Export Controls: The Spanish case» en GARRIDO, V.: MUELLER, H. y MARQUINA, A. (eds.): «The implications of the 1995 NPT Review and Extension Conference: A Spanish point of view» en *Unisci Papers*, número 7, pp. 59-74. Madrid, julio 1996.

circulación dentro del territorio de los Estados de la Unión Europea. Para eliminar ese «fleco» el Consejo de la Unión Europea creó un «Grupo Ad-Hoc de Alto Nivel sobre controles a la exportación de productos de doble uso». Los trabajos de este Grupo se iniciaron en marzo de 1992, considerando la necesidad de redactar un reglamento que constituyese el marco legal armonizado para la exportación de productos y tecnologías de doble uso. Además, era necesario consensuar una Lista Común Europea de doble uso; una Lista de exclusión de productos especialmente sensibles que se mantendrían bajo control en el comercio intracomunitario, durante un periodo transitorio; una lista de últimos destinos, sometidos a una situación especial y por último, otra de criterios comunes de autorización para la exportación a terceros países.

Tras dos años de debates, el 31 de diciembre de 1994 fue publicado el *Reglamento 3.381/94* sobre control de exportaciones de doble uso, junto a una decisión del Consejo relativa a la acción común adoptada por éste en base al artículo J.3 del Tratado de Maastricht (94/942/PESC). Con vistas a la incorporación de Austria, Suecia y Finlandia en la Unión Europea tuvo lugar la primera modificación de la mencionada legislación, el día 10 de abril de 1995, a través de la publicación del *Reglamento 837/95* el 21 de abril. La entrada definitiva en vigor del nuevo Reglamento, poniendo al día la lista europea de control de exportaciones nucleares a la del resto de los foros analizados, así como la armonización de todas las políticas nacionales de los Estados miembros de la Unión Europea a este respecto se produjo el 1 de julio de 1995.

Desde entonces, la Unión Europea ha seguido actualizando su legislación e materia de control de comercio exterior mediante la publicación de nuevos reglamentos y decisiones del Consejo. Así, por medio de la Decisión 97/100/PESC de 20 de enero de 1997, se incluyeron nuevos productos químicos cuyo control era considerado necesario por la entrada en vigor de la CAQ. Las Lista de productos sometidos a control también ha sido modificada para adecuarla a la del GSN (por medio de la Decisión 98/196/PESC) o del MTCR, relativo a la tecnología de misiles.

Entre los últimos avances, hay que destacar la posición común del Consejo de la Unión Europea de 17 de mayo de 1999 relativa al Protocolo de la CAB, apoyando las medidas para su adopción y que reemplaza a su vez una antigua posición de 1998 propuesta por Reino Unido.

España, por su parte, ha desarrollado un importante cuerpo normativo acorde con los compromisos adquiridos por nuestro país en calidad de

miembro de los citados foros. El nuevo Código Penal contempla por primera vez el delito de contrabando de exportación de material de defensa o de productos y tecnologías de doble uso. Además, la Ley Orgánica 3/1992 de 30 de abril, por la que se establecen los supuestos de contrabando de dichos productos establece penas de cárcel que pueden llegar a seis años para los infractores y multas de hasta el doble del valor de la mercancía exportada sin licencia o habiendo obtenido esta de forma fraudulenta.

NACIONES UNIDAS

La Asamblea General de la ONU constituye uno de los foros tradicionales de negociación para todas las cuestiones relacionadas con el control de armas de destrucción masiva y el desarme (36). Ésta opera a su vez sobre la base del I Comité sobre Desarme y Seguridad Internacional. Sin embargo, desde 1995 las negociaciones, tanto en la Asamblea General como el I Comité permanecen bloqueados por los continuos enfrentamientos entre los Estados nucleares y el grupo de países no alineados a la hora de definir la futura agenda de desarme.

En el ámbito específico que nos ocupa, en 1996 se adoptaron un conjunto de directrices a la exportación (dentro de una agenda de tres prioridades) que evitasen las transferencias internacionales ilícitas de armamentos, con base a la resolución de la Asamblea General 46/36H de 6 de diciembre de 1991.

Políticas nacionales para controlar los tráficoos ilícitos de armamentos de destrucción masiva y productos y tecnologías de doble uso

Teniendo en cuenta que la participación en los foros internacionales de control de exportaciones de productos y tecnologías de doble uso es voluntaria y que las decisiones se adoptan por consenso, algunos Estados han establecido mecanismos adicionales de control.

En el ámbito de la Unión Europea en donde como ya señalamos, ha habido una gran armonización de las políticas en materia de control de comercio exterior de productos y tecnología de doble uso, las sanciones penales y administrativas por exportaciones ilícitas o sin licencia de exportación

(36) Para más información acerca del papel de los diferentes órganos de Naciones Unidas al respecto véase, GARRIDO REBOLLEDO, V.: «El debate entre la no proliferación y el desarme», en *Anuario 1997*, pp. 161-176, CIP. Icaria. Barcelona, 1998.

varían en intensidad de un Estado a otro. Ello se debe a que, pese a que existen acuerdos en lo que respecta a los productos y tecnologías que deben controlarse y cuales deben quedar sometidos a mecanismos especiales de autorización en caso de violación de la normativa europea, la persecución de los delitos de contrabando sigue siendo una competencia exclusiva de los Estados (por ejemplo, a la hora de fijar penas privativas de libertad o a cuánto deben ascender las sanciones) (37).

Fuera del ámbito europeo, Estados Unidos es el país que más sensibilizado se siente en estos momentos con respecto a los riesgos derivados de los tráficos ilícitos de productos y tecnologías de doble uso susceptibles de ser utilizados para la fabricación de armas de destrucción masiva. Washington considera el terrorismo químico, biológico y el cibernético como los dos grandes peligros para la seguridad de Estados Unidos.

Los fondos que el presidente Clinton solicitó al Congreso en enero de 1999 (un incremento en el presupuesto de Defensa de 397.000 millones de pesetas a invertir a razón de 20.000 millones al año) irían destinados en primer lugar al almacenamiento de vacunas, antibióticos y otros medicamentos; segundo, a preparar y entrenar equipos de emergencia contra la guerra química o bacteriológica en el interior del país; tercero, a reforzar la seguridad de las instalaciones gubernamentales; cuarto, a investigar y desarrollar nuevas vacunas y tratamientos y quinto y último a mejorar la seguridad de las redes informáticas frente a los terroristas informáticos (38).

Con ello, Estados Unidos vuelve a estar a la cabeza del desarrollo de un ambicioso programa de defensa ante la eventualidad de un posible ataque químico o biológico contra su seguridad. Programa que según todos los expertos, sitúa a la Casa Blanca en una situación parecida a la de la Administración Reagan cuando ésta lideró la Iniciativa de Defensa Estratégica y que a diferencia de aquella (basada en el desarrollo de un sistema de defensa antimisiles y que previsiblemente será también de nuevo recuperada bajo el Programa Nacional de Defensa de Misiles, a partir del año 2000), la amenaza sería de tipo bacteriológico.

(37) Para un estudio comparativo de las legislaciones al respecto de los países miembros de la Unión Europea, véase MUELLER, H. (ed.): *Nuclear Export Controls in Europe...*, obra citada.

(38) *Remarks by the President on Keeping America Secure for the 21st Century*, White House Text, Speech to the National Academy of Sciences. Washington, 22 de enero 1999.

Conclusiones

Hemos visto que, en una época caracterizada por la ausencia de conflictos de carácter global (aunque los locales sean cada vez más numerosos) aparecen nuevos riesgos para la seguridad que, como en el caso de los tráficos ilícitos de armamentos de destrucción masiva y productos y tecnologías utilizados para su fabricación, requieren un tratamiento también global.

Si hasta hace pocos años el riesgo de contrabando se centraba exclusivamente en las armas ligeras y nucleares, en la actualidad el temor a que algún gobierno irresponsable, o incluso grupo terrorista, pueda lanzar un ataque armado como represalia o chantaje político contra otro Estado con armas químicas o simplemente, dejar escapar un virus o bacteria, ha dejado de ser una hipótesis de novela de policiaca o película de James Bond. Ello se debe a que los productos y tecnologías que se pueden emplear para la fabricación de dichas armas están prácticamente al alcance de cualquier Estado pero sobre todo, porque es muy difícil probar de antemano la finalidad civil o militar de una sustancia, que como señalamos puede ser a la vez la base de una vacuna o de un virus.

La única forma de tratar el problema de los tráficos ilícitos de estos productos y tecnologías es por lo tanto reforzar los regímenes multilaterales de no-prolifерación y sus instrumentos normativos, cuyo éxito dependerá de que contemplen medidas de verificación eficaces con el fin de que puedan detectarse a tiempo (y en su caso, sancionarse) las violaciones de sus disposiciones.

En la actualidad, existe una predisposición por parte de la comunidad internacional para que dichos regímenes sean universales. Se intenta convencer a los Estados al margen de dichos regímenes de que es más positivo, a efectos de intercambios comerciales, ser Parte en los tratados internacionales y acogerse a los mecanismos de control vinculados a éstos que tenerse que someter a estrictos procedimientos de autorización de importaciones reservados a los no signatarios.

En esa línea, la gran mayoría de los Estados apoya el refuerzo de los regímenes de no-prolifерación de armas de destrucción masiva mediante la adopción de medidas y acciones en el terreno diplomático y político, mientras que las acciones militares, que implican el uso de la Fuerzas Armadas, siguen siendo contempladas como medidas de último recurso, cuando fracasan todos los esfuerzos diplomáticos.

TRÁFICO DE MISILES Y DE TECNOLOGÍAS EN EL MARCO DE UN NUEVO CONCEPTO DE SEGURIDAD

Por BELÉN LARA FERNÁNDEZ

El tráfico de misiles y de tecnología como factor de inestabilidad

Hace una década la seguridad giraba en torno a alianzas enfrentadas y a capacidad nuclear. Durante el periodo de guerra fría, la seguridad se basaba fundamentalmente en el componente militar. Tras la desaparición de la confrontación entre el Este y el Oeste, las crisis y los conflictos regionales son los protagonistas indiscutibles. Conflictos históricos que estaban latentes, pero reprimidos por la bipolarización imperante, han eclosionado violentamente. Son crisis y conflictos que abarcan desde contradicciones sociales internas hasta rivalidades entre Estados vecinos, pasando por conflictos étnicos, religiosos y económicos, y cuyas repercusiones más inmediatas se dejan sentir en la demografía, los movimientos migratorios, la economía, la calidad de vida, el bienestar y el desarrollo, así como en el medio ambiente.

Para la comunidad occidental, los análisis del riesgo que esta nueva situación implica, deben tener como marco un concepto de seguridad más amplio, con nuevas dimensiones, y no deben limitarse a un aspecto concreto. Los análisis de riesgo tienen que contemplar la interdependencia de los procesos, relacionando las cuestiones políticas, sociales, económicas, demográficas y ecológicas y su incidencia sobre la seguridad, para poder así hacer una valoración estratégica de la situación. La cooperación

—incluida la cooperación de carácter subregional— es indispensable para poder abordar los retos que plantea un concepto de seguridad con nuevas dimensiones.

La seguridad aparece más que nunca, unida a la noción de estabilidad. Estabilidad política, económica, social, regional, etc. Y, por ende, debe evitarse y combatirse todo lo que produzca inestabilidad. Un ejemplo, el mantenimiento de los gastos de armamento puede llegar a agotar los recursos económicos de un país subdesarrollado; se producirá una conflictividad social, que puede dar lugar a enfrentamientos, convirtiéndose así en un factor de inestabilidad. Esta situación tiene, a su vez, efectos sobre los países industrializados, que sino han de llegar a intervenir directamente, sí que tendrán que detraer recursos para las operaciones de pacificación y para atender a los refugiados.

Pero ciñéndonos a los retos que ha de afrontar la seguridad en el cambio de siglo, hemos de señalar que el fenómeno que más inestabilidad produce y que más preocupa a la comunidad internacional es, sin duda, la proliferación de las armas de destrucción masiva.

Conviene desgranar esta expresión general y recurrente en la bibliografía y documentación al uso: «la proliferación de las armas de destrucción masiva», a fin de enmarcar adecuadamente el objeto de este estudio.

Por proliferación entendemos:

- La exportación, difusión o tráfico —ya sea de carácter lícito o ilícito— de los sistemas completos o de los equipamientos, tecnologías, materiales, conocimientos o especialistas relacionados con la fabricación de armas Nucleares, Biológicas y Químicas (NBQ) o de misiles, realizados por un país o una empresa constructora de armamentos.
- El esfuerzo realizado por un determinado Estado en el campo de la investigación, desarrollo y fabricación de los equipamientos y tecnologías de misiles y de armas de destrucción masiva, cuyo objetivo es poder contar con un sistema propio, sin excluir que pueda tratarse de un esfuerzo realizado clandestinamente.

Al referirnos a las armas de destrucción masiva incluimos:

- Las cargas o municiones NBQ propiamente dichas.
- Los misiles balísticos susceptibles de transportarlas y lanzarlas. El motivo de que se considere específicamente a los misiles balísticos armas de destrucción masiva y no a otro tipo de misiles, como los de crucero, se debe a que los misiles balísticos procuran al arma-

mento NBQ el máximo de efectos militares, estratégicos y psicológicos.

Así pues, la proliferación de armas de destrucción masiva supone un reto para la seguridad en los próximos años, y así se reconoció en el seno de la Organización del Tratado del Atlántico Norte (OTAN) cuando en la Cumbre de Washington de abril de 1999, al aprobar el nuevo Concepto Estratégico de la Alianza, se adoptó una iniciativa destinada a garantizar la capacidad de los aliados para hacer frente al reto que plantea la proliferación de armas NBQ y sus sistemas de lanzamiento, integrando los aspectos políticos y militares y creando en Bruselas un Centro de Coordinación sobre las Cuestiones Relacionadas con la Proliferación (39).

Interesa ahora detectar los canales de distribución que favorecen la proliferación de este tipo de armamento. Al tráfico del material NBQ se dedica un apartado de este mismo capítulo; este apartado está dedicado al tráfico de los misiles balísticos y de sus componentes y tecnologías. A continuación intentaremos aportar una serie de datos que puedan servir al lector para conocer en qué forma se van expandiendo este tipo de misiles, los misiles balísticos, a los que la comunidad internacional considera una seria amenaza y una fuente de inestabilidad en el umbral del siglo XXI. Si el tráfico de misiles y de tecnología de misiles continúa persistiendo, aumentará el número de escenarios afectados por la amenaza del uso o por el uso propiamente dicho de los misiles. El espectro de un devastador ataque químico, biológico o incluso nuclear realizado con un misil balístico desde un país subdesarrollado continúa constituyendo una amenaza que a corto plazo podría afectar a toda Europa y a una buena parte del territorio de Estados Unidos. La amenaza del uso de los misiles balísticos como portadores de armamento NBQ se favorece y refuerza con el tráfico de misiles y de sus tecnologías, y produce una gran inestabilidad. Es, por tanto, un hecho que hay que evitar, controlar y combatir para reforzar la estabilidad como componente básico de la seguridad.

La fabricación de misiles balísticos requiere especialistas y medios industriales en campos muy variados, pero las exportaciones que han realizado un pequeño número de países, incluidos países occidentales y Estados surgidos tras la desmembración de la Unión Soviética, han favorecido su amplia proliferación. La transferencia de misiles de un país a otro no

(39) Véase Consejo del Atlántico Norte, «Concepto Estratégico de la Alianza» y Crispin Hain-Cole, «La Iniciativa de la Cumbre sobre las Armas de Destrucción Masiva», ambos en *Revista de la OTAN*, número 2. Verano, 1999.

supone una novedad, sí lo es el intercambio de tecnología de misiles entre los países que van accediendo a ella. En Corea del Norte venden tecnología de misiles a cambio de divisas que puedan paliar su insostenible situación económica. Pakistán realiza supremos esfuerzos para mejorar su capacidad misilística y contraponerla a la de La India. Irán posee la infraestructura técnica necesaria para tener un sistema muy avanzado de misiles de largo alcance como consecuencia de la importante asistencia técnica recibida de Rusia, China y Corea. Los misiles de Irán, Irak y Siria son la amenaza más seria que sufre la estabilidad en Oriente Medio.

Para hacernos una idea de la magnitud del problema, a principios de 1998 (40) se estimaba que en aproximadamente 50 Estados había desplegados unos 13.000 misiles balísticos, y que de los casi 40 modelos existentes, alrededor de dos tercios tenían alcances inferiores a los 500 kilómetros. El resto tienen alcances superiores y China, por ejemplo, está intentando desarrollar misiles que superen los 12.000 kilómetros, lo cual le permitiría impactar sobre cualquier punto del territorio europeo y del norteamericano. A continuación se insertan los cuadros 1 y 2 que permiten hacerse una idea más exacta de la distribución de los misiles en el mundo. El cuadro 1 (41), es de los países con misiles balísticos que pueden impactar sobre Europa. El cuadro 2 (42), refleja la distribución de los misiles en función de su alcance kilométrico.

Estudio de los posibles canales de distribución (43)

Resultaría muy osado tratar de identificar todos los canales de distribución de equipamientos, tecnologías y materiales relacionados con los misiles, o del tráfico de misiles propiamente dicho. Más bien lo que se pretende en este capítulo es aportar una información que sirva de referencia a la hora de realizar el análisis de lo que supone el tráfico de misiles

(40) DIBB, P.: «The Future Military Capabilities of Asia's Great Powers», en *Jane's Intelligence Review*, volumen 7/5. 1998.

(41) Cuadro elaborado con los datos recogidos en «Ballistic Missile Systems and Capabilities», en *Arms Control Today*, volumen 26, número 2. 1996.

(42) Cuadro elaborado con los datos recogidos en Aaron Karp, *Ballistic Missile Proliferation*, SIPRI, Oxford University Press. 1996.

(43) Para la elaboración de este capítulo se ha utilizado principalmente: REED, J.: «Strategic Weapons-de-Militarisation Markets. Non-Proliferation, De-Militarisation and Decommissioning Markets Appraised», en *Jane's Special Report*. 1995.

Cuadro 1.- Países con misiles balísticos que pueden impactar sobre Europa.

País	Sistema	Alcance (km)	Tipo	Proveedor	Estatus
Afganistán	Scud-B	300	BM	Unión Soviética	Utilizado
Arabia Saudí	CSS-2	2.650	BM	China	Operativo
Argelia	Frog-7	65	BM	Unión Soviética	Operativo
Corea del Norte	Frog-7	65	BM	Unión Soviética	Operativo
	Scud-B	300	BM	Egipto-Irán	Operativo
	Scud-C	500	BM	China-Corea del Norte	Operativo
	No Dong-1	1.000	BM	China-Corea del Norte	Probado
	No Dong-2	<2.000	BM	Corea del Norte	Desarrollo
	Taepo Dong	6.000	BM	Corea del Norte	Desarrollo
Corea del Sur	NHK-1	180	BM	EE.UU.-Corea del Sur	Operativo
	NHK-2	260	BM	EE.UU.-Corea del Sur	Desarrollo
Egipto	Frog-7	65	BM	Unión Soviética	Utilizado
	Scud-B	300	BM	Unión Soviética	Utilizado
	Scud-100	600	BM	Corea-Egipto	Desarrollo
India	Prithvi-150	150	BM	Unión Soviética-India	Operativo
	Prithvi-250	250	BM	Unión Soviética-India	Probado
	Agni-II	2.500	BM	India	Probado
	Agni-III	3.500	BM	India	Desarrollo
Irak	Laith	90	BM	Unión Soviética-Irak	Probado
	Nissan	110	BM	Irak	Desarrollo
Irán	Mushak-120	120	BM	China-Irán	Utilizado
	Mushak-160	160	BM	China-Irán	Operativo
	Mushak-200	200	BM	China-Irán	Desarrollo
	8.610	300	BM	Corea del Norte	Operativo
	Scud-B	300	BM	Corea del Norte	Utilizado
	Scud-C	500	BM	Corea del Norte	Operativo
	Irán-700	700	BM	China-Irán	Desarrollo
	Tondar-68	1.000	BM	China-Irán	Desarrollo
	No Dong-1	1.000	BM	Corea del Norte	Cancelado
Israel	Lance	130	BM	Estados Unidos	Operativo
	Jericó I	650	BM	Francia-Israel	Operativo
	Jericó II	1.500	BM	Francia-Israel	Operativo
	Jericó lib	1.300	BM	Francia-Israel	Operativo
	Shavit	2.500	BM	Francia-Israel	Operativo
Libia	Scud-B	300	BM	Unión Soviética	Operativo
	Al-Fatah	<950	BM	Alemania-Libia	Desarrollo
	No Dong-1	1.000	BM	Corea del Norte	Negociación
Pakistán	Haft I	80	BM	Francia-Pakistán	Operativo
	M-11	280	BM	China	Sin ensamblar
	Haft II	300	BM	Francia-Pakistán	Probado
	Shaheen (H-III)	600	BM	Francia-Pakistán	Desarrollo
	Ghauri-II	1.400	BM	Pakistán	Probado
	Tippu	4.000	BM	Pakistán	Desarrollo
Siria	SS-21	120	BM	Unión Soviética	Operativo
	Scud-B	300	BM	Unión Soviética	Operativo
	Scud-C	500	BM	Corea del Norte	Operativo
	No Dong-1	1.000	BM	Corea del Norte	Negociación
Taiwan	Ching Feng	100	BM	Israel-Taiwan	Operativo
	Tien Ma	950	BM	Taiwan	Desarrollo
Ucrania	SS-21	120	BM	Unión Soviética	Operativo
	Scud-B	300	BM	Unión Soviética	Operativo

Cuadro 2.- Distribución de los misiles en función de su alcance kilométrico.

País	40-110	110-300	300-600	600-1.500	1.500-5.000	>5.500
Alemania	•	•				
Arabia Saudí	•					
Argelia	•	•			•	
Bélgica		•				
Bielorrusia	•	•				
Brasil	•					
Bulgaria	•	•	•			
China	•	•	•		•	•
Corea del Norte	•	•	•	•		
Corea del Sur	•	•				
Cuba	•					
Egipto	•	•				
Eslovaquia	•	•	•			
Estados Unidos	•	•			•	•
Francia	•		•		•	
Grecia	•					
Holanda		•				
Hungría	•					
India		•			•	
Irak	•	•				
Irán	•	•	•			
Israel	•	•	•	•		
Italia	•	•				
Kazajstán	•	•				•
Libia	•	•				
Pakistán	•	•			•	
Polonia	•	•				
Reino Unido	•	•			•	
República Checa	•	•	•			
Rumania	•	•				
Rusia	•	•			•	•
Serbia	•		•			
Siria	•	•				
Suráfrica				•	•	
Taiwan		•				
Turquía	•					
Ucrania	•	•				•
Yemen	•	•				

o de sus componentes, en el marco de un nuevo concepto de seguridad; y, aunque lo hemos dividido en zonas geográficas, se puede concluir que éstas quedan totalmente interrelacionadas si, someramente, echamos una mirada a lo acontecido años atrás: Rusia suministró a China misiles *Scud*, y China ayudó a Pakistán, que está vinculada a Irán. Este país mantiene relaciones con La India que, a su vez, está estrechamente ligada a Egipto, que fue el primer país que transfirió tecnología de misiles *Scud* a Corea del Norte, que proporciona misiles a Irán y a Pakistán.

Países que pertenecían a la órbita soviética

En general, los países que, en la ya superada división bipolar, estaban en la órbita de la Unión Soviética, poseían misiles estratégicos, o misiles tácticos, o ambos tipos de misiles y tenían grandes expertos en tecnologías asociadas con la guerra química. Por tanto, no se puede desechar la posibilidad de que esos países hayan sido o se conviertan en exportadores de tecnologías y de expertos en misiles y en armas químicas. Si bien las circunstancias hacen pensar que es difícil que se arriesguen a comprometer y perjudicar su nueva posición y el apoyo que están recibiendo de la comunidad occidental, y que restringirán sus actividades de exportación al armamento convencional. Veamos, a continuación, las peculiaridades de algunos de estos países con mayor potencial para exportar.

Bielorrusia

Contaba con dos divisiones de Misiles Balísticos Intercontinentales (ICBM) y el Ejército soviético reconoce que ha mantenido cuatro bases con técnicos en misiles sobre suelo bielorruso. A comienzos del año 1994 se retiraron dos regimientos de misiles SS-25 y posteriormente se retiraron tres regimientos más, con un total de 36 lanzadores. El resto, otros 18 lanzadores, se retiraron a mediados de 1996. Todos estos misiles retirados de suelo bielorruso no se han ido desmantelando y parece ser, según los datos que se manejan en las negociaciones sobre reducción de armamento, que han sido equipados con cabezas múltiples cuando han llegado de vuelta a Rusia.

Kazajstán

Tenía en su territorio dos silos de misiles balísticos estratégicos, cada uno con 52 misiles SS-18. Firmó el Tratado START y se comprometió a retirar sus armas nucleares y a devolverlas a Rusia, pero se quedó con los misiles SS-18 para utilizarlos como lanzaderas espaciales. Existe la fundada sospecha de que esta República se podría convertir en proveedora de materiales y/o tecnología nuclear y de misiles.

Ucrania

Tenía, en tiempos de la Unión Soviética, 176 misiles intercontinentales sobre su suelo: 46 del tipo SS-24 y 130 del tipo SS-19. En cumplimiento del acuerdo trilateral firmado en el año 1994 por Estados Unidos, Rusia y Ucrania están siendo retirados y Estados Unidos ha prestado asistencia

y financiación especialmente para el desmantelamiento de los SS-24, cuya avanzada tecnología y poder de destrucción aconsejan un control externo para evitar posibles tráfico. También poseía misiles balísticos tácticos del tipo SS-21 y *Scud-B*. Ucrania ha negado la acusación que pesaba sobre ese país de exportar misiles a China y a Libia. A principios del año 1998, Estados Unidos ofreció su apoyo al Gobierno ucranio para que entrase a formar parte del MTCR (*Missile Technology Control Regime*), a cambio de que cancelara el contrato que había firmado con Irán para proporcionarles las turbinas de una central nuclear. Ucrania fue admitida como miembro de pleno derecho del MTCR en el año 1998.

Rusia

Retiró sus últimos misiles nucleares tácticos de Ucrania en mayo del año 1993 y comenzó a retirar los misiles estratégicos nucleares de Bielorrusia y Ucrania un año después. Todo ello con una financiación occidental que ha servido, entre otras cosas, para reforzar los controles que impidieran el tráfico de misiles, de las cargas nucleares y de las tecnologías asociadas con ambos, pero que no ha servido para evitar que Rusia vendiera tecnología de misiles a China y a Brasil, y, más concretamente, sistemas de guiado a Irak. En el año 1997 Estados Unidos e Israel promovieron una fuerte protesta contra Rusia por prestar asistencia a Irán para desarrollar una versión del *Scud* con mayor alcance. Anteriormente, la Unión Soviética había exportado misiles balísticos *Scud* de 300 kilómetros de alcance a sus socios en Europa y en Oriente Medio; también había vendido versiones del misil SS-23 con carga convencional, cuyo alcance es de 500 kilómetros, a Bulgaria, Checoslovaquia y a Alemania del Este.

Por otro lado, muchos científicos y técnicos que trabajaban en las instalaciones dedicadas a la fabricación de misiles balísticos, han sido reciclados para evitar que se quedaran desempleados y que sus conocimientos les abocaran a trasladarse a otros países interesados en desarrollar tales tecnologías. De esta misión se ha encargado el Centro Internacional de Ciencia y Tecnología, con sede en Moscú, cuya financiación es internacional, aunque principalmente proviene de Estados Unidos. Esta política de ayudas ha sido criticada en un informe elaborado por la GAO (*General Accounting Office*) (44) de Washington, que opina que tales recursos estarían mejor empleados en otros programas de asistencia técnica que

(44) US General Accounting Office, *Nuclear Non-proliferation: Concerns with DOE's Efforts to Reduce the Risks Posed by Russia's Unemployed Weapons Scientists*, GAO/RCED-99-54. Washington, febrero 1999.

mejoraran las condiciones de seguridad. Además, otros muchos científicos y técnicos permanecen en suelo ruso, viviendo en condiciones de miseria y sin posibilidades de seguir profundizando en sus conocimientos o de realizar nuevas investigaciones. Es posible que éstos sí decidan marchar a otros países si se les brinda la oportunidad. Rusia es parte del MTCR desde 1995.

Oriente Medio y norte de África

Esta región puede considerarse un tentador pero indeseable mercado para la total propagación de las tecnologías aplicables al desarrollo y producción de misiles y de armamento NBQ. La comunidad occidental intenta que toda la región se declare zona libre de armas nucleares y aplicar las salvaguardas de la Agencia Internacional de la Energía Atómica, pero los países afectados tienen otras perspectivas. Israel no tiene intención de renunciar a su capacidad nuclear y sus vecinos árabes desean poseer esa misma capacidad destructiva, fundamentalmente por dos motivos:

1. Para no estar en desventaja en caso de enfrentamiento.
2. Para tener capacidad disuasoria y evitar ser atacados.

Pero también existen otras rivalidades en la zona, que ponemos de manifiesto a continuación.

Irán

Tiene unas Fuerzas Armadas muy mal equipadas de armamento convencional y su objetivo es contar con armas de destrucción masiva para compensar tal deficiencia y su relativo aislacionismo estratégico. El armamento nuclear convertiría a Irán en una potencia militar regional con capacidad para intimidar a sus vecinos y como sigue considerando a Irak —o más concretamente al régimen de Saddam Hussein— como la más seria amenaza para su seguridad, contaría con una forma de disuadir a Irak de utilizar sus armas de destrucción masiva en caso de enfrentamiento, tanto en el campo de batalla como en un ataque directo sobre ciudades iraníes. Tal potencial también le serviría para intimidar a Afganistán y a Azerbaiyán durante una crisis o durante un enfrentamiento armado, y, por último, resultaría una amenaza para países aliados de Estados Unidos tales como Arabia Saudí, Egipto, Israel y Turquía, lo cual le revalorizaría ante los ojos de Washington.

En el terreno económico, resulta la única forma que tiene Irán de convertirse en potencia militar sin destruir su economía, ya que un programa de desarrollo de armas de destrucción masiva es mucho más barato que reconstruir un potente armamento convencional. Así pues, en lugar de invertir y modernizar este tipo de armamento, han decidido que es preferible poseer misiles balísticos tácticos y estratégicos y armamento NBQ. Su producción de misiles parte de la adquisición de tecnología de Corea del Norte y de China. Ha obtenido suministros para sus misiles *Scud* de la Unión Soviética, de Libia y de Siria, y en el año 1986 comenzó a fabricar sus propios misiles *Scud-B*, a los que pretende incorporar tecnología del *No Dong-1* coreano. A mediados del año 1998, realizó pruebas de un misil *Shehab-3*, de alcance medio (1.290 kilómetros), y en sus planes está el desarrollar el *Shehab-4*, con un alcance estimado en los 2.000 kilómetros, y el *Shehab-5*, que podría llegar a los 10.000 kilómetros; pero para producir este tipo de misiles necesita ayuda exterior que, en la actualidad, sólo puede proporcionarle Rusia (45) .

Irak

Contaba con los siguientes tipos de misiles: *Laith*, con alcance para 90 kilómetros; *Nissan*, con un alcance de 110 kilómetros; *CSS-8*, con alcance para 150 kilómetros; *Scud-B*, con alcance de 300 kilómetros; y *Al Hussein*, con un alcance de 650 kilómetros. Después de la guerra del Golfo, mediante la resolución 687 del Consejo de Seguridad de Naciones Unidas, sólo se le autorizó a mantener aquellos misiles que no superaran los 150 kilómetros de alcance y a no adquirir, desarrollar o fabricar posteriormente ningún sistema de misiles que superara dicha distancia. En algunos informes realizados recientemente, se afirma que posee misiles *Scud* escondidos en hangares subterráneos y que conserva todos los componentes necesarios para volver a montar los misiles *Al Hussein*.

Israel

Posee armamento nuclear y misiles del tipo *Lance*, y del tipo *Jericó* y *Shavit*. Estos últimos desarrollados con asistencia y tecnología francesa. Para aumentar su capacidad defensiva en caso de que su capacidad disuasoria falle, está desarrollando misiles antimisiles *Arrow*, programa que está siendo financiado en un 80% por Estados Unidos. Pero, paradójicamente,

(45) EISENSTADT, M.: «Living with a Nuclear Iran?», en *Survival*, volumen 41, número 3. Otoño, 1999.

ha prestado asistencia técnica a Arabia Saudí y a Irán para que ambos países puedan desarrollar sus programas de misiles.

Libia

Al igual que Irán e Irak, no ofrece legitimidad comercial en el campo del armamento y sus intentos de obtener determinado tipo de tecnologías están sujetos a un escrutinio muy severo. Es un país sometido a constante presión y aislamiento y tal situación ha incidido en que haya abandonado sustantivamente lo que fue su gran símbolo de poder a finales de los años ochenta: poseer misiles y armas de destrucción masiva. No obstante, existen estimaciones de que posee 80 misiles *Scud-B* y otras fuentes señalan que podría tener 40 misiles *Frog-7*, además de un número desconocido de *Scud-C*, cuyo alcance es de 500 kilómetros. Asimismo tiene desplegados misiles defensivos en la costa, del tipo SSC-3 *Styx*.

Siria

Tiene una considerable potencia militar, pero intenta adquirir nuevas capacidades estratégicas desarrollando misiles balísticos y así mantenerse en paridad con otros Estados regionales. Empero, no parecen estar interesados en obtener capacidad nuclear, más allá de lo estrictamente necesario para uso civil. En la zona de Damasco tiene desplegados misiles *Scud-B* en plataformas de lanzamiento subterráneas, también cuenta con *Scud-C* dispersos y con algunas unidades de SS-21. A comienzos de los años ochenta recibió, según información de la prensa israelí, asistencia técnica de la empresa alemana OTRAG para desarrollar misiles balísticos tácticos y también intentó adquirir misiles M-9 y *No Dong-1* procedentes de China y Corea, respectivamente.

Egipto

Cuenta con una gran proporción de equipamientos producidos en los países que estaban en la órbita de la Unión Soviética y los ha mantenido en servicio sin un apoyo logístico demasiado significativo. Tiene un regimiento de misiles *Scud-B*, que alcanzan los 300 kilómetros; un regimiento de misiles *Frog-7*, con un alcance de 65-70 kilómetros; y un número no determinado de misiles *Sakr-325* de corto alcance. A principios de los años ochenta llegó a un acuerdo con Corea del Norte para desarrollar una versión mejorada de los misiles *Scud-B*, pero, al parecer, tal proyecto a sufrido problemas de financiación y Egipto ha intentado un nuevo pro-



grama de colaboración con Siria. También ha llegado a un acuerdo con China para mejorar la factoría de los misiles *Sakr* y poder producir misiles *Scud* y misiles *Sakr* que alcancen los 80 kilómetros y que puedan sustituir a los misiles soviéticos *Frog*. Egipto no parece tener un programa específico de armas nucleares ni es probable que lo tenga a corto plazo. Sí posee armas químicas y biológicas.

Argelia

Tiene un programa nuclear, que inició en el año 1984, y que en algunas informaciones aparece vinculado a los esfuerzos que está realizando Irán para poseer armas nucleares. No tiene capacidad suficiente para diseñar y producir misiles balísticos y parece improbable que a medio plazo pueda desarrollar sus propias armas nucleares y algún mecanismo capaz de liberarlas. Cuenta con misiles balísticos del tipo *Frog-7*, cuyo alcance no supera los 70 kilómetros.

Asia

Aunque esta región queda fuera del objeto general de este estudio, se incluye una breve referencia a algunos países a los que se relaciona con el tráfico de misiles por ser grandes productores de estos ingenios. Además, la región se ha convertido en una persistente fuente de preocupación debido a la existencia de programas nucleares y a la capacidad que tienen tanto India como Pakistán para ensamblar, en un breve periodo de tiempo, cabezas nucleares en sus propios misiles balísticos. Por otro lado, la zona de China, Corea del Norte y Corea del Sur, ofrece una problemática distinta:

India

Con el objetivo declarado de alcanzar la paridad con China en el aspecto misilístico, probaba, el día 11 de abril de 1999, su misil de alcance intermedio *Agni-II* (2.000 kilómetros), después de que en el año 1994 realizase la prueba de un misil *Agni-I*, y anunció que estaba desarrollando el *Agni-III* (3.500 kilómetros) y que estaba modernizando el *Prithvi* para que alcanzara los 350 kilómetros, en lugar de los 150 kilómetros actuales.

La emergente relación entre Rusia e India tiene implicaciones políticas, económicas, militares y geoestratégicas. La implicación rusa en el sector de la defensa de India se ha ido intensificando y se intensificará más en

la medida en que Estados Unidos no revoque las sanciones que han congelado su cooperación defensiva con India. De hecho, Rusia ha renunciado a vender armamento a Pakistán por considerar que supone una amenaza real e inmediata para La India, al mismo tiempo que participa en el programa de SLBM (*Submarine-Launched Ballistic Missiles*) indio, mejorando su sistema de lanzamiento (46).

Pakistán

Procedía a probar su misil *Ghauri-II*, con un alcance de 1.400 kilómetros, el día 14 de abril de 1999, y el día 15 de abril realizó el lanzamiento del misil *Shaheen-I*, con un alcance de entre 600 y 750 kilómetros. Según la prensa paquistaní, debido al exitoso resultado de la prueba, el Gobierno habría ordenado la masiva producción del misil *Shaheen-I*. Asimismo, Pakistán está desarrollando el misil *Tippu*, con un alcance de 4.000 kilómetros.

Tanto el *Ghauri-II* como el *Ghauri-I*, lanzado en abril del año 1998, están basados en tecnología de Corea del Norte con sistemas de guiado procedentes de China. El *Shaheen-I* está basado en tecnología China y es conocido que en 1992 China exportó alrededor de 30 misiles M-11, con un alcance de 280 kilómetros a Islamabad.

En estas circunstancias, resulta especialmente preocupante la falta de diálogo entre estos dos países para encontrar posibles soluciones a sus ya históricas diferencias políticas y religiosas, y más preocupante aún el enfrentamiento habido recientemente en la región de Cachemira. Ambos Estados han conseguido un alto grado de autosuficiencia, pero todavía tienen necesidades tecnológicas y han establecido mecanismos secretos para adquirir las tecnologías y el material que les resulta imprescindible. Parece ser que, comparativamente, Pakistán está más necesitado que La India de recibir transferencias tecnológicas en ciertas áreas clave. Al mismo tiempo, ambos países se han convertido en potenciales vendedores de misiles y de tecnologías de misiles, así como de lanzaderas espaciales.

China

Jamás ha confirmado oficialmente el número total de misiles operativos que posee. Existen diversas estimaciones al respecto y numerosos infor-

(46) KHRIPUNOV, I. y SRIVASTAVA, A.: «Russian-Indian Relations: Alliance, Partnership, or?», en *Comparative Strategy*, volumen 18, número 2. 1999.

mes, de los cuales se deduce que tiene cinco tipos de misiles balísticos estratégicos (entendiendo por estratégicos los que son capaces de alcanzar los 2.500 kilómetros) y que continúa desplegando misiles M-11 de corto alcance (300 kilómetros) y misiles M-9 de alcance intermedio (600 kilómetros) en su costa sur, con lo cual puede alcanzar perfectamente Taipei, situada a 204 kilómetros. En el año 1996 tenía desplegados entre 30 y 50 unidades de estos misiles; en la actualidad se estima que cuenta con un número que oscila entre los 160 y los 200. Asimismo, China está intentando obtener tecnología de misiles balísticos de Ucrania y Rusia para dotar a sus misiles de mayor alcance kilométrico y de mayor capacidad para maniobrar, y consiguió de Bielorrusia tecnología y equipamientos del lanzador SS-20.

Durante los años 1991 y 1993, China sufrió las sanciones que le impuso Estados Unidos por vender misiles balísticos M-11 a Pakistán. A cambio de que Estados Unidos levantara las sanciones, China se comprometió a observar el MTCR, aunque sin llegar a ser parte del acuerdo, y a no exportar misiles que fueran «inherentemente capaces» de exceder los parámetros del MTCR, aunque siguió transfiriendo componentes de esos misiles a Pakistán y le prestó asesoramiento para montar su propia planta de misiles M-11. Los medios occidentales han denunciado estas transferencias clandestinas a Pakistán, pero China ha continuado con ellas a pesar de las presiones. La razón es que, en interés de su propia seguridad, China prefiere que Pakistán tenga capacidad de disuasión frente a la hegemonía de India, cuyo ministro de Defensa ha manifestado que China constituye la amenaza más importante contra la seguridad de la India.

También China está bajo sospecha de exportar componentes y tecnología de misiles a Irán y a Siria y de seguir manteniendo un más que sospechoso comercio de equipamientos y asistencia con Irán, Libia y Pakistán.

Pero un nuevo conflicto surgió en mayo de 1999 en relación con China. Una versión desclasificada del denominado «Informe Cox» (47), elaborado por un Comité del Congreso norteamericano, salió a la luz pública denunciando que, ilegalmente, por medio del espionaje, China había obtenido tecnología norteamericana de un gran número de programas de defensa y, entre ellos, de los misiles balísticos. Este tráfico de tecnologías podría haberse evitado con unas medidas de seguridad más estrictas y con haber

(47) Un amplio resumen del «Informe Cox» puede consultarse en *The Arms Control Today*, volumen 29, número 3. Abril-mayo, 1999.

potenciado un sistema de contrainteligencia, pero a los sucesivos Gobiernos norteamericanos lo que les interesaba era fortalecer las relaciones comerciales con China. Por otro lado, si China era más poderosa militarmente, se forzaba a la Unión Soviética a desplegar fuerzas militares adicionales, lo cual beneficiaba a la seguridad nacional de Estados Unidos.

En el desfile militar del año 1999, que conmemoraba el quincuagésimo aniversario de la creación de la República Popular de China, se pudieron ver por primera vez los misiles balísticos intercontinentales *Dong Feng-31* capaces de alcanzar el suelo de la costa occidental de Estados Unidos, ya que su alcance es de 8.000 kilómetros. También fueron exhibidos los misiles DF-11 y DF-15 de corto alcance, que apuntan a Taiwan.

Corea del Norte

Tiene misiles tácticos *Frog* y *Scud B* y *C* en servicio, y ha desarrollado una versión propia del misil chino HY-2, utilizado para defensa de la costa. En mayo de 1993 realizó pruebas del misil *No Dong-1*, con un alcance de 1.000 kilómetros, y se piensa que comenzó a desplegarlo. Es significativo que a las pruebas realizadas en 1993 asistieran observadores iraníes y paquistaníes, países ambos interesados en establecer cooperación bilateral sobre misiles con Corea. Indudablemente el Programa No Dong se ha beneficiado de las pruebas e intercambios de los Programas Ghauri de Pakistán y Shehab de Irán. A pesar de su preocupante situación económica, en agosto de 1998 lanzó un misil *Taepo Dong-1* que atravesó el espacio aéreo japonés y se hundió en el Pacífico, y tiene previsto contar para el año 2000 con un número de misiles *No Dong* que se moverá entre los 50 y los 100, y en el año 2002 con misiles del tipo *Taepo Dong*, capaces de alcanzar los 6.000 kilómetros, para cuyo desarrollo y avanzado sistema de guiado cuenta con la colaboración de ingenieros procedentes de Rusia, Ucrania y China. Estados Unidos ha presionado para que no realicen más lanzamientos de misiles sobre Japón, amenazando con represalias económicas y diplomáticas. La presión ha surtido efecto ya que el 24 de septiembre de 1999, tras seis días de conversaciones bilaterales en Berlín, el Gobierno de Pyongyang anunciaba que suspendía las pruebas de lanzamiento de misiles de largo alcance a cambio de que Washington suavizara su embargo económico y se encontrara una salida negociada.

Esa misma situación económica es la que convierte a Corea del Norte en un potencial exportador de misiles y componentes. Egipto, Libia y Siria se han mostrado interesados en obtener misiles *No Dong* o bien tecnología

para producirlos, y existen indicios de que Egipto ha recibido alguna tecnología relacionada con el misil pero no componentes ni misiles propiamente dichos. Asimismo, existen indicios de que ha vendido a Vietnam un número indeterminado de misiles *Scud* —se cree que del tipo C— modificados para que alcancen los 550 kilómetros.

Corea del Sur

No cuenta con producción propia de misiles balísticos de corto o medio alcance y tiene un acuerdo firmado con Estados Unidos por el cual se compromete a no tener misiles con un alcance superior a los 180 kilómetros. Empero, cuenta con misiles del tipo *Nike Hércules*, de fabricación norteamericana, que han sido modificados para aumentar su precisión y para que puedan alcanzar distancias superiores a la antes mencionada.

Por otro lado, en abril de 1999, la prensa de este país informó de que se había probado un misil balístico con un alcance de 300 kilómetros. Oficialmente tal hecho no se ha confirmado, pero tampoco se ha desmentido y es bastante probable que sea así porque un misil con un alcance de 180 kilómetros, aunque fuese lanzado desde la frontera que separa las dos Coreas, no alcanzaría Pyongyang, y porque han intentado abrir negociaciones con Estados Unidos para que les permita superar ese límite de los 180 kilómetros.

Modelos no estandarizados de difusión de tecnologías

Los modos y maneras en que la tecnología se difunde, son, en realidad, muy diferentes de lo que la mayoría de las veces se presume. El tráfico de tecnologías puede tener lugar de formas tan diversas, que se hace preciso hablar de modelos no estandarizados para comprender, simplemente, las dinámicas de los flujos internacionales de la tecnología militar. Estos modelos no explican toda la complejidad del proceso, pero son útiles como indicadores de los métodos que están funcionando en la actualidad y permiten centrar la atención sobre ellos para así poder actuar disminuyendo el factor sorpresa y facilitando el poder tomar algunas medidas compensatorias.

Al hablar de modelos no estandarizados de difusión de tecnologías, nos referimos a los flujos que cruzan las fronteras sin ajustarse a los patrones de transferencia de armas, componentes y pericia para desarrollarlas. Por ejemplo, un modelo no estandarizado de difusión es el utilizado para

demostrar que, según la reciente experiencia, la utilización de las tecnologías extranjeras no constituye un aumento marginal de lo existente, sino que es el hecho central de su desarrollo. Es decir, estamos asistiendo a la utilización del comercio internacional como una tecnología base y no como una fuente supletoria para conseguir objetivos concretos. Por consiguiente, los países no necesitan desarrollar sus propias investigaciones e instalaciones industriales para conseguir producción e innovación; tan sólo necesitan acudir al mercado internacional.

Éste es un hecho que se viene produciendo en los últimos años, con tendencia creciente, pero que nunca se había producido a lo largo de la historia. Se consume y se va directamente al mercado internacional para restituir lo gastado. La consecuencia es que se produce un cambio cualitativo en el potencial militar a nivel nacional, al mismo tiempo que la velocidad de la modernización también cambia, acelerando la transformación.

Veamos unos ejemplos, Estados Unidos y la Unión Soviética han competido, directa y duramente, durante muchos años y tanto una superpotencia como la otra lo hacían desarrollando su propia tecnología, altamente especializada y autónoma. Irak en el año 1975, era un país árabe militarmente tradicional, con un Ejército politizado, un líder autoritario y técnicamente atrasado. En el año 1985, este mismo país, era una potencia militar a escala regional, que había desplegado un sofisticado sistema electrónico de inteligencia y de contramedidas como parte de su sistema de control y mando. Finalmente, Irak consiguió un arsenal de misiles balísticos y capacidad química y bacteriológica. Lo consiguió utilizando tecnología militar de la Unión Soviética, de Alemania, de Francia, de Italia y de Japón, que le habían transferido para defender sus propios intereses estratégicos cuando se enfrentó a Irán.

Otro modelo no estandarizado de difusión de tecnologías consiste en la introducción de un agente adicional al proceso de difusión: las multinacionales. Está emergiendo a nivel mundial un sistema de adquisición de tecnologías que se caracteriza por la, cada vez mayor, utilización de las multinacionales como fuente de recursos tecnológicos. A esto hay que añadir que las industrias que fabrican, lo que podríamos denominar, tecnologías militares sensibles están floreciendo rápidamente en muchos de los países que despiertan más interés a los analistas de la seguridad. Brasil, Corea del Sur, Egipto, India, Irak, Israel, Singapur y Turquía están comenzado a ser objeto de gran actividad por parte de las multinacionales. También es sabido que algunas grandes empresas norteamericanas

quieren introducirse en el mercado chino, y al menos dos están ayudando a China, desde el año 1996, a corregir los problemas de sus sistemas de lanzamiento de misiles, sin permiso gubernativo de Estados Unidos para la exportación de tecnología.

Pero es que, además, las empresas transnacionales carecen de control democrático alguno y su instalación por todos estos países acelera el proceso de aprendizaje para la absorción de esta tecnología, ya que organizan la transferencia de conocimientos en una forma que asigna responsabilidad y autoridad para conseguir un máximo de efectividad.

El proceso de transferencias se produce principalmente de multinacionales a empresas y, en menor medida, a través de los Ministerios de Defensa, a los que se atribuye menos eficiencia y menos capacidad para absorber nuevas tecnologías.

La combinación del acelerado aprendizaje que facilitan las multinacionales como agentes de transferencias, sumado a que el mercado internacional opere como principal fuente de suministro, ha producido un significativo impacto que se ha traducido en cambios estructurales. Estos cambios podrían resumirse en cuatro:

1. La absorción de tecnología se produce mucho más rápidamente que utilizando los modelos estándares. Las multinacionales son más rápidas reaccionando, motivadas por la obtención de beneficios y, al estar interesadas en los dobles usos de las tecnologías, pueden conocer con mayor exactitud las ventajas y las limitaciones de las diferentes tecnologías.
2. En la mayoría de los casos, resulta más eficiente utilizar las multinacionales como agentes de transferencias descentralizados del proceso de difusión tecnológica, en comparación con los modelos estandarizados que confían en el aumento de la producción autóctona y/o en el sector público como agente de transferencias.
3. Esta gran especialización en la transferencia de tecnologías está convirtiendo el proceso en más racional, pero también en más opaco, especialmente para los servicios de inteligencia nacionales encargados de controlar a las burocracias tecnológicas y científicas del extranjero.
4. El incremento de la opacidad lleva a no poder delimitar claramente la tecnología que realmente se posee, en contraposición a la percepción de lo que pueden poseer. Las esperanzas de que los países en vías de desarrollo sean incapaces de absorber sistemas modernos y avanza-

dos puede resultar trasnochada, incrementando el peligro de que se produzca lo que podríamos denominar una sorpresa tecnológica (48) .

La utilización de las armas de destrucción masiva por los grupos terroristas

Para el conjunto de los países occidentales las actividades terroristas con armamento convencional no constituyen una seria amenaza para su seguridad nacional. Pero las armas de destrucción masiva y los misiles podrían alterar significativamente el contexto, ya que dotan a las organizaciones terroristas de un poder de destrucción que nunca antes habían esperado obtener con las armas convencionales, permitiéndoles convertirse en una seria amenaza para la población de un país. Sin embargo, hasta ahora no parece ser esa la opción elegida por los distintos grupos terroristas.

Por contra, sí estamos asistiendo a un fenómeno que denota una creciente inestabilidad: la legitimidad de algunos Estados está siendo puesta en duda, desde dentro, por grupos que piden la autodeterminación con diversos fundamentos, ya sean grupos religiosos, movimientos aislacionistas, movimientos insurgentes, grupos étnicos, grupos racistas, fundamentalistas, etc. Todos estos grupos a menudo se aprovechan de la inseguridad en que está inmersa la población, ofreciendo satisfacer esas necesidades de seguridad que detectan y que a veces también ocasionan, ya sean necesidades psicológicas, sociológicas, políticas o religiosas.

Los grupos de orientación religiosa parecen reproducir un argumento ideológico común: rechazar las existentes estructuras sociales, económicas y políticas y demandar una revisión estructural del mundo. Este terrorismo, que algunos analistas denominan posmoderno (49), es el que amenaza con utilizar las armas de destrucción masiva. Aunque no se descarta que grupos terroristas tradicionales o aquellos otros que están financiados por algunos Estados no puedan suponer una amenaza de este tipo, dicha amenaza no resulta tan grave ni tan preocupante como la de los grupos que claman estar directamente conducidos por Dios. Un ejemplo claro lo constituye la secta terrorista japonesa *Aum Shinrikyo*, cuyos inte-

(48) BRACKEN, P.: «Non-Standard Models of the Diffusion of Military Technologies», en *Defense Analysis*, volumen 14, número 2. 1998.

(49) CAMPBELL, J. K.: «Excerpts from research Study Weapons of Mass Destruction and Terrorism: Proliferation by Non-State Actors», en *Terrorism and Political Violence*, volumen. 9, número 2. Verano, 1997.

grantes, el día 20 de marzo de 1995, liberaron un agente nervioso en «el metro» de Tokio, causando 12 muertos y más de 5.000 afectados.

Como respuesta a la creciente preocupación que generan las sectas religiosas, Alemania, Francia y Suiza han establecido unos cuerpos especiales de vigilancia para controlar las actividades de este tipo de organizaciones en sus respectivos países. Por otro lado, el Parlamento Europeo —aunque en una resolución no vinculante— propuso que la Oficina Europea de Policía (EUROPOL) y la Comisión Internacional de Policía Criminal (INTERPOL) trabajaran conjuntamente para controlar este tipo de terrorismo.

El terrorismo que podríamos denominar moderno, en contraposición al anteriormente descrito, se sostiene en una ideología basada en un propósito instrumental: es el instrumento del débil empleado contra el fuerte; la diplomacia coercitiva de los pobres. Estos terroristas no utilizan armas de destrucción masiva por varios factores, entre los que destacan su complejidad técnica, la reacción gubernamental y la reacción de la opinión pública (50). Cuando un atentado terrorista excede los límites de una violencia aceptable, la organización terrorista pierde apoyo popular y legitimidad. También puede provocar que el gobierno realice un esfuerzo extraordinario para eliminar al grupo terrorista. Este efecto también es aplicable a los Estados que apoyan a los grupos terroristas. Si les facilitan la utilización de armas de destrucción masiva, indudablemente tendrán que afrontar la respuesta de los países afectados. Además la continuada utilidad de las tácticas convencionales, que les reporta aparecer en los medios de comunicación y el apoyo de determinado público, disuade a los terroristas de aventurarse a correr riesgos innecesarios.

Por último, el terrorismo internacional presenta una paradoja: desde el punto de vista político se percibe como un asunto global, pero sus efectos físicos son limitados y sus efectos psicológicos desaparecen rápidamente de la opinión pública internacional. El terrorismo internacional utilizado indirectamente para provocar una confrontación entre gobiernos es políticamente más preocupante, porque destruye los parámetros aceptados internacionalmente al realizar ataques indiscriminados sobre población civil inocente. No obstante, puede ser reconducido más efectivamente porque las infraestructuras o células que desarrollan su actividad dentro del territorio de un Estado pueden ser descubiertas y destruidas.

(50) FOXELL, J. W.: «The Debate on the Potential for Mass-Casualty Terrorism: The Challenge to US Security», en *Terrorism and Political Violence*, volumen 11, número 1. Primavera, 1999.

El terrorismo internacional resulta mucho más problemático cuando se dedica a apoyar al terrorismo nacional o cuando sirve de apoyo a una amplia confrontación política, ideológica o religiosa, porque sus redes son mucho más difíciles de identificar y combatir. El terrorismo internacional se encuentra en un punto de desarrollo potencial con unas, relativamente, nuevas características: se está globalizando y está adquiriendo armas de destrucción masiva.

La experiencia demuestra que no ha habido un solo acto de terrorismo nuclear a pesar de que miles de armas nucleares han sido fabricadas, transportadas, desplegadas y desmanteladas sobre todo el planeta y a pesar de que ya han pasado muchos años desde la desmembración de la Unión Soviética, que provocó pánico al suponer que el material nuclear desaparecería e iría a parar a manos terroristas. La complejidad técnica, los mecanismos de autodestrucción, las dificultades para conseguir la detonación, unido al tamaño y a las dificultades que implica su transporte, hace que sean simplemente poco adecuadas para la acción terrorista clandestina, aunque su futura utilización no haya sido totalmente descartada por la comunidad internacional. Más fácil es, sin duda, utilizar armas químicas, que requieren un nivel menor de tecnología y que pueden ser producidas con mucha más facilidad. Y más fácil aún de producir son las biológicas, cuyas instalaciones resultan prácticamente indetectables.

Políticas de control en los foros internacionales

La comunidad internacional está adoptando una actitud cada vez más reguladora hacia las exportaciones de tecnología y materiales militares. A lo largo del año 1996 se produjeron cambios importantes en los foros internacionales dedicados al control de la exportación. Ejemplo de estos cambios son el que Corea del Sur se incorporase como trigésimo miembro al Grupo de Australia, y que Brasil, Ucrania y también Corea del Sur iniciasen su andadura en el Grupo de Suministradores Nucleares (más conocido por sus siglas en inglés NSG).

También en el año 1996 se estableció formalmente el Acuerdo Wassenaar sobre controles a la exportación, con 33 Estados miembros fundadores entre los que se encontraban Argentina, Bulgaria, Corea del Sur, Rumania y Ucrania. Brasil, que había sido aceptado como miembro del MTCR en el año 1995, participó en el plenario correspondiente a 1996, donde se reunieron los 28 Estados que se habían adherido a este acuerdo. A partir de 1996 todos estos foros se han ido consolidando.

Cuadro 3.- Países adheridos a MTCR, Wassenaar y NGS.

País	MTCR	WASSENAAR	NGS
Alemania	•	•	•
África del Sur	•		•
Argentina	•	•	•
Australia	•	•	•
Austria	•	•	•
Bélgica	•	•	•
Brasil	•		•
Bulgaria		•	•
Canadá	•	•	•
Corea del Sur		•	•
Dinamarca	•	•	•
Eslovaquia		•	•
España	•	•	•
Estados Unidos	•	•	•
Finlandia	•	•	•
Francia	•	•	•
Grecia	•	•	•
Holanda	•	•	•
Hungría	•	•	•
Irlanda	•	•	•
Islandia	•		
Italia	•	•	•
Japón	•		•
Letonia		•	•
Luxemburgo	•	•	•
Noruega	•	•	•
Nueva Zelanda		•	•
Polonia	•	•	•
Portugal	•	•	•
Reino Unido		•	•
República Checa	•	•	•
Rumania		•	•
Rusia	•	•	•
Suecia	•	•	•
Suiza	•	•	•
Turquía	•	•	
Ucrania	•	•	•
<i>Total</i>	<i>32</i>	<i>33</i>	<i>35</i>

Antes de pasar a analizar con más detalle los tres acuerdos relacionados con el tema que nos ocupa, que son el MTCR, el Acuerdo Wassenaar y el NSG, se inserta a continuación en el cuadro 3, (51) donde se puede apreciar qué países están adheridos a estos regímenes.

(51) Cuadro elaborado con datos recogidos en *The Arms Control Reporter*. 1999.

Régimen de Control de la Tecnología de Misiles

En el año 1983, los Gobiernos de Canadá, Estados Unidos, Francia, Italia, Japón, Reino Unido y República Federal de Alemania comenzaron a negociar con el fin de llegar a un acuerdo que limitara las exportaciones de la tecnología utilizada para producir misiles balísticos y misiles de crucero. Las conversaciones culminaron en abril de 1987 con la firma del MTCR. En este acuerdo se establecían unas líneas básicas para controlar la exportación y unos anexos que recogían el listado de las tecnologías y equipamientos, relacionados con los misiles, que necesitarían licencia de exportación expedidas por los países miembros. En un principio, el objetivo era controlar únicamente las transferencias de equipamientos y tecnologías que sirvieran para construir sistemas de misiles con capacidad para lanzar cabezas nucleares. En el mes de julio de 1993, se hizo una enmienda para dar cobertura a los misiles que pudieran lanzar, además de cabezas nucleares, cargas químicas y biológicas, es decir, cualquier tipo de carga de destrucción masiva. En el año 1996, el plenario del MTCR centró su atención en los aspectos regionales de la proliferación de misiles. En 1998, el objeto de análisis fueron las innovaciones relacionadas con la tecnología de los misiles que se estaban desarrollando en países de Asia y de Oriente Medio.

El MTCR es un acuerdo voluntario para aquellos países que están interesados en restringir la proliferación y el tráfico de misiles y sus tecnologías a través del intercambio de información y de la coordinación de las distintas políticas nacionales. Las decisiones se toman por consenso en las reuniones plenarias que se celebran anualmente, y no existe un órgano con autoridad para ejecutar esas decisiones, por lo que son los Estados miembros los que facilitan la consecución de los objetivos a través de leyes y regulaciones de carácter interno.

Uno de los principales asuntos sobre los que se ha debatido en las sesiones plenarias del MTCR, ha sido sobre la inclusión de nuevos miembros. También se ha discutido en numerosas ocasiones sobre la relación que debe establecerse entre los Estados miembros del MTCR y el resto de los países que están al margen de este régimen, ya que no existe un tratado multilateral para controlar la posesión, producción y comercio de misiles, y además hay que hacer frente a distintas variables: no es lo mismo la relación que ha de establecerse con países que tienen una significativa producción de misiles y no son miembros del MTCR, como es el caso de China y Corea del Norte, que la relación a mantener con aquellos países

que están desarrollando o comprando misiles balísticos, casos que se dan en el sur de Asia y en el golfo Pérsico. Por otro lado, incluso los países que proclaman una gran transparencia en asunto de armamentos, tienen grandes reservas a la hora de revelar sus *stocks* de misiles.

En la actualidad, 32 países forman parte del MTCR, un régimen que ha contribuido a parar la proliferación de los misiles, al hacer más complicado y más costoso adquirir la tecnología que se necesita para desarrollarlos. Empero, para que resulte más efectivo, debería progresar en dos direcciones:

1. Deberían adherirse al MTCR todos los países productores de misiles.
2. Todas las restricciones que recoge deberían tener fuerza legal internacional, para poder realizar inspecciones sobre el cumplimiento real de sus disposiciones.

Acuerdo Wassenaar sobre controles a la exportación

En julio de 1996, en la ciudad de Viena, se firmó el Acuerdo Wassenaar con el objetivo de evitar la desestabilización que supone la acumulación de armamento convencional y de las tecnologías específicas que pueden ser objeto de doble uso. En el marco de este Acuerdo, los Estados firmantes intercambian información y valoran la mejor forma de conseguir una línea política común o, al menos, más próxima y no tan dispar. Empero, el Acuerdo no establece un órgano con capacidad y autoridad para tomar decisiones y son los Estados los que las toman independientemente y los que las ejecutan adecuándolas a sus procedimientos nacionales internos.

No se elaboraron ni lista de municiones, ni lista de tecnologías de doble uso como parte de los denominados elementos iniciales del Acuerdo Wassenaar, aunque los gobiernos, a título individual, pueden elaborar su propia lista unilateralmente. Estos Estados se comprometen a mantener controles nacionales sobre las transferencias de los *ítems* recogidos en una lista elaborada por expertos procedentes de los países. Asimismo, se comprometen a comunicar a los restantes países miembros del Acuerdo las transferencias que realizan a los Estados no firmantes, así como los casos individuales en que se deniegan las licencias para transferir. Al menos en una primera etapa, los Estados miembros no se han comprometido a rehusar licencias para transferir el mismo producto al mismo destino donde otro miembro haya negado la licencia.

Aunque las medidas no están dirigidas contra un Estado o grupo de Estados determinado, en el marco del Acuerdo ciertos destinatarios de transferencias de tecnologías y armamento son actualmente considerados objeto de seria preocupación como, por ejemplo, Irán. La República Checa, Hungría, Polonia y Rusia han dado garantías a Estados Unidos —con carácter bilateral y, por tanto, al margen de Wassenaar— de que no transferirán ningún tipo de armamento o tecnología a Irán, aunque tampoco se han mostrado dispuestos a rescindir los contratos que tienen vigentes para reponer partes esenciales de los equipos ya transferidos con anterioridad.

Por último, hay que señalar que el Acuerdo estará abierto en principio a todos aquellos países que cumplan determinados requisitos, como que se adhieran al NPT (*Non-Proliferation Treaty*), al BTWC (*Biological and Toxin Weapons Convention*), y al CWC (*Chemical Weapons Convention*), y que mantengan una aplicación efectiva de los controles nacionales a la exportación. Además de participar en el plenario y en reuniones de otro carácter, seis países (Alemania, Estados Unidos, Francia, Italia Reino Unido y Rusia) han decidido reunirse para realizar consultas y compartir información más comprometida.

En relación con los misiles, en el plenario que reunió a los 33 miembros los días 2 y 3 de diciembre de 1998, se decidió reforzar el control a la exportación de los sistemas de defensa aéreos que pueden ser portados sobre los hombros. Por su tamaño, este tipo de misiles tierra-aire, no quedan incluidos en la categoría de misiles que cubren otros tratados. Asimismo, los miembros se reafirmaron en mantener las decisiones que habían tomado en reuniones anteriores y que consistían en no exportar armas a Afganistán y en ejercer al máximo las restricciones sobre las transferencias a las regiones de África que están en conflicto.

Grupo de Suministradores Nucleares (NSG)

Este foro tiene como objetivo coordinar las políticas de control a la exportación a fin de evitar que los Estados que no poseen armamento nuclear puedan adquirirlo. En el plenario de 1996 los Estados miembros se comprometieron a promover la apertura y la transparencia potenciando el diálogo y la cooperación con los países que no fueran miembros y se creó un grupo especial de trabajo para realizar esta misión. Uno de los logros más importantes del NSG ha sido el conseguir que se exija un acuerdo entre la Agencia Internacional de la Energía Atómica y el Estado receptor,

antes de que se produzca la transferencia de los materiales, equipos y tecnologías. Este acuerdo de establecer como requisito la aplicación de todas las salvaguardas sobre materiales fisibles, su estado y las actividades a las que se destina. Asimismo, el NSG requiere al Estado receptor que establezca un sistema de protección que impida que se utilicen los materiales y las instalaciones transferidos para usos no autorizados. Los miembros del NSG intercambian información sobre programas nucleares que resulten significativos desde el punto de vista de la proliferación y se realizan consultas antes de que se hagan efectivas las transferencias, para evitar el riesgo de que determinado componente contribuya a incrementar el riesgo de la proliferación del armamento nuclear. Especial atención se ha prestado a las exportaciones de material nuclear de doble uso realizadas por Bielorrusia, China Kazajstán y Lituania.

China es el principal suministrador de equipamiento nuclear de doble uso que está fuera del NSG, aunque el 11 de mayo de 1996 anunció que no daría más asistencia a las instalaciones nucleares de aquellos países que no estuvieran sujetos al sistema de salvaguardas de la Agencia Internacional de la Energía Atómica, tras llegar a un acuerdo con Estados Unidos, ya que una de las máximas preocupaciones del entonces secretario de Estado, Warren Christopher, era evitar la cooperación nuclear y militar entre China e Irán (52).

El diálogo y la cooperación entre Estados Unidos y Rusia

Ya son varios años los que lleva funcionando una intensa actividad diplomática al más alto nivel sobre el asunto de la exportación de tecnología de misiles. En septiembre de 1998, Clinton y Yeltsin se comprometieron a crear siete grupos de trabajo para controlar la exportación de tecnologías y equipamientos. Prácticamente, entre mediados de 1997 y mediados de 1998, Rusia ha contenido materialmente el tráfico ilícito con Irán (53), vigilando a las instituciones sospechosas de realizarlo. Pero en el último semestre de 1998 cesó tal efectividad, coincidiendo con la prueba del misil *Shehab* realizada por Irán.

En un informe realizado ese mismo año por especialistas rusos, se concluía que los intentos rusos de establecer un control estricto habían sido

(52) CHRISTOPHER, W.: *American Interest and the US-China relationship*, US Department of State. 27 de mayo 1996.

(53) MANN, P.: «Export Curbs Not Enough», en *Aviation Week & Space Technology*. Enero, 1999.

neutralizados por los enfrentamientos surgidos entre facciones gubernamentales y empresariales, y que las disposiciones del Gobierno para controlar la exportación cambiaban constantemente, produciendo confusión e incrementando los riesgos, en un momento en que el crimen organizado y el contrabando están muy extendidos. La solución pasaría por establecer controles más rigurosos, pero la Duma todavía no ha codificado cuales podrían ser esos controles.

El fenómeno de la proliferación de misiles se considera bastante menos preocupante en Moscú que en Washington. Moscú nunca ha considerado que la proliferación constituyera una amenaza seria para su seguridad, entre otras causas porque Rusia no tiene bases militares ni tropas desplegadas más allá de sus fronteras, que se puedan considerar vulnerables a un ataque con misiles. De hecho, el misil soviético *Scud* es la base a partir del cual la mayoría de los países subdesarrollados interesados en poseer misiles han comenzado a desarrollar sus propios programas. Gorbachov, en un intento de ser considerado un civilizado líder a escala mundial y poder aprovechar la ayuda económica y la cooperación que pudiera brindarle Occidente, se vio obligado a tomar en cuenta el fenómeno de la proliferación. Así que, al menos retóricamente, admitió que era necesaria la cooperación entre ambas superpotencias para frenar la proliferación.

Estados Unidos, por el contrario, siempre se ha mostrado tremendamente preocupado por la proliferación y especialmente desde el desmembramiento de la Unión Soviética, y por ello ha liderado todas las medidas de no-proliferación y ha invertido cuantiosas sumas en desarrollar medidas de contraproliferación tales como los sistemas defensivos antimisiles. Empero, los programas de misiles tanto de India como de Pakistán comenzaron a desarrollarse a partir de la transferencia de tecnología norteamericana que recibieron en los años sesenta para poder realizar lanzamientos espaciales desde sus respectivos territorios. Entre los años 1963 y 1975 se realizaron más de 350 lanzamientos espaciales desde suelo indio con propulsores de Estados Unidos, Francia y Reino Unido, mientras que Alemania instruía a los científicos indios sobre la construcción de los sistemas de guiado.

Volviendo al escenario actual, nos encontramos con que ningún dirigente político ruso considera seriamente que Irán se esté convirtiendo en una amenaza en este terreno y no quieren perder el mercado que la industria militar rusa mantiene con este país. Estados Unidos intenta convencer a Rusia de que el interés económico actúa en contra de su seguridad por-

que los misiles iraníes alcanzarán el territorio ruso, además del territorio de Europa Occidental. A las acusaciones de que Irán no es un país democrático, Rusia responde que aliados de Estados Unidos como Egipto y Arabia Saudí tampoco lo son. Estados Unidos ha penalizado a varias entidades rusas, ordenando una prohibición de importación-exportación, por prestar asistencia técnica y tecnología de misiles a Irán y ha lamentado pública y oficialmente que instituciones científicas y tecnológicas de Rusia, a quien sólo mueven intereses económicos, estén facilitando que Irán posea lo que se puede considerar una letal combinación de componentes de misiles y capacidad nuclear, creando la única amenaza de desestabilización en la región.

Estados Unidos defiende que tiene autoridad legal para actuar unilateralmente contra las violaciones de los regímenes internacionales de control, pero mantiene que sería más efectivo un sistema ruso de control a la exportación, porque sólo Rusia puede vigilar sus propias fronteras, sus propias fábricas y sus institutos de investigación. Rusia ha respondido a tales sanciones mostrando una gran frustración y enfado y advirtiendo de que esas medidas de fuerza no favorecen la relación entre ambas superpotencias, más aún cuando manifiestan que tales acusaciones son totalmente infundadas.

El surgimiento del comercio de armas entre China y Rusia también ha causado preocupación en Occidente. En el año 1995, Estados Unidos criticó a Rusia por la venta de misiles balísticos intercontinentales SS-18 a China y, en 1997, el secretario de Defensa norteamericano, William Cohen, denunció que China había adquirido buques equipados con misiles SS-N-22. Existe especial preocupación porque como consecuencia de las buenas relaciones chino-rusas se cree que un gran número de científicos, ingenieros y técnicos rusos están trabajando en China con la consiguiente transferencia de tecnología que va a facilitar el que este país cuente con misiles balísticos de largo alcance, misiles de crucero y submarinos nucleares. Dentro de Rusia también existe preocupación, pero por otros motivos: tales exportaciones benefician momentáneamente a la industria de defensa rusa, pero a la vuelta de unos años China producirá y comercializará ese mismo armamento, compitiendo con Rusia en el mercado. Sin olvidar que, desde una perspectiva estratégica, los intereses nacionales quedan afectados porque todavía China está considerada como una amenaza potencial para Rusia (54).

(54) HUXLEY, T. y WILLETT, S.: «International Defence Suppliers and the East Asian Market», en *Adelphi Paper*, número 329, capítulo 2. 1999.

Para prevenir el tráfico, la proliferación y el uso de los misiles balísticos, de los misiles de crucero y de las cargas NBQ, el diálogo y la cooperación entre Estados Unidos y Rusia deben y necesitan ser más intensos y más amplios. Rusia ha propuesto que el intercambio de datos sobre las actividades de los países del Tercer Mundo para desarrollar armas de destrucción masiva se realice en el marco del ICEMAW (*International Center for Early Missile Attack Warning*). Ambos países podrían trabajar conjuntamente, coordinando métodos de vigilancia situados en el espacio y creando un sistema conjunto de satélites espías para controlar y verificar la proliferación, sobre todo de misiles, cuyas instalaciones son más fáciles de detectar, ya que los agentes biológicos y químicos son fácilmente producidos en instalaciones con apariencia de utilidad civil y no militar.

Opciones para afrontar el tráfico de misiles en el umbral del siglo XXI

Echando la vista hacia atrás en el momento de escribir estas páginas, nos encontramos con un panorama no demasiado halagüeño: en los últimos 18 meses se han realizado pruebas de siete nuevos misiles. China ha realizado pruebas del *Dong Feng-31*; Corea del Norte ha probado el *Taepo Dong-1*; India, el *Agni-2*; Irán, el *Shehab-3*; y, finalmente, Pakistán ha realizado pruebas de los misiles *Ghauri-1*, *Ghauri-2* y *Shaheen*. Todos estos países, además, están embarcados en programas de desarrollo de nuevas tecnologías para conseguir misiles aún mejores y con mayor alcance.

Este auge del desarrollo de nuevos misiles es motivo de grave preocupación porque a pesar del fortalecimiento de los regímenes internacionales de no-proliferación, los retos fundamentales que plantea la proliferación no han desaparecido y ésta sigue constituyendo una amenaza militar directa. Detectar e impedir el tráfico ilegal de los materiales y la contratación de expertos para fabricar este tipo de armamento continúa siendo una tarea ardua y difícilmente se conseguiran establecer unos mecanismos adecuados.

Las opciones con que contamos en un futuro inmediato para dar respuesta a esta amenaza y disminuir los riesgos inherentes a la realidad, que en las páginas anteriores hemos tratado de dibujar, siguen siendo las dos que este mismo grupo de trabajo ha analizado en detalle con ante-

rioridad: potenciar las medidas de no-proliferación y seguir desarrollando medidas de contraproliferación (55) .

No obstante, en los próximos años seguiremos asistiendo a un incremento de la expansión de los misiles por el mundo porque:

- Las sanciones y los controles a la exportación y al tráfico de misiles han ralentizado pero no han llegado a parar totalmente los programas de desarrollo de estas armas de destrucción masiva.
- Los misiles balísticos siempre han sido instrumentos de la política geoestratégica, pero pueden convertirse en un potente instrumento geopolítico si se utilizan para amenazar indiscriminadamente a cualquier población.
- Los misiles balísticos una vez lanzados no pueden volver atrás y son muy difíciles de interceptar, por lo que utilizados para realizar un ataque nuclear resultan mucho más peligrosos que los misiles de crucero o que los bombarderos. Un país con capacidad nuclear pero que no posea misiles siempre será considerado menos amenazante que otro que los posea.
- A la inversa, debemos sospechar que el país que importa o produce misiles está planeando adquirir armamento NBQ.
- Si los países que conforman las regiones más inestables siguen beneficiándose del tráfico de misiles, aunque éstos pueden utilizarse con armamento convencional la propia tensión creada por la inestabilidad presionará a favor de que adquieran, aunque sea ilegalmente, armamento NBQ y más concretamente armas nucleares.
- Aunque la mayoría de los misiles adquiridos por países en vías de desarrollo son relativamente inseguros a la hora de alcanzar un objetivo específico, militarmente siempre serán muy efectivos ante la duda de que vayan equipados con armamento NBQ, lo cual les confiere una capacidad destructiva que palía la falta de puntería.

Para concluir, hay que señalar que esta evolución de la proliferación no ha originado en sí ningún cambio doctrinal por parte occidental ya que la única variación con respecto a escenarios anteriores se limita a que ha aumentado el riesgo derivado de la dispersión. Se trata, al igual que antes, de disuadir al adversario mediante la amenaza de daños inaceptables y la disuasión, para conservar su eficacia, debe poder seguir siendo creíble en todos los casos.

(55) Véase «Un estudio sobre el futuro de la no-proliferación», *Monografías del CESEDEN*, número 30. Centro Superior de Estudios de la Defensa Nacional, Ministerio de Defensa. Marzo, 1999.

Por otro lado, la primera línea de defensa es la prevención y ya se advierten algunos signos que deberían hacer que nos adelantáramos a las consecuencias que traerá la presión que se está ejerciendo sobre todo lo relacionado con los misiles balísticos, porque es muy probable que en el futuro aumente la proliferación y el tráfico de los misiles de crucero, que además se verá favorecido porque son menos costosos y técnicamente menos complejos, aunque resulten menos destructivos y tengan menor peso estratégico y psicológico. En la actualidad, más de 90 Estados poseen unos 130 tipos distintos de misiles de crucero, la mayor parte de los cuales no alcanza los 300 kilómetros, si bien algunos superan los 2.000 kilómetros.

CAPÍTULO SEGUNDO

MOVIMIENTOS MIGRATORIOS Y SEGURIDAD INTERNACIONAL

MOVIMIENTOS MIGRATORIOS Y SEGURIDAD INTERNACIONAL

Por JESÚS A. NUÑEZ VILLAVERDE

Introducción

Con el final de la guerra fría se ha producido un replanteamiento general de las teorías que tratan de explicar las relaciones internacionales y una modificación sustancial de los modelos que habían definido, durante las décadas anteriores, las cuestiones de seguridad y defensa. Incluso fenómenos que ya se habían detectado con anterioridad aparecen, a partir de entonces, bajo un nuevo prisma que enfatiza la necesidad de una aproximación holística a los problemas, como vía más adecuada para tratar procesos multidimensionales, en los que se adivinan complejas y no siempre bien conocidas interrelaciones entre variables que hasta ese momento habían sido estudiados de manera independiente.

El concepto de la seguridad nacional e internacional no escapa a esta tendencia que apuesta por la globalidad y la interdisciplinariedad. A los tradicionales enfoques, estrictamente centrados en el análisis del poder militar de los Estados o de las alianzas militares y de los equilibrios-desequilibrios que de ahí se derivaban, se añade paulatinamente un conjunto de elementos de carácter social, económico y político que deben ser tenidos en cuenta como partes esenciales del planeamiento de la seguridad. La ecuación de la seguridad se hace cada vez más problemática y exige la participación de especialistas que, anteriormente, parecían muy alejados de este ámbito. Al mismo tiempo, se constata que para la defensa de los propios intereses no basta con atender a lo que sucede en las fronte-

ras inmediatas sino que es preciso mirar más allá, atendiendo a la multiplicidad de riesgos que configuran la agenda actual de la seguridad. Así lo certificaba en enero del año 1992 el Consejo de Seguridad de Naciones Unidas, cuando afirmaba que:

«Las causas no militares de inestabilidad en los ámbitos económico, social, humanitario y ecológico se han convertido en amenazas para la paz y la seguridad.»

Desde esa perspectiva, el análisis de los movimientos masivos de población se integra plenamente en la nueva concepción de la seguridad; entendido como un fenómeno que es, simultáneamente, síntoma y vector de inestabilidad y conflicto. Es ésta la óptica bajo la que cabe contemplar tanto las migraciones por motivos fundamentalmente económicos, que parcialmente podrían considerarse voluntarias, como los flujos de refugiados y desplazados, bajo la presión de diferentes circunstancias. Ninguna de las dos modalidades es novedosa en la historia de la humanidad, pero es un hecho que ambas presentan perfiles más acusados y preocupantes cuando se analiza lo ocurrido desde la caída del muro de Berlín y, sobre todo, cuando se trata de establecer cómo será el escenario de la seguridad en la próxima década.

La inclusión de este tema en la agenda de la seguridad viene dada por la constatación de que estos flujos, aunque responden a motivaciones muy diversas, presentan como rasgo común un considerable potencial desestabilizador a escala nacional, regional e incluso, internacional. En el mejor de los casos, son la expresión de desajustes sociales, económicos y políticos que afectan al nivel de bienestar de un porcentaje considerable de la población, lo que provoca su pretensión de encontrar mejores condiciones de vida en otras latitudes. En su manifestación más aguda, expresa el fracaso de la convivencia entre diferentes grupos sociales dentro de un territorio determinado y, normalmente, la escalada de las diferencias hasta el nivel del conflicto armado.

Si se asume que la mejor manera de garantizar la estabilidad es prevenir la ocurrencia de conflictos en sus primeras etapas, se entenderá la conveniencia de estudiar las causas de estos flujos, así como su evolución y las posibles vías de solución para desactivar sus mecanismos de desarrollo y reducir la posibilidad de un estallido que obligue a adoptar otras medidas. Éste será el enfoque adoptado en estas páginas, analizando el problema desde la perspectiva de la Unión Europea, entendida como un conjunto de países que aparecen dotados de un atractivo innegable para

los ciudadanos de los países de sus periferias más inmediatas (Mediterráneo Sur, Europa Central y Oriental), dado el diferencial de desarrollo económico, social y político existente entre ellos.

Caracterización de los movimientos migratorios

El macabro recuento de fallecidos, mayoritariamente norteafricanos, en un intento por alcanzar a bordo de frágiles embarcaciones algún punto de las costas mediterráneas españolas forma ya parte del actual panorama informativo. Sin embargo, la magnitud del fenómeno es mucho mayor que lo que pueda derivarse de esa imparable sucesión de noticias puntuales, que apenas dejan rastro detrás de sí en la opinión pública.

No hay todavía una teoría global que explique el fenómeno de los movimientos migratorios. Se trata de un proceso multidimensional que ocupa entre otros a antropólogos, demógrafos, economistas, educadores, geógrafos, historiadores, juristas, sociólogos y, por supuesto, responsables políticos. En cualquier caso, existe un amplio consenso en cuanto a las causas que provocan estos flujos, al sostenerse que las razones económicas son las que actúan, en última instancia, como espoleta para disparar el proceso. Esto es precisamente lo que se enfatiza en la definición de las personas que se engloban en este concepto, como aquellas que se desplazan —de un país a otro, o dentro de un mismo país— con la idea de instalarse en otro lugar durante un cierto periodo y con el objetivo de trabajar o de buscar un empleo.

Se deduce, de esta definición, la existencia de dos tipos de movimientos que se distinguen por el marco geográfico en el que se desarrollan: los movimientos migratorios nacionales y los movimientos migratorios internacionales.

Los movimientos migratorios nacionales

En el primer caso, y a grandes rasgos, los movimientos migratorios nacionales están provocando un simultáneo vaciamiento de los núcleos rurales y una preocupante aglomeración urbana en las principales ciudades de la práctica totalidad de unos países que están, todavía, inmersos en una fase de alto crecimiento demográfico. El éxodo rural es la muestra de que las perspectivas de futuro para esta parte de la población son muy negativas, como efecto combinado de la caída estructural de los precios agrícolas, la pérdida de su poder adquisitivo, el avance de la desertización y

la marginación que sufren frente a otras prioridades gubernamentales. Si se tiene en cuenta, sobre todo en la periferia Sur, que el grueso de la población activa sigue integrada en el sector primario y que la producción agrícola sigue representando una porción importante en el Producto Interior Bruto (PIB) nacional, es inmediato concluir que este abandono supone, por sí mismo, un factor que en poco favorece a la estabilidad interna. Por otra parte, la gran mayoría de la población que deserta del campo se dirige, al menos en una primera etapa, a las ciudades que, en términos relativos, ofrecen aparentemente mayores posibilidades de bienestar y desarrollo. De esta forma, se produce un creciente hacinamiento de personas en los suburbios de unas urbes débilmente dotadas para garantizar los servicios elementales y para cubrir las necesidades básicas de quienes las habitan (educación, sanidad, vivienda, empleo, acceso a agua potable y saneamiento). Todavía podría añadirse que la aplicación de planes de ajuste estructural, como consecuencia directa de los problemas para hacer frente a la deuda externa, y la ineficacia y corrupción que caracterizan la gestión de muchos de estos gobiernos hacen aún más problemático el panorama.

En definitiva, ambos hechos tienen una significativa carga desestabilizadora, en el contexto de países escasamente estructurados que se enfrentan en desventaja a un escenario sometido a las reglas de la globalización y que no muestran una decidida voluntad política para emprender reformas estructurales en todos los ámbitos, incluyendo el político, que favorezcan al conjunto de la población. En ese contexto no es de extrañar que proliferen tanto las actividades informales y delictivas como las revueltas sociales que muestran, cada vez con mayor claridad, la gravedad de una situación que apunta hacia el estallido generalizado.

Los movimientos migratorios internacionales

Por lo que respecta a los movimientos migratorios internacionales, la preocupación actual no deriva en modo alguno de su novedad (cabe recordar que, tras la Segunda Guerra Mundial, fueron los países de la Europa Occidental quienes abrieron y fomentaron la llegada de trabajadores extranjeros para cubrir las necesidades que planteaba la reconstrucción). Lo que resulta nuevo, y al mismo tiempo inquietante, es la coincidencia de tendencias opuestas entre la Unión Europea y sus vecinos. Estos últimos se enfrentan al reconocimiento del fracaso cosechado por sus responsables políticos, en su objetivo de lograr unos niveles de desarrollo y bienestar equiparables a los de la Unión Europea, y a un crecimiento

demográfico que sigue estando por encima de las posibilidades de absorción de sus sistemas educativos y productivos. Por su parte, los Quince vuelcan sus esfuerzos en profundizar su propia integración, en un contexto de débil crecimiento demográfico, crisis económica y niveles de desempleo estructural difíciles de reducir a corto plazo. A esto cabe añadir un excesivo empeño en imponer sucesivos filtros que impidan la entrada en su territorio, y una falta de sensibilidad y de decisión política para actuar en el exterior con una voluntad firme, a favor de los más desfavorecidos y con el objetivo de reducir las desigualdades.

Son precisamente estas desigualdades, en continuo aumento, entre los Quince y sus vecinos del Sur y del Este, junto con la proximidad geográfica, los factores que explican en mayor medida la presión migratoria que se registra en las fronteras de la Unión Europea. Este fenómeno, que seguirá manifestándose con igual o mayor fuerza a medio plazo, está ya generando tensiones crecientes en las sociedades de acogida, con esporádicas pero imparable manifestaciones racistas y xenófobas que no auguran un futuro más estable. En esa línea, se impone una visión negativa de la inmigración, percibida como un factor desestabilizador y ante la que sólo cabe adoptar una actitud defensivo-represiva, articulando medidas legales y policiales que traten de impermeabilizar las fronteras comunitarias como forma de hacer frente a los supuestos riesgos que se derivan de su existencia.

Parece olvidarse que, junto a esa visión, cabe plantear otra que tenga en cuenta, entre otros, los siguientes aspectos:

— Según los datos ofrecidos por Oficina de Estadística Europea (EUROSTAT), en el año 1995 había un total de 15.921.700 extranjeros en los entonces 12 miembros de la Unión Europea (de los cuales 5.114.700 eran ciudadanos comunitarios que residían en otro país miembro), frente a algo más de 12 millones registrados en el año 1983. Esta cantidad estaba irregularmente repartida con más de siete millones en Alemania, casi tres y medio en Francia y dos en Reino Unido, mientras que España apenas llegaba al cuarto de millón.

En términos porcentuales, los extranjeros sólo representaban el 4,4% de la población comunitaria, aunque en el caso de Luxemburgo lleguen a suponer el 33,2% de su población (de ellos, el 90,5% ciudadanos comunitarios). En Alemania eran el 8,7% del censo (el 26,5% ciudadanos de la Unión Europea), en Francia el 6% (33,8% comunitarios), el Reino Unido el 3,4% (el 40,4% comunitarios) y en España un escaso 0,6% (41,2% comunitarios).

Las cifras relativas al mercado laboral de la Unión tampoco resultan especialmente alarmantes. El porcentaje de trabajadores extranjeros en el total de la población activa de la Unión Europea era, en 1995, del 4,7% (7.770.800 de los que 2.884.400 eran ciudadanos de algún país miembro empleado en otro país de la Unión Europea).

Aunque diversas fuentes estiman entre tres y cinco millones el número de ciudadanos no comunitarios en situación irregular que residen en la Unión Europea, la cantidad final resultante no debe llevar a conclusiones alarmistas sobre lo que, en determinados círculos sociales, se presenta como una «invasión» y una carga de profundidad contra las bases de la identidad comunitaria. Esto no quiere decir que no existan problemas puntuales en algunas localidades o comarcas de diferentes países de la Unión Europea, a los que es necesario hacer frente con los instrumentos propios de un Estado de Derecho, ni que la inmigración irregular no deba ser evitada, sino que se pretende únicamente destacar que la realidad de los datos no se corresponde con la imagen que parece instalarse fácilmente entre la opinión pública comunitaria.

- A la luz de esos mismos datos, tampoco se sostiene la idea de que los inmigrantes desplazan a los nacionales comunitarios del mercado de trabajo, compitiendo por las mismas labores a cambio de menores salarios. Afortunadamente, los Quince han logrado un nivel de desarrollo y bienestar generalizado, en el que subsisten bolsas de desigualdad evidentes (Cuarto Mundo), que tiene como consecuencia que determinadas labores hayan dejado de ser fuertemente demandadas por los trabajadores nacionales. Es precisamente en esas tareas (agricultura, construcción y algunos servicios), que exigen un bajo nivel de cualificación y que no se encuentran bien valoradas ni social ni económicamente, donde se concreta la oportunidad de integración de la inmensa mayoría de los inmigrantes que residen en la Unión Europea.

Por lo tanto estos trabajadores se encargan de realizar trabajos que no son demandados por los ciudadanos comunitarios, de la misma manera que, en décadas pasadas, ése era el papel de los emigrantes españoles, portugueses o griegos en los mercados laborales de los miembros fundadores de la Comunidad Económica Europea.

- La estructura demográfica de la Unión Europea plantea un incierto futuro para el sostenimiento de los sistemas de protección social, propios del Estado de bienestar del que se han ido dotando los Quince. Desde esta perspectiva, la aportación de los trabajadores extracomu-

nitarios puede resultar decisiva, a medio plazo, para mantener una relación adecuada entre contribuyentes y receptores al del sistema.

- En el marco de la asistencia que los países comunitarios prestan para el desarrollo de los países menos avanzados, no siempre se destaca suficientemente el efecto benéfico que la emigración tiene en múltiples sentidos. Por una parte, descarga al país emisor de la necesidad de emplear sus propios fondos para cubrir las necesidades de un considerable porcentaje de la población (vivienda, educación y sanidad). Además, contribuye a aliviar la presión sobre el mercado laboral de ese país, al tiempo que, a través de las remesas de emigrantes, transfiere divisas muchas veces vitales para permitir las relaciones comerciales con el resto del mundo.

Incluso cabe considerar al inmigrante como un importante factor de dinamización social, política y económica. En el país de acogida transmite una imagen que condiciona, para lo bueno y para lo malo, la actitud de los nacionales de ese país con respecto al de origen del inmigrante. En su sociedad de origen, con ocasión de su regreso o de sus visitas, actúa como transmisor de un «saber hacer» adquirido en contacto con modelos de gestión, producción y vida más avanzados y como promotor de actividades de carácter comercial y productivo nada desdeñables.

- En contra de lo que sostiene a primera vista la teoría económica clásica, aun en condiciones ideales de libertad, la movilidad del factor trabajo no es total entre dos países o zonas económicas en principio desiguales. En lugar de producirse una transferencia del factor trabajo desde la zona con menores salarios hacia la que los tiene más altos, hasta que ambas se equilibren idealmente, en la práctica resulta evidente que los salarios no bastan, por sí solos, para explicar los movimientos migratorios internacionales.

Existen diversas razones que permiten concluir que, incluso en un régimen de total libertad para el movimiento de personas, no se produciría la tan temida «invasión». Entre ellas se pueden mencionar: a) Costes. Al contrario de lo que ocurre con el capital, cuyo titular no precisa moverse para transferir este factor a otro mercado, la movilidad del factor trabajo lleva pareja la necesidad de que su propietario se traslade físicamente al nuevo mercado en el que desea operar. Ese movimiento tiene unos costes de transporte importantes, sobre todo cuando se refiere, como suele ser el caso de la emigración procedente

del Sur y del Este, a personas de bajo poder adquisitivo. b) Riesgos. Que van desde la exposición a diversos peligros que pueden llevar a poner en juego la propia vida, hasta la posibilidad de ser rechazados en la frontera del potencial país de acogida o de no lograr finalmente un puesto de trabajo. c) Barreras. Tanto las que derivan de diferencias lingüísticas, culturales y sociales como las que vienen impuestas por normas legales e, incluso, geográficas.

En resumen, todo indica que los movimientos migratorios internacionales con destino al territorio comunitario van a continuar. A ello apuntan tanto la problemática situación de los vecinos, que no consiguen garantizar un nivel de vida digno para la totalidad de sus ciudadanos, como el atractivo que sigue ofreciendo una zona próspera como la Unión Europea, a pesar de todas las medidas legales-policiales que traten de impedirlo. En estas condiciones, y a la luz de las parciales e incompletas soluciones ensayadas hasta ahora, se hace palpable la necesidad de su reformulación en profundidad, apostando, como se verá posteriormente, por una actitud más preventiva que reactiva.

Refugiados, desplazados y retornados

Desde la segunda guerra del Golfo hasta la crisis de Timor Oriental, pasando por las que han asolado a la antigua Yugoslavia y a la zona de los Grandes Lagos, el número de refugiados, desplazados internos y retornados no ha hecho más que aumentar de manera exponencial en la presente década. Las estimaciones del Alto Comisionado de Naciones Unidas para los Refugiados (ACNUR) elevan a 50 millones, en el año 1997, el total de personas sometidas a desplazamientos forzados (de las cuales 27.729.233 están bajo la responsabilidad del ACNUR).

De manera más detallada, ese volumen de desplazados comprende tres categorías distintas:

1. Refugiados. Así son calificados quienes se han visto obligados a abandonar su país de origen para huir de persecuciones, conflictos armados o la violencia. Es evidente que bajo esa definición caben muchas situaciones distintas, dado que no resulta fácil equiparar a un palestino de segunda o tercera generación en un campo de refugiados de Líbano, con un trabajador bosnio de clase media que ha encontrado acogida en Alemania o con un campesino afgano instalado en Irán o Pakistán. Sin embargo, el denominador común que los une es la nece-

sidad de protección que presentan, derivada ya de las dificultades materiales y psicológicas experimentadas por el abandono de su lugar de residencia, sino también por la incertidumbre y la hostilidad que, en demasiadas ocasiones, amenazan su seguridad física en su diario devenir en el país de acogida.

En términos más precisos, la Convención de Naciones Unidas sobre el Estatuto de los Refugiados (1951) emplea este concepto para quien «debido a fundados temores de ser perseguido por motivos de raza, religión, nacionalidad, pertenencia a determinado grupo social u opiniones políticas, se encuentre fuera del país de su nacionalidad y no pueda o, a causa de dichos temores, no quiera acogerse a la protección de tal país».

Según los datos de principios de 1997, el ACNUR, encargado de la estadística de los refugiados y de su protección, tenía registrados un total de 13.199.646 personas, a las que habría que añadir los casi tres millones de refugiados palestinos bajo el amparo de la Organismo de Obras Públicas y Socorro de las Naciones Unidas para los Refugiados Palestinos (UNRWA). El desglose por continentes de los refugiados a cargo del ACNUR muestra el siguiente panorama: Asia (4.808.624), África (4.341.480), Europa (3.166.039, de los que 1.266.000 están en Alemania), América del Norte (720.119), Latinoamérica (88.430) y Oceanía (74.954).

2. Desplazados internos. Aunque no existe un consenso total sobre este concepto, en términos generales, engloba a las personas que, como resultado de persecución, conflicto armado o violencia se han visto obligadas a abandonar el lugar donde residen habitualmente y permanecen dentro de las fronteras de su propio país.

Las dificultades para conocer su número arrancan de la inexistencia de un órgano encargado de su contabilidad, pero también de la resistencia que oponen los gobiernos de los países con los que se encuentran poco interesados en dar a conocer su magnitud, y al hecho de que una considerable proporción de los desplazados no llegan a registrarse como tales. En todo caso, diversas estimaciones coinciden en evaluar su cuantía a unos 30 millones de personas (16 en África, seis en Asia, cinco en Europa y tres en América). Si se tiene en cuenta que 15 años antes su volumen apenas era de 1,2 millones de personas y que, actualmente, el problema afecta a unos 35-40 países, resulta inmediato concluir que se trata de un serio problema con tendencia a agravarse.

Aunque inicialmente el ACNUR no tenía encargada la atención y protección de estas personas, su evolución ha obligado en estos últimos años a considerar la necesidad de ampliar el mandato original. De esta forma, a principios del año 1997, ACNUR ya atendía a 4.853.712 desplazados internos (dos millones en África, 1,7 en Asia y uno en Europa).

Es preciso reseñar que en esta trágica contabilidad no se incluyen los desplazados como consecuencia de los desastres y catástrofes naturales. El último Informe Mundial sobre Desastres (Federación Internacional de la Cruz Roja, 24 de junio de 1999) afirma que 300 millones de personas se han visto afectadas por catástrofes naturales en el año 1998. Por sí sola ésta es la causa del 60% de los desplazamientos internos, con mayor incidencia en los países menos desarrollados (en donde se registran de hecho, el 96% de las muertes que se producen como consecuencia de estos desastres).

3. Retornados. La finalización formal de algunos conflictos desde principios de la década ha permitido que un considerable número de refugiados y de desplazados internos hayan logrado retornar a sus lugares de origen. La decisión del regreso no siempre ha sido totalmente voluntaria (en contra de la propia Convención sobre los Refugiados), pero aunque así lo hubiera sido la reintegración nunca resulta sencilla. Por una parte, tras el conflicto que ha provocado el desplazamiento se manifiestan unas profundas fracturas sociales, así como una situación política inestable, un deterioro considerable del entorno y un clima psicológico muy delicado. Por otra, y como consecuencia directa de la crisis, poco cabe esperar de la mayoría de los sistemas productivos, de seguridad, educativos y sanitarios para resolver los problemas de quienes retornan.

De ahí que, gradualmente, se haya ido desarrollando la conciencia de que es preciso asistir a esta población en el intento por recuperar su lugar en sus sociedades de origen. Sin embargo, hasta la actualidad esta labor, al igual que ocurre con los desplazados internos, no está asignada estatutariamente a ningún organismo concreto. De esta forma, los más de nueve millones de retornados que, según el ACNUR, se habían registrado en el periodo 1991-1995 (frente a los 1,2 del periodo 1985-1990) deben enfrentarse con sus muy escasos recursos, y el apoyo de Organizaciones No Gubernamentales (ONG) sobre el terreno, a esta compleja tarea de reintegración.

También en este terreno ACNUR ha comenzado a desarrollar una labor de asistencia y protección que cubría, a principios del año 1997, a 3.311.233 personas (1.692.504 en África, 1.241.544 en Asia, 307.949 en Europa y 69.226 en Latinoamérica).

Lejos de reducirse, el problema planteado por los desplazamientos forzosos no ha hecho más que aumentar en estos dos últimos años. Para confirmarlo basta con recordar el último episodio de la tragedia que sufre la antigua Yugoslavia. Aunque la «limpieza étnica», practicada en Kosovo por el régimen serbio contra la población albano-kosovar, ya se había iniciado en marzo del año 1998, no alcanzó su máxima expresión hasta la primavera de 1999, cuando un millón y medio de personas (más del 90% de la población) fueron expulsadas de sus lugares de residencia en esta región de la República Serbia. Si bien la campaña militar dirigida por la Organización del Tratado del Atlántico Norte (OTAN) consiguió doblegar a las autoridades serbias e imponer el regreso a sus hogares de quienes habían sido expulsados, la solución del problema está lejos de alcanzarse.

Por una parte, tal como recordaba en junio de 1999 Sergio Vieira de Mello, (subsecretario general de la Organización de Naciones Unidas (ONU), encargado de coordinar la ayuda humanitaria a las víctimas del conflicto), sería imposible el regreso total de los refugiados y desplazados antes del otoño, aunque se iniciara inmediatamente la operación. Por otra parte, el regreso de los albano-kosovares y la aplicación de los acuerdos ha provocado, a su vez, una huida de la población serbia de Kosovo, ante el temor de sufrir represalias. Se trata de más de 80.000 personas, que se unen a los más de medio millón de serbios que ya habían abandonado Bosnia y Croacia en los años anteriores, en una reacción similar a la de ahora. Por último, el propio Carlos Westendorp (máximo responsable civil para Bosnia) afirmaba, en mayo del año 1999, que todavía quedaban 836.500 desplazados internos en Bosnia (de los 2,5 millones que generó la crisis), más de tres años después de los Acuerdos de Dayton (diciembre de 1995).

Precisamente el ejemplo yugoslavo permite destacar un rasgo que, sin ser nuevo, resulta cada vez más frecuente en las crisis ocurridas tras el final de la guerra fría. Tradicionalmente los desplazamientos forzosos han sido una de las consecuencias de los conflictos; sin embargo, en estos últimos años se aprecia que éstos han pasado a constituir una parte sustancial de la estrategia del agresor para lograr sus objetivos. Así ha ocurrido no sólo en el caso yugoslavo, sino también en Afganistán, con la idea de vaciar determinadas zonas en las que se desarrollarían posterior-

mente operaciones militares, o en Guatemala, como una variante más de la contrainsurgencia, en el intento de restarle apoyo logístico y social a los oponentes.

Vías de respuestas al problema

Hasta ahora, la reacción de la mal llamada comunidad internacional y la de cada uno de los países, desarrollados o en desarrollo, frente a los problemas que se derivan de la presión migratoria y de los desplazamientos forzosos no ha estado a la altura del reto que éstos representan. Como rasgos más sobresalientes de las parciales medidas que se han ido adoptando para tratar de gestionarlos cabe destacar:

- a) La falta de una voluntad política decidida que se plantee como objetivo último la erradicación a medio plazo de estos problemas, desactivando la carga de inestabilidad que conllevan.
- b) La descoordinación entre los distintos responsables nacionales e internacionales en materias que conectan directamente con estos procesos.
- c) La visión de los movimientos migratorios, sobre todo los de carácter internacional, desde una óptica eminentemente represiva, que trata de frenar su desarrollo a través de medidas legales y policiales.
- d) El tratamiento de los movimientos forzosos desde un punto de vista estrictamente reactivo, y con un objetivo puramente asistencial, limitándose a paliar en lo posible el sufrimiento de las víctimas.

Estos rasgos pueden identificarse por igual en los distintos niveles de decisión implicados en estas cuestiones.

Nivel internacional

La creación del ACNUR, por una decisión adoptada por la ONU en 1951, ha sido el principal logro de la Comunidad de Naciones en relación con el tema de los refugiados. Sin embargo, es preciso recordar que la razón de su existencia, limitada inicialmente a tres años, fue el interés de los vencedores en la Segunda Guerra Mundial para resolver los problemas planteados por los 1,2 millones de desplazados que el conflicto había originado en la Europa Occidental. Fue el agravamiento del problema en otras latitudes lo que obligo a mantener a este organismo hasta la actualidad, encargándose ya no sólo de los refugiados en sentido estricto sino también, como se mencionaba en páginas anteriores, de los desplazados internos, de los retornados e, incluso, de los apátridas.

Desde ese encargo inicial, el ACNUR ha llegado a los casi 23 millones de personas bajo su protección, tras pasar por los 5,7 en el año 1980 y los 15 en el año 1990. Para atender a estas funciones de asistencia cuenta con un presupuesto anual que sobrepasa ligeramente, desde el año 1992, los 1.000 millones de dólares (en el año 1990 apenas alcanzaba los 550).

Igual importancia tiene la labor que desarrolla la UNRWA, desde su creación en 1949 (resolución 302 [IV] de la Asamblea General de la ONU de 8 de diciembre de 1949), para tratar de facilitar asistencia a los refugiados palestinos, que constituyen actualmente el más antiguo colectivo de personas en esta situación. Este Organismo, encargado inicialmente de prestar asistencia humanitaria y ayuda de emergencia a los 750.000 palestinos que se vieron obligados a salir de sus lugares de residencia tras la creación del Estado de Israel (1948), ha pasado en estos 50 años de existencia a asistir a un total de 2,9 millones de refugiados distribuidos en campos de Gaza, Cisjordania, Líbano, Siria y Jordania. Su labor se concentra en proporcionar educación básica, asistencia sanitaria y socorro y servicios sociales a esta población, para lo que cuenta con un presupuesto anual que, ya desde 1994 y con ligeras variaciones, ronda los 700 millones de dólares (en el año 1992 era todavía de 267).

Al margen de estos logros, no existe ninguna iniciativa en el campo de los movimientos migratorios nacionales o internacionales, como señal de la incapacidad para actuar en el ámbito interno, en el que la soberanía nacional se impone sobre el derecho de injerencia, y de la falta de instrumentos adecuados con los que hacer frente a las fuerzas que dominan el escenario global, en el que se desarrolla la competencia política y económica mundial. Mientras tanto, sigue reduciéndose el volumen de ayuda internacional de emergencia, que sólo llegaba a los 2.149 millones de dólares en el año 1997 (frente a los 3.468 de 1994). Lo mismo sucede con la ayuda oficial al desarrollo que, con una media mundial del 0,22% del PIB, sigue muy lejos del objetivo del 0,7%, formulado ya en 1973 por la ONU.

Nivel nacional

En lo que hace referencia a las migraciones internas, la inmensa mayoría de los países afectados, sobre todo en los países de la periferia Sur, no han logrado responder con medidas eficaces al desequilibrio que se está produciendo en su seno entre el ámbito urbano y el rural. Su modelo de gestión política no se caracteriza, en general, por atender a las necesida-

des del conjunto de la población sino, más bien, a los intereses del grupo que representan. En esas circunstancias, la situación social no ha hecho más que deteriorarse gradualmente, hasta alcanzar un punto de inestabilidad difícilmente controlable por unos dirigentes que han optado, como mecanismo para recuperar la legitimidad perdida, por impulsar limitadas reformas económicas mientras mantienen férreamente controlado el escenario político. La insatisfacción derivada de esta situación, que provoca el empeoramiento de las condiciones de vida de gran parte de la población, es un germen desestabilizador que sólo puede conducir a un escenario más negativo si no se adoptan, con la decidida contribución de los países comunitarios, reformas profundas en las esferas sociales, políticas y económicas.

La evolución de los movimientos migratorios internacionales, por su parte, ha mostrado una evidente falta de colaboración entre las autoridades de los países emisores y las de los receptores. No se ha logrado establecer ningún sistema de gestión de un fenómeno en crecimiento, aunque, afortunadamente, no se han cumplido las alarmantes perspectivas presentadas a finales de la década pasada sobre la inminente llegada a territorio comunitario de millones de ciudadanos de los países de la Europa Central y Oriental, en búsqueda de trabajo. Para hacer frente a esa hipotética «invasión», Bruselas ha reforzado sus mecanismos de control (Schengen es el mejor ejemplo) y ha formulado una estrategia diferenciada con respecto a sus vecinos, con el doble objetivo de estabilizar esas zonas mediante una más estrecha asociación y ganar nuevos mercados para sus productos: oferta de integración plena en el club comunitario para algunos de los países de la periferia Este (con la perspectiva de futuras invitaciones al resto) y desarrollo de una Asociación Euromediterránea para los países del Magreb y de Oriente Medio.

Mientras tanto, se perciben síntomas de cambio en algunos países de la Unión Europea. Por una parte, la ministra francesa de Justicia declaraba que:

«El sistema de cuotas (para inmigrantes) me parece peligroso porque puede conducir a la discriminación» (*El País*, 25 de enero de 1999).

Por otra, Alemania iba mucho más allá, aprobando una ley que facilitaba, a pesar de que sus pretensiones iniciales hayan sido recortadas bajo la presión de ciertos sectores sociales, la oportunidad de adquirir la nacionalidad alemana a un gran número de extranjeros. Incluso España, tras haber llegado al convencimiento de que la inmigración se ha convertido en

un rasgo estructural de la sociedad actual, ha iniciado los trámites para aprobar una Ley de Extranjería más en consonancia con la situación real de quienes eligen este país como puerta de entrada en la Unión Europea.

La misma actitud defensiva se percibe en relación con el tratamiento dado a los desplazados forzados que llegan, o tratan de llegar, a territorio comunitario. La tendencia generalizada es la de resistirse a aceptar lo que se percibe como una carga impuesta, obstaculizando tanto su intento de entrada como el reconocimiento del Estatuto de Refugiados o de Asilo, sin que, por otra parte, se perciban iniciativas nacionales o comunitarias de carácter preventivo.

Lo que, en definitiva, se deduce de este comportamiento es una visión pasivo-reactiva por parte de los gobiernos y de los organismos internacionales, que no contribuye significativamente a reducir, y mucho menos a resolver, los problemas que se plantean en este terreno. Una de las mejores muestras de ello es la tendencia que se percibe hacia la reducción del número de refugiados (18,3 millones en el año 1993 y 13,2 en el año 1997) y un simultáneo incremento en el volumen de desplazados internos. Lejos de suponer una disminución del nivel de conflictividad, este hecho muestra claramente el interés y la presión que ejercen los Estados para mantenerse al margen de los conflictos que sufren sus vecinos, impidiendo la entrada en su territorio de potenciales refugiados o incluso obligándoles a retornar a su país, independientemente de que no se den las condiciones de seguridad requeridas para ello (en flagrante contradicción con la normativa de la Convención sobre los Refugiados, que proclama que toda repatriación debe ser absolutamente voluntaria).

Con este comportamiento se está poniendo no sólo en grave peligro el régimen internacional de protección de los refugiados (derecho de asilo, asistencia y protección al refugiado, no repatriación forzosa), sino que se está forzando a actuar al ACNUR y al resto de las ONG dentro de los países donde se ha generado la crisis, en unas condiciones de indefensión y de precariedad manifiestas. Unas condiciones en las que no puede descartarse, como ya ocurrió durante la crisis de los Grandes Lagos, que alguno de los bandos en conflicto ejerzan la violencia contra los desplazados internos, incluso aunque se hallen dentro de zonas teóricamente seguras.

Por otra parte, la reiterada falta de voluntad política para actuar en las primeras etapas de la crisis, y mucho más para articular estrategias preventivas que se adelanten a su estallido, viene enmascarada por una apuesta

artificial a favor de la acción humanitaria. Se pretende que esta última, en lugar de ser un complemento de la acción política, pase a ser su sustituta. Nada positivo puede derivarse de esta tendencia, dado que los organismos humanitarios no están concebidos ni equipados para hacer frente en solitario a contextos violentos o a emergencias políticas en los que peligra la seguridad física de las personas, ni, mucho menos, para disuadir a los violentos o para evitar que las tensiones previas desemboquen en un conflicto abierto.

Conclusiones

Al igual que ocurre con los demás riesgos para la seguridad internacional analizados en el resto de los apartados de este trabajo, la carga desestabilizadora que incorporan los movimientos migratorios puede no ser tan evidente, a primera vista, como lo eran las amenazas que caracterizaban el periodo de la guerra fría. Sin embargo, no por ello su potencial resulta de menor entidad ni puede justificarse su olvido, a la hora de establecer las prioridades inmediatas de la seguridad en el próximo siglo.

Por el contrario, su «invisibilidad» obliga a realizar un esfuerzo añadido para transmitir, a la opinión pública y a los distintos actores sociales y políticos, la necesidad de prestar mayor atención a su evolución y para articular una estrategia, que tienda tanto a solucionar los problemas ya existentes y a corregir las negativas tendencias reflejadas en el apartado anterior como a prevenir el desencadenamiento de nuevas crisis.

En este sentido cabe resaltar, una vez más, que las medidas preventivas constituyen la vía más eficaz para eliminar la inestabilidad generada por estos fenómenos. Esa voluntad preventiva, para ser eficaz, debe tomar en consideración, entre otros, los siguientes elementos.

El punto central sobre el que basar cualquier estrategia de acción que pretenda reducir o eliminar los efectos negativos de los desplazamientos forzados (considerando que también en los movimientos migratorios nacionales e internacionales existe un factor de obligatoriedad) es considerar que el bienestar del conjunto de la población es vital para la seguridad nacional e internacional. A todas luces resulta más estable un país con un mayor nivel de bienestar y de desarrollo político, social y económico que otro que presenta como mejor activo un sistema de seguridad y defensa más poderoso.

Desde la perspectiva de la seguridad, los problemas que plantean cada una de las modalidades de desplazamiento forzoso aquí analizadas afectan tanto a los responsables de los países que sufren directamente sus consecuencias como a los gobiernos de los países desarrollados y a los organismos internacionales. La mejora de la situación actual sólo puede alcanzarse a través del compromiso y de la coordinación de todas las partes.

Adelantarse al estallido de estos procesos implica actuar, de manera sostenida y directa, sobre las causas que desencadenan estos procesos migratorios: escasez de recursos, evolución demográfica, brecha de desigualdad entre ricos y pobres, subdesarrollo económico y socio-político. Esto supone un reto esencial tanto para los países donde se origina el problema como para el conjunto de los países desarrollados y de las instituciones internacionales. Para los primeros, implica un cambio radical en su manera de gestionar los asuntos públicos, permitiendo un giro drástico en la esfera económica para hacer más eficaz un sistema que, hasta ahora, ha profundizado las diferencias, condenando a la mayoría de la población al subdesarrollo. Además, reclama un conjunto de reformas de índole social y política, que favorezcan la instauración de un verdadero Estado de Derecho, en el que sea posible expresar y defender libremente las distintas sensibilidades que conviven en ese territorio.

Para los países desarrollados y los organismos internacionales presupone, en primer lugar, mostrar una actitud más generosa en su doble papel de donante y acreedor. Para ello no es necesario apelar al altruismo o a la solidaridad con los menos favorecidos, sino directamente al egoísmo inteligente de quien entiende que ésta es la mejor manera de defender sus intereses (basta, como ejemplo, mencionar las perspectivas que podrían abrirse para los condenados a la emigración si se lograra instaurar un régimen de gestión compartida de los flujos migratorios y las consecuencias de una apuesta decidida por el desarrollo económico del país emisor, fomentando la inversión con ánimo de generar actividades productivas, intensivas en mano de obra, en los lugares de residencia de esos potenciales emigrantes). En el plano socio-político exige abandonar la actitud mantenida durante décadas, de subordinar la urgencia de los cambios necesarios en estos países a la defensa del *statu quo*, contribuyendo de esta forma al sostenimiento de regímenes políticos poco respetuosos con los derechos humanos y con las normas básicas de la democracia. Es evidente que esta actitud chocará, en muchas ocasiones, con la resistencia de los actuales responsables políticos de esos países, pero parece claro

que, en términos de coste-beneficio, ésa es la opción más conveniente si que pretende abrir la vía a un entorno más equilibrado, desarrollado y, por lo tanto, estable.

A escala internacional también es preciso impulsar un cambio del modelo de relaciones políticas y económicas, orientado hacia la implantación de unas reglas de juego que frenen tanto el incremento de las desigualdades, en el ámbito económico, social y político, como el deterioro medioambiental.

Mientras tanto, será preciso adoptar medidas correctivas, allí donde se haya producido ya una crisis que provoque el tipo de problemas aquí analizado. La adopción de estas medidas siempre representa, en mayor o menor grado, el reconocimiento de un fracaso. En todo caso, a la hora de actuar ante situaciones dadas de desplazamiento, el orden de prioridades parece estar claro:

1. Salvaguardar la vida y el ejercicio de los derechos básicos de las personas afectadas por el problema:
2. Proteger los intereses del país de acogida (si se trata de un problema de refugiados).
3. Establecer las condiciones en el país de origen que faciliten, con garantías, el retorno o el restablecimiento de la situación original.

Para lograr esto último es preciso realizar un sinfín de tareas de mejora (en ámbitos como el empleo, los servicios básicos, la restitución de las propiedades, el alojamiento de los «sin techo», la superación de los traumas psicológicos, la reconstrucción o creación de sistemas de protección social, la autosuficiencia alimentaria, la asistencia sanitaria). Una labor en la que será imprescindible contar con la estrecha participación de los agentes humanitarios, ya no como sustitutos sino como complementos de la acción de los poderes públicos.

Aunque a primera vista pudiera parecer que estas propuestas están alejadas del objetivo que se pretende lograr e, incluso, que pueden calificarse de ilusorias, es necesario afirmar con rotundidad que lo realmente ilusorio es seguir creyendo que con los modelos actuales se puede poner solución a problemas creados en gran medida por ellos mismos y que escapan ya a su control. Es necesario definir y aplicar instrumentos nuevos para solucionar problemas irresolubles, con esquemas que han llegado al límite de sus posibilidades.

CAPÍTULO TERCERO

SISTEMAS DE INFORMACIÓN Y AMENAZAS A LA SEGURIDAD

LOS SISTEMAS DE INFORMACIÓN Y LAS TECNOLOGÍAS DE LA INFORMACIÓN EN EL SIGLO XXI

Por ALEJANDRO KLECKER DE ELIZALDE

La desregulación de las telecomunicaciones

En el inicio de los años ochenta se va a producir un fenómeno económico, que va a marcar la gran revolución el final del siglo xx, como es la liberalización del sector de telecomunicaciones en Estados Unidos, seguida de la producida en la Unión Europea, Japón, Nueva Zelanda y Australia.

El acontecimiento producido por el desmembramiento del monopolio de AT&T, en ocho compañías regionales, que compiten entre sí, empresas posteriormente conocidas como las *Baby bells*. En paralelo el proyecto del ARPA, para la creación de una red de ordenadores y de sistemas que fuera invulnerable a un ataque masivo a los grandes centros de defensa y Gobierno de Estados Unidos, dio origen a la actual red Internet.

La liberalización de los mercados a su vez en Europa Occidental al final de la década y principios de los noventa, abrió el camino para la pérdida del monopolio que, cada compañía, normalmente con mayoría de capital público, tenía en su país.

Si para la economía este factor introdujo un incremento de los servicios, unas tarifas aparentemente más controladas por el mercado y el acceso generalizado a la información a decenas de millones de usuarios en todo el mundo, por otra generó una nueva amenaza a la seguridad de los Esta-

dos por pérdida del control sobre las redes de comunicaciones que hasta entonces y debido al monopolio, detentaban los gobiernos.

Concentración en manos de pocos grupos multinacionales de: fabricación, Investigación y Desarrollo (I+D), distribución y mantenimiento de equipos y sistemas de telecomunicaciones.

Concentración igualmente en manos de escasísimos proveedores del *software* necesario para comunicar equipos y redes de comunicaciones. De hecho existe un dominio *de facto* de un solo proveedor.

Compra masiva de medios y compañías de comunicaciones e informática, por parte de pocos grupos que van a ofrecer una panoplia de medios de comunicación (televisión, televisión por cable, periodismo impreso, emisoras, etc.), con el consiguiente peligro de poder informar objetivamente ante una amenaza a la seguridad de un Estado.

Reconocimiento de aparición del «síndrome CNN», mediante el cual en una sola imagen visual y en un corto comunicado se informa a millones de ciudadanos en todo el planeta, condicionando a menudo decisiones políticas de primera magnitud. En el sentido de favorecer una intervención armada, un ejemplo fue el bombardeo del mercado de Sarajevo y en sentido contrario, las trágicas imágenes de un soldado norteamericano arrastrado por las calles en Somalia, conllevó la salida de las fuerzas de Estados Unidos de un conflicto no entendido por la mayoría de los ciudadanos de su país.

Aparición de un fenómeno de saturación de información e incapacidad física para controlarla. Escasez de espacio físico en lo que antes se denominaba éter. Lucha por el dominio del mismo. En este sentido cabe recordar la teoría de N. Negroponte de vuelta al cable y reserva de las redes de microondas, etc. Para determinadas aplicaciones como más adelante veremos.

Incapacidad para controlar la difusión de información sesgada o preparada contra un Estado. La liberalización de las comunicaciones, está suponiendo el mayor empuje para este espectacular incremento, pero sin embargo, pocos países han desarrollado un cuerpo legislativo que permita decir que esto es un hecho. Limitaciones a la aportación de capital extranjero, limitaciones de áreas, volumen mínimo de inversiones a realizar por una compañía extranjera en el país, u obligación de cubrir toda la superficie del país, incluyendo zonas semidesérticas, son los trucos que los gobiernos y compañías que todavía ejercen el monopolio imponen a nuevos entrantes en el mercado.

En enero del año 1998 la Unión Europea abrió los mercados de las telecomunicaciones de todos sus países miembros. Sin embargo, Grecia, Portugal y otros países europeos no comunitarios, como Hungría o la República Checa, mantiene todavía restricciones a sus mercados. Pero la dinámica del mercado, la demanda de empresas y ciudadanos barrerán cualquier tipo de dificultad a la apertura de los mercados de las telecomunicaciones.

Las telecomunicaciones, factor de desarrollo y dependencia

En el informe que bianualmente publica la Organización para la Cooperación Económica y el Desarrollo (OCDE), sobre este mercado, y del que recogemos en su edición del año 1999 una serie de datos, podemos observar la creciente importancia del mundo de las comunicaciones, cuyos mayores exponentes de cambio son Internet y la telefonía celular, conocida en España como «móvil».

Del espectacular crecimiento podemos señalar algunas cifras. En 1995 se facturaron en telecomunicaciones 532 billones de dólares estadounidenses, en el año 1997 se había pasado a 623 billones de dólares. El segmento que más creció fue el de los teléfonos móviles con un crecimiento medio de 20% anual.

De 15 millones de usuarios de estos equipos existentes en el año 1992, existían ya en el año 1997 más de 170 millones en la OCDE y 200 en todo el mundo. Sólo en el seno de la OCDE se calcula para el año 2000, más de 200 millones.

En España, las cifras hablan de casi tres millones y medio de teléfonos móviles, que supone un 10% cada 100 habitantes.

La media de los países de la OCDE es de 15,6% teléfonos por cada 100 habitantes. Países como Portugal tienen un 15,6 %, superior a nosotros. Esto es debido a que en los países con menor desarrollo hoy en día es más factible montar una red de telefonía móvil, que prácticamente se puede poner en seis meses en funcionamiento que una basada en el cobre o fibra óptica, que requiere más de tres años. Por lo tanto, lo que ocurre es que antes que un teléfono fijo se recurren a contratar uno móvil, de ahí esas diferencias.

En cuanto a la aportación que suponen las telecomunicaciones al Producto Interior Bruto (PIB) de los países de la OCDE, alcanza en el año

1997 el 2,71%, frente al 2,32 del año 1995. España se sitúa en un 2,60%, por debajo de la media, pero muy por encima de países más avanzados como Austria, Bélgica, Finlandia o Alemania.

Si presenciamos por otra parte, el absoluto dominio en manos de unos pocos de las tecnologías de las telecomunicaciones, que antes señalábamos como una amenaza para nuestra defensa, al depender absolutamente de ellos, podemos citar algún dato suficientemente explicativo.

Así de las patentes que se presentan en Estados Unidos, las referentes al sector que nos ocupa, han crecido de poco más de 15.000 en el año 1994 a 20.000 en el año 1997. De ellas, 9.811 pertenecen a empresas de Estados Unidos, casi 7.000 a Japón siendo el tercer país Alemania con 608.

Baste decir que en unas recientes declaraciones de una experta de Deloitte & Touche, se sostiene que:

«El escenario más probable es que queden entre tres y cinco “superoperadores” verticalmente integrados con una presencia realmente mundial, que coexistirán con miles de actores de nichos que ofrezcan servicios locales especializados.»

Si observamos las cifras de integración de fabricantes lo demuestra el estudio de Broadview, Technology M&A Report, que demuestra que en el año 1998 los 10 mayores acuerdos en telecomunicaciones representaron un 40% del valor total de las fusiones y adquisiciones de todas las transacciones de tecnología del pasado año y un 60% de todas las fusiones y adquisiciones en Estados Unidos. La cifra en tan sólo un año paso de 86.200 millones de dólares a 255.600. En la Unión Europea las fusiones y adquisiciones pasaron de 167 a 242 para el mismo periodo.

Si tenemos en cuenta quienes son las empresas que más invierten y controlan los equipos básicos para comunicarse en Internet, encontramos que son sólo cuatro y además de Estados Unidos las empresas, en concreto: 3Com, Bay Networks, Cabletron Systems y Cisco Systems.

Esta última puede ser un ejemplo del desarrollo del mercado, así en el año 1995 facturó 2,2 billones de dólares estadounidenses y en el año 1997, 6,5 billones.

Las cinco compañías que más invierten en I+D para telecomunicaciones son Siemens con más de 4.000 millones de dólares, Fujitsu, Ericsson, Lucent Technologies y NEC.

Más apabullante es el dominio de los microprocesadores, ya que prácticamente casi todos los ordenadores personales y servidores llevan Intel.

Los navegadores de Internet están en manos de Estados Unidos, así Netscape Navigator tiene el 70% del mercado que unido a Microsoft Explorer prácticamente dejan sin presencia al resto de proveedores.

Los *routers* de comunicaciones son igualmente mayoritariamente de Cisco e Intel, dejando en mera presencia testimonial al resto. Los módem de alta velocidad necesarios para transmitir imagen y vídeo, de origen Estados Unidos, crecieron en cuanto a facturación, en tan sólo dos años (1995–1997) de 501 millones de dólares a más de un billón.

Los sistemas operativos para manejar las Redes de Área Local (LAN en inglés) son o Novell o NT y sino de IBM.

Prácticamente cualquier dispositivo para comunicaciones en el mundo pasa en mayor o menor medida por fabricantes de Estados Unidos. En cuanto a la tecnología de satélites lo trataremos más adelante pero ocurre lo mismo. Todos los Sistemas de Posicionamiento Global (GPS) del mundo dependen de la red de satélites del Gobierno de Estados Unidos, que los facilita, para uso civil.

En la de encriptación el tema no tiene discusión, si se quiere seguridad, hay que recurrir a los proveedores de algoritmos de Estados Unidos. Y por cierto para manejarse en Internet se requiere de un protocolo de comunicaciones denominado Protocolo de Control de Transmisión/Protocolo Entre Redes (TCP/IP), desarrollado por la Universidad de Stanford.

En el mercado español, la dependencia tecnológica es también absoluta, incluso para las centralitas telefónicas digitales la opción es bien corta Ericsson, Siemens y Alcatel el resto también oferta internacional.

Internet. Algunas consideraciones

Desde luego la estrella de las redes de comunicaciones y de crecimiento del mercado de las telecomunicaciones es Internet.

Actualmente existen 780 millones de líneas de acceso a telecomunicaciones, prácticamente todas ellas en mayor o menor medida pueden acceder a Internet. Por ello se habla de un mercado de 1.000 millones de usuarios de Internet en los dos próximos años. Aunque el número real es de 100 millones en estos momentos.

El número de ordenadores, en julio del año 1998 en el seno de la OCDE, que actúan como *host* (o lugares donde un dominio está asociado a una IP) es de 35 millones habiendo crecido un 24% en tan sólo seis meses, y eso que la política de precios todavía hace que sea muy cara la comunicación para cualquier usuario.

En cuanto a servidores, se acercan a los dos millones y medio en todo el mundo. De ellos casi medio millón utilizan encriptación mediante SSL (*Secure Socket Layer*) del inefable navegador Netscape. Además de estos 25.000, se utilizaban para comercio electrónico, habiendo crecido un 128% en tan sólo 12 meses.

Como sabemos Internet nació para reducir el peligro de pérdida de información que ocasionaría un ataque nuclear soviético a Estados Unidos, por ello no existe un nodo central o centro principal de comunicaciones sino que es una nube de redes, intercomunicadas. Por ello su misma concepción de origen sin embargo, es la principal amenaza de la defensa de los sistemas de información de un Estado.

La nube de redes es de casi 55.000 a finales del año 1998, en más de 100 países, que requieren de un conjunto de protocolos como habíamos descrito ante el TCP/IP, cuya función es la de interconectar subredes y enrutar el tráfico de las mismas.

Ahora existe un serio debate sobre la utilización y acceso a las diferentes páginas y servicios que están en la red, pues muchos de los contenidos son atentatorios con los derechos humanos, favorecen la delincuencia, son utilizados por grupos terroristas y en algún caso afectan a la moral de naciones con regímenes fundamentalista del tipo que sea.

Por ello se están desarrollando paquetes que garanticen el uso debido de la red. Pero hay que insistir que no hay una autoridad sobre la red, es más esto choca frontalmente con los pioneros en la red que estiman que debe ser un servicio abierto y sin coste, frente a la postura de compañías de telecomunicaciones y gobiernos.

A efectos de nuestro trabajo simplemente hay que insistir, que Internet se soporta por la tecnología de Estados Unidos de la que todos somos beneficiados, pero sin Microsoft, Intel, NetsCape y los protocolos de comunicación y de encriptación originados allí, Internet no existiría. Es, si se quiere, la gran contribución de Estados Unidos, sin quererlo, hacía un mundo más abierto, comunicado y por lo tanto más libre.

Las amenazas a la seguridad

En primer lugar destacar, que las amenazas a la seguridad y defensa mediante la utilización de sistemas electrónicos del tipo que sean y clasificados más adelante, son de muy diversa índole y alcance en cuanto a los daños que pueden ocasionar y las medidas defensivas y preventivas a adoptar. Sin embargo, pocas pueden constituir una amenaza real y crítica para un Estado.

Por hacer una pequeña clasificación, la concreción de las amenazas a la seguridad se centran en:

- La posibilidad de ser agredido por un tercero desde el interior o desde puntos lejanos al propio país o centro que sufre la agresión.
- Imposibilidad de detectar en la mayoría de los casos el origen de la agresión. Por lo tanto incapacidad de reaccionar en la defensa clásica, pues no se puede identificar, en principio al enemigo.
- La relativa facilidad de ser atacado en centros neurálgicos y estratégicos para un Estado como la bolsa, centros militares y de seguridad, ordenadores con datos confidenciales de personas e instituciones, etc. Estos ataques pueden ser mediante el uso de tecnologías de información o mediante medios clásicos, como el atentado, en los años ochenta, a la central de la red de datos de Telefónica en la calle Ríos Rosas en Madrid, que dejó sin comunicación a casi todas las grandes instituciones españolas durante varios días. Hecho silenciado en la época por el éxito que los criminales se podían haber apuntado.
- El dominio en pocas manos de las tecnologías de la información tanto en los sistemas operativos, como lenguajes de programación avanzados como en los servidores, *routers*, etc. Baste recordar que el 98% de los equipos utilizan sistema operativo de Microsoft y que por supuesto sus códigos fuentes están protegidos y son secretos.

La dificultad de prever dónde, cuándo y cómo vamos a ser agredidos, frente a los ataques de tipo más convencional, donde se pueden plantear escenarios y establecer las respuestas en función de los mismos. En el conflicto del golfo Pérsico, 34 instalaciones del Ejército americano sufrieron incursiones. Tras larga investigación se averiguó que el ataque provino de *hackers* en Holanda, donde su legislación permisiva impidió el procesamiento de los mismos.

Fuentes de Estados Unidos clasificaron el incidente de muy grave y de hecho penetraron en su sistema logístico de tal forma que ante un pedido

de munición, el peticionario podría haberse encontrado con el envío de cepillos y pasta de dientes.

En el caso español la incapacidad tecnológica y de desarrollo para fabricar *software*, algoritmos matemáticos de encriptación, etc. para defenderse de este tipo de ataques, dado que no tenemos las tecnologías base (*chip*, sistema operativo o equipos altamente sofisticados).

Como ejemplo, basta recordar que la inutilización de parte del *hardware* de Irak, durante la guerra del Golfo, fue introducido en la memoria de impresoras de un conocido fabricante. El *software* fue desarrollado por una agencia estadounidense y activado como virus durante la guerra inutilizando las redes y equipos. Esto ha sido recogido en fuentes de información diversas como Infoworld o US News.

Incapacidad legal y material —no se puede controlar el espacio físico— para evitar un ataque interesado de desinformación intencionado por un grupo o país. Como ejemplo la crisis de la libra esterlina ante el ataque de fondos de inversión privados. El Gobierno británico y autoridades monetarias reaccionaron cuando la bolsa y la moneda estaban desplomadas.

Sin embargo, no todos los tipos de ataque se pueden considerar como problemas que afecten a la defensa o la seguridad. En Estados Unidos la doctrina identifica claramente los siguientes tipos de agentes que pueden constituir una amenaza, me permito citarlos desde la menor importancia a la mayor, en función de peligros reales contra la defensa o seguridad de un Estado.

Personal interno de una organización (*insiders* en terminología norteamericana), *hackers*, criminales o delincuencia organizada, empresas, terroristas, organizaciones de inteligencia y gobiernos extranjeros.

Los tipos de agresores contra los sistemas de información y tecnologías de la información

Hemos clasificado los agresores en función de su menor o mayor trascendencia, veamos su definición:

- Personal interino. Generalmente son empleados descontentos que realizan algunas modificaciones a los programas o utilizan virus o bombas lógicas como veremos posteriormente. Aunque el peligro es incluso crítico para cualquier organización, lo cierto es que no constituyen una grave amenaza real a la defensa o a la seguridad nacionales.

— *Hackers*. Son individuos o grupos de los mismos, que se dedican, por mero divertimento intelectual o reto, a destruir las barreras que fabricantes, usuarios y desarrolladores de virus ponen a su peligrosa actividad.

El *hacker* no busca enriquecimiento personal. Sin embargo, sus acciones son tan letales como cualquier delincuente o terrorista.

En un artículo de *New York Times* en marzo de 1997, recogido en el libro: *Information Warfare* de D. E. Denning, se cita que en la *web* existen 440 boletines de *hackers*, 30 otras publicaciones y 1.900 lugares en la red donde es posible encontrar herramientas y trucos para desarrollar actividad de *hackers*.

Incluye desde casi adolescentes a grupos organizados. Pero lo preocupante es que la tecnología que se requiere es accesible para muchos: ingenio, conocimiento, un módem para conexión a redes Internet y privadas y una escasa moral por no decir una mentalidad delincuente amparada por el anonimato y el escaso riesgo físico de esta actividad. Afortunadamente todos los países están haciendo legislaciones duras contra estos verdaderos delincuentes.

— Delincuentes. Tienen como finalidad el lucro, ya sea a título personal, de lo que hay abundantes casos, o como integrantes de redes organizadas.

Actúan vulnerando los sistemas informáticos de empresa, bancos y gobiernos con el objeto de manipular, información o acceden a ella para venderla a terceros (listados de clientes, patentes y secretos industriales, etc.). Son asalto a bancos tecnológicos o espías industriales que no necesitan introducirse físicamente en una empresa.

No vamos a citar casos pues entran en el ámbito policial pero no en el de la defensa de un país, con las excepciones que luego veremos.

— Empresas. No pocas empresas intentan obtener secretos de su competencia, directamente o través de delincuentes. Su base es obtener información reservada o hacer espionaje industrial. Igualmente pueden incluso intentar enviar virus a sus competidores.

— Terroristas. Son cualquier banda de las desgraciadamente conocidas que pueden desarrollar actividades en contra de los Estados y sus organizaciones críticas. Existen pruebas fehacientes de numerosas incursiones y atentados a través de las redes de comunicaciones.

Igualmente pueden hacer actuaciones de desinformación, propaganda etc. Aunque la realidad es que pocas acciones de envergadura se les conocen, por el momento.

- Organizaciones y gobiernos. Cualquier servicio de información e inteligencia de un país desarrolla actividades en este campo. Lo más habitual es entrar en sistemas de información de otros países con objeto de recabar información pero, por su carácter lo que se pretende es acceder sin ser detectado. Estaríamos en una guerra cibernética o de información cuando se paso al punto de destruir esos sistemas sin hacerlos inoperativos como ha ocurrido en la guerra del Golfo o de Kosovo.

Tipología de ataques, ciberguerra y guerra de la información

Estamos hablando de un tipo de guerra, la de la información, que ha sido definida por el experto W. Schwartau en los siguientes términos:

«La guerra de la información consiste en aquellas acciones que intentan proteger, explotar, corromper, denegar o destruir información o fuentes de información en orden a obtener una ventaja significativa, objetivo o victoria sobre un adversario.»

La guerra descrita puede ser mediante técnicas informáticas o mediante el empleo de armas y medios convencionales, consiguiendo por medios tan diferentes los objetivos propuestos.

Cualquiera de la tipología de actores descritos en el epígrafe anterior puede desarrollar una serie de actividades que persigan los diferentes fines que hemos visto. En el campo puro del *software* y *hardware*, las actuaciones más conocidas son. Virus, «caballos de Troya» y «bombas lógicas».

Para ello resaltaremos en esta parte que son los «caballos de Troya», las «bombas lógicas», los virus y cómo éstos han afectado ya en alguna ocasión a la seguridad de los Estados. Baste recordar el reciente artículo de la prensa en el que se demostró que durante el ataque de la aviación aliada contra Irak, se detectaron cientos de acciones de intentos de entrada en las redes del Pentágono, en lo que pareció un ataque preparado, coordinado desde diferentes puntos del planeta.

En primer lugar, la amenaza más peligrosa a las redes de comunicaciones, tanto para los centros de Internet como a redes privadas de tipo Intranet, son los denominados «caballos de Troya». El funcionamiento es

similar a la táctica empleada en Troya. Algo que parece lo que no es, aparece en nuestra pantalla, una vez abierto el fichero, éste muestra con sus efectos que pueden destruir la información, discos duros de manera total parcial o aleatoria, haciendo el servicio inoperativo. Por ejemplo, se puede introducir un *troyano* de tal forma que borre aleatoriamente listado de personal o de funciones. Como no se sabe qué es lo afectado, lo mejor es limpiar el sistema. Dando lugar a pérdidas de información que pueden ser vitales para un centro de defensa.

El segundo tipo es el clásico virus, de lo que hay sobradas pruebas de activación en nuestros propios sistemas de seguridad y defensa. El virus es introducido por un tercero a través de mensajes engañosos, archivos que se activan al ejecutar una fecha (viernes 13) o al abrir determinados mensajes (*melissa* o gusano).

La protección contra los virus es compleja pues continuamente aparecen nuevos o mutaciones de otros, mientras que los fabricantes de antivirus siempre va a la zaga y cuando el daño se ha realizado.

El virus una vez propagado, se extiende rápidamente. Así el «viernes 11» de junio de 1999 se detectó un virus, luego conocido como gusano, que en tan sólo ocho horas había contaminado más de 600.000 ordenadores personales, en todo el mundo.

Sin embargo, en sentido estricto, no puede considerarse un arma de la denominada «ciberguerra», pues al igual que ocurre en la guerra bacteriológica real, sus efectos pueden escaparse de las manos de sus propagadores y afectar indiscriminadamente a ordenadores «amigos o enemigos».

Por ello suponen un peligro más real y son una verdadera arma las llamadas «bombas lógicas». Al contrario que en el caso del virus, que actúa con imprecisión, estos sistemas de instrucciones están diseñados y preparados para actuar en aplicaciones o secuencias de las mismas determinadas, sistemas operativos o herramientas.

Un gobierno, como de hecho, ocurrió como hemos visto en la guerra del Golfo, puede suministrar *software*, equipos y dispositivos, que pueden alterarse a distancia, a través de las redes de datos, activando determinadas instrucciones y secuencias que imposibilitan su correcta ejecución o alterar resultados de operaciones sin el conocimiento de quien lo opera.

Con el antecedente de las impresoras en la guerra mencionada, un país como España está obligado, dada la absoluta dependencia tecnológica

de terceros a considerar que determinado equipamiento, procesadores matemáticos avanzados, sistemas expertos, etc. Pueda estar en un momento determinado o en caso de conflicto controlado por una potencia extranjera y ser inservible para lo que se adquirió.

Desde nuestro punto de vista, esta cuestión debiera tener atención desde Defensa y obligar a que los suministradores, con todas las garantías de respeto a la propiedad intelectual, depositen los códigos fuentes, que deben ser revisados para evitar sorpresas como las descritas.

Pero estos medios pese a su actualidad y realidad, requieren de un medio —redes de comunicaciones— mediante cable o frecuencia desde donde enviar las instrucciones de activación de «bombas lógicas». Luego en caso de conflicto se tendrán que activar además el chequeo de los programas los *firewalls* («muros» que impidan la propagación de virus, etc.).

Existen también otros tipos de armas, que pueden dejar un sistema de defensa de última generación totalmente destruidos o inoperativos. Estas armas del arsenal clásico son parte de la guerra de la información.

Éstas muy resumidamente pueden ser de tipo de creación de campos electromagnéticos que destruyan la información en disquetes u otros soportes magnéticos de la información.

Mediante radio-frecuencia, se emplean dispositivos que emiten radiaciones electromagnéticas y que en el radio de acción en el que operan, inutilizan o alteran cualquier dispositivo electrónico. En el conflicto de Kosovo esto ha sido un hecho.

También equipos que utilizan microondas de alto poder, que emiten radiación en frecuencia de entre 1 a 35 gigahertzios.

Bombas de partículas de fibra de carbono que cortacircuitan líneas eléctricas y de comunicaciones, base de la operativa de ordenadores.

Los medios y tecnologías para la defensa y la prevención

Vamos a revisar cuál es el estado del arte y cómo se organiza la defensa frente a los ataques de los agresores, antes descritos en las redes y tecnologías que veremos brevemente descritas en el capítulo siguiente.

La primera consideración que debemos hacer en el apartado de las redes de comunicaciones y hablando en lenguaje no técnico, es el funcionamiento de las diferentes redes de comunicaciones.

Lo primero que tenemos que distinguir es entre operadores de servicios de comunicaciones, y compañías que a través de los medios de las primeras facilitan igualmente servicios sobre la misma. Aquí lo verdaderamente vulnerable es EL medio de transmisión no quien ofrece servicios sobre éste. Penetrado en el sistema se accede a lo que pasa por ese medio

Por ejemplo, la actual Telefónica de España, dispone de los medios físicos, compuestos por redes de cables, enlaces microondas, ordenadores, placas, *routers*, etc. que permiten la transmisión de los datos o información a través de la misma. Pero además provee servicios a través de estos medios a otras compañías de telecomunicaciones que no disponen de la red física (cables o nodos).

Otras compañías al liberalizarse el mercado de las telecomunicaciones tienen la posibilidad también instalar sus redes de datos e infraestructura tecnológica para ello. La realidad sin embargo, es que esto es muy costoso. Baste pensar los miles de millones que han sido necesarios para que inicien sus actividades los proveedores de telefonía Sistema Global de Telecomunicaciones (GSM) en España. Por ello lo que suelen hacer el resto de compañías es utilizar las facilidades de infraestructura y cableado de las redes ya existentes del proveedor que normalmente operaba en régimen de monopolio en el país, mediante una compensación económica. De esta forma sobre un mismo cable físico, por entendernos, circula información o servicios de a menudo varios proveedores, cuando no cientos de miles como es el caso de Internet.

Otras compañías optan por utilizar sus propias centrales de comunicaciones, no alquilándoselas a otro, con la consiguiente inversión. Conviviendo en el país diversas infraestructuras de cables. El ejemplo más notorio es la televisión por cable, que en España por concesión administrativa de las Comunidades y Ayuntamientos, estará fuertemente atomizada.

Como defensa clásica, para evitar las intrusiones, tenemos dos fundamentales: la criptografía y la seconfonía. De la segunda ya hemos hablado y se utiliza para comunicación de voz o voz y datos. El nivel tecnológico que se requiere, es alto pero desde luego alcanzable para España, que de hecho tienen productos en funcionamiento en múltiples dependencias del Estado. Aquí el saboteador o escucha no puede entender la conversación.

La criptografía, aplicada siempre en el campo militar desde los años sesenta ha conocido un espectacular incremento, motivado por la nece-

sidad de evitar el espionaje industrial, transacciones y fraudes electrónicos en el sector privado, etc.

La seguridad tiene unos niveles físicos, los que no describiré y otros electrónicos, cuyos primeros elementos son la introducción de *passwords* y claves de usuario final, que todos conocemos y los *firewalls* (cortafuegos) que evitan la introducción de virus.

Pero estas medidas son medianamente eficaces y se requiere de algoritmos matemáticos sofisticados y que se colocan en las aplicaciones o en dispositivos de entrada y salida de información.

El más popular es el desarrollado por el National Bureau of Standards y consiste en una clave de 64 bits. Pero existen otros de 128 bits como la IDEA (*International Data Encryption Algorithm*).

Las claves de los sistemas criptográficos, son según J. M. Huidobro:

- Inviolabilidad de la transformación utilizada.
- Garantizar la seguridad a pesar de que el interceptor conozca el método utilizado.
- Radicar la protección en la clave, siendo ésta además fácil de generar, almacenar, transmitir y modificar.
- Complejidad de la transformación.

El problema para España, radica en que la mayoría de los algoritmos son de muy complejo desarrollo y la verdad es que la mayoría de los Estados se han visto obligados a desarrollos conjuntos.

Así la OCDE a través de la ICCP (*Information, Computer and Communications Policy*) adoptó en el año 1992, unas guías básicas para promover una fundación que facilitara el desarrollo e implementación de mecanismos, prácticas y procedimientos para la seguridad de los sistemas de información. En Estados Unidos fue el National Institute of Standards and Technology quien adoptó sobre la base del anterior una política de seguridad para los sistemas del Gobierno de Estados Unidos.

La importancia del tema llevó en el año 1996 a la promulgación de una orden ejecutiva del presidente Clinton estableciendo la *President's Commission on Critical Infrastructure Protection*. Ésta en primer lugar identificó ocho infraestructuras que constituyen «el sistema de vida de la nación» y cuyas vulnerabilidades debían ser protegidas. Éstas son: telecomunicaciones, banca y finanzas, electricidad, gas y petróleo en distribución y almacenamiento, transporte, servicios de emergencia, y de servicios gubernamentales.

Considera una serie de escenarios y las respuestas a adoptar ante ellas como desastres naturales, errores y omisiones, *insiders*, *hackers* aficionados, actividades criminales, espionaje industrial, servicios de inteligencia exteriores, terrorismo y guerra de información.

Nuevamente en el año 1998 han actualizado a través de la Directiva PDD 63, que amplía el contenido de la anterior y en base a la cual se establece la política de exportación de tecnologías de encriptación. Es responsabilidad del Departamento de Estado garantizar el cumplimiento de esta política y concreta la necesidad de autorización del Gobierno para la exportación y con especiales cautelas para claves de 112 o 168 bis.

Lo que queda claro a través de estas diferentes disposiciones es que el tema es claramente estratégico para Estados Unidos y la mayoría de los países de la OCDE.

Como conclusión se debe afirmar que cualquier clave, algoritmo o técnica de defensa y ataque es vulnerable igualmente sólo cuestión de tiempo y desarrollo pero no existe información fiable, salvo la que se guarda en el cerebro.

Los sistemas de comunicaciones

Es necesario revisar cuales son las diferentes redes y tipos de telecomunicaciones que existen, aunque sea de manera breve y adaptándonos en gran medida a lo existente en España:

1. En cuanto a redes, la más conocida es la que utilizamos para conectarnos por teléfono, que además en gran medida es la utilizada en los hogares para acceder a Internet y otros servicios básicos de Telefónica la denominada Red Telefónica Conmutada (RTC).

Desde el punto de vista de defensa es la más vulnerable, porque es fácilmente accesible a la intrusión, la señal no va encriptada y ante un ataque es fácil dejarla fuera de servicio, con ataques clásicos a los nodos principales de comunicaciones.

Aunque como sabemos, en nuestro país existe una red paralela utilizada para la defensa, pero puede presentar las mismas debilidades, al menos teóricamente, que la de uso civil.

Las medidas que se suele emplear son el empleo de secrafonos que distorsionan llamadas y las hacen ininteligibles para quien intente

escucharlas. El inconveniente es que requieren de costosos aparatos a ambos lados de la línea que se está comunicando.

2. La segunda red de importancia en España, es Iberpac, que además fue la pionera en Europa para la transmisión en conmutación de paquetes de información, que supone el poder enviar a un coste razonable datos, no voz principalmente como en el caso de la RTC.

La red soporta una serie de protocolos como X.25 los servicios de la Red Uno de Telefónica que es una red privada «virtual», sobre Iberpac. Orienta a la transmisión de datos de grandes empresas que necesitan una red dedicada para sus datos.

La debilidad de la red es similar a la anterior, en cuanto a que existen nodos y puntos sensibles, que mediante armas clásicas puede ser inutilizada. De hecho ETA, atacó en su día la central de transmisión de datos de la red, con graves consecuencias para bancos y compañías eléctricas.

3. Ibercom, es otra red virtual para empresas, donde cada cliente de Telefónica tiene un nodo que se comunica con ésta. Aquí se proporcionan otros servicios como videoconferencia, buscapersonas, etc.

En cuanto a tecnologías de telecomunicaciones, tenemos varias que describiremos a continuación:

- Red Digital de Servicios Integrados (RDSI), que constituye un paso muy avanzado sobre la telefonía conocida, al permitir enviar voz, datos, imagen y mejor calidad de audio. Actualmente se está iniciando la puesta en marcha de la tecnología Modo de Transferencia Asíncrono (ATM) que puede soportar servicios multimedia, vídeo a la carta, o clan de televisión de alta definición. Es la red que actualmente tiene Telefónica como oferta básica de sus servicios para empresas. Por ello constituye un elemento clave para los intereses de la defensa pues como vemos es el canal apropiado para dar una larga serie de servicios de futuro.
- *Frame Relay* es una técnica para conmutar paquetes con mayor ancho de banda y facilidades para las empresas que las utilizan, siendo más rápido que el protocolo X.25. pero sin embargo, tiene limitaciones en cuanto a tiempo de respuestas requeridos en servicios con mucha transmisión de imagen.

- Para suplir esta carencia aparece la tecnología ATM, que reduce tiempos, mejora la calidad y garantiza mejor control de la red.
- DECT (*Digital Enhanced Cordless Telecommunications*) es un desarrollo europeo para interconectar voz y datos en espacios limitados (edificios, fábricas o bases) o pequeñas poblaciones.
- GSM es el estándar europeo de comunicación digital de teléfonos móviles.

Aparentemente es un sistema seguro pues requiere de tarjetas especiales y de costosos sistemas para captar sus señales, aunque realmente para cualquier servicio la escucha de los mensajes.

Desregulación y defensa en España

El proceso de liberalización de las comunicaciones en España ha llegado ya tarde y está inconcluso todavía, pero desde el punto de vista de la Defensa Nacional hay que hacer una breve reflexión sobre las ventajas e inconvenientes que la misma ha tenido.

Como inconvenientes cabe citar la práctica desaparición de la industria que giraba en torno a Telefónica que, en economía de mercado, apenas ha aguantado la competencia nacional o extranjera. La pérdida de control del Gobierno sobre un pilar básico de la economía y la seguridad de un país como era el monopolio Telefónica, ha obligado a revisar la política de adquisiciones de Defensa, que antaño solamente tenía un solo suministrador para sus redes de comunicaciones, con la ventaja de mantenimiento, y formación de técnicos.

Las ventajas son más evidentes. En primer lugar permite por la competencia disponer de una oferta más variada y tecnológicamente más avanzada en cuanto a equipos, medios de transmisión, nivel de servicio, etc.

Al disponer de diferentes compañías muchas de las cuales tienen sus propias centrales, nodos de comunicaciones y cable, se reduce las amenazas en un remoto e hipotético ataque de un país hostil o incluso de un atentado terrorista. En caso de conflicto existen diversos operadores que alternativamente podrían ofrecer sus medios.

Ha desarrollado una industria auxiliar muy competitiva en el mundo de las comunicaciones, que nos permiten acceder a tecnologías ni soñadas hace años, dada la lentitud de la puesta en marcha de la I+D de Telefónica.

Se ha producido por lo tanto una diversificación de proveedores, de los que Defensa puede elegir el más adecuado para cada una de sus necesidades sin depender de un solo proveedor, que a su vez tenía un reducido número de suministradores exteriores.

Se ha reducido la amenaza a la destrucción mediante guerra de la información a las redes de transmisión de datos o al menos a parte de ellas. Disponemos de una panoplia de tecnologías alternativas (DSI, *Frame Relay*, GSM, ATM, etc.), que garantizan una diversidad de alternativas ante amenazas potenciales.

Las comunicaciones del futuro

Una de las grandes cuestiones que se van a poner sobre la mesa en la batalla por el control de las comunicaciones en el siglo que viene, el medio físico sobre el que se enviara la información (imagen, voz y datos).

Hasta ahora hemos asistido a la puesta en marcha de servicios basados en la transmisión vía satélite (como los GPS) o en enlaces por ondas de diverso tipo de frecuencia como la telefonía móvil (GSM) o el enlace entre ciudades o puntos lejanos. La televisión y las emisoras de radio también utilizan una comunicación no física (cable). Sin embargo, esto ha tocado a su fin, apenas hay espacio para enviar tantas frecuencias y se puede, como ya ha anticipado N. Negroponte, director en el MIT, producirán colapso en lo que denominamos éter.

Los Estados necesitan reservar frecuencias para uso civil o militar y la actual explosión de servicios de comunicaciones tiene que suponer la vuelta al cable. Según este autor debemos reemplazar las comunicaciones a través del espacio para el manejo de información entre objetos que no pueden viajar por un cable de fibra óptica (aviones, barcos, coches, etc.)

La gran incógnita es el papel de Internet, que dispondrá de 1.000 millones de usuarios en todo el planeta, siendo actualmente la red de redes y que está haciendo cambiar la vida y el ocio en muchos rincones del mundo abriendo la competencia más allá de los mercados locales y nacionales. Esta competencia restará aún más el poder de los Estados que no podrán ya regular o controlar la información que circule, llegue o se emita en su país por que será imposible hacerlo.

Otra de las tecnologías emergentes es la DBS (*Direct Broadcast Satellite*) es una televisión que no requiere del cable ni de costosas plataformas de

transmisión, la primera emisora vio la luz en Estados Unidos en el año 1994 con Direct TV. Hoy podemos encontrar estos servicios con más de 200 canales en todo Europa, incluida España.

Los satélites constituyen un universo en plena expansión y de ahí deriva la preocupación de N. Negroponte. Debemos citar que existen varios tipos de satélites y funciones para los que fueron diseñados.

En función de la órbita son:

- GEO (*Geosynchronous Earth Orbit*), situados a 36.000 kilómetros son los de mayor vida útil y se caracterizan por ocupar una posición estacionaria con la Tierra.
- HEO, que operan desde los 42.000 kilómetros hasta tan sólo 500 kilómetros de distancia.
- ICO (*Medium Earth Orbit*), entre 10.000 y 20.000 kilómetros Se utilizan para GPS y para cubrir la Tierra necesita una docena de satélites.
- LEO, operan a corta distancia entre 500 y 1500 kilómetros. El mayor proyecto es el de Microsoft que colocará casi 1.000 satélites para servicios varios de telefonía celular.

Los satélites permiten el funcionamiento de dos grandes tipos de sistemas GPS, que permiten posicionar cualquier objeto que disponga el receptor-transmisor, situarse geográficamente. El sistema de satélites en el que se apoyan todos los servicios es del Gobierno de Estados Unidos, poseyendo otro Rusia, que se integrará con el norteamericano.

La otra aplicación son los sistemas de GPS combinados con los de Trunking, que permiten la conexión vía frecuencias de radio de diferentes flotas de vehículos y estaciones. Permite gestionar por ejemplo, emergencias que requieren la incorporación de variados servicios de protección civil y militar actuando como un grupo cerrado de comunicaciones. De esta forma se evita la descoordinación de medios ante crisis y catástrofes al utilizar los actores diversas tipos de frecuencias y equipos transmisión incompatibles entre sí.

Pero seguramente el mercado más potencial es el basado en cable terrestre, que supondrá otra fuente de entrada y salida de información en el mundo de las telecomunicaciones. El control de la información será en este caso, nueva fuente de preocupación para gobiernos y centros de defensa pues si sigue la concentración de medios en pocas manos, cada vez estos grupos son un elemento de presión más directo sobre los Estados.

La defensa de cualquier país se basaba en fronteras, en intereses identificables y en un control o por lo menos la oportunidad ejercerlo en caso de crisis. Esto hoy ha saltado por los aires, no hay fronteras, no hay mercados locales o regionales, sino mundiales, hay descentralización y nadie es propietario de nadie o de nada porque el mundo está tan interrelacionado que cualquier cosa puede afectar a los intereses de cualquier Estado.

LA UTILIZACIÓN DE LAS COMUNICACIONES Y SISTEMAS DE INFORMACIÓN COMO AMENAZAS A LA SEGURIDAD ACTUAL

Por RICARDO MARTÍNEZ ISIDORO

Introducción

La «agresión informática», en términos estratégicos, constituye toda una novedad como forma de dirimir las diferencias entre Estados, grupos u organizaciones. Su utilización a pequeña escala siempre ha sido posible, merced a las habilidades de ciertos talentos, que al dotarse de un ordenador han sorprendido a muchos por su capacidad para pasar barreras de protección y alcanzar los sistemas de información neurálgicos de un país u organización importantes; sus actos han sido recogidos en medios informativos, rodeándoles de una falsa apariencia de ganadores.

La utilización de la «agresión informática», repetidamente, de forma coordinada, con la finalidad de obtener ventajas que puedan ser jugadas en el plano político, económico o militar, constituye una nueva forma de agresión planificada, que cobra hoy día una importancia inesperada, cuando ciertos Estados basan su gestión general en los Sistemas de Información y Comunicaciones (CIS), y lo hacen de forma tan profusa y extendida que generan unas vulnerabilidades que no les son extrañas a los posibles agresores.

La guerra informática, la guerra de los sistemas de información, o la guerra de la información estratégica, como ha venido finalmente a conocerse, representa, sorprendentemente, el reconocimiento de una posibilidad de

agresión, basada en el estudio de las vulnerabilidades que produce el auge actual de los CIS, y en la posibilidad, comprobada, de que es posible un ataque contra la información estratégica que gestiona la infraestructura crítica de un Estado.

Si bien en el ámbito de la guerra electrónica cabe la lucha contra los efectos de una agresión tal, los nuevos agresores informáticos persiguen objetivos que se sitúan en sectores privados fundamentalmente, de difícil inclusión en una defensa global.

La edad de la información, la seguridad internacional y la Defensa Nacional

Los modernos Sistemas de Mando y Control

La pujanza de la información como recurso inestimable para la toma de decisiones, la utilización de la herramienta informática para obtenerla, procesarla y difundirla, y la expansión de todos los sistemas inimaginables de comunicaciones, como canales para llevar a distancia la información e inteligencia necesarias, son características que anidan en todo los sectores de actividad de la sociedad moderna actual.

El último tercio del siglo xx puede ser considerado como el principio de la Era de la Información, y su proyección sobre el siglo xxi no puede ser más que un incipiente efecto proyectivo, muy probablemente modificable por cualquier nuevo descubrimiento electrónico que mejore exponencialmente las actuales capacidades de los existentes.

Lo que es determinante en los sistemas actuales de información es su gran capacidad de interrelación, aspecto básico que produce su potencial y real capacidad de expansión; la tendencia a evitar obstáculos que limiten su extensión horizontal y vertical, en aras a llevar la información hasta el usuario más lejano y más humilde, es otro de los factores presentes en la problemática que se va a analizar; la globalización de las redes de información, tanto en su tratamiento, gestión así como en la temática que los ocupa, es quizás la tercera y no menos importante de esta explosión de información que se extiende hasta el lugar más recóndito del planeta, con tal de que exista una roseta telefónica, un módem y un potente ordenador.

El ámbito actual de la seguridad internacional es cada vez más complicado y el entramado relacional que es necesario erigir para intercomunicar los sistemas de mando y dirección, requieren cada vez más co-

municaciones e informática. Los soportes de las comunicaciones, satélites, fibra óptica, radioenlaces, etc., y los medios de comunicación necesarios, centrales automáticas, centrales de tránsito, sistemas de tratamiento automáticos de mensajes, etc., son a su vez gobernados y gestionados por la informática.

Las personas y organismos de los diferentes sistemas de mando y control de la seguridad internacional precisan disponer de una enorme cantidad de datos, intercomunicados en niveles, diversificados hacia los principales actores, los Estados implicados, y penetrantes en dirección a sus Fuerzas Armadas, Ministerio de Asuntos Exteriores y otros, de tal forma que se puede admitir que los principales órganos de dirección de los países miembros están imbricados en un enorme Red Extendida (WAN) que une las diferentes Redes de Área Local (LAN) de los usuarios.

La función de mando y control es una moderna función de combate cuya finalidad es proporcionar a las autoridades militares, que tienen que concebir, planificar, decidir y conducir las operaciones, los elementos necesarios para hacerlo.

Para ello cuentan con una serie de elementos, como son sus estados mayores, con misión de asesoramiento, pero además disponen de los sistemas de información para mando y control, y de las comunicaciones, aspectos que han venido a resumirse e integrarse en un concepto que de ahora en adelante conoceremos como CIS, siglas que resumen en un todo indivisible a ambos sistemas.

La función de mando y control ha sido considerada por la doctrina española del Ejército de Tierra como una función de combate, debido a su gran influencia en toda operación militar, cobrando capital importancia en las mismas. La actuación de los contendientes tratando de anular los sistemas de mando y control del oponente es considerada como prioritaria, y al conjunto de dichas acciones se ha venido a llamar guerra de mando y control.

La función de mando y control se ha convertido en una nueva forma de combate o batalla, sin soldados enfrentados directamente, pero cuyo resultado puede ser definitivo.

Los diferentes requerimientos de los Centros de Conducción de la Defensa, de los Centros de Situación de los jefes de Estado Mayor de la Defensa, y de los mandos operativos, suponen que se les asegure una mayor capacidad de compenetración entre los diferentes niveles, sur-

giendo necesidades de control político-militar y operaciones, dando lugar a los conceptos:

- Mando e Información (C1).
- Mando, Control e Información (C2I)
- Mando, Control, Comunicaciones e Información (C3I).
- Mando, Control, Comunicaciones, Computadores, Información, Vigilancia y Reconocimiento (C4ISR).

Todos ellos a través de un sistema técnico que se apoya en los CIS, interoperables en el ámbito conjunto y combinado.

Los diferentes países participantes en las coaliciones u organizaciones internacionales disponen de sistemas de mando y control con CIS interoperables, a través de pasarelas elaboradas a tal fin.

A través de ellos, y con un uso profuso de la informática, las diferentes órdenes, boletines de inteligencia, bases de datos de todo tipo, son llevados por las modernas comunicaciones a los diferentes cuarteles generales, desde el mando político de una crisis hasta el último dispositivo militar implicado en una acción.

Las modernas misiones de las Fuerzas Armadas, al servicio de lo que ha venido a llamarse, según la terminología británica, defensa diplomática, suponen también muy frecuentemente la proyección de fuerzas, su conexión con las redes de infraestructuras propias y con las del país con el que se suscriben los acuerdos correspondientes (Host Nation Support).

La interdependencia informática actual

Por ello se puede admitir que todos los sistemas de mando y control de los actores de la seguridad internacional se encuentran potencialmente enlazados, siendo gestionados por la informática tanto a nivel general del sistema operativo que los gobierna como en los elementos básicos de la red ampliada que los conforman; así las modernas centrales automáticas son verdaderos desarrollos informáticos a los que se puede acceder a distancia, incluso hasta las tarjetas, verdaderos centros neurálgicos de dichas centrales.

En un moderno sistema de comunicaciones, autopistas que unen las redes informáticas que sirven a las autoridades, las diferentes alternativas para el establecimiento de un circuito entre dos correspondientes son regidos, aleatoriamente, por verdaderos cerebros informáticos, los «muy inte-

ligentes», que saben encontrar en cada situación el camino mejor para cada comunicación.

Los centros de operación y supervisión, tanto nacionales como zonales, tienen capacidades directas de acceso a cada uno de los elementos del sistema de comunicaciones, a efectos de detectar averías o configurar, por ejemplo un nuevo enlace.

La gran interconexión vertical y horizontal que han logrado alcanzar los sistemas de información, a través del gran desarrollo de las comunicaciones, ha venido a globalizarse con la aparición de redes tipo Intranet, de contenido nacional, o del tipo Internet, que interconecta todos los sistemas de los abonados que voluntariamente acceden a ella, de forma ya prácticamente mundial.

Estos aspectos de desarrollo horizontal y vertical en el ámbito del mando y control de la seguridad y Defensa Nacional tiene, obviamente, un elemento homólogo, de enorme extensión en la vida civil, cuyas actividades básicas para la vida, confort, funcionamiento de los servicios, operaciones económicas, etc., de la población están gobernadas por la informática, se basan en la informática y utilizan comunicaciones con las mismas características que las descritas para las telecomunicaciones militares.

Tanto en el ámbito puramente económico como en el de la seguridad nacional e internacional, la versatilidad de la herramienta informática ha llevado al hombre a confiarse en sus brazos, de tal forma que las actividades complejas que hoy se realizan sería imposible reanudarlas con otras de menor potencial de gestión, no atisbándose por el momento nada que pueda sustituirlas.

La cualidad de gran necesidad de permeabilidad esférica, es otro de los aspectos clave en la ausencia de solución de continuidad entre usuarios, así como su gran intercomunicabilidad y por tanto la gran accesibilidad de unos a otros.

Estos aspectos, en un mundo de riesgos, con actores que no siempre utilizan procedimientos legales, encaminan este análisis a la presentación de un nuevo tipo de agresión, letal en algunos casos, excesivamente barata, para los rendimientos que puede obtener, sutil, por la reducida identificación del origen, y sobre todo porque atenta contra los centros neurálgicos de todos los sectores de actividad, entre los que obviamente se encuentran la seguridad y Defensa Nacional.

Un nuevo concepto de guerra electrónica

Tradicionalmente, el concepto de guerra electrónica se refiere al conjunto de medidas activas y pasivas que tienen como finalidad determinar y neutralizar los sistemas electrónicos del adversario, base de su sistema de mando y control. Así, uno de los efectos básicos de aquella era determinar el «orden de batalla» electrónico, a efecto de obtener un esquema básico de la importancia derivada de la actividad electrónica existente en cada órgano objetivo. Las actividades incluidas dentro de la guerra electrónica, inteligencia de señales (*Sigint*) con sus variantes de comunicaciones (*Comint*), señales radar (*Elint*) e imágenes (*Photing*) se combinan con la determinación del lugar origen de la radiación, merced a las modernas técnicas de la radiogoniometría, dando como resultado una gran precisión en la determinación de los centros de emisión electrónica del adversario.

La otra disciplina de la guerra electrónica, las medidas activas, tienen como finalidad la perturbación, intrusión e incluso la desinformación de los sistemas de mando y control enemigos, base de su actividad, mediante la acción sobre sus CIS.

La irrupción de los Sistemas de Información propiamente dichos y de las modernas comunicaciones, regidas y soportadas por la informática, no ha hecho más que ampliar el campo de la guerra electrónica, hacia objetivos más difíciles de proteger que antaño con los sistemas convencionales; su alta capacidad de radiación propia puede ser emulada fácilmente, descriptada e interpretada, a pesar de la progresiva mejora de las medidas para su protección (medidas Tempest).

Pero ahí no está el verdadero peligro, dado que la evolución de los métodos de prevención de las diferentes fuentes de radiación mejorará sensiblemente su impenetrabilidad a la detección y la intrusión. El verdadero riesgo estriba en la enorme accesibilidad e interconexión de los sistemas de información, de la que se ha hecho referencia en apartados anteriores, mejorada y potenciada por las excelentes comunicaciones actuales.

Estos aspectos, referidos al mando y control en Defensa, pueden perfectamente extrapolarse al ámbito civil, donde el desarrollo de estos CIS se realiza con menores requerimientos de seguridad y en el que, a través de redes globales como Internet, prácticamente se produce una interconexión total.

El peligro, y la amenaza contrastada, ha tomado una envergadura tal que se puede encontrar ya entre los nuevos riesgos de seguridad detectados y denunciados como objetivos para el próximo siglo, por el Consejo Nacional de Seguridad norteamericano, en su documento *A National Security Strategy For a New Century* (octubre, 1998).

Así, en el mismo, en su prefacio, el presidente Clinton advierte sobre la necesidad de proteger las infraestructuras críticas en territorio norteamericano e impedir las acciones que perturben la dirección de las operaciones y la utilización de las armas. Más tarde, cuando define las amenazas a los intereses de Estados Unidos, se refiere a los grupos y Estados criminales que a través de tecnologías avanzadas pueden infligir daños muy altos al país; también hace mención, claramente, a las que se basan en la utilización de informaciones sensibles mediante la penetración en sistemas de ordenadores y redes informáticas, que pueden atacar contra los CIS, esenciales para las operaciones, la economía y el Gobierno.

También, en un documento similar del Reino Unido, presentado por su ministro de Defensa, George Robertson, en su capítulo dedicado a «Las prioridades de seguridad en un mundo en evolución», la revisión de la estrategia de defensa británica se refiere a este problema actual y de futuro, indicando que el cambio tecnológico y social que se atisba para el próximo siglo tendrá un profundo efecto sobre la seguridad colectiva del Reino Unido; muchos de los desarrollos actuales, en la gama de doble uso, traerán nuevas oportunidades pero también nuevas vulnerabilidades, entre ellas, nuevas formas de combate, como la guerra de la información, entendiendo como tal a los ataques a través de los sistemas de ordenadores contra las fuerzas británicas y la sociedad civil, ámbitos que dependen ya profundamente de los citados sistemas.

Concepto de guerra de información estratégica

Las grandes potencias y en particular Estados Unidos, han tomado con gran seriedad lo que ellos denominan la guerra de información estratégica, que parte de una amenaza real de países hostiles, e incluso aliados, grupos de sofisticados delincuentes o criminales, que utilizan sus conocimientos informáticos y de telecomunicaciones para agredir a los servicios básicos, sistemas de defensa, economía, etc., tratando de obtener una victoria sobre el Estado, que no podría llegar por la vía de los instrumentos de combate tradicionales. Para ello han creado agencias espe-

cializadas, planes y autoridades *ad hoc*, que deberán determinar la amenaza y combatirla.

Concepto de guerra de información

Estado Unidos teme un «Pearl Harbour» electrónico, y lo temen porque es tal la dependencia de este país de los CIS en lo que respecta a sus Fuerzas Armadas, instituciones financieras y a la sociedad en sí, que una acción planeada muy precisamente y ejecutada por un adversario tremendamente inteligente, muy centrado en su objetivo, con los medios y nivel tecnológico suficientes, y sin un ápice de escrúpulos, podría crear un ambiente de confusión y caos de difícil recuperación.

El golpe de guerra informática, con ser dramático, parece el escenario menos dañino. Se teme más una acción continuada, con finalidad de reconocimiento y adaptación, posiblemente una guerra de guerrillas informática, que trata de obtener información sobre objetivos importantes, para combinarlos, en su momento, con acciones militares convencionales, actos de terrorismo, operaciones especiales, etc., todas convergentes, coordinadas e integradas para obtener el mayor efecto.

La finalidad lejana se asentaría en la posibilidad de que Estados Unidos perdiera su hegemonía en muchos ámbitos, lo que da a este tipo de guerra su carácter estratégico.

Se está produciendo en Estados Unidos un fenómeno que de algún modo está invirtiendo el liderazgo de la revolución informática. Si bien hace pocos años era el Gobierno americano quien dominaba el proceso de evolución del *software* y del *hardware*, en los últimos años es el sector civil quien se ha hecho cargo del «tirón» tecnológico espectacular de la informática, manteniendo un litigio legal importante con los sectores más productivos en la materia, e invirtiendo pequeñas cantidades que hacen del aparato oficial un nuevo usuario, sin gran intervención e influencia en los desarrollos tecnológicos de la informática.

En lo que respecta a las telecomunicaciones, el otro gran factor del CIS, el sector productivo y el de servicios están en una fase de completa privatización y sin apenas regulación, complicando enormemente el reto del control de la guerra de la información.

La industria de la seguridad de los CIS no evidencia un gran atractivo por los sofisticados sistemas de protección que encarecerían los ele-

mentos y que tampoco, a nivel civil, precisan de grandes complicaciones, dada la actividad económica en la que se centran. Los grandes constructores de infraestructura sensible (energía, economía y transportes) tampoco están convencidos de la necesidad de hacer frente a unos riesgos de ataque tecnológico que todavía el gobierno está lejos de perfilar y en cuya determinación no participa el todopoderoso sector privado norteamericano.

Quizás hasta este momento ha sido más interesante y justificado conocer este nuevo riesgo como guerra de información, aunque de lo que se está hablando es de un proceso hostil en el que los que combaten son los CIS, depósito y soporte de los datos necesarios para desarrollar una actividad compleja.

La guerra de información estratégica sería una nueva forma de agresión, tecnológica, llevada a cabo desde orígenes exteriores e interiores de un Estado, contra las bases de datos informáticos, *software*, a través de la penetración no autorizada en las redes de informática o mediante ataques físico electrónicos o convencionales, con la finalidad de explotar los datos del adversario, producir decepción, interrupción de servicios o destrucción de los mismos.

Los sistemas de información, como ya puede asegurarse a estas alturas del análisis, están compuestos por procedimientos, personal, organización e información tecnológica, en la que se incluye *hardware*, *software* y *firmware*, a efectos de adquirir, almacenar, gestionar, transmitir, difundir y presentar la información al usuario, incluyendo en aquél bases de datos, servicios informáticos, proceso de datos y redes de servicios, enlaces de comunicaciones y servicios de información electrónica.

Tipos de ataques en la guerra de información

Los tipos de ataques que se pueden producir pueden proceder tanto del exterior como del interior de los objetivos y se pueden resumir en algunas de las formas que se detallan a continuación:

- Ataque por medio de datos que el hipotético enemigo instala en los sistemas de información objetivo obteniendo respuestas de éste en beneficio del primero. El resultado puede ser un funcionamiento anómalo, la generación de acciones no autorizadas, perturbaciones de funcionamiento, propaganda, y lo que es más peligroso, el deterioro de los archivos básicos del sistema.

- Ataque por medio de *software*. Se distingue del anterior porque se trata de un ataque más sutil, transmitido normalmente por herramientas multimedia, como cintas o discos CD, a través de cable, fibra óptica, etc. Su comportamiento puede ser muy sofisticado, llegando incluso a generar, el *software* atacante, sus propias contramedidas cuando el sistema atacado trata de defenderse. Este, bajo su efecto, puede producir un funcionamiento diferente al diseñado por el *software* original. (Virus, puertas-trampa, por ejemplo).
- *Hacking* o *cracking*, pues si bien tienen su origen en algún programa eficiente o complementario, su utilización con fines criminales consiste en apoderarse del control de un sistema de información o de una de sus partes vitales, impidiendo su uso, facilitando el robo de datos valiosos o causando daños al sistema.
- Ataque físico directo al sistema de información o a los elementos que se integran en el mismo, incluidas las comunicaciones.

Efectos de los ataques a los sistemas de información

De los diferentes tipos de ataque típicos de la guerra de información se deducen los efectos que buscan dichas acciones, que en general pueden ser clasificadas de la forma siguiente:

- La destrucción de los sistemas de información en sí mismos, cuya ausencia perturbaría y anularía en muchos casos las actividades que gobernaban.
- La perturbación o negación del servicio que prestaba el sistema de Información. Si bien el ataque no destruye el objetivo, lo deja inoperativo o falto de la fiabilidad de funcionamiento.
- La decepción puede ser otro efecto buscado, ya que el ataque no impide que el sistema siga funcionando, pero lo hace manipulando la información, la obtención de datos y el propio análisis que realiza el sistema en su proceso.
- El ataque puede producir, en la mayoría de la ocasiones, un efecto de extracción de información o inteligencia, del propio sistema de información, o de los recursos de todo tipo, incluido los militares, a él conectados.

Realidad de los ataques y amenazas de la guerra de la información

La disposición de medios de ataque por un amplio abanico de potenciales adversarios de Estados Unidos ha llevado a sus autoridades a aumentar su dedicación al análisis de la guerra de la información; la realidad y la verosimilitud de la amenaza reside en la aceptación de los siguientes hechos:

- Aumento del acceso del público en general al mundo de las comunicaciones y de la multimedia.
- Incremento de las capacidades de la población, y de ciertas organizaciones, para la utilización de los herramientas que ofrece el mercado para vulnerar sistemas de seguridad informáticos y penetración en redes.
- Descenso acusado de los precios de estas herramientas y gran disponibilidad de las mismas.
- Disposición por personal especializado de ciertos programas de detección de vulnerabilidades informáticas asociadas a *softwares* invasivos.
- Difusión de procedimientos aplicables a la guerra de la información a través de Internet, conferencias y bibliotecas públicas.
- Multiplicación de los efectos anteriores por la vulnerabilidad de los Estados modernos, que no disponen de las defensas adecuadas. El aumento de la habilidad para trabajar en red no ha tenido el mismo desarrollo que la protección de los sistemas.
- Constatación de que, a pesar del aumento del número de ataques informáticos perpetrados, la amenaza principal está representada por aquellas intrusiones que todavía no han sido detectadas.
- La reducida concienciación de los sistemas privados de información, más atentos a proteger la confianza del cliente y el valor del accionista que a su propia seguridad, etc.

Todos estos factores concatenados han llevado a Estados Unidos a tomar muy en serio esta realidad y nueva amenaza a su seguridad.

La Agencia Nacional de Seguridad (NSA) norteamericana, encargada de analizar cualquier radiación electromagnética, capaz de servir de soporte a una agresión contra Estados Unidos, ha visto aumentar sus dedicaciones defensivas a este nuevo campo de la guerra de información, reconociendo que estos «ataques intencionados contra los sistemas críticos estaban desde hace tiempo en marcha».

El armamento de la guerra de la información, reconocen los expertos del otro lado del Atlántico, desborda la concepción de seguridad que proporciona el despliegue de las Fuerzas Armadas, y puede comprometer no sólo la eficacia de éstas, sino la propia infraestructura civil y militar.

El FBI reconoce que los ataques electrónicos del tipo que se describen están costando más de 10.000 millones de dólares al año, aunque sólo un bajo porcentaje de las empresas atacadas ponen en conocimiento sus intrusiones a las organizaciones oficiales encargadas de su neutralización.

Las estafas a través de Internet han proliferado y muy pronto las transacciones financieras utilizando esta red podrían estar llenas de trampas y señuelos.

El Pentágono también es un objetivo preferido por los piratas informáticos, cifrándose en decenas de miles por año sus ataques, a través de países terceros que camuflan los orígenes de las mismas. Los especialistas de Defensa americanos indican que, un equipo de 30 virtuosos del ordenador, estratégicamente localizados, con un presupuesto de unos 10 millones de dólares, podrían montar un ataque organizado que pondría fuera de servicio a los sistemas de información que gestionan las centrales eléctricas y todo tipo de servicios vitales, hasta los centros de control de tráfico aéreo.

En un ejercicio al efecto que se realizó a través de la Comunidad de Inteligencia Norteamericana en 1997, un equipo de una treintena de especialistas utilizaron la «herramienta» habitual de los piratas informáticos, simulando un ataque de los descritos procedente de un país de extremo oriente. El resultado, utilizando las comunicaciones disponibles, fue la desconexión de largos tramos de la red eléctrica y del sistema de mando y control del mando del Pacífico en Honolulu.

La Agencia de Defensa de los Sistemas de Información americana lanzó cerca de 40.000 ataques sobre sus propios sistemas, a efectos de comprobar sus vulnerabilidades. Sólo el 4% de los objetivos se dieron cuenta de que estaban siendo atacados, y únicamente un número ínfimo informó a la autoridad competente.

Se estima que para el año 2005, 1.000 millones de personas estará en Internet, de las cuales dos tercios no serán residentes en Estados Unidos. (Actualmente de los 120 millones de usuarios, 70 millones son americanos).

Para los encargados de velar por la seguridad, la cuestión de la supervisión se complica, dado que las capacidades de almacenamiento de los actuales sistemas informáticos han vuelto su trabajo improbable, siendo además tentados por las buenas ofertas de las empresas informáticas que se llevan los mejores talentos.

La economía criminal se ha vuelto global y se ramifica profusamente en dimensiones similares a la economía legal; para los nuevos cibercriminales es ya fácil realizar transacciones electrónicas sin fondos y edificar economías sin inventarios.

Las capacidades oficiales para obtener tecnología punta para aplicarla en la lucha están declaradas cinco a diez años con respecto a la que disponen estos criminales transnacionales. Los bajos y apretados presupuestos oficiales no llegan a conseguir, con similar rapidez, los sistemas que les permitirían luchar en pie de igualdad con estos nuevos delincuentes. A menudo, los investigadores de los organismos dedicados a perseguir estos delitos se encuentran con la sorpresa de que sus investigaciones son conocidas por los objetivos, que se cubren con nuevos ataques.

Internet se está convirtiendo en una verdadera autopista para la desinformación, dirigida a aquellos que tienen que tomar decisiones, en la que el mensaje cierto se combina, imperceptiblemente, con el manipulado, en una amalgama peligrosa.

No existe debate al respecto, ni preparación para la defensa. La nueva arma, el «ciberataque», está a disposición de más de una decena de países, con potencia similar a la norteamericana. Muchas de las prerrogativas de los Estados, que configuran la definición de su soberanía nacional, están siendo desbordadas por las posibilidades del «ciberespacio» en esta nueva revolución de la información.

Las expectativas de mejora tecnológica de la informática tienen sus puertas abiertas de par en par; los pequeños ordenadores portátiles actuales tienen hoy la velocidad de los superordenadores de hace unos años.

En definitiva, la amenaza es una realidad y se configura a través de la habilidad para acceder a redes sin autorización, para alterar datos, extraer información financiera o de la propiedad, introducir virus, etc., demostrando que la vía para una agresión de gran alcance está abierta para aquellos países tecnológicamente bien implantados.

Estas convicciones han sido recogidas en dos directivas norteamericanas sobre estrategia de seguridad nacional y militar, así como creado puestos y organismos en diferentes niveles para oponerse a esta amenaza. (Coordinador Nacional de Seguridad, Protección y Contraterrorismo y Oficina de Seguridad de la Infraestructura Crítica, ambos en el Consejo Nacional de Seguridad de Estados Unidos).

A pesar del esfuerzo realizado por el aliado atlántico, los analistas del asunto estiman que la respuesta no está adaptada a la amenaza y que el desarrollo de una estrategia de defensa contra la agresión que representa la guerra de información estratégica no ha dado más que sus pasos iniciales.

Los actores de la amenaza de guerra de información estratégica

Volviendo a recoger el concepto de guerra de información estratégica, y considerando a este como la posibilidad de sufrir ataques sistemáticos y coordinados, a través de los CIS, la guerra de la información es una amenaza del próximo siglo, como resultado de la revolución de la información y de su modo de gestión por la moderna tecnología de la informática y de las comunicaciones. El adversario, que se analiza, trataría, mediante la utilización de un ataque asimétrico, de agredir sin exponerse a la represalia de un ataque convencional, alternativa en la que no tendría opciones de éxito.

La facultad de ser actor en este nuevo tipo de guerra reside fundamentalmente en la «facilidad de penetración», ya explicada a lo largo de este análisis, que puede esgrimir cualquiera de aquéllos, junto con la dificultad, para el que se defiende, de conocer los planes de agresión, normalmente protegidos por sistemas cifrados informáticos, también disponibles a bajo coste por estos nuevos ciberagresores.

Por ello, la multiplicidad de actores puede resumirse en las categorías que se presentan:

- Estados potencialmente agresores que incluyen la guerra de información estratégica como una nueva capacidad que se suma a su potencial militar.
- La actuación contra los CIS tiene la finalidad de obtener ventajas generales para tiempo de guerra, en la inteligencia de la gran vulnerabilidad que están adquiriendo ciertos Estados en el funcionamiento de sus sectores civil y militar.

- Grupos y movimientos de carácter global y transnacional, en los que pueden incluirse los de tipo religioso, étnico, terrorista, etc., cuya ubicación geográfica no tienen en cuenta el concepto frontera.
- La adopción, por estos nuevos y desequilibrantes actores internacionales, de nuevas tecnologías, entre ellos la descrita, parece demostrada.
- Corporaciones multinacionales, cuya patria parece cada vez más desdibujada y cuyos intereses comerciales e industriales son el límite de su respeto a las reglas.
- El espionaje industrial, practicado desde hace décadas, se incluye en estas acciones y proyecta un factor más a incluir dentro del concepto de guerra de información estratégica.
- Organizaciones criminales, guiadas por intereses fuera del orden legal, que se introducen en los sistemas de información, en sus redes, a fin de obtener información, modificarla y proceder a la generación rápida de beneficios. En algunos países, con débil fuerza política, el poder de estos grupos ha llegado a suplantar al propio Estado, apropiándose de su legitimidad, mediante la utilización de sus prerrogativas.
- Las actividades financieras ilegales, las operaciones de blanqueo de dinero procedente del narcotráfico, son las más frecuentes en las que se detecta este tipo de ataques.

La respuesta a la amenaza contra los sistemas de información

La posibilidad de una guerra de información estratégica, y por lo tanto su respuesta, suscita una serie de reflexiones que se exponen, teniendo siempre en cuenta la dificultad de poner en marcha políticas efectivas para hacerles frente.

En primer lugar, será siempre difícil demostrar que se está planeando un ataque informático de carácter estratégico, dado que el hipotético enemigo, tecnológicamente muy capaz, sabrá también ocultar sus preparativos.

Ante estos aspectos, parece necesario aplicar soluciones radicales que impliquen profundamente al sector civil, no siendo suficiente las directivas iniciales al respecto si no se produce la implementación necesaria, aspecto problemático debido a la pérdida de influencia de los gobiernos para con el sector civil, en el ámbito de los sistemas de información.

La enorme extensión de la informática, a todos los niveles, y las comunicaciones que los unen, están en manos prácticamente privadas. Cual-

quier solución que se aplique debe tener en cuenta la demostración de la relación institucional de protección de esos bienes por el Estado, dado que tradicionalmente han permanecido separados.

Readaptar el objetivo empresarial del sector privado, que domina la informática, dentro de la economía global actual, va a precisar todo un esfuerzo de convencimiento e imaginación.

Los sistemas de armamento de gran presupuesto y la capacidad industrial para generarlos se vuelve prácticamente inútil ante los ataques de la guerra de información estratégica. Convendría saber y profundizar en la posibilidad de que sería necesario invertir la curva de inversiones en armamentos convencionales y quizás aplicar presupuestos mayores a la protección contra los ataques de los CIS.

Es muy posible que se precisen nuevas organizaciones y líderes que sean capaces de poner en marcha políticas eficaces que reexaminen las bases en que se apoya la seguridad nacional.

Es necesario no olvidar, como así lo reconocen los analistas americanos al respecto, que la meta de la guerra de información estratégica es la consecución de objetivos que superen los conseguidos en el campo de batalla, o a los que se alcancen en los campos político o económico. El objetivo final bien pudiera residir en alterar los liderazgos actuales en los ámbitos político, militar y económico, en especial en Estados Unidos.

También parece necesario insistir, antes de pasar a la política de respuestas, en las características fundamentales de este nuevo tipo de guerra, detectadas en un reciente estudio sobre un ataque ficticio de este tipo a Estados Unidos:

- Su bajo coste; a diferencia de los que imponen los sistemas de armas tradicionales, los medios para estos ataques no requieren una profunda financiación, sólo se precisan expertos en los CIS y el acceso a redes.
- Baja distinción de los límites geográficos entre agresor y agredido, dada la gran interacción entre ambos que existe, debido a los sistemas de información.
- La mejora substancial de las nuevas técnicas en poder del agresor puede aumentar su poder de decepción y de manipulación de actividades, complicando los esfuerzos de los gobiernos para estructurar una política de seguridad adecuada.
- El desconocimiento de este nuevo tipo de guerra complica la efectividad del ciclo de inteligencia clásico; es absolutamente necesario pro-

ceder a establecer un nuevo concepto de análisis ajustado a la guerra de información estratégica.

- Falta de adecuación de los sistemas de señales y alarmas establecido para los ataques tradicionales, no aplicables a la guerra de información estratégica.
- Dificultad para estructurar y mantener coaliciones contra este tipo de ataques, dato que la extensión de las alianzas aumentará sensiblemente las vulnerabilidades del conjunto.
- Vulnerabilidad acusada de Estados Unidos tanto en sus intereses continentales como en los de su periferia, debido a la gran conectividad existente y omnipresente en su sociedad, de gran rendimiento y tecnificación, que presenta blancos rentables a este tipo de ataques.
- En el ámbito militar, fuerzas como las de Estados Unidos depende, por ejemplo, de los servicios comerciales de transporte y de las instalaciones civiles, para su movilización y apoyo logístico. Muchas de esas facilidades de transporte, control de tráfico aéreo, etc., poseen sistemas de información específicos.
- La mayoría de las comunicaciones del Departamento de Defensa de Estados Unidos son operadas por redes comerciales.
- En muchas ocasiones, los funcionarios de Defensa no tienen prácticamente control sobre los sistemas de información utilizados en sus equipos. Estados extranjeros están, en muchos casos, en el origen de estos medios que pueden exportar con el ataque implícito en su seno.
- Estos aspectos constituyen una base de partida para el análisis de la respuesta a este tipo de ataques, que por interesar a varios sectores clave de la Defensa Nacional de un país tipo, pueden ser considerados como estratégicos.
- Algunas de las cuestiones que se plantean a continuación matizan la problemática de una respuesta, analizadas por expertos norteamericanos que tratan de esbozar los problemas concretos para evaluar la amenaza:
 - En primer lugar, la dificultad de aplicar un proceso de disuasión, tal y como es concebido para ataques convencionales o nucleares, dado que incluso con los avances técnicos actuales será muy difícil identificar al agresor, a pesar de que pueda localizarse el origen técnico, y mucho menos su origen geográfico, cultural, etc., bases para una respuesta adecuada.
 - Sin esta identificación, será imposible convocar a la opinión pública y a las fuerzas políticas, para legitimar la respuesta adecuada.

- La dificultad, siempre presente, de la identificación de la amenaza impedirá la concertación entre el sector oficial, responsable de la política de defensa contra estos ataques, y las corporaciones civiles, que a menudo sospechan de los intereses oficiales citados.

Todo ello obliga a los responsables a clarificar nuevas posturas para poder encajar la respuesta adecuada a las amenazas que se describen, muy diferentes a los que se vienen esbozando desde el final de la guerra fría, siendo uno de los grandes retos, precisamente, la modificación de las actuales doctrinas de seguridad nacional.

Los analistas que han desarrollado en Estados Unidos las simulaciones necesarias, al respecto de cómo prepararse para la guerra de información estratégica, recomiendan tener en cuenta las siguientes reflexiones:

Protagonismo del liderazgo en la respuesta a la amenaza

Se admite que la dirección superior debe residir en la Oficina Ejecutiva del presidente, en el caso de Estados Unidos. Sólo en este nivel se podría realizar una coordinación intergubernamental e interagencias responsables, dado el amplio número de organizaciones gubernamentales implicadas y que aseguraría la imprescindible vinculación con el Parlamento.

La citada Oficina Ejecutiva tendría como obligación la coordinación con el sector industrial, actor imprescindible.

Esta institucionalización del análisis y de las soluciones estaría en disposición de revisar las actuales directivas al respecto.

Análisis y asesoramiento del riesgo

La organización predeterminada anteriormente debería emitir un amplio asesoramiento sobre la extensión de la vulnerabilidad de los elementos clave de la actual seguridad nacional, estratégica y militar, de Estados Unidos ante ataques como los citados.

La determinación de objetivos, los efectos de estos ataques y los riesgos resultantes, serían los componentes de esta nueva revisión.

Participación clave de los gobiernos

Es necesario conocer el papel de los gobiernos, que deben ejercer una doble función, la de liderar los esfuerzos coordinables oficiales, y la de cooperar con el sector civil en pie de igualdad.

Deberían también mejorar ciertas funciones, como la organización, equipamiento, entrenamiento y apoyo logístico a las Fuerzas Armadas.

Finalmente, los gobiernos podrían asegurar la supervivencia de los centros de infraestructura crítica, así como animar ciertas políticas fiscales en vías a disminuir las vulnerabilidades descritas.

Enunciación de una nueva estrategia de seguridad

La preparación contra la guerra de información estratégica, una vez detectados los riesgos, debería asegurar todos aquellos objetivos a proteger, yendo desde el sector civil al militar, desde la amenaza originada desde el exterior hasta el interior, y desde el ámbito nacional hasta el local.

Una mínima infraestructura debería asegurarse a pesar de que se produzcan ataques de este tipo, aspecto que proporcionará la seguridad de funcionamiento de los CIS críticas.

Emisión de una nueva estrategia nacional militar

A pesar de que la actual estrategia militar enfatiza la capacidad de Estados Unidos para proyectar la fuerza militar a los teatros de operaciones de las regiones clave de Europa y Asia, existen nuevos teatros estratégicos que se deben tener en cuenta progresivamente:

- El teatro de operaciones tradicional.
- La líneas transoceánicas de operaciones.
- Las zonas del interior de los países aliados.
- La zona del interior de Estados Unidos.

La influencia de la distancia, en este tipo de guerra tendrá mucho menos significación y quizás será menos importante proteger los dispositivos C3I que la infraestructura nacional crítica que sirva de apoyo a las operaciones militares.

Modificar y preparar la comunidad de inteligencia para la guerra de información estratégica

El desarrollo de nuevos métodos de inteligencia y la reorganización de la comunidad de inteligencia para adaptarla al nuevo reto, a fin de hacerlos menos rígidos y menos jerárquicos, parecen medidas iniciales adecuadas.

Es imperativo, también, poseer un código de señales y alarmas para este tipo de ataques, y el camino posible parece apuntar a una cooperación importante con el sector privado.

Fomentar el reclutamiento del personal con la formación y cualidades personales para poder actuar en el campo de la detección de este tipo de agresiones, se antoja una decisión favorable a esos fines.

Conclusiones

La extensión del uso de los CIS en las actividades de la sociedad de hoy ha alcanzado un nivel de desarrollo y tecnificación tal, que países considerados como grandes potencias pueden verse especialmente sometidos a vulnerabilidades importantes, tanto más cuanto mayor es su nivel de tecnificación.

En la actualidad los CIS forman un todo único, de tal forma que la existencia de estos Sistemas no puede ser en solitario, por ello las ventajas o los defectos de uno repercuten inmediatamente en el otro.

Las condiciones de liberalización de las comunicaciones y de la informática, sus derivas hacia la total privatización, el gran fenómeno de la interrelación, la proliferación de redes por tanto, crean unas condiciones de penetrabilidad muy adecuadas para posibles agresores informáticos.

En el ámbito militar, la función de mando y control, con el apoyo de la guerra electrónica, se ha convertido en función de combate y ya se puede hablar con propiedad de guerra de mando y control. No existen grandes análisis militares sobre la amenaza de ataques contra los sistemas CIS, aunque se comienza a reaccionar, a través de la Infosec, articulando medidas para proteger la información de Defensa, siempre desde un punto de vista pasivo por el momento.

La guerra de información no parece ser una novedad entre las amenazas que gravitan contra un ejército, y puede incluirse dentro de las alternativas de la guerra electrónica.

El carácter estratégico de la guerra de información da a la herramienta constituida por los CIS un nuevo valor, tanto ofensiva como defensivamente, al tener la capacidad de actuar en teatros operacionales sino en las retaguardias.

La posibilidad de que un hipotético agresor tenga acceso a las redes informáticas que se tejen entre aliados o entre la infraestructura crítica nacional e internacional, y que pueda influir en los CIS que gobiernan dichos centros neurálgicos, es ya un hecho.

Existe un espacio dominado por los CIS, el ciberespacio, donde los más dotados técnicamente pueden utilizar sus capacidades para lograr fines criminales (cibercrímenes), terroristas (ciberterrorismo) o simplemente para conseguir una ventaja estratégica dentro de un proceso de anulación del potencial de un Estado frente a otro (guerra de información estratégica).

Los Estados muy tecnificados se podrían encontrar inermes ante una amenaza coordinada, perfectamente planificada y ejecutada sobre los puntos neurálgicos más rentables, pudiendo ver anulada la ventaja política, económica o militar que ostentaban como potencia.

Gran parte de los objetivos de la guerra de información estratégica reside en el sector privado, en expansión, falta de regulación, y difícil de coordinar para la detección de una posible amenaza de ataques de este tipo.

La reacción ante esta situación está siendo llevada a cabo por países como Estados Unidos, que estiman que a pesar de la actual concienciación puede ser tardía la respuesta.

Una buena percepción del reto a que se exponen los Estados tecnificados, las organizaciones de seguridad y defensa extremadamente entrelazadas, contemplada desde el más alto nivel, debe tener en cuenta la necesaria legislación del mayor rango, la creación de órganos *ad hoc*, la necesaria atracción de la industria y sectores privados, la edificación de un nuevo sistema de inteligencia y, posiblemente, un giro importante en la estrategia militar diseñada hasta ahora.

La percepción de estas situaciones en Estados Unidos es tan importante que es muy posible que se esté en el umbral de una propuesta norteamericana para crear las necesarias protecciones y defensas contra los ataques de la guerra de información estratégica, con las implicaciones de todo tipo, incluidas las industriales, que eso puede significar.

Bibliografía

Armees d'aujourd'hui (1998).

Cybercrime, Cyberterrorism, Cyberwarfare, Averting an Electronic Waterloo (CSIS), Washington.

Doctrina CIS OTAN.

Doctrina del Ejército de Tierra.

Proyecto de Doctrina para Mando y Control (Escuela Superior del Ejército de Tierra).

Strategic Information Warfare, a New Face of War (Rand).

CAPÍTULO CUARTO

AMENAZAS Y RIESGOS DE CARÁCTER MILITAR

AMENAZAS Y RIESGOS DE CARÁCTER MILITAR

Por GONZALO PARENTE RODRÍGUEZ

La amenaza militar en tiempo de cambio

El riesgo militar viene siendo presentado como una posibilidad teórica a medio o largo plazo, con un escenario bélico en los territorios de países europeos de la Organización del Tratado del Atlántico Norte (OTAN), caso que podría conducir a la guerra total, aunque ésta fuera defensiva. Tal posibilidad es contemplada por dos publicaciones militares de prestigio, como son: *El Libro Blanco de la Defensa*, del Reino Unido (*British Security 2010*) y *el Informe Anual Estratégico* del Instituto Nacional de Estudios Estratégicos (INNS) de Estados Unidos, de 1998.

En este ambiente, conviene comenzar por situarse en el tiempo en que vivimos. Tiempos de cambio y transición de tal importancia psicológica que, escribiendo este trabajo en el segundo milenio y siglo xx, probablemente verá la luz en los siguientes siglo y milenio.

Para Alvin Toffler (*Las guerras del futuro*, 1994; p. 19):

«Las contiendas bélicas, auténticas, potenciales e imaginarias, conforman nuestra existencia, pero existe una realidad inversa completamente olvidada. Porque nuestras vidas están modeladas también por las guerras no libradas, porque fueron evitadas por las victorias prematuras de las “antiguerras”... en su nivel más alto, las antiguerras suponen aplicaciones estratégicas del poder militar, económico e informativo para reducir la violencia asociada, tan a menudo, con un cambio en la escena mundial.»

En estos tiempos de cambio y transición, ante la posibilidad bélica grave, medianamente remota pero nunca imprevisible, podemos y debemos hacernos varias preguntas de importancia trascendente, en cuyas respuestas trataremos de reflexionar en este capítulo del estudio sobre la amenaza militar en el horizonte del año 2010:

- ¿Cuáles son los principales retos militares a la seguridad colectiva?
- ¿Cómo son los conflictos bélicos en el fin de siglo?
- ¿Qué son las organizaciones de seguridad y defensa?
- ¿Cómo puede ser la guerra del siglo XXI?
- ¿Cuáles serán las nuevas misiones de los ejércitos?

Desde el punto militar hay que reconocer que estamos viviendo una auténtica Revolución de los Asuntos Militares (RMA) en inglés, *Revolution in Military Affairs*. Es una revolución porque supone un cambio no previsto, por la influencia que los nuevos medios tecnológicos de la sociedad de la información han operado en las posibilidades de actuación de las fuerzas militares. Pero además la tecnología informática, ha coincidido en su avance, con el desarrollo enorme del empleo de los satélites en el campo de la información y con los nuevos medios de guiado de misiles. De esta forma aseguramos que se está produciendo un salto tecnológico revolucionario en el ámbito militar que indudablemente tendrá gran influencia en el futuro de la guerra.

En lo que respecta a los retos a la seguridad, se observa que la globalización, no por afectar a zonas alejadas, puede implicar riesgos menores. De esta forma podríamos preguntarnos: ¿Cuánto tiempo sobrevivirían las sociedades industriales avanzadas sin recibir productos energéticos básicos, como el petróleo o el gas? Es evidente, que el corte de las líneas de comunicación, transporte y distribución de estos recursos vitales amenazaría la supervivencia de nuestras industrias y poblaciones por tanto. Otro defecto de la globalización de la seguridad es la necesidad de aportar fuerzas militares a la comunidad internacional, en las acciones dirigidas a frenar y prevenir conflictos regionales que puedan desestabilizar zonas más amplias y poner en riesgo la paz internacional.

Por otro lado, la seguridad internacional se ve también afectada por la multiplicidad de los actores, porque el final de la guerra fría ha liberado unas 20 naciones (en la región europea), cuyos líderes buscan nuevos planteamientos para su seguridad nacional. Pero también la globalización de la información ha producido efectos sobre la seguridad, tales son: el interés por conseguir la internacionalización de los conflictos; la pugna

por alcanzar los intereses enfrentados y la entrada en acción de grupos anónimos, dispuestos a conseguir beneficios de todo tipo, aunque sea a costa de la inseguridad y desestabilización social. Tales son las acciones del terrorismo, la droga, el tráfico de armas o el crimen organizado.

Finalmente, hay que considerar como riesgos importantes a la seguridad nacional e internacional, las disputas por la libre disposición de los espacios internacionales, marítimos y aéreos, aspectos tan discutibles como la posición de satélites en el espacio exterior o el control del tráfico aéreo, cada día más congestionado. Pero no podemos olvidar, aspectos fundamentales para el futuro de la humanidad, tan importantes como los límites internacionales marítimos o las investigaciones en los aspectos submarinos y el consiguiente derecho de control de los Estados sobre ellos.

La globalización de los mercados ofrece en todo el espacio terrestre un campo más amplio de consumo mundial, de tal magnitud, que se está dibujando un panorama de competitividad económica que puede sumir a las naciones en conflictos de intereses desconocidos hasta hoy. En este ambiente, los Estados frágiles, las sociedades desorganizadas y los sectores de población marginales corren sin duda graves riesgos de desestabilización.

Esto es lo que está sucediendo en los países del Sureste Asiático. El caso de Indonesia es paradigmático como Estado frágil basado en un extenso territorio con 30.000 islas, con dificultades para ejercer la ley.

Con un enorme potencial económico, pero con grandes carencias de orden político y social que producen una continua inestabilidad interna. El caso de Timor Oriental refleja perfectamente esta situación que ha obligado a la comunidad internacional a intervenir con un contingente militar de 8.000 soldados para pacificar este territorio. Se confirma así la globalización de la seguridad internacional que se observa claramente en dos direcciones: la primera está en el ámbito del Derecho Internacional, con los esfuerzos para establecer un Tribunal Penal Internacional dedicado a juzgar las conductas criminales de líderes políticos que ignoren los derechos humanos y practiquen el genocidio; en segundo lugar, está la práctica del derecho de injerencia que supone el envío de fuerzas de paz internacionales para la ayuda humanitaria de poblaciones desvalidas. Todo ello implica una activación del empleo de unidades militares para acudir a las zonas conflictivas con capacidad de intervención.

Los conflictos del nuevo siglo

El panorama de los comienzos del siglo XXI presenta un cuadro de conflictividad compleja y de difícil diagnóstico, razón por la cual, tendremos que referirnos a tres aspectos concretos: al tiempo precursor, el ámbito geográfico y la tipología de conflictos que requieren el empleo de fuerzas militares para su solución.

Partiendo de la situación del tiempo de posguerra fría que vivimos, tenemos que referirnos a la perspectiva de los conflictos que pueden afectar a Europa o bien a la Alianza Atlántica, todo ello en un periodo de tiempo como mínimo de una década, es decir, hasta el año 2010. Pero nuestras referencias son las dos últimas décadas vividas en este siglo. Son 20 años de cambios en la geografía europea que han dejado un escenario estratégico incierto e inestable, sobre todo en el este y centro del continente. Por ello tenemos que considerar que una zona de amenaza se ha transformado en un espacio de riesgo. Para un observador atento, los conflictos no saltan sin motivos; los conflictos tienen sus raíces y sus causas, que facilitan que puedan ser abortados, prevenidos o neutralizados antes de que se produzcan.

La guerra fría llegó a esta conclusión cuando en 1992 organizó en Viena el Centro de Prevención de Conflictos, dependiente de la entonces Conferencia sobre Seguridad y Cooperación en Europa (CSCE) —hoy Organización para la Seguridad y Cooperación en Europa (OSCE)—. En aquellos tiempos se vivía bajo el influjo del «Fin de la Historia», de Francis Fukuyama que muchos identificaron con el «fin de la guerra» que ya había sido desmentida por la emergencia de dos conflictos sangrientos, el del Golfo y el de Bosnia.

Respecto al ámbito geográfico tendremos que señalar que la conflictividad europea está orientada hacia el Este y el Sur, donde chocan las diferentes civilizaciones que han pugnado en suelo europeo por el dominio y hegemonía de los espacios estratégicos. Señalaba el profesor Huntington, de la Universidad de Harvard, que los conflictos del futuro tendrán bases fundamentales etnográficas, ideológicas y económicas, que producirán choques entre las civilizaciones supervivientes, en las grandes fallas cuyas trazas están precisamente en el sur y este europeos.

El choque de las civilizaciones que señala Huntington será el gran argumento para explicar las grandes líneas de la política internacional. De esta forma, las diferentes civilizaciones —en grande— y las diversas culturas

—en pequeño—, parece que saltan a la arena del conflicto para defender sus raíces, atemorizadas por la ola de globalización que avanza inexorable sobre la humanidad. Así, los choques etnográficos van a originar muchos conflictos en las zonas que localizan los intereses históricos, sean éstos, eslavos, islámicos o los occidentales latino-sajones.

La explosión geopolítica que ha transformado Europa en este fin de siglo ha tenido repercusiones en todo el ámbito internacional y dado pase, en el conflicto general Este-Oeste, a la multiplicación de los conflictos bélicos, la mayoría de carácter internacional. Si tratamos de esbozar una tipología del conflicto, podemos recurrir a Mariano Aguirre, con la siguiente división de los conflictos complejos.

Las raíces de los conflictos son muy variadas. Conquistar el poder político o territorio son causas evidentes, pero la guerra de fin de siglo es compleja en sus razones, manifestaciones y legitimaciones. Según Michael Klare, de Amherst University:

- Conflictos regionales de potencias regionales en claro ascenso.
- Guerras por recursos naturales, por ejemplo, el agua, el petróleo, minerales estratégicos, etc.
- Conflictos separatistas y nacionalistas, con grupos étnicos que pretenden tener su propio Estado.
- Conflictos irredentistas por grupos que tratan de extender sus fronteras para abarcar territorios donde habitan comunidades afines.
- Luchas étnicas, religiosas o fundamentalistas que tratan de ganar influencia y poder dentro del mismo Estado.
- Guerras revolucionarias que tratan de imponer su ideología política en el suyo o en otros países de la misma región.
- Luchas a favor de la democracia, el anticolonialismo, y las reivindicaciones indígenas.

A pesar de que los conflictos del entorno europeo de fin de siglo se inscriben en un contexto más regional y focalizado en los intereses de los Estados, se ha demostrado su situación en el escenario internacional, las luchas se han demostrado extremadamente violentas con la población civil. Según Pierre Garcin, periodista francés de prestigio internacional: las dinámicas grupusculares (que influyen y radicalizan la lucha), de identidad (que buscan sus raíces culturales), comunitarias (que buscan la unidad de sus grupos), nacionalistas (con el espíritu de conquista colectiva), autonomistas (veleidad equívoca de la soberanía), independentistas (con

ambiciones políticas declaradas). Estas aspiraciones se apoyan en las reivindicaciones territoriales la mayoría de las veces.

La violencia desatada en los conflictos actuales, no se debe sólo a la ferocidad de los combatientes, muchas veces guerrilleros jóvenes, pueblos embarcados en luchas atávicas como los sudaneses, eritreos, ruandeses o afganos. También hay situaciones de conflictos más próximos que demandan una solución política interior, como el caso de Argelia, o exterior, como sucede con la población saharui que todavía no ha alcanzado su estatus político.

Los Estados desorganizados se prestan a una conflictividad de aspectos irregulares y de difícil control. Fue Butros Gali quien señaló que los conflictos actuales implican no sólo a los ejércitos regulares, sino también a paramilitares, milicias y civiles armados que practican una guerra totalmente irregular, en la cual la mayoría de las víctimas son civiles. En la Segunda Guerra Mundial, el 50% de las víctimas eran civiles, ahora esta cifra llega al 90%.

Son estas guerras civiles mucho más cruentas, porque el mercado de armas se vuelca en ventas de toda clase, generalmente con armamentos de segunda mano. No funcionan las autoridades que no protegen a la población, a la que muchas veces son los primeros en masacrar, para llamar la atención internacional. Así surge el bandolerismo y el caos en este tipo de naciones que se debaten en la anarquía, mientras que columnas de refugiados huyen de sus propios conciudadanos.

Las organizaciones europeas de seguridad y defensa

El escenario europeo, donde se han librado dos guerras mundiales en este siglo y en el cual ha habido el mayor despliegue de fuerzas nunca conocido, ha quedado con el fin de la guerra fría, jalonado por una serie de organizaciones que se ocupan de la seguridad y defensa en distinta medida y modo. Así, la Organización de Naciones Unidas (ONU), la OSCE, la OTAN y la Unión Europea-Unión Europea Occidental (UEO), ofrecen diversas capacidades para contribuir a las misiones de paz, crisis o guerra, en aplicación de la doctrina expuesta en la Agenda para la Paz, de Butros Gali. Pero también la OSCE (antes CSCE) ha contribuido a la paz y seguridad europea con la doctrina basada en los principios de Acta de Helsinki que entre los años 1975 y 1990 sirvió para neutralizar las amenazas de la guerra fría. Por su parte, las dos Organizaciones defensivas

(OTAN, UEO) han contribuido a la seguridad europea, a través de la defensa colectiva.

Si en tiempos de la guerra fría, la ONU no tuvo capacidad alguna para intervenir los conflictos bélicos, porque el Consejo de Seguridad estaba bloqueado, a causa del veto de las potencias mayores que se alineaban de la cooperación entre naciones para ejercer acciones pacificadoras. En los conflictos que se están produciendo en esta década, como es el caso de la antigua Yugoslavia, el Consejo de Seguridad ha emitido sucesivos mandatos que facilitaron la intervención de las fuerzas de la comunidad internacional. Pero si entre los años 1991 y 1995 no hubo problemas con el veto de las grandes potencias, posteriormente en el conflicto de Kosovo, Rusia y China han adoptado actitudes distintas que han dificultado las posibilidades de actuación de las naciones occidentales que no encontraron el respaldo para las operaciones aéreas de castigo a Serbia.

Este cambio de postura de las potencias orientales pudiera ser debido al reforzamiento del eje ruso-chino, posiblemente provocado por la ampliación de la OTAN hacia el Este, incluyendo en la Alianza Atlántica a países del antiguo Pacto de Varsovia. Pero no debemos olvidar el precedente de la guerra de Corea (1950) cuando ante el veto soviético en el Consejo de Seguridad, se acudió a la Asamblea General para conseguir la autorización del uso de la fuerza, cosa que fue posible. Esta cuestión volvió a ser repetida en el año 1954, en el conflicto de Suez, por el veto de Francia y Gran Bretaña.

Es evidente que ante la multiplicación de conflictos que padece la humanidad en el fin de siglo, la ONU se muestra incapaz de acudir a todos ellos con la misma intensidad. Por ello parece lógico, y así lo ha anunciado el secretario general que descansará en las organizaciones de seguridad, de carácter regional como la OSCE. Precisamente a esta Organización se han ofrecido tanto la OTAN como la UEO para cumplir misiones de pacificación de conflictos.

La OSCE goza de amplia experiencia en el ámbito político y diplomático para las negociaciones de paz, ha participado en los conflictos de Chechenia, Bosnia y Kosovo, con el envío de observadores militares que los bandos beligerantes han respetado como representantes de una organización neutral. Pero su actuación se mueve en todo caso en el ámbito de la negociación y mediación para alcanzar las condiciones del alto el fuego o tregua que faciliten la iniciación de un proceso de paz.

Cuando una agresión en curso o inminente, haga necesaria la intervención de las fuerzas previstas en el artículo 43 de la Carta de Naciones Unidas, tendrán por misión lograr el alto el fuego y mantenerlo. Las acciones militares contarán con la capacidad de imponer la paz, con unidades que serán proporcionadas por los Estados miembros, con militares voluntarios. Para ello se necesita un mando del Consejo de Seguridad que requiera la imposición de la paz primero y sea capaz de mantenerla después.

Pero la seguridad europea tiene una mayor referencia a los asuntos político-militares en los principios rectores y valores comunes del Acta Final de Helsinki, la Carta de París y el Documento Final de Helsinki, de 1992. En ellos, los Estados firmantes reconocen la seguridad de cada uno de ellos está vinculada a la de todos los demás.

La función de la OSCE, respetando la igualdad soberana de todos los Estados, es promover las relaciones en materia de seguridad por la cooperación europea y transatlántica, con iniciativas laterales y multilaterales. Es por ello que esta Organización encauza las medidas de solidaridad internacional en el ámbito europeo ante una amenaza que pueda afectar a la estabilidad regional. Los documentos señalados en el párrafo anterior, incluyen el compromiso de no recurrir a la amenaza o el uso de la fuerza contra la integridad territorial o la independencia política de cualquier Estado, o de cualquier otra forma de agresión incompatible con lo expresado en la Carta de Naciones Unidas. Sin embargo, se reconoce el derecho a la legítima defensa individual o colectiva, así como a pertenecer a las organizaciones de seguridad conforme a sus intereses nacionales.

Las dos organizaciones internacionales que en el ámbito europeo son capaces de proporcionar fuerzas para operaciones de paz o de guerra, son la OTAN y la UEO, en mayor o menor medida. Ellas recogen la necesidad de aportar unidades de los países miembros, previstas en la UEO desde la reunión de Petersberg en el año 1992, según que Estados Unidos quiera o no participar en este tipo de operaciones de paz, que en su caso podrían tener que utilizar los medios que le proporcione la Alianza. Para este evento se diseñó el concepto de empleo de fuerzas conjunto-combinadas en la Cumbre de Bruselas de 1994, y dejó establecida la posibilidad de que estas unidades multinacionales pudieran ser empleadas por la UEO bajo mando europeo.

El Nuevo Concepto Estratégico aprobado en Washington el pasado 24 de abril, con ocasión del quincuagésimo aniversario de la Alianza Atlántica,

comprende unos principios de actuación de la OTAN que no resultan tan nuevos, puesto que todos ellos estaban siendo considerados anteriormente.

Las cuestiones que revisten esta relativa novedad se pueden reducir a cuatro: las intervenciones aliadas que responden a las misiones «no-artículo 5», la Identidad Europea de Seguridad y Defensa (IESD); el «diálogo mediterráneo» y los riesgos no militares de la seguridad.

Las misiones «no artículo 5» contemplan la posibilidad de afrontar conflictos tipo crisis que puedan afectar a la seguridad de los países miembros, por la posible inestabilidad de la región euroatlántica.

La IESD tuvo su respaldo definitivo en la Cumbre de Madrid, en julio de 1997, en la que la OTAN aceptó que la UEO pudiera preparar y conducir ciertas operaciones bajo mando europeo, utilizando el mecanismo de Fuerzas Operativas Conjunto-Combinadas (FOCC). Esto significaría que en una crisis de interés exclusivo europeo, la OTAN descargaría la responsabilidad en la UEO, pero utilizando los medios de mando, apoyo y control de la Alianza.

El «diálogo mediterráneo» conlleva el reconocimiento de que la seguridad europea está ligada a la estabilidad del área mediterránea, lo que se pretende conseguir fomentando medidas de cooperación política y militar. Estas líneas de acción se han venido desarrollando en forma bilateral con Israel, Jordania, Egipto, Túnez y Mauritania, desde el año 1995.

Finalmente, el Nuevo Concepto Estratégico de la OTAN contempla factores de carácter no militar pero que afectan a la seguridad de la Alianza Atlántica. Por ello señala especialmente contramedidas para neutralizar los riesgos que provengan del terrorismo, el crimen organizado, las crisis de recursos estratégicos y los movimientos masivos de población.

El nuevo papel de las Fuerzas Armadas

No cabe duda que las misiones que vayan a asumir los ejércitos en la primera década del siglo XXI dependerá de varias premisas y factores sobre lo que haremos unas reflexiones básicas que sirvan para establecer unas conclusiones, como respuesta a cual será el nuevo papel de las Fuerzas Armadas.

Premisas

1. Que nos vamos a referir a los ejércitos del ámbito occidental, sin especificar, nación o tipo de unidad terrestre, naval o aérea.
2. Que las predicciones deben basarse en términos reales, sin aventurar confusiones de aplicaciones tecnológicas superavanzadas.
3. Que las Fuerzas Armadas en los países democráticos se ven sometidas al influjo de la opinión pública, que se preocupa más por las operaciones de paz y no presta demasiada atención a los temas de seguridad y defensa.

Factores

Teniendo en cuenta estas premisas, podemos considerar que los temas de la defensa se ven sometidos a cierto margen de factores imponderables, dependientes de los programas políticos y de las circunstancias estratégicas ambientales, que en los tiempos actuales son cambiantes.

Debemos reconocer los riesgos que supone la tarea de predecir el futuro, aunque sea a corto plazo. Nos limitaremos por ello a reconocer las tendencias factoriales referidas a los factores más influyentes.

LOS FACTORES TECNOLÓGICOS

La sociedad de comunicación está viviendo una revolución tecnológica que también afecta a los ejércitos. Éstos se ven en la necesidad de incorporar los avances tecnológicos a la organización militar, lo que supone que a su vez cambios de doctrina.

Los principales sistemas de nuevas tecnologías militares afectan a las áreas de: la información, de comunicación, de Procesado de Datos en Forma Automática (ADP), la vigilancia de los teatros de operaciones de tiempo real, por la utilización de satélites; la aplicación de las tecnologías *stealth* que dan capacidad de no detección de radar y la inclusión de las Municiones de Guiado de Precisión (PGM) que han mejorado la capacidad de hacer blancos más efectivos. En general, las tecnologías que van a tener gran repercusión en la ciencia militar, por su desarrollo en la sociedad civil son aquellas que se refieren a las áreas de información y la comunicación.

LOS FACTORES ECONÓMICOS

Las dificultades presupuestarias de la defensa provienen de que la opinión pública no ve la necesidad de mantener las fuerzas militar en su nivel

óptimo, porque no sienten amenazas reales, y el aumento de los costes, tanto en personal como en material, y la modernización para adaptarse a las nuevas tecnologías requiere enormes gastos.

Ante esta situación presupuestaria de la defensa, los responsables tienen que enfrentarse al dilema de la elección equilibrada entre las necesidades de la organización militar y las disponibilidades económicas. Esta problemática se presenta como asignación de grandes prioridades: personal o material, nacional o extranjero, tierra, mar o aire, cantidad o calidad, convencional o especial.

La aplicación presupuestaria de la defensa constituye un problema de hondo calado político, por la necesidad de atender a los compromisos internacionales, por el prestigio que supone la actuación nacional en el exterior y la necesidad de mantener una Defensa Nacional eficaz.

LOS FACTORES HUMANOS

La problemática de personal para cubrir las plantillas de la defensa, se complica a medida que aumentan las exigencias de la selección, formación y promoción de los militares.

Las necesidades de la alta especialización militar requiere que la motivación del personal sea recompensada con el reconocimiento moral y material. En caso contrario, será muy difícil evitar los traspasos de personal a mejores posiciones de la vida civil, en todas las escalas de tropa, suboficiales u oficiales.

Esta problemática de personal está siendo afrontada en muchos países con el empleo de personas civiles en aquellos puestos que no requieran una práctica militar estricta. También se palián los problemas de personal con un mayor empleo de las reservas bien organizadas y dotadas.

LOS FACTORES POLÍTICOS

La política de defensa tiene hondas repercusiones en los ámbitos nacional e internacional, si bien hay que reconocer que en los tiempos que vivimos, ambos conceptos están cada vez más entrelazados, hasta el punto que llegan a confundirse. En este sentido, podemos referirnos a una serie de interrogantes que tendrán que ser resueltos en los próximos años:

— ¿Cuál será el futuro peso europeo en la estructura militar de la Alianza Atlántica?

- ¿Llegará en algún momento a tener la Unión Europea una organización eficaz de la defensa?
- ¿Conseguirá mantenerse la actual situación nacional de los conflictos periféricos por mucho tiempo?
- ¿Persistirá la tendencia al empleo de fuerzas multinacionales o se volverá a renacionalizar la defensa?

Conclusiones sobre las nuevas misiones de los ejércitos

Las Fuerzas Armadas del siglo XXI serán —evidentemente— durante la primera década, las mismas que existen en la actualidad, sometidas a los lógicos cambios reestructuraciones y modernizaciones que se están verificando en los ejércitos para adaptarlos a la nueva situación internacional que vivimos.

En función de las premisas y el desarrollo de factores que hemos visto anteriormente, podemos establecer que las nuevas misiones de los ejércitos, no son tan nuevas, pero se observan las tendencias siguientes:

- Estarán influenciadas por la evolución del proceso de Unión Europea que se verá obligado a prestar mayor atención a los temas de defensa y seguridad, y asumir mayores responsabilidades en el empleo de la fuerza.
- En función de esta previsión política los efectivos militares de las naciones europeas prestarán mayor atención a la cooperación internacional, lo cual exige una alta cualificación de idiomas, tecnología y motivación.
- Los ejércitos que van a cooperar con unidades de países de un alto desarrollo tecnológico, requieren un esfuerzo para ponerse a nivel y por ello, tendrán que especializarse en campos a los cuales puedan acceder con mayor facilidad.
- En general, las nuevas tendencias de las misiones militares irán dirigidas a:
 - Mantener la vigilancia de los espacios de interés nacional o internacional, para facilitar información a los responsables, políticos y militares.
 - Obtener una capacidad de movilidad estratégica de larga distancia y táctica en el campo operacional.
 - Alcanzar un nivel tecnológico apropiado a los nuevos sistemas de armas, de alta precisión y potencia.
 - Organizar el apoyo logístico de abastecimiento y mantenimiento y reposiciones de personal y material, con previsiones de operaciones de altos consumos.

Dotar a las fuerzas de una mentalidad expedicionaria y capacidad de proyección.

La guerra en el siglo XXI

Para contribuir con una reflexión al tema de este estudio, comenzaremos por hacernos tres preguntas:

1. ¿Qué tipo de conflicto bélico es previsible?
2. ¿Cuáles han de ser las respuestas que deben prepararse en el ámbito de la defensa?
3. ¿Continúa siendo válido el concepto de guerra que expuso Clausewitz?

Para contestar a las dos primeras preguntas he consultado tres informes de procedencia norteamericana, británica y española que señalo en las referencias bibliográficas; he procurado mantener mis observaciones en el nivel operacional, conjunto-combinado pues no se puede concebir que se preparen operaciones de un solo ejército en un conflicto, con exclusión de los otros, y sin contar con los apoyos de los órganos conjuntos de la defensa, sean de inteligencia, apoyo logístico o de Estado Mayor.

Pero comencemos por la tercera pregunta. El famoso estratega alemán considera la guerra como un acto de fuerza para imponer la voluntad al contrario y también, que la guerra es siempre un acto político. Estas dos afirmaciones son rigurosamente ciertas, a pesar de los cambios que se han producido en la humanidad; no obstante los avances que se observan en las relaciones internacionales y en los desarrollos tecnológicos que han hecho del mundo el espacio interrelacionado en que vivimos, es evidente que la guerra como expresión última del conflicto violento, sigue siendo posible, aunque cada vez menos probable, como guerra declarada entre Estados.

Dada la enorme capacidad destructiva que caracteriza el potencial militar actual, con la capacidad de alcanzar el umbral nuclear, hace que la guerra total tenga niveles de contención máximos, ya que el rechazo a la guerra nuclear es opinión generalizada y los líderes políticos no están dispuestos a asumir los riesgos de este tipo de guerra sin el apoyo popular.

Esta condición ha hecho que el valor de la disuasión haya disminuido notablemente y así, sólo se pueden producir enfrentamientos bélicos en el ámbito convencional, aunque intervengan potencias nucleares, aún en el caso tan extremo como es el conflicto de India-Pakistán o los casos de Irak con Estados Unidos o de Rusia con Chechenia.

El conflicto de Kosovo, nos confirma lo anterior, y que para imponer la voluntad al contrario, se puede intentar no tener que llegar al combate terrestre, aunque éste deberá estar preparado y asumido como un empeño mayor, con los riesgos que ello implica. Pero tales casos pueden conducir a que, mediante la aceptación de condiciones impuestas, se llegue a obtener una prolongación del conflicto que favorece al perdedor, que empleará la estrategia de ganar tiempo, en espera de que condiciones más favorables.

La campaña de Kosovo se nos muestra como la confirmación de lo que fue la llamada guerra del Golfo contra Irak entre una gran fuerza expedicionaria de medio millón de soldados (1991) y un gran ejército nacional desplegado en defensiva con 22 divisiones. La superioridad tecnológica proporciona una ventaja estratégica que facilita la capacidad de conseguir la iniciativa, factor fundamental para conducir las operaciones hasta el final.

Sin caer en fáciles triunfalismos o derrotismos que han llenado páginas, después del fin de los bombardeos que doblegaron la voluntad de Milosevic, podemos reflexionar sobre esta estrategia aliada, basada en conjunción de esfuerzos multinacionales, apoyados en una enorme superioridad tecnológica. Mientras que la otra parte no le queda más estrategia que la defensa a ultranza, con una postura victimista para resistir el castigo, a la vez que trata de conseguir apoyos de la opinión pública internacional mostrando sus sufrimientos. Mientras tanto reserva sus fuerzas que al final servirán para seguir manteniéndose en el poder.

En el teatro de operaciones de Kosovo se emplearon con el esfuerzo principal los medios aéreos de ataque y bombardeo de largo alcance, los aviones B-52, B-1 y B-2 que lanzaron bombas guiadas JDAM (*Joint Direct Attack Munition*) y compitiendo con los misiles *Tomahawk* lanzados desde plataformas navales. Dos armas que comparadas en efectividad arrojan resultados parecidos, ambas produjeron Efectos No Deseados (END), también llamados «errores colaterales», con el leguaje políticamente correcto del tiempo en que vivimos. Pero la cuestión económica pone mucha ventaja en el platillo de las bombas, pues mientras que éstas cuestan tres millones de pesetas por unidad, los misiles valen 160 millones. (*Revista de Enseñanza de Defensa* números 137/138). Por otro lado está claro que la aviación requiere superioridad aérea en la zona, mientras que el despliegue naval es más seguro. Además, en Kosovo, lo mismo que en Bosnia fueron utilizados con profusión los avio-

nes estacionados en la base de Aviano, F-16 y F-18 entre otros que rindieron al máximo en la batalla aérea. El propio general Lombo (jefe del Estado Mayor del Ejército del Aire) señalaba las ventajas del empleo de poder aéreo en esta campaña (*Revista Española de Defensa*, mayo 1999): 32.000 salidas sin una sola baja propia; 40.000 armas lanzadas de las que sólo 15 produjeron END.

Sin embargo, no debemos pasar por alto que las fases de la guerra requieren la ocupación de fuerzas terrestres y navales, pues en otro caso, como ocurrió en Irak, los conflictos permanecen latentes y en cualquier momento pueden volver a abrirse, porque fueron cerrados en falso.

La guerra continúa siendo una cuestión de intereses por los que se lucha, siempre que existan posibilidades de alcanzarlos. Pero los políticos tienen claro cuando hay que abandonar la lucha y empezar las negociaciones. Por eso, todos los países refuerzan sus defensas con alianzas, aunque éstas nunca van a substituir sus condiciones defensivas nacionales. La seguridad nacional se vincula así con la seguridad exterior y por eso, cuando se produce un conflicto, se internacionaliza rápidamente.

La guerra del siglo XXI aparece así ubicua y compleja, pero ya podemos entrever, por los datos de los conflictos de fin de siglo, como serán los de la primera década del 2000 en sus ámbitos político, estratégico, operacional y técnico. También Clausewitz nos advirtió que:

«Cada tiempo tiene su forma peculiar de guerra... cuando uno tendrá también su propia teoría de la guerra... y quienes deseen entender la guerra tienen que dirigir su mirada atenta a los rasgos de la época en que se vive.»

Pero cada vez está más claro que la guerra ya no produce entre las sociedades industriales avanzadas; más bien se pueden esperar los conflictos bélicos en las naciones de otros niveles de desarrollo. Se están produciendo los conflictos bélicos periféricos en las naciones subdesarrolladas o bien en países en vías de desarrollo. Son guerras civiles entre facciones internas de los países del Segundo y Tercer Mundo. Pero hay que contar siempre que las intervenciones humanitarias o interesadas del Primer Mundo en forma de coaliciones.

Recién acabada la guerra fría, cuando aún sonaban los clarines triunfalistas de quien proclamaban el «Fin de la Historia», volvieron a tronar los cañones en las arenas rojas del desierto árabe, cuando en el año 1990 Irak invadió Kuwait.

La crisis del Golfo desató una nueva forma de guerra que nos va a servir de modelo, aunque aún con unas condiciones distintas, la intervención se ha vuelto a repetir en el conflicto yugoslavo. El empleo del poder aéreo masivo para «ablandar» la voluntad del adversario, mientras se organiza la concentración para una intervención terrestre, se mantiene un bloqueo marítimo y se ofrecen condiciones a la negociación diplomática.

Al adversario sólo le queda, ante la superioridad aplastante de lo que se le viene encima, adoptar la estrategia defensiva y resistir los golpes fríos y calculados que sistemáticamente le van destruyendo sus defensas militares y políticas. Pone su esperanza en ganar la compasión de la opinión pública internacional adoptando la postura victimista y proclamando la dureza del castigo.

Junto a estos conflictos periféricos, podemos esperar que se produzca otro tipo de guerra ubicua y oscura sin frentes claros, es la guerra que discurre por las alcantarillas del poder político y económico y se libra de muchas formas que no llegan al gran público. Es la guerra que utiliza la inteligencia para conocer las tramas terroristas, de la droga o de la delincuencia organizada, para llevar hasta los centros de mando y desorganizar sus planes y objetivos. Por eso de vez en cuando, sorprenden reacciones de aplicación del poder militar contundente, que tratan de demostrar una determinación de represalia, como fueron los casos de bombardeos americanos sobre Sudán y Afganistán, después de la destrucción de sus embajadas en Tanzania y Kenia, con 263 muertos.

En la guerra ubicua, no declarada, unos ponen bombas para demostrar su poder y capacidad, mientras que los otros con lo que Raimon Aaron llamó «la sorpresa tecnológica», son operaciones de baja intensidad que requieren tiempo y momento oportunos, precisión matemática y apoyo logístico. Por ello, este tipo de operaciones tienen que estar basadas en una preparación exhaustiva y un conocimiento preciso de la situación.

Bibliografía

- AGUIRRE, M.: «Los conflictos a fin de siglo», *Le Monde Diplomatique*. París, mayo 1999.
- ALVIN T.: *Las guerras del futuro*. Edición Plaza y Janes. Madrid, 1994.
- GARCI, T.: «Los nuevos conflictos armados», *Defence Nationale*. París, 1998.
- Informe Anual Estratégico del INNS*. Washington, 1998.
- Libro Blanco de la Defensa*. Reino Unido, 1998.

Revista Española de Defensa. Mayo, junio y julio 1999.

VAN RIPER, P.: «La guerra en el siglo XXI», *Parameters*. Otoño 1997.

VON CLAUSEWITZ, C.: *De la guerra*. Ediciones Ejército. Madrid, 1978.

COMPOSICIÓN DEL GRUPO DE TRABAJO

- Presidente:* D. DARÍO VALCÁRCEL LEZCANO
Director de la Revista Política Exterior.
- Coordinador y secretario* D. JOSÉ M.^a SANTÉ RODRÍGUEZ
Capitán de navío (G).
- Vocales:*
- D. DIONISIO GARCÍA FLÓREZ
Doctor en Relaciones Internacionales.
 - D. VICENTE GARRIDO REBOLLEDO
Doctor en Ciencias Políticas y Sociología.
 - D. ALEJANDRO KLECKER DE ELIZALDE
Licenciado en Ciencias Políticas y de la Administración.
 - D. RICARDO MARTÍNEZ ISIDORO
General de brigada del Ejército de Tierra (DEM).
 - D. JESÚS A. NÚÑEZ VILLAVERDE
Licenciado en Ciencias Económicas y Empresariales.
 - D. GONZALO PARENTE RODRÍGUEZ
Coronel de Infantería de Marina (DEM)
Profesor emérito del CESEDEN.

Las ideas contenidas en este trabajo son de responsabilidad de sus autores, sin que refleje, necesariamente, el pensamiento del CESEDEN, que que patrocina su publicación.

ABSTRACT

The subject developed within the present essay has become extremely interesting since it covers three main security risks when we are proceeding towards the new Century. These risks include the social and political instability posed by massive migratory flows, the illegal arms and information systems trafficking as well as the threats and risks of proper military character.

The end of the Cold War has produced a new perspective within the international relations theories. Also, other phenomena detected before, like those included in this essay, appear now under a new prism stressing the emphasis in the need of a more global and interdisciplinary approach to problems as the best way to manage multidimensional processes, as is the case of national and international security ambiances.

A new set of social, economic and political elements has been added to the traditional approaches, which were strictly focused in analysing military power of states or alliances in past times. This new approach must be taken into account as an essential part of the security planning, which requires the participation of experts who were perceived as outsiders before.

ÍNDICE

	<u>Página</u>
SUMARIO.....	7
INTRODUCCIÓN.....	9
<i>Capítulo primero</i>	
TRÁFICOS ILÍCITOS DE ARMAS	15
• TRÁFICOS ILÍCITOS DE ARMAS: ARMAMENTO CONVENCIONAL	17
Introducción.....	17
— <i>Tráfico de armas y crimen organizado en el nuevo concepto de seguridad</i>	17
— <i>Las armas ligeras y sus problemas</i>	19
Tráfico de armas	21
— <i>Historia</i>	21
— <i>Funcionamiento del tráfico de armas</i>	22
— <i>Lazos entre las transferencias legales e ilegales de armas</i>	27
Arsenal de Europa Oriental: controlando los flujos de armas a zonas de conflictos.....	28
Soluciones	30
— <i>Organización de Naciones Unidas (ONU)</i>	31
— <i>El Grupo de los ocho (G-8)</i>	32
— <i>Unión Europea</i>	33
— <i>Organización de Estados Americanos (OEA)</i>	35

— OTAN-Organización para la Seguridad y Cooperación en Europa (OSCE)	36
Conclusiones	39
— <i>Munición y conflicto armado</i>	40
— <i>Recomendaciones</i>	41
• ARMAMENTO NUCLEAR, QUÍMICO Y BIOLÓGICO	43
Algunos problemas relacionados con el control de las armas de destrucción masiva	43
Breve clasificación de las armas químicas y biológicas y de sus efectos.	49
— <i>Armas químicas</i>	50
— <i>Armas biológicas</i>	52
Proliferación de armas NBQ y tráfico ilícito de materiales nucleares y agentes químicos y biológicos.	55
Medidas políticas y diplomáticas para controlar los tráfico ilícitos de armamento NBQ y las transferencias de productos y tecnologías de doble uso	57
— <i>Controles con base convencional: tratados internacionales y medidas de verificación</i>	58
— <i>Foros internacionales de control de comercio exterior de productos y tecnologías de doble uso</i>	65
— <i>Políticas de control adoptadas en el seno de organizaciones internacionales</i>	70
— <i>Políticas nacionales para controlar los tráfico ilícitos de armamentos de destrucción masiva y productos y tecnologías de doble uso</i>	73
Conclusiones	75
• TRÁFICO DE MISILES Y DE TECNOLOGÍAS EN EL MARCO DE UN NUEVO CONCEPTO DE SEGURIDAD.	77
El tráfico de misiles y de tecnología como factor de inestabilidad	77

	<i>Página</i>
— <i>Ucrania</i>	83
— <i>Rusia</i>	84
Oriente Medio y norte de África	85
— <i>Irán</i>	85
— <i>Irak</i>	86
— <i>Israel</i>	86
— <i>Libia</i>	87
— <i>Siria</i>	87
— <i>Egipto</i>	87
— <i>Argelia</i>	87
Asia	88
— <i>India</i>	88
— <i>Pakistán</i>	89
— <i>China</i>	89
— <i>Corea del Norte</i>	91
— <i>Corea del Sur</i>	92
Modelos no estandarizados de difusión de tecnologías	92
La utilización de las armas de destrucción masiva por los grupos terroristas	95
Políticas de control en los foros internacionales	97
— <i>Régimen de Control de la Tecnología de Misiles</i>	99
— <i>Acuerdo Wassenaar sobre controles a la exportación</i>	100
— <i>Grupo de Suministradores Nucleares (NGS)</i>	101
El diálogo y la cooperación entre Estados Unidos y Rusia	102
Opciones para afrontar el tráfico de misiles en el umbral del siglo XXI	
105	

Capítulo segundo

MOVIMIENTOS MIGRATORIOS Y SEGURIDAD INTERNACIONAL	109
Introducción	111
Caracterización de los movimientos migratorios	113
— <i>Los movimientos migratorios nacionales</i>	113
— <i>Los movimientos migratorios internacionales</i>	114
Refugiados, desplazados y retornados	118

	<i>Página</i>
— <i>Nivel internacional</i>	122
— <i>Nivel nacional</i>	123
Conclusiones	126
 <i>Capítulo tercero</i>	
SISTEMAS DE INFORMACIÓN Y AMENAZAS A LA SEGURIDAD.	129
• LOS SISTEMAS DE INFORMACIÓN Y LAS TECNOLOGÍAS DE LA INFORMACIÓN EN EL SIGLO XXI.	131
La desregulación de las telecomunicaciones	131
Las telecomunicaciones, factor de desarrollo y dependencia	133
Internet. Algunas consideraciones	135
Las amenazas a la seguridad	137
Los tipos de agresores contra los sistemas de información y tecnologías de la información	138
Tipología de ataques, ciberguerra y guerra de la información	140
Los medios y tecnologías para la defensa y la prevención	142
Los sistemas de comunicaciones.	145
Desregulación y defensa en España.	147
Las comunicaciones del futuro	148
• LA UTILIZACIÓN DE LAS COMUNICACIONES Y SISTEMAS DE INFORMACIÓN COMO AMENAZAS A LA SEGURIDAD ACTUAL	151
Introducción.	151
La edad de la información, la seguridad internacional y la Defensa Nacional.	152
— <i>Los modernos Sistemas de Mando y Control</i>	152
La interdependencia informática actual	154
Un nuevo concepto de guerra electrónica	156
Concepto de guerra de información estratégica	157
Concepto de guerra de información	158
Tipos de ataques en la guerra de información	159
Efectos de los ataques a los sistemas de información	160
Realidad de los ataques y amenazas de la guerra de información	161
Los actores de la amenaza de la guerra de información estratégica	164
La respuesta a la amenaza contra los sistemas de información	165

	<i>Página</i>
— <i>Protagonismo de liderazgo en la respuesta a la amenaza</i>	168
— <i>Análisis y asesoramiento del riesgo</i>	168
— <i>Participación clave de los gobiernos</i>	168
— <i>Enunciación de una nueva estrategia de seguridad</i>	169
— <i>Emisión de una nueva estrategia nacional militar</i>	169
— <i>Modificar y preparar la comunidad de inteligencia para la guerra de información estratégica</i>	169
Conclusiones	170
 <i>Capítulo cuarto</i>	
AMENAZAS Y RIESGOS DE CARÁCTER MILITAR	173
La amenaza militar en tiempo de cambio	175
Los conflictos del nuevo siglo	178
Las organizaciones europeas de seguridad y defensa	180
El nuevo papel de las Fuerzas Armadas	183
— <i>Premisas</i>	184
— <i>Factores</i>	184
Conclusiones sobre las nuevas misiones de los ejércitos	186
La guerra en el siglo XXI	187
COMPOSICIÓN DEL GRUPO DE TRABAJO	193
ABSTRACT	195
ÍNDICE	197

RELACIÓN DE MONOGRAFÍAS DEL CESEDEN

- *1. Clausewitz y su entorno intelectual. (Kant, Kutz, Guibert, Ficht, Moltke, Sehlieffen y Lenia).
- *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. (Antología de textos en inglés).
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. (Antología de textos en inglés).
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. El Ejército y la Armada de Felipe II, ante el IV centenario de su muerte.

23. V 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. El Ejército y la Armada en 1898: Cuba, Puerto Rico y Filipinas (I).
30. Un estudio sobre el futuro de la no-prolifерación.
31. El islam: presente y futuro.
32. Comunidad Iberoamericana en el ámbito.
33. La Unión Europea Occidental tras Amsterdam y Madrid.
34. Iberoamérica, un reto para España y la Unión Europea en la próxima década.
35. La seguridad en el Mediterráneo.
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. La Aviación en la guerra española.

* Agotado. Disponible en las bibliotecas especializadas y en el Centro de Documentación del Ministerio de Defensa.



MINISTERIO
DE DEFENSA



SECRETARÍA GENERAL TÉCNICA
CENTRO DE PUBLICACIONES



Colección Monografías del CESEDEN