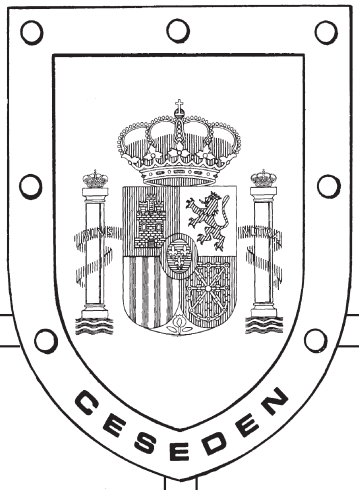
BOLETÍN DE INFORMACIÓN

núm. 324

COLABORACIONES

año 2012

MINISTERIO DE DEFENSA



BOLETÍN DE INFORMACIÓN

(CENTRO SUPERIOR DE ESTUDIOS DE LA DEFENSA NACIONAL)

Colaboraciones

Actividades del Centro

CORREO ELECTRÓNICO: ceseden@oc.mde.es
esfas@oc.mde.es
PÁGINA WEB: www.ceseden.es

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

Edita:

MINISTERIO DE DEFENSA
SECRETARÍA GENERAL TÉCNICA

NIPO: 083-12-027-3 (edicion en libro-e)
ISSN: 2254-2523

Depósito Legal: M-4350-1987
Fecha de edición: junio 2012

NIPO: 083-12-026-8 (edición en línea)

URL de la obra:
http:/www.portalcultura.mde.es/publicaciones/

COLABORACIONES

LA GUERRA GLOBAL CONTRA EL TERRORISMO (GWOT)

Cristóbal Julián Paulo Pérez Pacificador
Teniente coronel del Ejército filipino
Jorge García Iraola
Comandante del Ejército de Tierra
y Antonio Lago Ochoa
Comandante de Intendencia de la Armada

La GWTO nace como respuesta ineludible de la Administración estadounidense a los atentados del 11 de septiembre de 2001 (11-S). Si su inicio gozó de un amplio respaldo de la comunidad internacional, su naturaleza difusa y su implementación generaron importantes controversias. Las estrategias seguidas por las administraciones de Bush y Obama en su lucha contra Al Qaeda durante la última década presentan grandes diferencias, pero también evidentes similitudes. En este artículo se realiza un análisis de las mismas, señalando sus luces y sombras en clave de lecciones aprendidas, que permitan establecer conclusiones y realizar una prospectiva del conflicto.

Introducción

La GWOT surge como la respuesta ineludible para la Administración estadounidense que presenció los atentados del 11-S. Estos atentados no pueden interpretarse de otra manera que como una declaración de guerra a la primera potencia mundial. Unos ataques dirigidos contra los pilares fundamentales de esta superpotencia: su poder económico, con el ataque contra las Torres Gemelas del World Trade Center en Nueva York; la cúpula del poder militar, con el ataque contra el Pentágono en Virginia; y el poder político; con el avión que no alcanzó su objetivo estrellándose en Shanksville (Pensilvania), cuyo destino pudo haber sido el Congreso de Estados Unidos.

Como consecuencia de estos ataques suicidas fallecieron cerca de 3.000 personas y otras 6.000 resultaron heridas. No hay antecedentes en la Historia de un acto de este tipo, ni para la vileza de su naturaleza y sus

resultados. Existían antecedentes de ataques terroristas contra Estados Unidos, como el coche bomba en el World Trade Center en el año 1993, el atentado contra las Torres Khobar en Arabia Saudí en el año 1996, los ataques contra las Embajadas norteamericanas en Kenia y Tanzania de 1998 (el presidente Clinton ordenó en represalia el ataque contra diversos objetivos en Sudán y Afganistán), y el atentado en Yemen contra el destructor USS *Cole* en el año 2000, pero ninguno de la importancia y la trascendencia de éstos. Hay autores que identifican el 11-S con el ataque a Pearl Harbour, con un efecto similar al del año 1941, convenciendo a los estadounidenses de que debían involucrarse más a nivel mundial (1).

No cabe duda de que el 11-S supuso un punto de inflexión en la Historia contemporánea, con consecuencias de una importancia similar a las de la caída del muro de Berlín el 9 de noviembre de 1989. De hecho, los acontecimientos del 11-S cerraron el periodo de transición de los años noventa, que se podría denominar periodo de entre-guerras, la guerra fría y la GWOT, para abrir una nueva etapa en las relaciones internacionales, todavía en fase de transición (2).

La GWOT y Al Qaeda

El 20 de septiembre de 2001, en una sesión conjunta del Congreso y del Senado, el presidente Bush habló por primera vez del concepto que pasó a ser conocido por el acrónimo GWOT *(Global War On Terror)* en el marco de un enfrentamiento de carácter global comparable a la guerra fría, analogía empleada por el propio Bush:

> «La actual guerra contra el terror es igual que la guerra fría. Es una pugna ideológica con un enemigo que desprecia la libertad y persigue fines totalitarios…. Como en la guerra fría, América está de nuevo respondiendo a la llamada de la Historia con confianza, y como en la guerra fría, la libertad prevalecerá» (3).

---

(1) El historiador estadunidense Robert Kagan, entrevista en el diario español *El Mundo*,10 de septiembre de 2011.

(2) Ruiz González, Francisco J.: «Tendencias y dilemas internacionales tras el 11-S de 2001: ¿un sistema internacional en transición?», DIEEEA23-2011, Instituto Español de Estudios Estratégicos (IEEE), Madrid, 2011.

(3) Extracto del discurso de George Bush en la Paul H. Nitze School of Advanced International Studies, abril de 2006.

El terrorismo global

El enfoque que en los últimos 10 años le ha dado el Gobierno de Estados Unidos al terrorismo global no es estático, sino que ha ido evolucionando. Esta variación queda claramente recogida en la evolución de las diferentes estrategias nacionales para combatir el terrorismo que se han ido aprobando.

En la *Estrategia Nacional para Combatir el Terrorismo de 2003*, la amenaza terrorista posee una estructura flexible, transnacional y en red, permitida por la tecnología moderna y caracterizada por la interconectividad entre grupos. Según este modelo, los terroristas de todo signo trabajan juntos en su financiación, compartiendo inteligencia, entrenamiento, logística, planeamiento, y ejecución de ataques. Los grupos terroristas con objetivos en un país o región pueden prestar ayuda a grupos en otros países o regiones. La amenaza terrorista es presentada como resistente y difusa debido a su capacidad de reforzarse mutuamente y la estructura dinámica de la Red.

Se presentan tres niveles de organizaciones terroristas: en primer lugar las que operan únicamente en un solo país, con un alcance limitado, pero sus acciones pueden tener consecuencias internacionales. Estos grupos pueden crecer geográficamente si sus ambiciones y capacidades se lo permiten. En el nivel siguiente están las organizaciones terroristas regionales, que superan al menos un límite internacional. En el tercer nivel aparecen las organizaciones terroristas con alcance global. Sus operaciones atraviesan varias regiones y sus ambiciones pueden ser transnacionales e incluso globales. Según esta interpretación estos tres tipos de organizaciones se alían de dos maneras. En primer lugar, pueden cooperar directamente compartiendo inteligencia, personal, maestría, recursos, y refugios seguros. En segundo lugar, pueden apoyarse de una manera más reducida, por ejemplo promoviendo la misma agenda ideológica y potenciar los esfuerzos de cada uno por cultivar una imagen internacional favorable para su «causa».

La naturaleza interconectada de las organizaciones terroristas hace necesario que sean perseguidas a través del espectro geográfico para tener la seguridad de que todos los enlaces entre las organizaciones estén quebrados, dejando a cada uno de ellas aislada, expuesta, y vulnerable a la derrota.

La disponibilidad de las Armas de Destrucción Masiva (WMD, en sus siglas inglesas) plantea una amenaza directa y seria a Estados Unidos y a la

comunidad internacional. Se mantiene que la probabilidad de que una organización terrorista emplee un agente químico, biológico o radiológico, o un arma nuclear, ha aumentado considerablemente en los últimos años.

Todas las organizaciones terroristas aparecen vinculadas como algo único que es preciso derrotar. Aunque todo el terrorismo es condenable, la mayoría de las organizaciones terroristas no amenazaban a Estados Unidos. Muchas persiguen agendas locales que tienen poco o nada concerniente a los intereses estadounidenses.

En la *Estrategia Nacional para Combatir el Terrorismo de 2006*, la amenaza terrorista aparece más centrada en Al Qaeda como principal enemigo, y se hace más hincapié en su ideología islamista radical, pero se sigue mencionando a las demás organizaciones terroristas y no se supera el anterior concepto de ideología totalitaria, que une a todos los grupos terroristas del mundo y que pretende socavar la libertad alcanzada a nivel global.

En la *Estrategia Nacional para el Contraterrorismo de 2011*, se establece que la amenaza preeminente sobre la seguridad de Estados Unidos continúa siendo Al Qaeda y sus afiliados (4) y adheridos (5), y que una década después de los ataques terroristas del 11-S, Estados Unidos permanece en guerra con Al Qaeda para asegurar la seguridad de sus ciudadanos e intereses.

Por lo tanto se pasa a una definición más centrada en un enemigo asumible y se supera la idea de desterrar al terrorismo como método, que aunque siendo deseable se convierte en un objetivo inalcanzable.

Al Qaeda

La organización Al Qaeda, fundada por el saudí Osama ben Laden en el año 1988, fue responsabilizada de diversos ataques terroristas contra intereses norteamericanos a lo largo de la década de los años noventa, y llegó a declarar públicamente la *guerra santa* contra Estados Unidos y sus aliados en el año 1998. Sin embargo, no fue hasta las acciones terroristas del 11-S cuando realmente adquirió la importancia necesaria para

(4) Grupos alineados con Al Qaeda.

(5) Individuos que han mantenido relaciones de colaboración, actúan en nombre de, o son inspirados para tomar la acción en el fomento de las metas de Al Qaeda –la organización y su ideología– incluyendo el empleo de la violencia sin importar si tal violencia está dirigida contra Estados Unidos, sus ciudadanos, o sus intereses.

modificar la política exterior y de seguridad de Estados Unidos, siendo ella la única organización terrorista responsable.

En las reivindicaciones de Al Qaeda, plasmadas en la *fatwa* de 1998, se establecen los tres «crímenes y pecados» cometidos por los estadounidenses en opinión de sus autores:

1. Apoyo militar de Estados Unidos a Israel.
2. Ocupación militar de la península Arábiga por Estados Unidos.
3. Agresión estadounidense contra el pueblo de Irak (previa a la invasión del año 2003).

La *fatwa* establece además que Estados Unidos:

1. Saquea los recursos de la península Arábiga.
2. Dicta la política a seguir a los gobernantes de dichos países.
3. Apoya a regímenes y monarquías abusivos que oprimen a su propia gente.
4. Tiene bases e instalaciones militares en la península Arábiga, violando así su «Tierra Santa», con el fin de atemorizar a los Estados vecinos.
5. Intenta dividir a los Estados árabes con la finalidad de debilitarlos como fuerza política.
6. Apoya a Israel, y desea distraer a la opinión mundial de la ocupación de los Territorios Palestinos.

De lo anterior se deduce que sus reivindicaciones no son de orden global, sino que están delimitadas a una zona concreta del mundo. A su vez, Al Qaeda tiene como último objetivo estratégico la creación de un «califato islámico mundial», idea en la que busca legitimar la persecución por medios violentos de ese proyecto panislámico, asociado a la multiplicación de teocracias en el mundo musulmán y su unificación bajo un nuevo califato (6), que igualmente, sólo podría alcanzar un carácter regional.

Al Qaeda ejemplifica cómo las redes terroristas han aprovechado las ventajas de nuestro cada vez más abierto, integrado, y modernizado mundo, para servir a su agenda destructiva. La red de Al Qaeda es más que una organización terrorista, es un movimiento que intenta inspirar y coordina a otros grupos e individuos, siendo capaz de establecer células terroristas en cualquier país, en un mundo donde más de 190 millones de perso-

(6) De la Corte Ibáñez, Luis: «El futuro de Al Qaeda tras el X aniversario del 11-S: posibles trayectorias y variables involucradas», *Documento de Opinión*, número 62, IEEE, 7 de septiembre de 2011.

nas viven fuera de su país de origen y con fronteras internacionales que son cruzadas diariamente millones de veces (7).

Crítica general al concepto

La definición monolítica de terrorismo a nivel global que trata de erradicar la libertad y cuyo objetivo común es la imposición de modelos totalitarios en todo el planeta se ha demostrado incorrecta. Los grupos terroristas buscan fines diferentes aunque puedan cooperar en determinadas circunstancias, pero agruparlos a todos en una amenaza global se ha demostrado un error que despreciaba el concepto básico de que una estrategia adecuada obliga a la discriminación de la amenaza y a la armonización razonable de fines y de medios (8).

La amenaza real para Estados Unidos provenía simple y llanamente de los autores de los atentados del 11-S, es decir, la organización terrorista de alcance global Al Qaeda. Además muchos grupos terroristas que operan a lo largo del mundo nada tienen en contra de los intereses estadounidenses y en muchos casos ni se hubiesen atrevido a participar en un ataque como el del 11-S.

Por otra parte, tratar de erradicar el terrorismo como un método de combatir, aunque fuese encomiable, se ha demostrado inviable. El terrorismo es el recurso de aquellos cuyas carencias materiales y morales les llevan a operar de esa manera (9), además de suponer un método en el que la relación «coste-eco internacional» no tiene competidor en cualquier otro método de lucha.

Análisis de la GWOT. Desarrollo, críticas y lecciones aprendidas

Aunque los enfoques de lucha contra el terrorismo aplicados por las administraciones de los presidentes Bush y Obama coinciden en ciertos

(7) Keeley, Brian: *International Migration. The Human Face of Globalization*, Organización para la Cooperación y el Desarroloo Económico, 2009.

(8) Record, Jeffrey: *Bounding the Global War on Terrorism*, Strategic Studies Institute, 2003.

(9) Woods, Joshua: *Framing Terror: an Experimental Framing Effects Study of the Perceived Threat of Terrorism, Critical Studies on Terrorism*, West Virginia University, 2011.

aspectos de su ejecución, su formulación oficial, como se ha expuesto, ha ido variando.

Por ello, a efectos de afrontar el análisis del desarrollo del conflicto, se ha decidido considerar el mismo en dos bloques temporales, los correspondientes a las citadas presidencias. En ellos se muestran sus principales hitos, consecuencias y críticas recibidas, así como las lecciones aprendidas que se han podido extraer.

GWOT durante la administración Bush

PRINCIPALES HITOS

Se relacionan a continuación algunos de los hitos principales en los que se enmarcó durante estos años el desarrollo de la GWOT, cuadro 1.

Cuadro 1.— *Cronología principal de la GWTO en la administración Bush.*

Fecha	Hitos
11 de septiembre de 2001	Atentados del 11-S.
5 de octubre de 2001	Ben Laden se felicita en video por los atentados.
7 de octubre de 2001	Inicio de la operación *Libertad Duradera* contra Al Qaeda y Afganistán.
12 de octubre de 2002	Atentado en Bali, 200 fallecidos.
20 de marzo de 2003	Se inician los bombardeos en Irak.
9 de abril de 2003	Cae Bagdad y el régimen de Sadam Hussein.
16 de mayo de 2003	Atantados en Casablanca, 45 fallecidos.
16 de octubre de 2003	Ben Laden amenaza a países que participen en Irak (España).
13 de diciembre de 2003	Sadam Hussein es apresado.
11 de marzo de 2004	Atentados en Madrid, 192 fallecidos.
9 de octubre de 2004	Karzai es elegido presidente de Afganistán tras elecciones.
7 de julio de 2005	Atentados en Londres, 56 fallecidos.
23 de julio de 2005	Atentados en Egipto, 64 fallecidos.
15 de octubre de 2005	Aprobación de la Constitución de Irak.
9 de noviembre de 2005	Atentados de Amman (Jordania), 60 fallecidos.
8 de junio de 2006	El líder de Al Qaeda en Irak, Abu Al Zarqawi es eliminado.
30 de diciembre de 2006	Ejecución de Sadam Hussein.
29 de enero de 2008	Eliminación de Abu Al Libi en Pakistán.

Fuente: Blanco Navarro, José María: «Seguridad e Inteligencia 10 años después del 11-S», IEEE, 2011.

DIMENSIONES DE ENFRENTAMIENTO EN LA GWOT

En respuesta a los atentados del 11-S, el Gobierno de Estados Unidos inició una guerra mundial al terrorismo en cinco frentes: diplomático, militar, de inteligencia, de aplicación de la ley y de financiamiento.

FRENTE DIPLOMÁTICO

La ofensiva diplomática tuvo dos vertientes (10). La primera de ellas fue la diplomacia pública. Consciente del valor de la opinión pública y de los medios de comunicación creó un cargo de subsecretario de Estado para Diplomacia Pública y Asuntos Públicos y la unidad de respuesta rápida diseñada para ayudar a los funcionarios estadounidenses en el extranjero para responder a las noticias del día.

Los proponentes de la diplomacia pública argumentaron que podría desempeñar un papel importante en ganar los «corazones y mentes», afectando, no sólo a las actitudes de las poblaciones y las acciones de los gobiernos, sino también a las acciones de los grupos terroristas. Una diplomacia pública efectiva frente a los medios de comunicación podría ayudar a movilizar la opinión pública en otros países presionando a los gobiernos a tomar medidas contra el terrorismo.

La segunda faceta fue la de diplomacia exterior, orientada a fortalecer los esfuerzos internacionales contra el terrorismo y la creación de una coalición antiterrorista global. Se trataba de «convencer a los fuertes, permitir a los débiles y obligar a los no dispuestos a trabajar con Estados Unidos en su guerra global contra el terror».

Estados Unidos consiguió así recabar una amplia cooperación internacional en la lucha contra el régimen talibán en Afganistán (57 países).

La administración Bush también exploró la posibilidad de alistar a Estados que patrocinan el terrorismo en el tiempo, como: Libia, Sudán y Siria, en una amplia coalición islámica contra Al Qaeda y sus seguidores. Obtuvo cierta colaboración (caso de Arabia Saudí, que considera Al Qaeda como una amenaza para su régimen, e influenció en los pequeños Estados del Golfo), si bien no exenta de ambigüedades en casos como el de

(10) Congressional Research Service: *International Terrorism: Threat, Policy and Response,* enero de 2007.

Pakistán, que pareció «jugar a dos bandas», socavando la actuación de la alianza.

Por otro lado, la incapacidad de la administración Bush para obtener la aprobación de la Organización de Naciones Unidas (ONU) para la invasión de Irak llevó a la creación de la «coalición de la voluntad», con el objetivo de desarmar a Sadam Hussein. Esta coalición integró a unos 46 países que apoyaron, militar o verbalmente, la invasión de Irak en el año 2003 y posterior presencia militar en el país.

OPERACIONES MILITARES

La participación militar en la guerra global contra el terrorismo comenzó oficialmente el 7 de octubre de 2001 con el lanzamiento de la operación *Libertad Duradera* en Afganistán. Si la operación comenzó modestamente –algunos aviones y fuerzas de operaciones especiales–, escaló a un ritmo frenético (a finales de la administración Bush, Estados Unidos tenía unos 160.000 soldados directamente involucrados en la guerra contra el terror).

Un año más tarde, en 2002, la administración Bush abrió otro frente en la GWOT lanzando la operación *Libertad Iraquí*, basada en la posesión del régimen de Sadam Hussein de armas biológicas y químicas.

Estas guerras involucraron a un número tan elevado de unidades que fue difícil mantenerlas en términos de personal. Aparte de los directamente implicados en las dos operaciones, había otros 230.000 marineros, *marines* y soldados apoyando la guerra contra el terror o en el extranjero, destinados en Alemania, Japón y Corea.

Durante los primeros años de la guerra, 26 de las 33 brigadas de combate del *U.S. Army* participaron en las misiones. Este *tempo* operacional era insostenible, ya que, si la duración de las misiones era de seis meses, se necesitaban tres brigadas por cada una despleagada (otra en descanso, y otra en preparación), por lo que la necesidad total era de 78 brigadas de combate, que tampoco podía ser cubierta con el personal de reserva. La estructura de fuerzas y la estrategia del *U.S. Army* se habían diseñado con estos parámetros, pero debieron ser cambiados drásticamente. Algunos ejemplos de estos cambios fueron:

– En cuanto a estructura, el *U.S. Army* se expandió a 48 unidades ligeramente menores en tamaño a una brigada de combate, pero con mejoras en la tecnología de los medios.

– Se implementaron rotaciones de 12 meses en Afganistán e Irak.
– El *U.S. Army* aumentó su dependencia de la reserva para la ocupación de Irak, que llegó a suponer el 40% de los efectivos.
– Se tuvo que recurrir al empleo de los *marines* en tareas de ocupación terrestre durante las rotaciones de invierno.
– Se decidió impedir la pérdida de unidades activas por falta de personal y conservar las de reserva, lo que implicó acuartelar a sus soldados con 90 días de antelación a su despliegue (en el caso de las de reserva, en cuanto sus unidades eran alertadas para la movilización).

Estas operaciones y los nuevos roles a adoptar influyeron en las relaciones de los militares con la sociedad estadounidense.

POTENCIACIÓN DE LA INFRAESTRUCTURA DE INTELIGENCIA

Evidentemente el 11-S tuvo lugar porque las vulnerabilidades de los sistemas de inteligencia eran profundas. Así quedó patente en los diagnósticos (11 que emitieron las correspondientes comisiones de investigación, destacando la falta de coordinación, la ausencia de visión global, la falta de medios humanos y materiales, la ausencia de cooperación internacional, la rigidez general y burocratización, el poco aprovechamiento de la información de fuentes abiertas, la escasez de la inteligencia clásica persona a persona, inteligencia de medios humanos y su integración con otras fuentes (inteligencia de operaciones, de señales, de imagenes, etc.), la falta de capacidad de imaginar supuestos, falta de un enfoque global sobre el fenómeno terrorista en su conjunto, etc.

Tras el 11-S se experimentaron unos rápidos incrementos en personal, presupuesto y medios tecnológicos. Las estructuras fueron modificadas, creándose nuevos órganos de coordinación (12) y agencias propiamente antiterroristas (13).

En este sentido es de destacar la creación de la Oficina del Director Nacional de Inteligencia en Estados Unidos. Fue establecida por la *Intelligence Reform and Terrorism Prevention Act* de 2004, para unificar, coor-

(11) Blanco Navarro, José María: «Seguridad e Inteligencia 10 años después del 11-S», IEEE, Madrid, 2011.
(12) En Estados Unidos se creó el Director of Nacional Intelligence, o el Security and Intelligence Coordinator en Reino Unido.
(13) En Estados Unidos se creó el National Counterterrorism Center, o el Joint Terrorism Analysis Centre en Reino Unido.

dinar y gestionar los esfuerzos de toda la comunidad de inteligencia (16 agencias y organizaciones). Además gestiona la ejecución del Programa Nacional de Inteligencia, y aconseja al presidente y al Consejo Nacional de Seguridad en materias de inteligencia relacionadas con la Seguridad Nacional.

CERCO LEGAL

La necesidad de enfrentarse a las nuevas amenazas provocó múltiples reformas legislativas (14).

En Estados Unidos las reacciones normativas tras los atentados del 11-S fueron casi inmediatas. El 24 de septiembre de 2001 se adoptó la Orden Ejecutiva (13224) sobre financiación terrorista. El 9 de noviembre se aprobaba una nueva Orden Ejecutiva para la preparación de los ciudadanos en la guerra contra el terrorismo. Pero la iniciativa más destacada fue, la *Patriot Act*, firmada el 26 de octubre de 2001 con un amplio respaldo. Según esta Ley, el FBI podía vigilar la correspondencia y las comunicaciones a través de Internet o por teléfono de los sospechosos de vinculación con el terrorismo, concepto que se definía en términos extraordinariamente vagos. Además, en ciertos casos, un fiscal federal podía decidir esta intervención sin autorización judicial por 48 horas. Esta nueva Ley tipificaba el ciberterrorismo cuando los ataques informáticos supusieran pérdidas superiores a 5.000 dólares.

También se obligaba a las empresas de Internet a entregar el registro de actividad y los correos electrónicos de un sospechoso. Para evitar posibles abusos, el Congreso de Estados Unidos dio un plazo de cuatro años de validez, hasta el 31 de diciembre de 2005, a la vigilancia telefónica y electrónica. La Ley, además, permitía a la Policía detener a extranjeros residentes sin necesidad de formular cargos contra ellos durante siete días. En resumen, muchos derechos individuales podían ser vulnerados, en ausencia de autorización judicial, ante la sospecha de actividades terroristas, siendo muy criticada por defensores de los derechos y libertades.

Pero, sin lugar a dudas, la más polémica de las medidas adoptadas por el Ejecutivo fue la creación de tribunales militares de excepción para juzgar

(14) VV.AA.: «Legislación antiterrorista comparada después de los atentados del 11 de septiembre y su incidencia en el ejercicio de los derechos fundamentales», *ARI*, número 7, Real Instituto Elcano, Madrid, 2006.

a ciudadanos extranjeros sospechosos de participar en actividades terroristas, o poner en peligro la Seguridad Nacional, en virtud de la Orden Presidencial de 13 de noviembre de 2001.

En el ámbito internacional también se introdujeron nuevas regulaciones legales contra las actividades terroristas (15).

CERCO ECONÓMICO AL TERRORISMO

Estados Unidos diseñó una estrategia financiera antiterrorista basada en tres pilares: detectar, desmantelar e impedir la constitución de redes de financiamiento del terrorismo.

El Departamento de Estado encabezó la creación del Grupo de Trabajo sobre Financiamiento de los Terroristas (GTFT) para coordinar, diseñar y suministrar entrenamiento y asistencia técnica a países considerados más vulnerables al financiamiento del terrorismo. Por medio del desarrollo de su capacidad, un país puede reforzar sus capacidades en materia legal, reglamentación financiera, inteligencia financiera, policial y judicial para combatir el financiamiento del terrorismo. Este grupo interinstitucional multiplicó el conocimiento existente en el Gobierno de Estados Unidos en sus esfuerzos por combatir el blanqueo de dinero y los grupos delictivos organizados. Su objetivo era acabar con el financiamiento de los terroristas.

Los registros financieros y las auditorías proporcionan, en muchos casos, el plan maestro de la arquitectura de las organizaciones terroris-

---

(15) La Unión Europea adoptó la Decisión Marco del Consejo de 13 de junio de 2002 sobre lucha contra el terrorismo (2002/475/JAI), que por primera vez aporta una definición al delito de terrorismo para todos los Estados miembros. Obligaba a éstos a incluir el delito de terrorismo en sus Códigos Penales antes de finales de 2002. Posteriormente siguieron cambios legales en todos los países de la Unión Europea. Así, en España, sobre todo a consecuencia del 11 de marzo de 2004, se acometieron modificaciones en materia de explosivos, de protección de infraestructuras críticas, de financiación del terrorismo, de blanqueo de capitales, etc. Principalmente con la reforma del Código Penal mediante la Ley Orgánica 5/2010, que tiene tres contenidos fundamentales:

- Incluye como colaboración con el terrorismo las conductas tendentes a la captación, adoctrinamiento, adiestramiento y formación.
- Penaliza las acciones de distribución o difusión pública de consignas para alentar o favorecer la perpetración de estos delitos, incrementando el riesgo de su comisión.
- Incorpora como delito específico la financiación del terrorismo, incluyendo la forma culposa o negligente.

tas. La identificación y el aislamiento de las fuentes de financiamiento de los grupos terroristas inhiben no sólo la ejecución de atentados, sino también su capacidad de mantener alianzas internacionales, de crear infraestructuras de reclutamiento y adiestramiento en todo el mundo. Se han aprovechado de causas benéficas, empresas fachada, donantes acaudalados y delitos de todo tipo para recaudar dinero. Han hecho uso de bancos, redes informales de envíos de remesas conocidas como *jawalas* (16), transferencias de fondos, casas de cambio de moneda y el correo para mover su dinero o sus valores a través de las fronteras nacionales.

A las pocas semanas del 11-S, la comunidad internacional se comprometió a luchar contra la financiación del terrorismo en varios frentes, entre ellos la congelación oportuna de activos sospechosos de pertenecer a grupos terroristas, el arresto de los implicados en la provisión de apoyo financiero a las células terroristas, y el compromiso internacional de hacer reformas judiciales y estructurales a largo plazo para asegurar la integridad del sistema financiero internacional (17).

---

(16) Los Sistemas de Transferencia Informal de Fondos (TIF) se usan en muchas regiones para transferir fondos, dentro del país e internacionalmente. El sistema *jawala* es uno de los sistemas de TIF que existen, con nombres diferentes, en varias regiones del mundo. Aun cuando el sistema *jawala* se usa para la transferencia legítima de fondos, su naturaleza anónima, la carencia de registro y su documentación mínima lo han hecho también vulnerable al abuso por parte de individuos y grupos que transfieren fondos para financiar actividades ilegales. Aunque sería imposible ofrecer una cifra precisa, las cantidades involucradas en las transacciones *jawala* implican probablemente miles de millones de dólares.

(17) La ONU: adoptó la importante resolución 1373 del Consejo de Seguridad de Naciones Unidas y las ocho recomendaciones especiales sobre la Financiación Terrorista por el Grupo de Trabajo de Acción Financiera (FATF). Así, la ONU ha aumentado sus esfuerzos para combatir la financiación del terrorismo y requiere a todos los países:

– Prevenir y suprimir la financiación de los actos terroristas (incluido en la resolución 1373 del Consejo de Seguridad de Naciones Unidas).
– Congelar los bienes de individuos y entidades vinculados a Osama ben Laden, el movimiento talibán, o Al Qaeda (resolución 1267 y resoluciones pertinentes subsiguientes del Consejo de Seguridad de Naciones Unidas, resolución 1526).

La ONU ha establecido un proceso para examinar las solicitudes de los Estados miembros, en el sentido de agregar a una lista consolidada y mantenida por su Comisión de Sanciones según la resolución 1267, los nombres de los individuos y entidades sujetos a la congelación de bienes. La Unión Europea: adoptó los Reglamentos 2580/2001 y el 881/2002, haciendo posible la preparación de su lista de entidades terroristas cuyos activos están sujetos a bloqueo por Estados miembros. Otros orga-

Un elemento muy importante lo constituye la Orden Ejecutiva 13224, firmada por el presidente Bush el 24 de septiembre de 2001, que instaba al secretario de Hacienda, y en algunas circunstancias al secretario de Estado, a que designen a los terroristas, sus financiadores y facilitadores. Estas designaciones aíslan financieramente a entidades al bloquear o congelar sus intereses y activos en Estados Unidos, y evita que utilicen el sistema financiero de bancos de compensación del área del dólar.

De igual importancia es el establecimiento de un proceso interagencial coordinado y dirigido por el Consejo de Seguridad Nacional. El mismo incluye los Departamentos de Estado, Hacienda, Justicia, Seguridad Interna y Defensa, así como también los servicios de inteligencia y las agencias de aplicación de la Ley.

El Congreso de Estados Unidos respondió a los trágicos eventos del 11-S aprobando la *Patriot Act*. La mayoría de las provisiones, sin embargo, fracasaron en cuanto a ocuparse de ese crimen en particular. La información que las agencias de ejecución de la Ley proporcionaron tras el 11-S hace evidente que, en su mayor parte, el tipo de transacciones financieras que utilizaron los secuestradores de los aviones no es detectado adecuadamente por la *Patriot Act*. El hecho es que las instituciones financieras estadounidenses, sin datos de inteligencia gubernamentales adicionales, no pueden detectar ni impedir transacciones relacionadas con el financiamiento del terrorismo.

La financiación del terrorismo parece ser más descentralizada que antes. El dinero proveniente de organizaciones benéficas, sistemas alternativos

---

nismos internacionales y organizaciones regionales: como el Fondo Monetario Internacional, el Banco Mundial, el Grupo de los Siete (G-7), el Grupo de los Ocho (G-8), el Grupo de los Veinte (G-20) y el Foro de Cooperación Económica del Asia y el Pacífico (APEC) también han desempeñado un papel clave en promover la voluntad política y abordar las deficiencias en los sistemas nacionales a fin de combatir el terrorismo. El Grupo Egmont de Unidades de Inteligencia Financiera, que ahora suman casi 100 países en todo el mundo, concentró su intercambio de información financiera en la financiación terrorista. Arabia Saudí: a mediados del año 2004 todas las instituciones benéficas extranjeras con sede en Arabia Saudí se pusieron bajo una organización general coordinadora controlada por el Gobierno. Esta medida cerró en efecto las filiales extranjeras de la Fundación Al-Haramain, una importante organización benéfica internacional, algunas de cuyas sucursales habían provisto apoyo a Al Qaeda. La decisión permitió también al Gobierno saudí controlar las transacciones entre las organizaciones benéficas saudíes y sus afiliadas en el extranjero.

de remesas monetarias e incluso de actividades criminales, se transporta frecuentemente por correo. En el terreno de la capacitación y la asistencia técnica, sigue habiendo grandes necesidades internacionales.

En vista de que el dinero llega a manos de los terroristas en todo el mundo, la única manera en que se podrán reducir sus recursos financieros es por medio de una continua y activa intervención internacional.

ACCIONES Y EVOLUCIÓN ESTRATÉGICA DE AL QAEDA

A lo largo de estos años Al Qaeda ha ido realizando numerosas adaptaciones estratégicas, aunque no constan en documentos escritos. Muestra de ellas son el reguero de acciones que desarrolla en estos años (ataques, declaraciones, alianzas, etc.) y que se relacionan con detalle en la cronología del Anexo, p. 41.

En primer lugar, Al Qaeda aumentó su producción de medios audiovisuales (18) para su difusión en los medios de comunicación en los años siguientes al 11-S para compensar la pérdida de sus infraestructuras y mantener su papel central entre los grupos yihadistas. Este aumento también refleja su maduración como una organización terrorista que busca sacar provecho de su reconocimiento como «marca». De ahí la declaración de Ayman al-Zawahiri (número uno actual de la organización) de que «al menos la mitad de la batalla global contra el enemigo cruzado-sionista se lleva a cabo en los medios de comunicación». Después del año 2003, Al Qaeda fue particularmente hábil para explotar el sentimiento negativo generalizado sobre la invasión y ocupación estadounidense de Irak. También trató de oponerse a la ocupación etíope de Mogadiscio, instando a la milicia islamista *al-Shabaab* a «luchar», como «campeones de Somalia».

El segundo elemento de la evolución estratégica de Al Qaeda después del 11-S fue su determinación de aprovechar las debilidades percibidas de Occidente. Al Qaeda y sus asociados tienen cada vez más controladas e identificadas las brechas en las defensas occidentales mediante la lectura de la literatura occidental y descarga de materiales de los sitios *web* occidentales. Esta táctica yihadista nueva se reflejaba en un nuevo

(18) Las producciones por parte de Al Qaeda fueron: de seis en el año 2002, 11 en 2003, 13 en 2004, 16 en 2005, 58 en 2006, y alcanzando un máximo en 2007 con 97. El número se redujo a 49 en 2008 y se recuperó ligeramente para llegar a 79 en 2009, pero pareció caer de nuevo en 2010.

género de publicaciones yihadistas denominadas «estudios estratégicos yihadistas», que se basan en escritos occidentales racionalistas. Siendo capaces de identificar y analizar las debilidades de ambas partes, teniendo en cuenta los factores políticos, económicos y culturales en el conflicto, y recomendar estrategias realistas.

La revista *Inspire*, una revista yihadista en inglés producida por Al Qaeda en la península Arábiga (AQAP), ilustra esta tendencia. La primera edición de *Inspire* ofreció un «Mensaje al pueblo estadounidense y a los musulmanes en Occidente» que apunta a un futuro de intolerancia religiosa para los musulmanes en Estados Unidos. En sus sucesivas ediciones, *Inspire* propone ejemplos amplificados de la islamofobia en Occidente, tales como la propuesta de quemas del Corán y las protestas por el establecimiento de mezquitas, para subrayar la narrativa de Al Qaeda de una guerra contra el islam.

En tercer lugar, después del 11-S Al Qaeda se volvió más político en términos de sus comunicados, así como en el tiempo y en la focalización de sus ataques. Ha tratado de crear una brecha entre Estados Unidos y sus aliados, llevando a cabo ataques contra las fuerzas españolas, británicas, alemanas, y otras para socavar el apoyo popular a los esfuerzos en la guerra en Afganistán, Irak y otros teatros. La oferta de Osama ben Laden de una tregua a los países europeos en abril de 2004 tenía una meta similar. Además, el grupo comenzó a explotar el calendario político occidental, como fueron los atentados del 11 de marzo de 2004 en Madrid, que se llevaron a cabo justo antes de las elecciones presidenciales españolas.

En cuarto lugar, aparece el énfasis de Al Qaeda en la *yihad* económica, sobre todo apuntando a instalaciones petroleras en Oriente Medio y los Estados del Golfo. Antes de los ataques del 11-S, Ben Laden reconoció la importancia estratégica del sector energético, como es evidente en su declaración de guerra de 1998, donde hizo también un llamamiento a los *muyahidin* a:

> «Proteger esta riqueza (petróleo) y no (lo) incluyen... en la batalla, ya que es una gran riqueza islámica y un gran poder económico esencial para la próxima creación del Estado islámico.»

Sin embargo, en el año 2004 se produjo un cambio en la estrategia de Al Qaeda para hacer hincapié en estos objetivos, cuando en el mes de diciembre Ben Laden declaró la estrategia de:

> «Purga hasta la quiebra y concluyó que había una oportunidad única y de oro para hacer sangrar a Estados Unidos en Irak, tanto económicamente como en términos de pérdidas humanas y la moral...».

Las fusiones con los grupos militantes, incluyendo *Jama'at Tawhid wal Jihad* en Irak, el Grupo Salafista para la Predicación y el Combate (GSPC) en Argelia –transformándose en Al Qaeda en el Magreb Islámico (AQMI)–, *al-Shabaab* en Somalia, y la reconstitución de AQAP, han dado lugar a una organización multipolar, con un eje central en Waziristán del Norte (Pakistán) y un pequeño número de nodos regionales autónomos. Al ofrecer su lealtad a la organización Al Qaeda, estas organizaciones extienden la influencia ideológica y operativa de Al Qaeda en sus respectivas regiones, además de permitir a Al Qaeda participar en la creación de redes, propaganda y movilización de recursos en dichas zonas.

La consecuencia más trascendente de la transición estructural de Al Qaeda en una entidad multipolar se encuentra en las ubicaciones resultantes, los objetivos «locales» y la adopción de tácticas comunes de la violencia terrorista. Por lo tanto, los teatros más probables para los ataques actuales y futuros contra objetivos occidentales y locales son aquellos en proximidad a los principales centros territoriales de Al Qaeda central y sus filiales.

CRÍTICAS Y LECCIONES APRENDIDAS ADICIONALES

ERRORES EN EL ENFOQUE DE LA GWOT

En la formulación inicial de la GWOT, la administración Bush incluyó una multiplicidad de enemigos, incluyendo Estados «gamberros» *(rogue States)*; WMD; organizaciones terroristas de alcance global, regional, y nacional; y el terrorismo en sí mismo como forma de lucha. A todos se les agrupó en una amenaza monolítica, de esta manera se sacrificó la claridad estratégica por un deseo moral en la política exterior estadounidense, llevando el conflicto a entidades estatales y no estatales que no planteaban ninguna amenaza seria para Estados Unidos.

De preocupación especial fue la supuesta relación de Al Qaeda y el Irak de Sadam Hussein como una amenaza terrorista. Éste constituyó un error estratégico de primer orden, por no considerar las diferencias críticas entre los dos en carácter y nivel de la amenaza, y sobrevalorar la capacidad de la acción militar de Estados Unidos.

El resultado fue una guerra de opción preventiva (19) innecesaria contra un Irak disuadido que creó un nuevo frente en Oriente Medio que convocó a más terroristas que cualquier otra acción de la GWOT y donde se tuvo que enfrentar a una insurgencia iraquí con un potencial inesperado. La guerra de Irak inicialmente iba a durar tres semanas y a suponer un coste económico de 60.000 millones de dólares, acabó durando siete años, costando la vida a casi 4.500 soldados estadounidenses (y unos 300 soldados aliados más) y a unos 100.000 civiles iraquíes, y suponiendo un desembolso de 784.000 millones de dólares (según un informe del Servicio de Estudios del Congreso de Estados Unidos) (20).

La GWOT, como se desarrolló inicialmente, pretendía alcanzar unos objetivos inasumibles y amenazaba con disipar los recursos militares estadounidenses, y de otras clases, sobre demasiados extremos, y violaba los principios estratégicos fundamentales de discriminación y de concentración.

Además, la mayor parte de los objetivos declarados de la GWOT, que incluyen la destrucción del Al Qaeda y de otras organizaciones transnacionales terroristas, la extirpación del terrorismo como medio de guerra irregular, y la terminación de la proliferación de WMD para los enemigos verdaderos y potenciales de todo el mundo, eran poco realistas y condenaban a Estados Unidos a una búsqueda desesperada de la seguridad absoluta. Como tales, las metas de la GWOT eran política, fiscal y militarmente insostenibles.

CRÍTICAS A LA INVASIÓN DE IRAK

Los opositores a la guerra preventiva contra Irak, incluyendo los anteriores consejeros de Seguridad Nacional, Brent Scowcroft y Zbigniew Brzezinski y la anterior secretaria de Estado, Madeleine Albright, hicieron una distinción clara entre el carácter, los objetivos, y las vulnerabilidades

(19) La guerra contra Irak no era parte integral de la GWOT, sino un desvío de ella. Una guerra que perseguía transformar Irak en una democracia próspera, estable, la democratización del resto de Oriente Medio autocrático, suponiendo un cambio estratégico radical en la región y de esta manera asegurar el acceso a las vastas reservas de crudo de la zona y evitar la extensión y fortalecimiento de la amenaza terrorista.

(20) Según un estudio de 2008 del Premio Nobel de Economía, Joseph Stiglitz y la profesora de Harvard, Linda Bilmes, si a esa cifra se le suman futuros gastos como las indemnizaciones a las familias de los soldados fallecidos o las pensiones vitalicias por invalidez a los heridos, el montante asciende a los tres billones de dólares.

de Al Qaeda e Irak, distinguiendo que la amenaza de Al Qaeda era mucho más inmediata, peligrosa, y difícil de derrotar. Temían que una guerra de opción contra Irak debilitaría a Estados Unidos para la guerra de necesidad contra Al Qaeda, llevando la atención estratégica de Estados Unidos a Irak, consumiendo el presupuesto y los recursos que serían mucho mejor aplicados en la Defensa Nacional, y, porque una guerra americana en Irak era tan profundamente impopular alrededor del mundo, especialmente entre musulmanes, que debilitaría la buena voluntad de los países con capacidad para compartir la información y la inteligencia tan vitales para ganar la guerra contra Al Qaeda.

Estratégicamente, la operación *Iraqi Freedom* no era parte de la GWOT; constituyó una distracción de la guerra de necesidad contra Al Qaeda. De hecho, se convertiría en mucho más que una distracción. La experta en terrorismo Jessica Stern advirtió en agosto de 2003 que el ataque terrorista contra la Jefatura de la misión de Naciones Unidas en Bagdad era:

> «La evidencia más reciente de que América ha tomado un país en el que no había una amenaza terrorista y lo ha convertido en uno en que sí la hay.»

Es decepcionante que una guerra iniciada en nombre de la GWOT termine creando:

> «La situación que la administración ha descrito como tierra de crianza para los terroristas: un Estado incapaz de controlar sus fronteras o proveer las necesidades básicas de sus ciudadanos.»

El anterior director de Operaciones de Contraterrorismo y Análisis de la Agencia Central de Inteligencia (CIA), Vincent Cannistraro, mantiene que:

> «No había información que ligase a Sadam con el terrorismo internacional antes de la guerra. Ahora hemos creado las condiciones que han hecho de Irak el lugar donde ir a atacar a americanos.»

CRÍTICAS JURÍDICAS A LA GWOT

La ausencia de autorización del Congreso de Estados Unidos para lanzar la invasión a gran escala de Irak sólo se puede justificar a través de una interpretación excesivamente expansiva de la autoridad del presidente.

La detención indefinida de combatientes enemigos ha sido duramente criticada por suponer un quebranto de los principios constitucionales de Estados Unidos. Existe un vacío legal en referencia a los miembros de

Al Qaeda detenidos en el extranjero a los que no se les considera prisioneros de guerra. Además, los tribunales que inicialmente juzgaban a estos detenidos eran tribunales militares, hasta que, el 29 de junio de 2006, el Tribunal Supremo estadounidense declaró ilegales los tribunales militares especiales creados para juzgar a los presos en la base naval de Guantánamo (Cuba).

El empleo de la tortura en los casos de interrogatorio a los supuestos terroristas ha sido claramente rechazado a nivel judicial en Estados Unidos y en otros Estados como Reino Unido e Israel. Se descartan las posibles justificaciones del empleo de la tortura en la GWOT.

Han surgido numerosas voces que mantienen que abandonar el imperio de la ley amenaza la propia identidad nacional de Estados Unidos.

ERRORES DE EMPLEO DE LOS MEDIOS DE COMUNICACIÓN EN LA GWOT

Desde una perspectiva de la comunicación, las capacidades de los medios de comunicación actuales llevan las informaciones sobre los actos terroristas a todos los rincones del mundo, en cualquier momento y en un plazo de tiempo muy reducido. Esta realidad aumenta la notoriedad de los actos terroristas más allá de las verdaderas consecuencias físicas de esos actos. Esta característica es conocida y explotada por las propias organizaciones terroristas y no ha tenido, en contrapartida, una adecuada campaña de comunicación por parte de los Estados que llevaban a cabo las actividades contraterroristas. Una adecuada difusión de los éxitos antiterroristas que se han sucedido hubiera evitado la sensación de derrota que en algunas ocasiones se estaba produciendo.

Por otra parte se han realizado actividades que difícilmente pueden ser explicadas y justificadas por la mejor campaña informativa. El empleo de la tortura, la detención indefinida de combatientes enemigos, incidentes en los que el número de civiles muertos alcanzaba niveles injustificables, hacen que el grado de impopularidad de la GWOT haya sido generalizada.

La imagen pública de cualquier actividad de seguridad de la envergadura de la GWOT debe tener en consideración que una imagen negativa de la misma proyectada sobre la sociedad puede suponer un obstáculo muy difícil de superar, y que, seguramente, conduzca al fracaso en la consecución de los objetivos debido al rechazo y, por lo tanto, la falta de apoyo de las sociedades que llevan a cabo este esfuerzo.

Por otra parte, la violencia pueda llevar a las sociedades a una deformación de las percepciones. Un ejemplo de esto puede ser la modificación que el término multicultural (21) ha sufrido con la GWOT. Antes del 11-S, este concepto se aceptaba como señal de progreso de sociedades avanzadas, pero el miedo, la inseguridad y otros factores avivados por los actos terroristas, han llevado a este término al campo de la seguridad, convirtiéndose en sinónimo de posibilidad de conflicto. Esto también es explotado por el terrorismo. De manera que la comunicación también deberá orientarse a evitar que se identifiquen a ciertos colectivos como origen de la violencia cuando realmente es una minoría de esa comunidad la que origina los actos terroristas.

Por otra parte, la rivalidad entre los viejos *media (old media)*, compuesta por los medios tradicionales como periódicos, radio, televisión, etc… y la nueva *(new media)* vinculada principalmente con Internet y sistemas de comunicación móviles, tiene un peso importantísimo en la actualidad, y la GWOT no iba a ser ajena a este hecho.

En comparación, la nueva *media* es extremadamente más descentralizada e individualizada que los viejos medios. Estas características la han puesto en la vanguardia de la GWOT. La conectividad de los nuevos medios ha sido aprovechada de manera sobresaliente y diversa por los terroristas y los que apoyan sus causas. Se han detectado tres maneras dominantes: para promover y diseminar mensajes en los sitios *web* para el reclutamiento; para la operatividad de las redes, para trazar y ejecutar actos terroristas; y para distribuir el material audiovisual para uso de las organizaciones hacia los medios de comunicación. Todo esto permitiéndoles enlaces transnacionales, flexibles y móviles.

Los viejos medios representaron un sistema centralizado vertical, donde las grandes organizaciones de comunicación, públicas y privadas, controlaron la difusión de la información. Por su parte los nuevos medios permiten la distribución y el establecimiento de una red «múltiple horizontal», con líneas descentralizadas.

Desde una perspectiva de la seguridad, los nuevos medios tienen cualidades anárquicas que los terroristas pueden utilizar, por lo tanto el foco

---

(21) VV.AA.: *Media and Mediation in the «War on Terror»: Issues and Challenges*, Critical Studies on Terrorism, Department of Media and Communication, University of Leicester, Leicester, Reino Unido, 30 de abril de 2009.

de la seguridad en la GWOT se centra en la supervisión de todas las comunicaciones digitales. Otro aspecto a tener en consideración, es la capacidad de los medios digitales actuales, al alcance de la mayoría de la población, que permiten la captura de imágenes o la posibilidad de comunicar hechos en tiempo real, pudiendo convertir a cualquier persona en emisores de información que puede llegar a tener una repercusión nada despreciable, tanto con mensajes positivos, como negativos.

Todo lo anterior redunda en un elevado grado de exigencia sobre los encargados de realizar las actividades de la GWOT, siendo examinado continuamente, desde el punto de vista de la opinión pública por la capacidad de los medios actuales, mientras los terroristas están sujetos a un tipo de escrutinio mucho menor (22).

ACIERTO EN LA POTENCIACIÓN DE LA INTELIGENCIA

Se ha demostrado la necesidad de que las actividades de inteligencia deben, no sólo continuar su evolución, sino también realizar un esfuerzo en el establecimiento de supuestos y en el desarrollo de una intensa obtención de información por todos los medios.

DISMINUCIÓN DEL APOYO MUSULMÁN A AL QAEDA

Al Qaeda también ha cometido errores que le ha ocasionado una pérdida paulatina de apoyos desde, al menos en el año 2004, debido fundamentalmente a dos hechos: en primer lugar, por la constatación de que la inmensa mayoría de las víctimas del yihadismo global eran musulmanes. Los defensores acérrimos de la doctrina del terrorismo islamista les negaban esa condición, al no comportarse de acuerdo con esa misma doctrina. En segundo lugar, influyó el hecho de que algunas autoridades con reconocido título religioso se hicieron oír manifestándose en contra de Al Qaeda a lo largo del mundo islámico (entre las que se incluían influyentes doctrinarios salafistas del mundo árabe que en el pasado estuvieron alineados ideológicamente con esa estructura terrorista) (23).

---

(22) Sólo ante casos muy flagrantes, que puedan provocar rechazo y amenazar los objetivos de los terroristas, éstos se pueden ver sujetos a ciertos límites en sus actuaciones como fue el caso de los límites establecidos por el número dos de Al Qaeda a su responsable en Irak, Al Zarqawi, sobre la emisión de imágenes de decapitaciones, recordándole que lo que se buscaba era el corazón y las mentes de los creyentes.

(23) Reinares, Fernando: «Después de Osama Ben Laden ¿cómo quedan Al Qaeda y el terrorismo global?», *ARI*, número 83, p. 4, Real Instituto Elcano, Madrid, 3 de mayo de 2011.

GWOT DURANTE LA ADMINISTRACIÓN OBAMA

PRINCIPALES HITOS

Cumplidos tres años desde la llegada de Barack Obama a la Casa Blanca, se muestran a continuación los principales hitos que jalonan este periodo. Como se indicó anteriormente, en el Anexo, p. 41, se relacionan también las acciones terroristas de Al Qaeda.

Año 2009:

– 20 de enero: toma de posesión de Barack Obama como presidente de Estados Unidos.
– 22 de enero: Obama firma tres órdenes ejecutivas sobre el cierre de Guantánamo, la prohibición de torturas en interrogatorios y la revisión de las políticas y procedimientos de detención, así como la revisión de todos los casos existentes.
– 24 de marzo: los periódicos se hacen eco del abandono oficial del término GWOT por la Administración estadounidense, prefiriendo la utilización de OCO *(Overseas Contigency Operations)*.
– 4 de junio: discurso de Obama en la Universidad de El Cairo.

Año 2010:

– Febrero: aprobación de la QDR *(Quadrennial Defense Review)* en Estados Unidos.
– Marzo: discurso de Obama en la Academia de West Point.
– Mayo: aprobación de la *National Security Strategy* de Estados Unidos.
– 31 de agosto: Obama anuncia el fin de la misión de combate en Irak.

Año 2011:

– 2 de mayo: fuerzas especiales de Estados Unidos localizan y matan a Osama ben Laden en Abbottabad (Pakistán).
– 21 de octubre: Barack Obama anuncia la retirada de las tropas estadounidenses de Irak en dos meses.
– 17 de diciembre: el Senado de Estados Unidos aprueba la Ley de Financiación de la Defensa Nacional.
– 18 de diciembre: los últimos soldados estadounidenses abandonan Irak.

Año 2012:

– 3 de enero: aprobación del Documento *Sustaining U.S. Global Leadership: Priorities for 21st Century Defense*.

MODIFICACIONES EN EL ENFOQUE DE LA GWOT

REORIENTACIÓN DE LA POLÍTICA DE GWOT

En los primeros días tras su toma de posesión, el presidente Obama anunció una serie de medidas que en principio iban a marcar una clara diferencia en la actuación de su administración respecto a la de su predecesor, el presidente Bush (24). Así:

– Pidió a los militares un plan de retirada de Irak.
– Ordenó el cierre del centro de detención de Guantánamo, que debía completarse en el plazo máximo de un año, así como de las cárceles secretas de la CIA en todo el mundo.
– Ordenó la revisión inmediata de todas las detenciones y procesos contra los presos retenidos en Guantánamo.

En marzo de 2009 diversos medios de comunicación se hacen eco del abandono en la administración Obama del término GWOT, utilizando en su lugar OCO. Dos meses antes, la Comisión Internacional de Juristas le urgía a tomar esta decisión, alegando que el término «había dado a la administración Bush justificaciones espurias para violar leyes y derechos humanos», entre las que se incluían prácticas de detención y métodos de interrogatorios que el Comité Internacional de la Cruz Roja había calificado como tortura (25). Este término comenzó progresivamente a ser utilizado en todas las ocasiones en que era necesario referirse a esta lucha contra el terrorismo fuera de las fronteras de Estados Unidos.

Otro hito en el cambio de tendencia anunciado se produjo el 4 de junio de 2009, fecha en la que Obama pronuncia un discurso en la Universidad de El Cairo (26), en el que hizo un vibrante alegato al acercamiento entre Estados Unidos y el mundo musulmán, centrado en recordar los numero-

(24) El 22 de febrero de 2009, Obama firmó las órdenes ejecutivas de las dos últimas de las medidas adoptadas, *CNNPolitics*, «Obama signs order to close Guantanamo Bay facility», 22 de octubre de 2009, disponible en: *http://articles.cnn.com/2009-01-22/politics/guantanamo.order_1_detention-guantanamo-bay-torture?_s=PM:POLITICS* (descargado el 11 de enero de 2012).

(25) Kamen, Al: «The End of The Global War on Terror», *The Washington Post*, edición *web,* 25 de marzo de 2009, disponible en: *http://voices.washingtonpost.com/44/2009/03/23/the_end_of_the_global_war_on_t.html* (descargado el 12 de diciembre de 2011).

(26) Disponible en la *web*: *http://www.fund-culturadepaz.org/spa/DOCUMENTOS/Conferencias/2009/Discurso_Obama_ElCairo_040609.pdf* (descargado el 3 de enero de 2012).

sos puntos de encuentro y sin dejar de abordar las tensiones existentes de una manera abierta.

En ese mismo mes de junio, Estados Unidos solicita a varios países de la Unión Europea, entre los que se encuentran: España, Francia, Italia, Portugal, Irlanda, Eslovaquia y Hungría, que se hiciesen cargo de varios presos de Guantánamo, para ayudar a la clausura del centro. El Gobierno español se mostró partidario, indicando que se estudiaría «caso por caso», siempre «dentro de la legalidad» (27).

CAMBIOS DOCTRINALES EN LA ESTRATEGIA DE LUCHA CONTRA EL TERRORISMO

La administración Obama centró inicialmente su estrategia contraterrorista en un objetivo menos ambicioso pero más preciso que su predecesor: «desbaratar, desmantelar y derrotar a Al Qaeda en Pakistán… y Afganistán» (28).

Pese a que este enfoque parece más racional que la de enfrentarse a los extremismos violentos en todo el mundo, no estuvo exento de críticas, fundadas principalmente en una pérdida de atención global a la amenaza terrorista (29). De hecho, tuvo que ser corregida con urgencia cuando el 25 de diciembre de 2009 un ciudadano nigeriano, con conexiones con Al Qaeda en la península Arábiga, con base en Yemen, no en las zonas tribales de Afganistán, intentó detonar una bomba a bordo del vuelo 253 de *Delta* que se dirigía de Ámsterdam a Detroit.

---

(27) Declaraciones de la vicepresidenta del Gobierno de España, María Teresa Fernández de la Vega, y del ministro de Asuntos Exteriores, Miguel Ángel Moratinos, citado en la *web* de Radio Televisión Española: «Estados Unidos pide a España que acoja a cuatro presos de Guantánamo», 17 de junio de 2009, disponible en: *http://www.rtve.es/noticias/20090617/eeuu-pide-espana-acoja-cuatro-presos-guantanamo/281178.shtml* (descargado el 11 de enero 2012).

(28) *White Paper of the Interagency Policy Group's Report on U.S. Policy toward Afghanistan and Pakistan*, 2006, disponible en: *http://www.whitehouse.gov/assets/documents/afghanistan_pakistan_white_paper_final.pdf* (descargado el 12 de enero de 2012).

(29) Reinares, Fernando: *opus citada*, p. 3. De la misma forma, se le acusó de dejar de prestar atención a posibles radicalizaciones del fenómeno terrorista dentro y fuera de la sociedad norteamericana, centrándose en la «detención o muerte de individuos especialmente señalados, pertenecientes a cuadros medios y superiores de Al Qaeda, en el convencimiento de que destruir a esta estructura terrorista suponía, en la práctica, acabar con la amenaza más grave que tiene ante sí Estados Unidos y estrangular al resto del yihadismo global.»

En la QDR 2010 (30) se vuelve a mencionar la necesidad de prevenir la emergencia y reemergencia de las amenazas terroristas transnacionales, entre las que se incluye Al Qaeda, y en la Estrategia de Seguridad Nacional de 2011 (31), además de centrarse en la acción de este grupo en Pakistán y Afganistán, se incluyen también sus afiliados en el mundo.

En definitiva, la GWOT se ha ido modificando para adecuarse a los intereses de seguridad definidos en cada momento y los límites del potencial estadounidense. Se consideró necesario:

– La separación y diferenciación de las amenazas evitando el enemigo monolítico.
– La sustitución de la guerra preventiva por una disuasión creíble como el vehículo primario para tratar a los *rogue States* que persiguen WMD.
– Refocalizar la GWOT y la Seguridad Nacional de Estados Unidos, poniendo como enemigo primario a Al Qaeda y sus aliados.
– Preparar Irak para que sea capaz de gestionar su propia estabilidad.
– Proceder a una nueva valoración de Estados Unidos sobre la fuerza militar necesaria, especialmente los niveles de las fuerzas terrestres.

CAMBIOS Y CRÍTICAS EN LA DIMENSIÓN MILITAR DE LAS OCO. RETIRADA DE IRAK Y SURGE *EN AFGANISTÁN*

Retirada de Irak. Desde el primer día como presidente de Estados Unidos, Obama había ordenado revisar de manera integral la estrategia en Irak, para poner fin a esa larga misión de combate.

En abril de 2009, en su primera visita a las tropas en Irak anunció que había llegado el momento de comenzar una transición hacia el traspaso a los iraquíes de la responsabilidad sobre su país y su propia soberanía.

Esta transición la consideró completada poco más de un año más tarde, en agosto de 2010, con el anuncio del fin de la misión de combate en Irak, a la que siguió el compromiso de ayudar en la construcción de la estabilidad del país, basado en el fortalecimiento de sus Fuerzas de Seguridad y el apoyo a su pueblo y a sus gobernantes. Para entonces, habían regresado casi 100.000 soldados estadounidenses de suelo iraquí (32).

---

(30) Department of Defense: *Quadrennial Defense Review*, febrero de 2010.
(31) The White House: *National Security Strategy*, mayo de 2010.
(32) Sitio *web: Promise kept*, The White House, disponible en la *web: http://www.whitehouse.gov/iraq* (consultado el 14 de enero de 2012).

A finales del año 2011 los últimos soldados estadounidenses dejaron Irak. No son pocas las voces que señalan los problemas que puede originar la retirada de Irak (33). Altos funcionarios estadounidenses e iraquíes han expresado su preocupación de que los partidarios de Al Qaeda en Irak, conocidos como Al Qaeda en Mesopotamia, que habían llevado al país a una guerra civil utilizando la insurgencia, y que habían sido derrotados por los principales grupos tribales iraquíes y las tropas estadounidenses, están preparando su resurgimiento. Aunque es poco probable que recuperen su capacidad anterior, están cambiando sus tácticas (como atacar a las Fuerzas de Seguridad iraquíes en pequeñas unidades) para explotar huecos dejados por los estadounidenses y reavivar la violencia sectaria en el país. Incluso se teme que se estén reforzando los lazos entre Al Qaeda y miembros del Partido Baaz, gobernante en el anterior régimen iraquí.

Puesta en práctica de la surge *en Afganistán*. El presidente Obama aumentó el número de personal desplegado en Afganistán en dos ocasiones en el año 2009: en el mes de febrero acordó enviar 17.000 soldados más, y en diciembre, otros 33.000 en tan sólo unos meses. La cifra de efectivos estadounidense en ese país alcanzaría así el valor de 98.000 soldados (34).

Estos incrementos de tropas, denominados *surge* (oleada), se corresponden con una necesidad percibida de ganar el *momentum* (impulso) para luego retirarse. El presidente Obama consideró que era un «interés nacional vital» el envío de esas tropas, en su respuesta al «dilema de la búsqueda de una política posimperial en medio de una crisis imperial», en palabras del conocido analista Fareed Zakaria (35). En un intento de acabar con intervenciones de la era Bush, caracterizadas por ser abiertas en el tiempo, sin fecha prevista de finalización, decidió que proceder a una desescalada podría ser considerado como un abandono precipitado.

Para varios analistas estos movimientos se interpretaron dentro de un ambicioso proyecto de reorientación de la política exterior hacia posi-

---

(33) Schmidt, M.: «Leaving Iraq, U.S. Fears New Surge of Qaeda Terror», edición *on-line* de *The New York Times*, 5 de noviembre de 2011, disponible en: *http://www.nytimes.com/2011/11/06/world/middleeast/leaving-iraq-us-fears-new-surge-of-qaeda-terror.html?pagewanted=all* (descargado el 15 de enero de 2012).

(34) Schmitt, Eric: «Obama Issues Order for More Troops in Afghanistan», *The New York Times on-line*: 30 de noviembre de 2009, disponible en: *http://www.nytimes.com/2009/12/01/world/asia/01orders.html* (descargado el 11 de enero de 2012).

(35) Zakaria, Fareed: «The Post-Imperial Presidency», *Newsweek-The Daily Beast*, diciembre de 2009.

ciones menos contradictorias. El cambio de rumbo comienza con una disminución de la WOT, restringiendo el conflicto con el mundo islámico a los países que representan una amenaza grave y directa para Estados Unidos (36).

En sentido contrario, el aumento de tropas de Afganistán fue presentado por otros críticos como un incremento de la acción intervencionista de Estados Unidos.

LA MUERTE DE BEN LADEN. ACIERTOS, ERRORES Y CONSECUENCIAS INMEDIATAS

La captura de Ben Laden era fundamental para Obama, ya que el presidente se había volcado con la guerra de Afganistán, en opinión de algunos expertos (37), para evitar las críticas sobre su posible falta de compromiso militar, al haber descalificado la guerra de Irak (a la que llegó a considerar una distracción de la lucha contra el terrorismo). De hecho, se llegó a denominar a Afganistán como «la guerra de Obama».

El 2 de mayo de 2011, en Abbottabad (Pakistán), un comando de los SEAL estadounidenses, en una operación coordinada por la CIA denominada *Gerónimo,* consigue matar a Osama ben Laden.

Además del esfuerzo de inteligencia realizado por la CIA (de octubre a mayo había recolectado información que finalmente les condujo hasta Ben Laden) se considera otra clave del éxito, ya que colaboró a que el líder de Al Qaeda abandonase las montañas, el extraordinario (38) incremento desde la llegada al poder de Obama de los ataques con misiles lanzados por Estados Unidos desde vehículos aéreos no tripulados. Si bien tuvo el inconveniente de poner en contra a la población local, acabó con la vida de un número creciente de mandos de Al Qaeda que se refugiaban en zonas tribales, forzando a muchos, como pudo ser el caso de Ben Laden, a trasladarse a zonas urbanas o metropolitanas densamente pobladas (39).

---

(36) *Ibídem.*

(37) Solana, Javier y Basset, Lluís: *Primaveras, terremotos y crisis*, Random House Mondadori, S. A., Barcelona, 2010.

(38) Reinares, Fernando: *opus citada*, p. 3: «Si entre 2004 y 2008 se registraron, en total, 42 de esos ataques en las zonas tribales de Pakistán, sólo en el año 2009 fueron 53 y en 2010 alcanzaron la cifra de 118. En lo que iba transcurrido de 2011 hasta que se produjo el abatimiento de Osama ben Laden en Abbottabad (Pakistán), se habían lanzado más de 20 ataques con misiles en aquella misma demarcación.»

(39) *Ibídem*, en el lugar citado.

En este éxito se ha alabado la excelente coordinación entre la CIA, dirigida entonces por Leon Panetta (que pasaría a ser en el mes de junio, según anunció el propio Obama tres días antes del ataque, secretario de Defensa, sustituyendo a Robert Gates) y el jefe de las tropas de la Fuerza Internacional de Asistencia y Estabilización en Afganistán, David Petraeus, que le sucedió en el cargo.

Como consecuencia directa de esta operación, la CIA recuperó el prestigio que, como agencia de seguridad había perdido dentro y fuera de Estados Unidos por haber errado clamorosamente en la valoración de la amenaza terrorista inmediatamente antes al 11-S y, posteriormente, al no ser capaz de dar con el paradero de Osama ben Laden (40).

Por otra parte, deben mencionarse dos aspectos colaterales de la operación. El más delicado fue la invasión del espacio aéreo paquistaní, ya que no existía la más mínima confianza en que Pakistán fuese a cooperar; el otro, las críticas vertidas sobre la muerte de Ben Laden, menores en Estados Unidos, y mayores fuera, especialmente en Europa.

La violación del espacio aéreo paquistaní por aviones casi indetectables *(stealth)* y la noticia de que Ben Laden había vivido durante años en el mismo lugar en que se encuentra la Academia Militar de Pakistán, situaron las relaciones entre Estados Unidos y Pakistán bajo mínimos (41). Pakistán llevó a cabo acciones que mostraban este distanciamiento utilizando a China, su tradicional aliado: visita del primer ministro de Pakistán a China, declaraciones de amistad «en toda circunstancia», contratos de armamento y conversaciones sobre una futura base naval china en Pakistán, afectando así al equilibrio de poder de ambas potencias en el océano Índico.

CRÍTICAS Y LECCIONES APRENDIDAS ADICIONALES

EL USO DEL LENGUAJE

Obama es más sensible que su predecesor al poder del lenguaje, al que considera capaz de impactar en las percepciones y relaciones entre los pueblos y los Estados.

El presidente ha hecho un esfuerzo por evitar los términos más ofensivos de la administración Bush, que incluye la etiqueta «guerra contra el te-

---

(40) Reinares, Fernando: en el lugar citado.
(41) Solana, Javier y Basset, Lluís: *opus citada.*

rror», al que considera una táctica, no un enemigo», o términos polémicos como «islamofascismo» o «malhechores» *(evildoers)* (42).

Con sus afamadas intervenciones públicas, Obama consiguió, utilizando términos esperanzadores, acercar posiciones entre el mundo occidental y el islámico, si bien mantiene ciertas políticas contradictorias que ponen en entredicho su mensaje.

¿ADMINISTRACIÓN DESPUÉS DE GWOT?

En enero de 2010 no se produjo el cierre de Guantánamo, como había sido ordenado, aduciendo el Gobierno estadounidense que «dificultades jurídicas y técnicas le obligaron a posponer la clausura sin fecha fija» (43). Varios de los presos del centro penitenciario comienzan a ser enviados a países europeos, según los acuerdos firmados el año anterior (44).

Esta situación, lejos de ser cambiada, se agravó con la recientemente aprobada Ley de Financiación de la Defensa Nacional para el año 2012 (aprobada por el Congreso de Estados Unidos el 17 de diciembre de 2011). En ella se incluyen una serie de disposiciones que dan legalidad a la política penitenciaria estadounidense puesta en práctica tras los atentados del 11-S. Si hasta entonces, esta política se basaba en una interpretación, a veces muy generosa, de normas preexistentes, a partir de la aprobación de esta Ley, la Casa Blanca está legalmente autorizada a detener *ad aeternum* a todo aquel que considere sospechoso de actos terroristas.

Se considera otro paso atrás del presidente, que no sólo no ha cerrado Guantánamo, como prometió al arrancar su mandato, sino que ha renovado la autorización para pinchar líneas telefónicas y conexiones de Internet de ciudadanos extranjeros residentes en Estados Unidos autoriza-

---

(42) Mullin, Corinna: «The U.S. discourse on political Islam: is Obama's a truly post-"war on terror" administration?», *Politics and International Studies*, School of Oriental and African Studies, University of London, 2011.

(43) «España amplía de dos a cinco el número de presos de Guantánamo que está dispuesta a acoger», Agencia EFE, Madrid, 15 de febrero de 2010, citado en la página *web* de Radio Televisión Española, disponible en: *http://www.rtve.es/noticias/20100215/espana-amplia-dos-cinco-numero-presos-guantanamo-que-esta-dispuesta-acoger/318056.shtml* (descargado el 11 de enero de 2010).

(44) España se mostró dispuesta a acoger a cinco presos, recibiendo cuatro, de distintas nacionalidades.

ción de la Justicia, y ha sancionado y expandido la política de «asesinatos selectivos» iniciada por su predecesor (45).

Situación actual y prospectiva del conflicto

Reorientación de la estrategia de defensa estadounidense

El pasado 3 de enero, Obama aprobó las directrices a seguir en materia de Defensa en los próximos años (46) basándose en el entorno internacional previsto y las prioridades de Estados Unidos.

Teniendo en cuenta la retirada prevista de Afganistán y la necesidad de mantener un equilibrio de fuerza y seguridad a un riesgo aceptable, en la lucha contra el terrorismo se contempla un esfuerzo mundial más ampliamente distribuido y caracterizado por ser una mezcla de acción directa y de asistencia a las Fuerza de Seguridad.

Se pretende, incorporando las lecciones aprendidas de la década pasada, construir y mantener las capacidades de manera apropiada para luchar contra el terrorismo y la guerra irregular.

Se reconoce que la capacidad de Al Qaeda para operar se ha reducido considerablemente, pero que la organización terrorista y sus aliados siguen activos en: Pakistán, Afganistán, Yemen y Somalia, entre otros. Asegura asimismo que también se mantendrán vigilantes a las amenazas planteadas por otras organizaciones terroristas como *Hezbolá.*

Prospectiva

RETIRADA DE AFGANISTÁN

Obama comenzó la retirada de efectivos de Afganistán en el año 2011 (10.000 soldados) y anunció que los 33.000 efectivos de la *surge* de diciembre de 2009 saldría de Afganistán en el verano de 2012, considerando que en ese periodo los comandantes habrán tenido tiempo de poner en práctica una «retirada responsable» (47).

---

(45) Pardo, Pablo: «… Y elimina derechos civiles», *El Mundo*, 19 de diciembre de 2011.

(46) Department of Defense: *Sustaining U.S. Global Leadership: Priorities for 21st Century Defense*, enero de 2012.

(47) Sitio *web*: «The Way Forward in Afghanistan», The White House, disponible en: *http://www.whitehouse.gov/issues/defense/afghanistan*

A medida que se vayan efectuando estas reducciones, la misión de las tropas estadounidense irá pasando de ser una misión de combate a serlo de apoyo, lo que concuerda con el compromiso de la Organización del Tratado del Atlántico Norte (OTAN) de apoyar al Gobierno de Afganistán, mientras va asumiendo la responsabilidad total en materia de seguridad en todo Afganistán, para finales del año 2014.

Si bien la comunidad internacional ha declarado recientemente en Bonn su voluntad de no abandonar Afganistán una vez se retiren las tropas de la OTAN en 2014 (48), las organizaciones de ayuda y algunos organismos afganos han manifestado que las ganancias en términos de democracia obtenidas en los últimos años ya están bajo amenaza por los recortes presupuestarios para ayuda al desarrollo en los países occidentales.

La ayuda económica al Gobierno afgano se ha comprometido hasta el año 2024, año en el que el Fondo Monetario Internacional prevé que Afganistán será autosuficiente debido a su riqueza en recursos minerales.

En este escenario se podría esperar que la organización terrorista mantenga dormidas sus células en la zona, esperando la asunción total de la seguridad por las fuerzas policiales afganas para reanudar su actividad terrorista y la dificultad económica que pueda tener Occidente para financiar al régimen afgano. El anuncio de una fecha concreta del final de la presencia de tropas extranjeras aumenta sin duda la ya constatada gran capacidad de resiliencia de la organización en el país.

AL QAEDA Y EL TERRORISMO GLOBAL

En el momento que Osama ben Laden muere, Al Qaeda tiene su estructura francamente menoscabada y había perdido buena parte del apoyo popular en diferentes países (49). No obstante, la organización terrorista

(48) Borger, Julián: «Afghanistan Conference Promises Support After Troop Withdrawal», edición *web* de *The Guardian*, 5 de enero de 2011, disponible en: *http://www.guardian.co.uk/world/2011/dec/05/afghanistan-conference-support-troop-withdrawal* (consultada el 4 de enero de 2012).

(49) Reinares, Fernando: *opus citada*, pp. 3-4. Afirma que «parece tener objetivamente degradadas sus capacidades operativas, cuenta con un número de miembros propios que posiblemente no llegue al millar, ha visto muy aminoradas sus infraestructuras terroristas desde que se reubicó en las zonas tribales al noroeste de Pakistán y ha ido progresivamente perdiendo apoyo popular en los países.»

ha demostrado a lo largo de los años su capacidad para adaptarse y sobreponerse a las adversidades.

Como se ha expuesto anteriormente, aunque mermada, no se considera que vaya a desaparecer en un corto o medio plazo de tiempo. Con probabilidad seguirá intentando imponer su estrategia a través de su articulación jerárquica, su organización y bajo el marcado liderazgo de su principal dirigente en cada momento (el egipcio Al-Zawahiri, en la actualidad).

Por otra parte, no se pueden despreciar otras caras que también forman parte del polimórfico terrorismo yihadista, como son sus extensiones territoriales (una muestra de su capacidad es el reciente ataque y posterior control de la ciudad yemení de Rada) (50), las franquicias que constituyen sus grupos afines (como los actuales ataques del grupo islamista *Boko Haram* en Nigeria) (51), y células independientes o individuos aislados. En la medida en que sean capaces de combinar sus esfuerzos sin ser interceptados eficazmente por la comunidad internacional, así evolucionará en el mundo la amenaza del terrorismo global.

En estas circunstancias no sería descabellado pensar que una eventual mayor implicación de los países emergentes, cuya capacidad de crecimiento no está seriamente comprometida, podría ayudar a atajar el terrorismo en los focos en que se manifieste. No obstante, la contraprestación a ese esfuerzo podría pasar por la concesión de una mayor capacidad de decisión en el ámbito internacional, alterando el *status quo*, posibilidad que no parece viable en la actualidad.

Conclusiones

Desde su aparición inmediatamente después del 11-S, tanto el concepto de guerra global contra el terrorismo como los frentes y dimensiones que adoptó en su evolución o su legitimidad como un enfoque para la segu-

---

(50) Agencia EFE: artículo «Seguidores de Al Qaeda se hacen con el control de la ciudad yemení de Rada», edición *on-line* de *El Mundo*, descargada el 16 de enero de 2012, disponible en la dirección: *http://www.elmundo.es/accesible/elmundo/2012/01/16/internacional/1326698184.html.*

(51) Agencias: «Aumenta a 162 el número de muertos por varios atentados en Nigeria», edicion *on-line* de *El Mundo,* disponible en: *http://www.elmundo.es/elmundo/2012/01/21/internacional/1327150596.html* (consultada el 21 de enero de 2012).

ridad global han sido ampliamente cuestionados. Ya sea por su ambigua definición, por la falta de preocupación que los que la impulsaron sintieron o por el elevado coste económico, militar y en vidas que se asumió, no se puede ignorar la controversia que levantó.

Se ha precisado en varias ocasiones que las guerras no pueden ser llevadas a cabo para derrotar fenómenos como el terrorismo. Una guerra contra el terror tiene poco significado en Derecho Internacional o tradiciones diplomáticas.

La administración Bush inició y sostuvo dos guerras bajo la lupa de una comunidad internacional dividida, enfrentada por un lado a la necesidad de buscar el equilibrio en la balanza de la seguridad de sus poblaciones y el coste que necesariamente debe asumir por ello y por otro escandalizándose ante los atropellos cometidos a las leyes.

La nueva Administración que pasaría a ser dirigida por un Premio Nobel de la Paz arrojó esperanzas de cambio. Si bien se anunciaron nuevos enfoques en la lucha contra el terrorismo, las políticas seguidas siguen mostrando contradicciones.

Si Bush marcó en el calendario el inicio de las guerras de Irak y Afganistán, Obama ha marcado su finalización. El esfuerzo empleado ha dado sus frutos, pero está por ver si éstos son duraderos. La inviabilidad de continuar su sostenimiento en el tiempo y sus propios intereses como nación en el debilitado contexto económico en el mundo occidental, le ha forzado a ser más selectivo en la delimitación del objetivo a batir (Al Qaeda) y el ámbito territorial (Afganistán y Pakistán), aunque la realidad de un enemigo que se vuelve a mostrar difuso, aún en su debilidad, le ha obligado a no olvidar las conexiones existentes entre grupos terroristas de ámbito local y con afines ideologías.

Por el momento, la comunidad internacional afirma estar comprometida con la lucha contra el terrorismo, pero parece estar pensando en concederse un respiro para poder dirigir sus esfuerzos hacia otros ámbitos que reclaman insistentemente su atención. El tono del músculo militar mostrado se diluye en favor de otras prioridades.

Es en estas circunstancias, cuando un enemigo aparentemente debilitado, pero resiliente y adaptable, como es un terrorismo movido por causas ideológicas, puede, una vez más, asestar un nuevo zarpazo, para el que Occidente debería estar preparado.

Anexo

Cronológía de las acciones terroristas de Al Qaeda en el contexto de la GWOT

Año 2001:

– 11 de septiembre: en una operación organizada por Al Qaeda y llevada a cabo por 19 suicidas, dos aviones secuestrados destruyen el World Trade Center de Nueva York y otro se estrella contra el Pentágono. Un cuarto avión secuestrado se estrella en Pennsylvania. Más de 3.000 personas pierden la vida.
– 7 de octubre: Estados Unidos, junto con una coalición de Estados lanzan operaciones militares en Afganistán destinadas a eliminar del poder a los talibán. *Al Jazeera* emite un mensaje grabado por Osama ben Laden: «Estados Unidos no volverá a estar seguros».
– 22 de diciembre: un ciudadano británico nacido en Sri Lanka, Richard C. Reid, intenta hacer estallar un avión de American Airlines de París a Miami, utilizando explosivos C-4 insertado en uno de sus zapatos.

Año 2002:

– 28 de marzo: Abu Zubaida, alto miembro de Al Qaeda y coordinador de los ataques a las Embajadas de Estados Unidos en Nairobi y Dar es Salaam en agosto de 1998, es arrestado en Faisalabad (Afganistán).
– 11 de abril: ataque con un camión bomba llevado a cabo por el islamista tunecino Nizar Naouar contra la sinagoga Al Ghriba, en la isla de Djerba en Túnez, matando a 21 personas, entre ellas 14 turistas alemanes.
– 8 de mayo: en Karachi (Pakistán), una bomba explota frente al hotel «Sheraton» matando a 14 personas, de las cuales 11 son franceses, ingenieros de la construcción naval.
– 14 de junio: una bomba explota frente al consulado de Estados Unidos en Karachi, matando a 12 personas e hiriendo a 45.
– 11 de septiembre: Ramzi Ben al Shaiba es arrestado en Karachi (Pakistán), junto con ocho yemeníes, un saudí y un egipcio.
– 6 de octubre: un atentado con bomba se lleva a cabo contra un petrolero francés, el *Limburg*, cerca de Saná (Yemen).
– 12 de octubre: atentado en un club nocturno en Bali (Indonesia), matando a 202 personas, en su mayoría turistas australianos.
– 28 de noviembre: en Mombasa (Kenia), se disparan dos misiles SAM-7 contra un *Boeing 757* de la compañía israelí de vuelos charter Arkia.

Al mismo tiempo, se comete un atentado con coche bomba a la entrada del hotel «Paraíso», donde residen varios turistas israelíes. El asalto mata a 18 personas, entre ellas tres israelíes.

Año 2003:

– 1 de marzo: Khaled Sheikh Mohamed, el planificador de los ataques del 11-S, es arrestado en Rawalpindi, cerca de Islamabad (Pakistán).
– 20 de marzo: Estados Unidos y Reino Unido invaden Irak. Bagdad cae en poder el Ejército de Estados Unidos el 9 de abril.
– 12 de mayo: en Riad (Arabia Saudí), el complejo residencial Al Hamra, donde se alojaban estadounidenses y británicos, es blanco de tres ataques con bombas, que matan a 39 personas, incluidos 12 ciudadanos de Estados Unidos y 149 heridos.
– 16 de mayo: en Casablanca (Marruecos), 14 atacantes suicidas realizan cinco ataques simultáneos en el Consulado de Bélgica, el centro cultural español (Casa de España), un restaurante italiano (en el hotel «Farah-Maghreb»), y en la Alianza Círculo de Israel, dejando 45 muertos y 100 heridos.
– 5 de agosto: coche bomba en el hotel «Marriott» en Yakarta (Indonesia), mata a 15 personas y hiere a 150.
– 8 de noviembre: en Riad (Arabia Saudí), bomba en un edificio residencial donde viven diplomáticos extranjeros, dejando 17 muertos y 120 heridos.
– 15 de noviembre: en Estambul (Turquía), ataque con un camión bomba contra dos sinagogas, matando a 24 e hiriendo a 300.
– 20 de noviembre: dos coches bomba contra el Consulado británico y el banco británico HSBC en Estambul, 27 muertos y 400 heridos.

Año 2004:

– 11 de marzo: cuatro atentados simultáneos, reivindicados por el ala europea de Al Qaeda, tienen lugar en Madrid. Entre las 7:39 y 7:55 horas, 10 bombas en cuatro trenes distintos explotan en las estaciones de Atocha, El Pozo, Alcalá de Henares y Santa Eugenia matando a 192 personas e hiriendo a 1.434.
– 15 de abril: en un mensaje de audio difundido por el árabe por satélite *Al Arabiya* y los canales de *Al Jazeera*, Ben Laden renueva su compromiso de luchar contra Estados Unidos y se ofrece a «cesar sus operaciones» contra los países europeos que cesasen en sus «agresiones contra los musulmanes». La propuesta de tregua es rechazada por los líderes europeos.

– 1 de mayo: una refinería de petróleo en Yanbu (Arabia Saudí), es atacada por hombres armados. El ataque se dirigió contra los ejecutivos senior de la instalación, en parte propiedad de Exxon Mobil. Cinco extranjeros son asesinados, entre ellos dos estadounidenses.
– 29 de mayo: en Khobar (Arabia Saudí), hombres armados atacan un edificio que alberga oficinas de compañías occidentales matando a 22 personas.
– 18 de junio: el ingeniero estadounidense Paul M. Johnson jr., es secuestrado y decapitado en Jeddah (Arabia Saudí).
– 29 de octubre: *Al Jazeera* emite un mensaje grabado de Ben Laden a Estados Unidos.

Año 2005:

– 7 de julio: explosiones coordinadas en tres trenes subterráneos y un autobús de dos pisos en el centro de Londres, matando a 56 personas e hiriendo a 700.
– 23 de julio: explosión de tres bombas en la ciudad turística egipcia de Sharm al-Sheikh, donde mueren 63 personas. Dos de las bombas se dirigen contra un complejo de viviendas turísticas para occidentales y el tercero explota en el mercado de la ciudad.
– 1 de octubre: tres atacantes suicidas atacan restaurantes turísticos en Bali (Indonesia), muriendo 20 personas.
– 9 de noviembre: explotan tres bombas contra hoteles occidentales en Amman, el hotel «Radisson SAS», el hotel «Days Inn» y el «Grand Hyatt», matando a 76 personas e hiriendo a 300.

Año 2006:

– 7 de enero: *Al Jazeera* emite un mensaje de Ayman al Dhawahiri en el que afirma que George W. Bush ha perdido la guerra en Irak.
– 19 de enero: en un mensaje de cinta de audio difundida por *Al Jazeera*, Osama ben Laden ofrece una tregua a Estados Unidos y amenaza con nuevos ataques dentro de Estados Unidos.
– 8 de junio: Abu Musab al Zarqawi, y varios de sus hombres mueren por un ataque aéreo de Estados Unidos en una casa cerca de Baquba (Irak).
– 1 de julio: *Al Jazeera* emite un mensaje de cintas de audio de Ben Laden en la que anima a Abu Hamza al Muhajir, relevo de Al Zarqawi como jefe de Al Qaeda en Irak, continuar los ataques contra los estadounidenses.

– 12 de julio: la sexta guerra árabe-israelí comienza. Se lleva a cabo entre el Estado de Israel y el grupo armado libanés no estatal *Hezbolá* y dura 33 días.
– 27 de julio: *Al Jazeera* emite un mensaje grabado en video en el que Al Dhawahiri declara que Al Qaeda no se quedará mientras que el Líbano y Palestina son atacados, y advierte que: «el mundo entero es un campo de batalla abierto para nosotros, y ya que nos atacan por todas partes, vamos a atacar en todas partes».
– 11 de septiembre: Al Dhawahiri anuncia que la organización islamista de origen argelino creada en 1998 y conocida como el GSPC se ha unido a las filas de Al Qaeda.

Año 2007:

– 11 de enero: el GSPC anuncia que cambia formalmente su nombre a Al Qaeda en el Magreb Islámico (comúnmente conocido como AQMI, por sus siglas en francés).
– 11 de abril: AQMI utiliza coches bomba contra la oficina del primer ministro de Argelia y una comisaría en Argel. Las explosiones matan a 33 personas.
– 11 de diciembre: AQMI ataca varios objetivos en Argel, como el Consejo Constitucional de Argelia y la Oficina de Naciones Unidas, 63 personas pierden la vida.

Año 2008:

– 2 de junio: Al Qaeda se atribuye el atentado contra la Embajada danesa en Pakistán en el que perecen seis personas. El líder de Al Qaeda en Afganistán y Pakistán, Mustafá Abu Al Yazid, lanza una declaración indicando que el ataque fue en represalia por la publicación en Dinamarca de las caricaturas despectivas del profeta Mahoma.
– 19 de noviembre: *Al Sahab* emite un mensaje de Al Dhawahiri en el que afirma que la sustitución del presidente George W. Bush por el presidente Obama no altera los fundamentos del conflicto entre Al Qaeda y Estados Unidos.
– 26 de noviembre: en una serie de ataques coordinados que duró tres días en Mumbai (India), militantes de *Lashkar-e-Taiba* utilizan lanchas rápidas con material inflamable contra dos hoteles, la estación de trenes de la ciudad, una cafetería, un centro judío, un hospital y la zona portuaria, mueren 164 personas.

Año 2009:

– 7 de enero: el mayor del *U.S. Army* Nidal Malik Hassan, que había estado en contacto con el clérigo de Al Qaeda, Anwar al Awlaki, en la península Arábiga, mata a 13 personas en la instalación militar Fort Hood en Texas (Estados Unidos).
– 20 de enero: toma de posesión de Barack Obama como presidente de Estados Unidos.
– 22 de enero: Obama firma tres órdenes ejecutivas sobre el cierre de Guantánamo, la prohibición de torturas en interrogatorios y la revisión de las políticas y procedimientos de detención, así como la revisión de todos los casos existentes.
– 24 de marzo: los periódicos se hacen eco del abandono oficial del término GWOT por la Administración estadounidense, prefiriendo la utilización de OCO.
– 4 de junio: discurso de Obama en la Universidad de El Cairo.
– 31 de mayo: AQMI mata a un rehén británico, Edwyn Dwyer, quien había sido secuestrado junto con otros tres europeos el 22 de enero.
– 27 de agosto: un atentado suicida de Al Qaeda en la península Arábiga cuyo objetivo era el ministro adjunto del Interior de Arabia Saudí se ve frustrado en Riad.
– 25 de diciembre: un ciudadano nigeriano, Umar Faruk Abdulmuttalab, con conexiones con Al Qaeda en la península Arábiga, intenta detonar una bomba a bordo del vuelo 253 de *Delta* que se dirigía de Ámsterdam a Detroit.

Año 2010:

– Febrero: aprobación de la QDR en Estados Unidos.
– Marzo: discurso de Obama en la Academia de West Point.
– 1 de mayo: un ciudadano estadounidense de origen paquistaní y analista de presupuesto, Faisal Shazad, intenta un atentado con coche bomba en Times Square (Nueva York), que logra ser frustrado.
– Mayo: aprobación de la *National Security Strategy* de Estados Unidos.
– 25 de julio: el líder de AQMI, Abdelmalek Droukdel, anuncia que su grupo ha ejecutado a un rehén francés que había sido secuestrado el 19 de abril. El anuncio tiene lugar tres días después de una redada infructuosa de militares franceses y mauritanos en un campamento de AQMI, en el norte de Mali.
– 16 de septiembre: en el Níger, AQMI secuestra a siete trabajadores de la empresa francesa Areva, entre ellos hay cinco franceses.

– 29 de octubre: se descubren dos paquetes de correo que contenían explosivos a bordo de aviones de carga que se dirigían de Yemen a Estados Unidos. Al Qaeda en la península Arábiga reclama esta operación frustrada.

Año 2011:

– 7 de enero: AQMI intenta secuestrar a dos franceses en un restaurante en Niamey, la capital de Níger. Las fuerzas francesas interceptan a los militantes cerca de la frontera con Mali. Los dos rehenes y cuatro de sus secuestradores mueren durante el enfrentamiento.
– 8 de febrero: aprobación de la *National Military Strategy* de Estados Unidos.
– 2 de mayo: fuerzas especiales de Estados Unidos localizan y matan a Osama ben Laden en una villa en Abbottabad (Pakistán).
– 21 de octubre: Barack Obama anuncia la retirada de las tropas estadounidenses de Irak en dos meses.
– 15 de diciembre: escenificación del repliegue de Irak mediante el arriado de la bandera en Bagdad, a la que asistió el secretario de Defensa, Leon Panetta.
– 17 de diciembre: el Senado de Estados Unidos aprueba la Ley de Financiación de la Defensa Nacional.
– 18 de diciembre: los últimos soldados estadounidenses abandonan Irak.

Año 2012:

– 3 de enero: aprobación del Documento *Sustaining U.S. Global Leadership: Priorities for 21st Century Defense*.
– 15 de enero: Al Qaeda ataca y toma el control de la ciudad yemení de Rada.

Bibliografía

Blanco Navarro, Jose María: «Seguridad e Inteligencia 10 años después del 11-S», Instituto Español de Estudios Estratégicos (IEEE), Madrid, 2011.

Borger, Julián: «Afghanistan Conference Promises Support After Troop Withdrawal», edición *web* de *The Guardian,* 5 de diciembre de 2011.

Congressional Research Service: *International Terrorism: Threat, Policy and Response,* enero de 2007.

De la Corte Ibáñez, Luis: «El futuro de Al Qaeda tras el X aniversario del 11-S: posibles trayectorias y variables involucradas», *Documento de Opinión,* número 62, IEEE, Madrid, 2011.

Department of Defense: *Quadrennial Defense Review,* febrero de 2010.

Kamen, Al: «The End of The Global War on Terror», *The Washington Post*, edición *web,* 25 de marzo de 2009.

Keeley, Brian: *International Migration. The Human Face of Globalization,* Organización para la Cooperación y el Desarrollo Económico, 2009.

Mullin, Corinna: «The U.S. discourse on political Islam: is Obama's a truly post-"war on terror" administration?», *Politics and International Studies, School of Oriental and African Studies,* University of London, 2011.

Pardo, Pablo: «… Y elimina derechos civiles», *El Mundo,* 19 de diciembre de 2011.

Record, Jeffrey: *Bounding the Global War on Terrorism*, Strategic Studies Institute, 2003.

Reinares, Fernando: «Después de Osama ben Laden ¿cómo quedan Al Qaeda y el terrorismo global?», *ARI,* número 83, Real Instituto Elcano, Madrid, 3 de mayo de 2011.

Ruiz González, Francisco J.: «Tendencias y dilemas internacionales tras el 11-S de 2001: ¿un sistema internacional en transición?», DIEEEA23-2011, IEEE, Madrid, 2011.

Schmidt, M.: «Leaving Iraq, U.S. Fears New Surge of Qaeda Terror», edición *on-line* de *The New York Times,* 2011.

Schmitt, Eric: «Obama Issues Order for More Troops in Afghanistan», *The New York Times on-line,* 30 de noviembre de 2009.

Solana, Javier y Basset, Lluís: *Primaveras, terremotos y crisis*, Random House Mondadori, S. A., Barcelona, 2010.

The White House: *National Security Strategy,* marzo de 2006.
— *National Security Strategy,* mayo de 2010.
— *National Strategy For Combating Terrorism,* febrero de 2003.
— *National Strategy For Combating Terrorism,* septiembre de 2006.

VV.AA.: «La guerra mundial contra el financiamiento del terrorismo», *Economic Perspectives E Journal,* septiembre de 2004.

— «Legislación antiterrorista comparada después de los atentados del 11 de septiembre y su incidencia en el ejercicio de los derechos fundamentales», *ARI,* número 7, Real Instituto Elcano, Madrid, 2006.

— *Media and mediation in the «war on terror»: issues and challenges,* Critical Studies on Terrorism. Department of Media and Communication, University of Leicester, Reino Unido, 30 de abril de 2009.

White Paper of the Interagency Policy Group's Report on U.S. Policy Toward Afghanistan and Pakistan, 2006.

Woods, Joshua: *Framing Terror: an Experimental Framing Effects Study of the Perceived Threat of Terrorism, Critical Studies on Terrorism*, West Virginia University, 2011.

Zakaria, Fareed: «The Post-Imperial Presidency», *Newsweek-The Daily Beast,* diciembre de 2009.

Páginas web

En: *www.cnn.com*

En: *www.elmundo.es*

En: *www.fund-culturadepaz.org*

En: *www.guardian.co.uk*

En: *www.rtve.es*

En: *www.washingtonpost.com*

En: *www.whitehouse.gov*

LA UNIÓN EUROPEA Y LA REFORMA DEL SECTOR DE LA SEGURIDAD

Manuel S. Herráiz Martínez
Coronel de Ingenieros (DEM)

En el presente artículo se intenta analizar la labor que la Unión Europea desempeña actualmente en el ámbito de la Reforma del Sector de la Seguridad (SSR), la importancia que concede a este relativamente novedoso concepto, y el lugar que quiere ocupar en el concierto internacional en su contribución a la estabilidad y sostenibilidad de aquellos Estados que de una u otra forma están necesitados de este tipo de reformas.

Introducción

Los anhelos de paz perpetua y las condiciones para lograrla han sido objeto del estudio de eminentes filósofos como Kant ya desde el siglo XVIII, y de elaboración de numerosas teorías para alcanzar el deseado objetivo, y continúan siendo objeto de debate, de elaboración de nuevas fórmulas y de realización de renovados esfuerzos si cabe aún más en la actualidad.

Si diversos son los actores que enarbolan el protagonismo en esta decidida cruzada en la búsqueda de la paz, la Unión Europea no es un elemento menor. En el presente artículo se pretende hacer un análisis de la importancia que este organismo concede a este relativamente nuevo concepto, del lugar que Europa quiere ocupar en el concierto internacional, y del papel que desempeña actualmente en su contribución a la estabilidad y sostenibilidad de los gobiernos necesitados de estas reformas.

Aunque pueda parecer que el concepto de SSR en sus siglas inglesas, que es como nos referiremos a este concepto en lo sucesivo, contiene en sí mismo su propia definición, una descripción que podría ayudar a entender la complejidad del mismo sería la de un malabarista que tiene que mantener permanentemente en el aire un número determinado de

bolos para alcanzar el éxito en su espectáculo, de modo que la caída de tan sólo uno de ellos puede llegar a malograrlo.

Estos elementos, tomados al azar y sin pretensión de establecer *a priori* ninguna relación o prelación entre ellos, pueden ser tan aparentemente variados como los de conflicto, democracia, milicias, donantes, justicia, derechos humanos, legitimidad, género, pobreza, bienestar, y también conceptos más novedosos y específicos como propiedad local *(local ownership)* o prácticas de buen gobierno, a los que continuamente se siguen añadiendo otros nuevos en función del contexto y de las experiencias que se viven sobre el terreno en este campo.

Lo anterior sirve para ilustrar alguna de las señas distintivas de la SSR: su carácter abierto, al ser un concepto en continua evolución y cuya definición varía sustancialmente en función del contexto al que se aplique, y su naturaleza holística, porque no se puede pensar en una SSR sin tener en cuenta aspectos políticos, económicos y sociales, y a la inversa, el desarrollo de estos últimos se dificulta enormemente si no se dan las necesarias condiciones de seguridad que permitan su implantación.

En relación con la denominación del concepto, hay que señalar que ha habido, y seguramente aún hay en la actualidad, diversos términos para referirse a este tipo de reformas, aunque quizá el que más se está imponiendo actualmente sea el de «sector» de la seguridad al que nos referiremos en el presente artículo. Llamamos la atención sobre este aspecto para alertar sobre impresiones engañosas que puedan llevarnos a pensar que el concepto SSR «pertenece» más a unas organizaciones que a otras si atendemos exclusivamente a la similitud de los términos, y siguiendo esa misma lógica a caer en el error de dejar de lado a otros organismos que se han dedicado en profundidad a estas cuestiones, simplemente por el hecho de haber empleando o de estar empleando una terminología distinta.

Este sería el caso de la Organización para la Seguridad y Cooperación en Europa (OSCE), cuya razón de ser está precisamente en el origen del concepto SSR, aunque empleando otros términos, como prevención de conflictos, gestión de crisis, rehabilitación en el posconflicto, control del armamento, derechos humanos, minorías, democratización y desarrollo económico, entre otros. Otras organizaciones sí se han adecuado a la terminología SSR, como la Organización para la Cooperación y el Desarrollo Económico (OCDE), las Naciones Unidas y organizaciones

regionales, principalmente en el contexto africano, adoptando términos como «la reforma del sistema de seguridad», «la reforma del sector de la justicia y la seguridad», o la «transformación del sector de la seguridad» respectivamente.

Conviene finalizar esta introducción, en primer lugar, poniendo de manifiesto el reconocimiento unánime de la comunidad internacional acerca de esta necesidad y de la importante dimensión que la SSR ha adquirido en el marco de la seguridad global, y en segundo lugar y refrendando lo anterior, aportando una valoración, a modo de tesis, recogida en la monografía de un alumno del Curso de Estado Mayor de las Fuerzas Armadas, que este autor considera muy acertada y útil para entender la esencia del concepto y la relevancia que se le está dando en el mundo occidental:

> «La SSR es el nuevo paradigma occidental de intervención a favor de la paz y del desarrollo» (1).

Antecedentes y marco general

Como ya se ha comentado, quizá haya que buscar los orígenes del concepto SSR en la OSCE, o más exactamente en su predecesora, la Conferencia para la Seguridad y la Cooperación en Europa (CSCE), que ya desde su creación en los años setenta, si bien orientada únicamente a las relaciones Este-Oeste derivadas de la guerra fría, ha perseguido abordar la cuestión de la seguridad desde un Enfoque Integral *(Comprehensive Approach)* incorporando aspectos político-militares, económicos, ambientales y humanos, y abarcando una amplia gama de asuntos como los ya mencionados de democratización, desarme y control de armamento, respeto a las minorías y desarrollo económico, por citar sólo unos pocos, labor que continúa en la actualidad. A partir de la desintegración de la Unión Soviética, la Organización del Tratado del Atlántico Norte (OTAN) y la Unión Europea entraron a desempeñar un papel principal en este tipo de reformas, cada una con su particular enfoque: la OTAN dirigiendo sus actuaciones a la reforma de la Defensa, y la Unión Europea concentrando sus esfuerzos en aspectos de seguridad interior como la policía, el control de fronteras o las políticas de asilo y de ayuda a los refugiados.

---

(1) Cadoudal, R.: «La reforma del sector de seguridad. Nuevo paradigma occidental de acción a favor de la estabilidad global», *Monografía* del Curso de Estado Mayor de las Fuerzas Armadas.

Es a partir de finales de los años noventa cuando todos estos aspectos comienzan a aglutinarse en torno al término SSR. Así, en el año 1999 el, a la sazón, secretario general de Naciones Unidas, Kofi Annan, defendió ante el Banco Mundial refiriéndose al buen gobierno la necesidad de reformar los servicios públicos, entre los que había que incluir el sector de la seguridad, que debía estar sujeto a los mismos estándares de eficiencia, equidad y sometimiento a la Ley que cualquier otro servicio público. Es también en esta época cuando el concepto SSR empieza a ser considerado como una condición previa al desarrollo estable, y comienza a ser empleado por la denominada «comunidad del desarrollo» para que los donantes pudieran justificar su mayor implicación en asuntos tan impopulares y espinosos como la potenciación de todo lo relacionado con la seguridad.

La vinculación de la SSR a la idea de desarrollo ha propiciado una participación muy activa en este área de la OCDE. Prueba de ello es que el Manual elaborado en el año 2007 por su Comité de Ayuda al Desarrollo (DAC) está considerado como uno de los principales Documentos de referencia en la actualidad (2). De este Documento hay que señalar que está orientado fundamentalmente a los donantes, y marca las pautas por las que se ha de regir el esfuerzo económico que realizan estos importantes actores para obtener los resultados deseados de eficiencia y sostenibilidad de las donaciones.

Paradójicamente, el Manual de la OCDE no contiene una definición de la SSR en las más de 200 páginas que dedica a tratar exclusivamente de este concepto. Como quiera que siempre resulta conveniente contar con una definición para ayudar a entender un concepto, acudiremos de nuevo a la *Monografía* del Curso de Estado Mayor de las Fuerzas Armadas ya mencionado para adoptar la excelente definición que se recoge en la misma:

> «Proceso cuyo objeto principal es proporcionar seguridad estatal y humana eficiente en un marco de gobierno democrático, adoptando un enfoque integral. La SSR contribuye a la promoción y consolidación de la democracia y los derechos humanos. Su implementación tiene dos aspectos principales: el desarrollo de unos cuerpos e instituciones de seguridad eficaces, y el desarrollo de

(2) *The OECD DAC Handbook on Security System Reform (SSR)*, Supporting Security and Justice.

los mecanismos de control de los mismos conforme a normas democráticas» (3).

A los contextos ya mencionados de democratización de los países del Este, cuya denominación internacionalmente reconocida es la de contexto posautoritario, y de ayuda al desarrollo, denominado contexto de desarrollo, hay que añadir un tercero, el contexto del posconflicto, que completa el conjunto de los tres grandes contextos en los que encuentra aplicación el concepto SSR.

Para hablar del último de ellos, el contexto de posconflicto, hay que referirse ineludiblemente al Centro de Ginebra para la Democratización y el Control de las Fuerzas Armadas (DCAF). Éste fue creado en el año 2000 por iniciativa de la Confederación Helvética con la finalidad de contribuir a mejorar la Gobernanza del Sector de Seguridad (SSG) a través de la SSR.

El DCAF es una institución líder en el sector. Está compuesta por 61 Estados miembros de todo el mundo, y se dedica a proporcionar asesoramiento y apoyo a los Estados y organizaciones que lo soliciten, principalmente países en conflicto y «Estados frágiles», en el área de SSR. El Equipo Internacional Asesor en el Sector de la Seguridad (ISSAT) se creó en el año 2008 como parte integral del DCAF, está constituido por estamentos y organismos de 14 Estados miembros, todos ellos europeos excepto Canadá, entre los que no se encuentra España, y de tres organizaciones internacionales: la Organización de Naciones Unidas, la OCDE y la Unión Europea, y apoya a sus miembros proporcionando diversos servicios, entre los que se encuentra el de adiestramiento.

El *soft-power* y el *hard-power*

El término *soft-power* que en el año 1990 acuñara Joseph Nye para tratar de desmentir la opinión cada vez más extendida por aquel entonces de que Estados Unidos estaban comenzando su periodo de decadencia, ha sido utilizado desde entonces y sigue siéndolo en la actualidad para diferenciar dos formas radicalmente distintas de percibir también la política internacional.

---

(3) Cadoudal, R.: «La reforma del sector de seguridad. Nuevo paradigma occidental de acción a favor de la estabilidad global», *Monografía* del Curso de Estado Mayor de las Fuerzas Armadas.

En los últimos tiempos este término ha servido de argumento para marcar diferencias políticas de unos países con respecto de otros, principalmente equiparando el término a la idea de multilateralismo en contraposición al supuesto unilateralismo que errónea o interesadamente se ha querido atribuir consecuentemente al término *hard-power*.

A este respecto conviene señalar la definición de *soft-power* que hace Joseph Nye (4) según la cual el *soft-power* «es la abilidad para conseguir lo que quieres mediante la atracción en lugar de la coerción o los pagos». De esta definición se deduce que la coerción –el palo– en sus distintas formas, ya sea esta puramente militar o de otra índole, como por ejemplo económica, y los incentivos –la zanahoria– del tipo que sea son en realidad dos caras de la misma moneda: el denominado *hard-power*. El *soft-power* tendría que ver según esta definición con el atractivo que un país o una comunidad despierta por su cultura, sus ideales o su política.

Este fue el principal activo de Estados Unidos durante al guerra fría, época en la que los ideales de democracia, libertad individual y prosperidad de Estados Unidos ejercían un enorme atractivo si se confrontaban con el sistema totalitario y opresivo del bloque soviético. En aquel entonces se trataba de ganar una guerra en la que existía una amenaza directa, tangible y medible contra Occidente.

Aquella guerra se ganó. Sin embargo, los atentados del 11 de septiembre de 2001 llevaron a Estados Unidos a declarar una nueva guerra, esta vez global, contra un enemigo mucho menos definido y medible y que ya no amenazaba de forma tan directa y tangible a todo el Occidente en su conjunto: el terrorismo. Esta percepción desigual de la nueva amenaza, junto con una desconcertante actitud comprensiva en algunos casos hacia los pretextos que los terroristas esgrimían para la perpetración de sus atentados terroristas, llegaron a encontrar eco incluso en organismos tan respetables como Naciones Unidas, que llegó a argumentar que el terrorismo era la única respuesta posible del débil ante los abusos del poderoso, y condujeron a una fractura dentro del mundo occidental que ha llevado a Europa a hacer lo posible por apartarse de la impopular política estadounidense de la última década.

Ahora de lo que se trata es de ganar la Paz con mayúsculas, una paz sostenible, esa paz perpetua tan anhelada, y para ello el *soft-power* se ha

(4) Nye, J. S. jr.: «Soft power: the means to success in world politics», *PublicAffairs*, 2004.

convertido en un elemento esencial. Desde esta perspectiva, puede decirse que, aunque mal empleado, el término *soft-power* es visto como un elemento distintivo de la Unión Europea para marcar las líneas maestras de su acción exterior y diferenciarlas de las del espejo en que continuamente se mira: Estados Unidos de América.

La aproximación *Bottom-Up*

Vista desde el terreno, la solución aportada por Occidente para la resolución de las crisis regionales ha estado basada principalmente en el despliegue de fuerzas militares que han asegurado mediante su presencia la implantación de los acuerdos de paz entre las partes en conflicto. La filosofía que se escondía detrás de este modo de actuación ha sido siempre la de que eran las propias fuerzas internacionales los principales, cuando no los únicos, garantes de la seguridad y la estabilidad del país en cuestión. La consecuencia de todo ello ha sido que la desaparición de dichas fuerzas ha llevado inevitablemente aparejada la desaparición también de la seguridad y estabilidad necesarias para garantizar el futuro de las regiones afectadas.

Es este convencimiento de la insuficiencia de la solución militar para «ganar la paz» el que ha llevado a las diferentes organizaciones a sentir la necesidad de adoptar un Enfoque Integral *(Comprehensive Approach)* que implique a instrumentos políticos, civiles y militares para las gestiones de crisis. Este es el caso de la OTAN, cuyo último Concepto Estratégico, aprobado en la cumbre de Lisboa en noviembre de 2010, recoge como una de las lecciones aprendidas de sus operaciones la necesidad de adoptar este enfoque integral para mejorar la capacidad de esta organización de contribuir a la estabilización y la reconstrucción en las situaciones posconflicto.

La aproximación *Top-Down* o el desarrollo normativo del concepto y la transformación de las estructuras

La Unión Europea ha recorrido un largo camino que arranca desde el final de la Segunda Guerra Mundial. Aunque inicialmente orientado a cuestiones económicas, siempre ha tenido como telón de fondo la preocupación

por la seguridad. Inicialmente referida esta preocupación a la preservación de la paz en la propia Europa, la seguridad ha pasado con el paso de los años a formar parte de las dos grandes políticas que conforman lo que se ha venido en denominar el segundo pilar de la Unión: la Política Exterior y de Seguridad Común (CFSP, en sus siglas inglesas), y la Política de Seguridad y Defensa Común (CSDP, en sus siglas inglesas).

A pesar de los claros vínculos que deberían existir entre ambas, estas dos políticas no han ido siempre de la mano. De hecho, cuando la CFSP fue establecida en el Tratado de Maastricht a comienzos de los años noventa, la CSDP, o más bien su antecesora, la Política de Seguridad y Defensa Europea (ESDP, en sus siglas inglesas) no existía aun formalmente. Y a la inversa, cuando en el año 2003 se lanzó las primeras misiones de la ESDP, la CFSP estaba estancada debido a las diferencias entre los países miembros sobre la guerra de Irak.

A lo anterior hay que añadir que la política de la Unión Europea en materia de SSR no está contenida en un solo documento, sino en tres Documentos distintos correspondientes cada uno a organismos diferentes. Elaborados entre los años 2005 y 2006, estos Documentos establecen el apoyo de la ESDP a la SSR (5), el apoyo de la Comunidad Europea al SSR (6), y las conclusiones del Consejo sobre el marco político de la Unión Europea en materia de SSR (7) respectivamente. A pesar de que en este último se pone de manifiesto la necesidad de coordinación, cooperación y coherencia en las actividades de los diferentes pilares de la Unión Europea, no proporciona un método sistematizado para alcanzar este objetivo, dejando sin resolver los continuos problemas de solape de responsabilidades y de división del trabajo entre ellos.

La aprobación del Tratado de Lisboa en diciembre de 2007, y la creación del cargo de alto representante de la Unión para la Política de Asuntos Exteriores y de Seguridad han significado, en el primero de los casos, el fin definitivo de las vidas paralelas que seguían la CFSP y la ESDP, al

---

(5) *EU Concept for ESDP Support to Security Sector Reform*, Council of the European Union, Bruselas, 13 de octubre de 2005, 12566/4/05 REV 4

(6) *A Concept for European Community Support for Security Sector Reform*, Communication from the Commission to the Council and the European Parliament, Bruselas, 24 de mayo de 2006, COM(2006) 153 final.

(7) *Council Conclusions on a Policy Framework for Security Sector Reform*, 2736th General Affairs Council Meeting, Luxemburgo, 12 de junio de 2006.

presentar a esta última, la CSDP ya con sus siglas actuales, como una parte integral de la CFSP, y en el segundo, la consecución de una mayor coherencia institucional y una mayor eficacia en la acción exterior de la Unión Europea.

El cargo que estrenó y sigue ocupando en la actualidad la británica Catherine Ashton asume los cometidos de los ya desaparecidos altos comisionados para CFSP, por un lado, y de Relaciones Externas, por otro, a los que sustituye. Esta fusión permite poner fin al tradicional conflicto entre el primer y el segundo pilar de la Unión Europea –el pilar del desarrollo, bajo la Comunidad Europea, y el de la seguridad, a cargo de la CFSP-ESDP, respectivamente– en materia de SSR, por los problemas ya mencionados de solape de competencias entre ambos y de falta de claridad en la división de tareas y en los procedimientos de coordinación entre ellos.

El Tratado de Lisboa contempla asimismo la creación de un nuevo órgano para asistir a la alta representante en el desempeño de sus cometidos, el Servicio de Acción Exterior Europeo (EEAS por sus siglas inglesas). Sin detenernos a examinar las complejas relaciones y estructura de este nuevo organismo, baste decir que el EEAS integra en él las nuevas delegaciones de la Unión Europea, es decir, las «embajadas» de la Unión, que dejan de ser delegaciones de la Comisión, y las estructuras de gestión de crisis, como la Dirección de Gestión de Crisis y Planificación (CMPD), la Capacidad Civil de Planeamiento y Ejecución (CPCC), y el Estado Mayor de la Unión Europea (EUMS).

La SSR desde el punto de vista de la Unión Europea

En primer lugar, hay que decir que la Unión Europea reconoce el liderazgo de la OCDE en este campo, al adoptar explícitamente la definición de la SSR que establece ese organismo, lo cual no es de extrañar teniendo en cuenta el importante papel que concede la Unión Europea a la faceta del desarrollo en su política exterior.

El marco de la política de la Unión Europea para la SSR está constituido por los dos Documentos ya mencionados sobre el concepto de apoyo a la SSR de la ESDP y de la Comunidad Europea respectivamente, tal y como lo establecen las conclusiones de la 2736 reunión del Consejo Europeo celebrada en Luxemburgo el 12 de junio de 2006. En dichas con-

clusiones se marcan también los principios que debe presidir la actuación de la Unión Europea en este campo.

Estos principios pueden resumirse en la necesidad de que el proceso de reforma sea asumido por la propia nación *(national ownership)* y que esté diseñado para fortalecer el buen gobierno, las normas democráticas, el imperio de la ley, y el respeto a los derechos humanos. Otros requisitos son la sensibilidad hacia las cuestiones de género, el reconocimiento de la importancia del papel de la sociedad civil, y la necesidad de transparencia y de supervisión parlamentaria de los procesos de reforma de la seguridad.

Entre estas conclusiones del Consejo hay que destacar la necesidad que establece este órgano de analizar las situaciones caso por caso para asegurar una acción exterior de la Unión Europea efectiva y coherente en esta área, así como la de trasladar estos conceptos al campo operativo.

No se puede dejar de señalar la referencia que se hace en el Documento a la importancia de contribuir a alcanzar los compromisos de la Declaración del Milenio de septiembre del año 2000 y de los Objetivos de Desarrollo del Milenio de Naciones Unidas, como tampoco la alusión que hace a los objetivos de seguridad contenidos en la Estrategia Europea de Seguridad (ESS).

La ESS (8), adoptada por el Consejo Europeo en diciembre de 2003, es uno de los principales documentos de referencia en los que se basa la política europea para la SSR, como así lo reflejan los tres documentos ya mencionados que conforman este marco político.

En la ESS se señalan las principales amenazas para Europa, a saber, el terrorismo, la proliferación de armas de destrucción masiva, los conflictos regionales, los «Estados fallidos», y el crimen organizado, y se recogen los tres objetivos estratégicos de la Unión Europea: hacer frente a las amenazas en un mundo globalizado, construir seguridad a nuestro alrededor *(neighbourhood)*, y contribuir a un orden internacional basado en un multilateralismo eficaz.

El Documento finaliza analizando las implicaciones políticas para Europa de esta estrategia, que se deben traducir en una Europa más activa

(8) E*uropean Security Strategy: A secure Europe in a better world*, Bruselas, 12 de diciembre de 2003.

(preventive engagement), más capaz, aumentando los recursos para la Defensa y el uso compartido de los mismos *(pooled and shared assets)*, más coherente, integrando los diferentes instrumentos y capacidades disponibles; y en una Europa que trabaje con sus socios *(partners)*, y que considere el vínculo transatlántico como «irreemplazable».

El proceso de implantación SSR de la Unión Europea

El proceso de implantación de la SSR de la Unión Europea comenzó en 2007, un año después de adoptar también su política en materia de SSR ya mencionada.

Informes relevantes sobre el proceso de implantación de la política SSR de la Unión Europea muestran que hay una diferencia sustancial entre la definición de dicha política y el enfoque en la práctica. Como se mencionó anteriormente, la política define la SSR no sólo como un requisito para la seguridad del Estado, sino también para las personas, y al mismo tiempo, define el sector de la seguridad como un sistema que incluye no sólo a los actores principales en el campo de la seguridad, sino también a organismos de gestión y supervisión, de administración de justicia, y agentes de seguridad no estatales. Por lo tanto, sobre el papel, la política de la Unión Europea comporta un enfoque holístico de la SSR. Sin embargo, en la práctica, la mayor parte de los proyectos de apoyo a la SSR de la Unión Europea de los últimos años no han reflejando este carácter integral de la SSR, concentrándose únicamente en uno o dos aspectos del sector de la seguridad. No sólo se han ignorado casi por completo elementos tan relevantes como la supervisión democrática o el ejercicio de una gestión pública transparente, sino que, además, al concentrarse únicamente en los diversos aspectos de forma individual se ha tendido a ignorar las interrelaciones existentes entre ellos.

El paradigma de la SSR: Suráfrica

Suráfrica es un ejemplo claro de la importancia que puede llegar a adquirir el principio de *local ownership* para resolver con éxito situaciones tan difíciles como las que tuvo que afrontar ese país a partir del año 1994, tras la caída del régimen de segregación racial del *apartheid*.

El recién creado gobierno de Nelson Mandela se propuso como objetivo prioritario dentro del proceso de reconciliación nacional la reforma del sector de la Defensa, para dotar de legitimidad a las Fuerzas Armadas y alejar de la población la imagen de régimen militarista y excluyente que había presidido la vida del país desde el año 1948, cuando se promulgaron las primeras leyes racistas.

Así se puso en marcha un proceso integrador que duró más de dos años y en el que las mujeres desempeñaron un importante papel en sus demandas para que tanto el gobierno como las instituciones militares rindieran cuentas *(accountability)* de sus actuaciones durante el proceso, para que este fuera transparente y para que se involucrara a la sociedad civil en el mismo.

El resultado de todo ello fue que el proceso de revisión de la Defensa se convirtió en un proceso consultivo nacional en el que se procuró que todo el mundo pudiera expresar sus opiniones y sus preocupaciones. Esta participación contribuyó decisivamente a construir un consenso nacional en torno a los asuntos de Defensa, y dotó de legitimidad a las nuevas estructuras de seguridad.

Seguramente este gran éxito en el proceso de la reforma de la seguridad en Suráfrica no se habría conseguido de no haberse dado dos factores que perfectamente pueden tener encaje en el concepto de *local ownership*: el compromiso decidido del propio Gobierno surafricano para transformar el sector de la seguridad, sin necesidad de influencias externas, las de los donantes, que trataran de inculcar previamente esos principios para luego exigirlos como condición previa a las ayudas, y la legitimidad del propio Gobierno ante su población para poner también en marcha dichos procesos.

Un caso práctico: Guinea-Bissau

Guinea-Bissau es un interesante caso que ilustra a la perfección algunas realidades acerca de la aplicación práctica del concepto SSR, en particular en lo relativo a la propiedad local *(local ownweship)* y a las enormes exigencias económicas de este tipo de programas.

En relación con el concepto de «propiedad local», según el cual debe ser el propio país el que sancione e impulse las reformas necesarias, hay

que decir que una de las principales amenazas para que se cumpla esta condición es la existencia de regímenes políticos impredecibles y volátiles, circunstancia esta que se da con mucha frecuencia en Estados en proceso de consolidación democrática como el de Guinea-Bissau.

Desde su independencia de Portugal en el año 1974, Guinea-Bissau ha llevado a cabo un proceso lento de democratización que ha manteniendo en su Constitución un sistema de partido único durante 17 años, hasta su abolición y la adopción de un sistema político pluripartidista en el año 1991.

A esta lentitud en el proceso de consolidación democrática hay que añadir la presencia permanente del Ejército en la turbulenta vida política del país desde su independencia, debido a la sucesión de golpes de Estado, autonombramientos de cargos militares, como el de Jefe de Estado Mayor de la Defensa (JEMAD) del general N'djai, hasta ese momento segundo JEMAD, tras arrestar a su titular, el vicealmirante, Zamora Induta, en los sucesos del 1 de abril de 2010; asesinatos, como el del mismo presidente Vieira en el año 2009, e incluso guerras civiles, como la que sufrió el país entre los años 1998 y 1999.

Como cabía esperar, la corrupción también parece estar presente en medio de este torbellino que son las Fuerzas Armadas de Guinea-Bissau. En efecto, Guinea-Bissau se ha convertido en los últimos años en el epicentro del tránsito de la cocaína procedente de Iberoamérica con destino a Europa. A este respecto, informes recientes de Naciones Unidas señalan que altos cargos militares de este país estarían involucrados en actividades de tráfico de drogas. Corrobora esta sospecha, a modo de ejemplo, el nombramiento en octubre de 2010 del almirante Na Tchuto, como jefe de Estado Mayor de la Armada, a pesar de estar en la lista negra de tráfico internacional de droga de Estados Unidos.

El fallecimiento en enero del presente año del presidente Sahna, responsable de la confirmación oficial en su cargo en junio de 2010 del hasta entonces autonombrado JEMAD, el general N'djai, parecía haber eliminado un obstáculo para el necesario impulso de la comunidad internacional a la implantación del plan de SSR en Guinea-Bissau. Sin embargo, el 12 de este mismo mes de abril, dos semanas antes de celebrarse la segunda ronda de las elecciones presidenciales, se ha producido el enésimo golpe de Estado que pone en peligro la celebración de los comicios y amenaza con dejar una vez más en suspenso el proceso SSR también en aquel país.

Por su parte, la Unión Europea cerró su misión en apoyo de la SSR en Guinea-Bissau en septiembre de 2010, debido al incumplimiento de todos los requisitos exigidos para continuar con la misión, esto es, el restablecimiento del orden constitucional y del imperio de la ley, el fin de la detención ilegal del depuesto JEMAD, Zamora Induta, y el castigo de los responsables de los incidentes del 1 de abril. Esta misión se había lanzado en junio de 2008 bajo el segundo pilar de la Unión Europea, la CSDP, y ha invertido un total de ocho millones de euros en distintos proyectos encaminados a crear las condiciones para la implantación de la Estrategia Nacional de Seguridad de Guinea-Bissau, que había sido aprobada por la Asamblea Nacional de aquel país en enero de 2008.

A esta hay que añadir aportaciones adicionales de la Unión Europea por valor de más de 10 millones de euros, así como las de otras organizaciones globales y regionales como la Organización de Naciones Unidas (13 millones de dólares) o la Comunidad Económica de los Estados de África Occidental (ECOWAS), y de países como: Brasil, Portugal, China, Estados Unidos, Angola, Suráfrica, Italia, España o Canadá.

Es difícil cuantificar el alcance de la ayuda de todos estos donantes desde que se iniciara el proceso de reforma, pero las cifras que se han podido aportar en este artículo y el considerable número de actores involucrados en esta tarea dan sin lugar a dudas una idea del enorme esfuerzo que se requiere para afrontar un proyecto de esta naturaleza, máxime teniendo en cuenta que en este caso se trata de uno de los países más pequeños de África, con tan sólo 30.000 kilómetros cuadrados de extensión y 1,5 millones de habitantes, y que todo ese esfuerzo no ha impedido que el país se encuentre sumido de nuevo en una situación de extrema incertidumbre tras el último golpe de Estado del pasado 12 de abril. Todas estas consideraciones obligan necesariamente a plantearse si merece la pena realizar el esfuerzo que supone emprender este tipo de reformas cuando no se dan las condiciones mínimas que permitan alentar expectativas realistas de que se puedan alcanzar los objetivos deseados.

Otras aplicaciones de la SSR

En los dos epígrafes anteriores hemos abordado el análisis sucinto de la SSR en dos países: Suráfrica y Guinea-Bissau, y hemos visto que los

procesos SSR en estos países se desarrollan en dos contextos distintos uno del otro.

En el caso de Suráfrica, el proceso SSR se produce tras la caída de un régimen autoritario. Por tanto, este caso entraría dentro del contexto denominado «posautoritario» que hemos definido en estas páginas. Pero esta catalogación quedaría incompleta si no se tuviera en cuenta una seña distintiva del régimen surafricano: su carácter segregacionista. De hecho, es esa particularidad y su deseo de erradicarla la que mueve el motor de las reformas en ese país, prestando para ello una especial atención a lo que en terminología SSR se denomina «cuestiones de género», que aquí tiene una acepción mucho más amplia de la comúnmente entendida, referida únicamente a la mujer, y se aplica a todo colectivo que sea objeto de discriminación, y por tanto de inseguridad, y que en este caso se centró principalmente en la población no blanca.

En el caso de Guinea-Bissau la situación de partida es distinta. Nos encontramos aquí con un país que consigue su independencia de Portugal y decide emprender un proceso de transición democrática, y cuya situación puede ser catalogada de «posconflicto»: inestabilidad política, administración frágil, pobreza y subdesarrollo, corrupción, infraestructuras deficientes, etc.

Estos dos ejemplos representan la importancia y la atención que se ha concedido hasta ahora a estos dos contextos. Sin embargo, esta forma de catalogar la acción SSR refiriéndola exclusivamente a los contextos posautoritario, posconflicto y de ayuda al desarrollo se está demostrando insuficiente para abarcar otros supuestos en los que la comunidad SSR internacional entiende que también podrían ser de aplicación dichas reformas, como los de preconflicto, crimen organizado, e incluso otros como el de la «primavera árabe», en los que la oportunidad en la adopción de reformas en ese sector podría evitar futuros conflictos o el deterioro de la estabilidad de los países en cuestión.

Habría que plantearse por tanto que quizá los principios SSR puedan tener una aplicación universal, sin tener que estar circunscritos a contextos predeterminados, y ser de aplicación también a los países del mundo desarrollado, incluso como medida preventiva de hipotéticas tensiones que pudieran poner en peligro en un momento determinado la estabilidad de un país o de una región.

Viabilidad del proyecto

A lo largo del presente artículo se ha puesto de manifiesto las dificultades de aplicar los principios y de alcanzar los objetivos de la SSR marcados por la Unión Europea. Estos problemas provienen principalmente de una organización compleja y excesivamente fragmentada de la propia Unión, que dificulta la necesaria coherencia en sus actuaciones, y de una implantación defectuosa de dichos principios, que no tiene en cuenta en la mayoría de los casos el necesario Enfoque Integral que garantice el éxito de los proyectos.

A estas dos causas achacables a la propia Unión Europea hay que añadir otras dos, estas externas a la organización, y por tanto universales, que pueden llegar a poner en peligro igualmente la viabilidad de las reformas. Nos referimos al principio de *local ownership* y a la propia viabilidad económica del proyecto.

La primera de ellas, la que se refiere al principio de *local ownership*, es posiblemente la más determinante desde el punto de vista de la percepción de las reformas por parte de la sociedad civil. En efecto, aquí siempre se planteará el dilema de si se debe respetar este principio, aunque pueda ir en ocasiones en detrimento de la «propiedad» de los donantes, es decir, de la firmeza en sus exigencias como condición previa a la donación, o si, por el contrario, han de prevalecer las condiciones de los donantes, aún a riesgo de que el apoyo económico aparezca ante la población como un intento de «comprar» la voluntad nacional.

En cuanto a la viabilidad económica del proyecto, en el caso de Guinea-Bissau antes explicado se pone de manifiesto el ingente esfuerzo, tanto económico como de aportación de recursos personales y materiales, que es necesario realizar para obtener resultados, en la mayoría de los casos, cuanto menos dudosos en relación con las expectativas del proyecto. En el caso de Somalia por ejemplo, la Comisión Europea ha invertido 592 millones de euros en apoyo a la creación de un Estado viable en ese país.

El problema de costes que para el mundo occidental y para Europa en particular supone apostar fuerte por este tipo de soluciones debe llevar a plantearse la posibilidad de una actuación muy selectiva, orientada exclusivamente a aquellos países en los que su inseguridad pueda afectar de forma directa a la propia seguridad de la Unión Europea, países para los que sería de aplicación el principio de que «su seguridad es nuestra

seguridad». A este respecto, Somalia y Guinea-Bissau son sin duda dos países cuya estabilidad y control democrático son importantes para los intereses de Europa, e incluso puede detectarse la mayor prioridad que la Unión Europea concede al primero de ellos si nos fijamos en el apoyo económico que recibe, 70 veces superior en términos absolutos y ocho veces mayor en ayuda *per cápita* que el recibido por Guinea-Bissau.

La cuestión que se plantea es si el gigantesco esfuerzo económico que con toda seguridad supondría el apoyo a todos aquellos países que pudieran entrar en la órbita de las políticas prioritarias de la Unión Europea, ya sea por razones de vecindad, de ampliación de la Unión, regionales o globales, esfuerzo que sería imprescindible cuantificar en cada caso, merecería la pena de ser realizado al confrontarlo con las expectativas reales de alcanzar los objetivos de buen gobierno, control democrático, imperio de la ley y respeto a los derechos humanos que se pretende alcanzar.

Bibliografía

AFRICA, S.: *The Transformation of the South African Security Sector: Lessons and Challenges,* Geneva Centre for the Democratic Control of Armed Forces, 2011.

CADOUDAL, R.: «La reforma del sector de seguridad. Nuevo paradigma occidental de acción a favor de la estabilidad global», *Monografía* del Curso de Estado Mayor de las Fuerzas Armadas.

COMMISSION OF THE EUROPEAN COMMUNITIES: *A Concept for European Community Support for Security Sector Reform,* {SEC(2006) 658}, 2006.

COUNCIL OF THE EUROPEAN UNION: *EU Concept for ESDP support to Security Sector Reform (SSR),* 2005.

— *Policy Framework for Security Sector Reform-Council Conclusions,* Press Release 2736th Council Meeting, 2006.

DCAF: *Reform Security Sector,* 2006.

DERKS, M. and MORE, S.: *The European Union and Internal Challenges for Effectively Supporting Security Sector Reform,* Clingendael Institute, 2009.

DIRECTORATE FOR SECURITY POLICY OF THE FEDERAL MINISTRY OF DEFENCE AND SPORTS OF THE REPUBLIC OF AUSTRIA: *Handbook on CSDP,* 2010.

European Security Strategy: A secure Europe in a better world, 2003.

GLOBAL FACILITATION NETWORK FOR SECURITY SECTOR REFORM: *A Beginner's Guide to Security Sector Reform (SSR),* 2007.

LARRABURE, J. L. and VAZ, E.: *Consultant Peace Building Fund Programme in Guinea Bissau 2008-2011,* Final Evaluation Mission, Final Report, 2011. 26 de septiembre-14 de octubre de 2011.

NYE, J. S. jr.: «Soft power: the means to success in world politics», *Public Affairs,* 2011.

The OECD DAC Handbook on Security System Reform (SSR), Supporting Security and Justice.

UN GENERAL ASSEMBLY RESOLUTION 55/2: *United Nations Millennium Declaration,* 2000.

UNITED NATIONS PEACEBUILDING SUPPORT OFFICE: *Mapping of Resources & Gaps For Peacebuilding in Guinea-Bissau,* 2008.

DELITOS EN INTERNET: CLASES DE FRAUDES Y ESTAFAS Y LAS MEDIDAS PARA PREVENIRLOS

Gemma Sánchez Medero
Profesora de la Universidad Complutense de Madrid

La enorme dependencia de las sociedades occidentales respecto a los sistemas informáticos y electrónicos está haciendo que éstas sean más vulnerables a los posibles ataques cibernéticos y el fraude en la Red. Además, Internet es un medio de fácil acceso, donde cualquier persona, sin tener que relevar su identidad, puede proceder a realizar un ataque que es complicado de asociar, virtualmente indetectable y difícil de contrabandear, por no hablar de alto impacto que alcanza una acción de este tipo al golpear directamente y por sorpresa al adversario. Con lo cual, la Red se está convirtiendo en ese lugar ideal para que los delincuentes lleven a acabo sus acciones y actividades. Por tal razón, a la lo largo de este artículo nos hemos dedicado a estudiar el uso que cada uno de estos actores están haciendo de Internet (clases de estafas y fraudes) y que medidas se están tomando para evitar los posibles ataques cibernéticos y las actividades delictivas, comprando que están obteniendo un resultado parcialmente positivo.

Introducción

Las Tecnología de la Información y el Conocimiento (TIC) han ocasionado una revolución sin precedentes cuyo alcance todavía es insospechado. La globalización está sacudido los pilares de las instituciones y las bases de nuestra sociedad, hasta el punto de sugerir el nacimiento de otra sociedad paralela –a la meramente física– que se conoce como Sociedad de la Información y del Conocimiento. El ciberespacio se está convirtiendo en un punto de encuentro para millones de personas, gracias a su flexibilidad en el uso y a la cantidad de información que pone a disposición de los usuarios. Y esto indudablemente está contribuyendo a que la Red no deje de crecer, llegándose incluso a afirmar que su aparición ha marcado un antes y un después en la era de la información y la comunicación.

Es más, hoy en día todo parece estar interconectado, los sistemas de seguridad, defensa, comerciales, energéticos, sanitarios, comunicación, transporte, bancarios, alumbramiento, bibliotecarios, etc. De tal manera que nos encontramos ante un mundo hiperconectado, donde la Red es un elemento crucial y vital para las sociedades más avanzadas. Pero a pesar de los avances que ha podido suponer no todo ha sido positivo, ya que la Red está favoreciendo el surgimiento de nuevos problemas a los que tiene que hacer frente la sociedad. Así, los términos cibercrimen, ciberdelitos, ciberdelincuencia, ciberterrorismo o ciberguerra se están haciendo un hueco entre nosotros, hasta tal punto que los ciudadanos están aprendiendo a convivir con esta nueva realidad, ya que cada vez está siendo más frecuente encontrar noticias sobre algún hecho ilícito que se ha producido a través de la Red. De ahí que a lo largo de este artículos hayamos marcado como objetivo estudiar las actividades que están realizando los delincuentes en la Red, y que soluciones se están dando y buscando para intentar contrarrestar este tipo de actividades delictivas.

La presencia de los delincuentes y criminales en la Red

La ciberdelincuencia es aquella actividad que emplea los ordenadores o las redes como una herramienta delictiva (1). De ahí, que el ciberdelito suponga un peligro, tanto para los ordenadores como para la información recogida a través de ellos. Más cuando en la mayoría de los países del todo el mundo no existen leyes contra este tipo de delitos, y por no hablar que esta tecnología proporciona a los delincuentes rapidez, comodidad y anonimato. En cualquier caso entre este tipo de delitos cabe destacar: el acceso ilegal a sistemas ajenos, la intercepción ilegal, la interferencia y la pérdida de datos, la interferencia de sistemas, la pornografía infantil, los delitos contra la propiedad intelectual, el robo, la extorsión y el fraude electrónico, etc.

---

(1) La Convención sobre la Ciberdelincuencia del Consejo de Europa define los delitos informáticos como «los actos dirigidos contra la confidencialidad, la integridad y la disponibilidad de los sistemas informáticos, redes y datos informáticos, así como el abuso de dichos sistemas, redes y datos.» *Council of Europe Convention on Cybercrime*, número 185, disponible en: *http;//conventions.coe.int*.

Obtener dinero de forma fraudulenta

Tal vez el más corriente de los fraudes a través de la Red sea el *mail spoofing* y la *web spoofing*. El primero es un procedimiento mediante el cual se pretende suplantar el correo electrónico de un usuario o crear correos electrónicos supuestamente verídicos a partir de un dominio para poder enviar mensajes como si formasen parte de esa identidad. Por ejemplo, cada vez es más frecuente encontrar en nuestros correos mensajes de una entidad bancaria como el Banco Bilbao-Vizcaya-Argentaria o la Caja de Ahorros para el Mediterráneo que dispone de una dirección correo electrónica que solemos identificar con *nombre@bbva.es* o *nombre@cam.org*. En estos mensajes los presuntos clientes suelen recibir la siguiente información:

> «Este mensaje fue enviado automáticamente por nuestro servidor para verificar su dirección de correo electrónico. A fin de validar su dirección de correo electrónico, por favor haga clic en el enlace de abajo.»

De esta manera, obtienen la dirección de su correo electrónico y sus datos, pero también es común que el *mail spoofing* se emplee como una estratagema de ingeniería social para solicitar el número de las tarjetas de crédito a determinados usuarios confiados, que piensan que la procedencia del mensaje se deriva supuestamente de la propia empresa de la que son clientes. El segundo, consiste en una técnica de engaño mediante la cual se hace creer al internauta que la página que está visitando es la auténtica cuando en realidad se trata de una réplica exacta de la misma, pero que se encuentra controlada y monitorizada por un ciberdelincuente que pretende extraerle información y dinero, dependiendo, si se limita a seguir, vigilar, leer y grabar todas las actividades que realice el usuario, o bien, si se dedica a manipular algunos de los datos o, simplemente, le sustrae dinero o utiliza estos datos para efectuar compras en su nombre.

Otro de fenómeno relacionado con este aspecto sería los ciberocupas, que son aquellos individuos o empresas que registran para sí dominios asociados a marcas, empresas o instituciones con la intención de obtener un beneficio revendiéndolo a su propietario legítimo. Otra cuestión son las llamadas telefónicas, un fraude que se realiza entre el módem del ordenador y el proveedor de Internet. Este proceso se realiza habitualmente mediante un nodo local de modo que la tarifa telefónica a pagar le corresponde a una llamada local, de ahí, que el fraude consista en desviar

inadvertidamente la llamada del nodo local a otros prefijos de tipo comercial muchos más caros.

Otro tema es el cibersexo, uno de los negocios más rentables de la Red, ya que la libertad de acceso y el supuesto anonimato contribuye a este hecho. El sexo en Internet no esta penalizado, siempre y cuando cumpla con todos los requisitos legales. El problema es que éste se convierte en ilegal cuando hacemos referencia a la pornografía infantil, o la venta de sexo sin consentimiento a través de Internet, o cuando se engaña a los clientes haciéndoles creer que el acceso a los contenidos de sus páginas es gratuito, cuando son tarifados por una línea de alto coste.

Otro lugar frecuentado por los ciberdelincuentes son los portales de subastas, desde los cuales se ofrece un gran surtido de productos y servicios. El problema es que en la mayoría de las ocasiones estos productos pueden ser falsos o, simplemente, son adquiridos por un comprador pero nunca le son entregados, es decir, pagar sin recibir nada a cambio. La venta de productos farmacéuticos es otro espacio permisible para el fraude. En España la comercialización de medicamentos está prohibida por Internet, sin embargo, cada vez es más frecuente acudir a este medio para hacerse con una serie de productos que en nuestro país sólo pueden ser adquiridos bajo preinscripción médica.

Pero los ciberdelincuentes también se están valiendo de la Red para vender estupefacientes y crear verdaderos mercados temáticos sobre las drogas con una información muy diversas: suministrar, bajo un precio, información sobre todo tipo de actividades ilícitas como, por ejemplo, las debilidades de sistemas de alarma y antirrobo, trucos sobre cómo abrir un coche, asaltar una casa, burlar los sistemas de seguridad, etc., ofrecerse para adentrarse en los sistemas o los ordenadores de empresas o instituciones para robarles, manipular o dañar los datos a cambio de dinero; robar información para después venderla al mejor postor, crear foros dedicados exclusivamente a la compra-venta de datos robados, como números de tarjetas de créditos y otros elementos relacionados con el fraude, sólo mencionar algunos casos.

La estafa nigeriana es otro fraude dentro de esta categoría. Éste consiste en enviar mensajes electrónicos para pedir ayuda a los destinatarios, y de esta forma poder transferir importantes cantidades de dinero a terceros con la promesa de darles un porcentaje si aceptan esa operación a través de sus cuentas personales. Piden también que les transfieran a su nom-

bre una pequeña cantidad de dinero para verificar los datos de la cuenta bancaria con la que se hará la transacción, o que simplemente les envíen los datos de la cuenta bancaria. Una vez que envíen el dinero, las víctimas no volverán a saber nunca más nada de esos estafadores.

Bloquear páginas web

Consiste en adentrarse en las *web* de instituciones, organizaciones, empresas o gobiernos para paralizarlas durante un determinado tiempo con el fin de generar caos, confusión e incertidumbre. Tal vez, el más conocido haya sido el protagonizado por Estonia el 27 de abril de 2007, cuando las páginas oficiales de varios departamentos estonios, las del Gobierno y las del gobernante Partido de las Reformas quedaron bloqueadas por ataques informáticos provenientes del exterior. Al mismo tiempo que los sistemas de algunos bancos y periódicos estuvieron inaccesibles durante varias horas por una serie de ataques Distribuidos de Denegación de Servicio, DDoS *(Distributed Denial of Services).* Hecho que se produjo justo después de que Rusia presionara a Estonia por la retirada de las calles de Tallin de un monumento de la época soviética.

Pero también los que se produjeron durante el conflicto bélico entre Rusia y Georgia. Los mismos tuvieron como consecuencia que distintas páginas *web* gubernamentales se viesen comprometidas, con continuos ataques de denegación de servicio distribuidos contra otras páginas del Gobierno, teniendo como resultado la migración de ciertos sitios a servicios de *posting* de Estados Unidos. Incluso un grupo de ciberactivistas proruso proporcionó ayuda en su página oficial para potenciar a los usuarios de Internet con herramientas para realizar ataques distribuidos de denegación de servicio, proporcionar una lista de páginas georgianas vulnerables a inyección SQL y publicar una lista de direcciones de correos de políticos georgianos para ataques dirigidos y *spam* (2).

Propagar malware

La cantidad de *malware* y la evolución de sus técnicas de infección y propagación se han incrementado de manera considerable a través de los últimos años. No obviemos, que cuando hablamos de *malware* pode-

(2) Informe Cibercrimen de 2008, en: *http://www.s21sec.com/descargas/S21sec-ecrime-Informe-Cibercrimen-2008.pdf*

mos hacer referencia a un virus, un caballo de Troya, una puerta trasera *(backdoor)*, un programa espía *(spyware),* o un gusano. Además, a causa de un *malware* puede derivarse otros ataques como puede ser: DDoS, distribución de correo *spam*, propagación de virus y gusanos hacia otras redes, sitios *phishing*, expansión de *botnets* (redes de equipos comprometidos), fraudes de banca electrónica, *pharming* y *driving*, entre otros muchos otros (Fuentes, 2008; p. 4).

Difamación e información falsa

Internet puede utilizarse para la divulgación de información errónea con la misma facilidad que la información fidedigna. Los sitios *web* pueden contener información falsa o difamatoria, especialmente en los foros y salas de charla donde los usuarios pueden publicar sus mensajes sin la verificación de los moderadores. La difamación puede dañar la reputación y la dignidad de las víctimas en un grado considerable, dado que las declaraciones en línea son accesibles por la audiencia mundial. Aunque la información se corrija o se suprima poco después de su publicación, puede haber sido duplicada «en servidores espejo» y esté en manos de personas que no desean retirarla o suprimirla.

Robo de identidad

Los ataques de suplantación de la identidad presentan varias posibilidades, siendo una de las más conocidas la denominada *IP Spoofing*, mediante la cual un atacante consigue modificar la cabecera de los paquetes enviados a un determinado sistema informático para simular que proceden de un equipo distinto al que verdaderamente los ha originado. Así, por ejemplo, el atacante trataría de seleccionar una dirección *IP* correspondiente a la de un equipo legítimamente autorizado para acceder al sistema que pretende ser engañado. Otro posible ataque sería el secuestro de sesiones ya establecidas, lo que se conoce como *hijacking*, donde el atacante trata de suplantar la dirección *IP* de la víctima y el número de secuencia del próximo paquete de datos que va a transmitir.

Con el secuestro de sesiones, se podrían llevar a cabo determinadas operaciones en nombre de un usuario que mantiene una sesión activa en un sistema informático como, por ejemplo, transferencias desde sus propias cuentas corrientes, siempre que en ese momento se encuentra conectado al servidor de una entidad financiera. Pero también, se pue-

de enviar mensajes con remitentes falsos, *masquerading*, para tratar de engañar al destinatario o causar un daño en la reputación del supuesto remitente. O simplemente se puede capturar las contraseñas, y suplantar la identidad de la persona atacada, o conectarse a conexiones pertenecientes a otras personas.

Espionaje informático

El espionaje consiste principalmente en la obtención no autorizada de datos almacenados en algún fichero automatizado, con lo cual se produce una violación del secreto de información. Para ello, se suele emplear distintas técnicas como, por ejemplo, el «pinchado de líneas» o *wiretapping*, que consiste en la intercepción programada de las comunicaciones que circulan a través de las líneas telefónicas, con el objetivo de procurarse ilegalmente información. O, la «recogida de información residual», que es fruto del propio descuido del propio usuario por no mantener mínimas medidas de seguridad.

¿Cómo intentar reducir los peligros en la Red?

Realmente está resultado sumamente difícil poder encontrar soluciones que resulten efectivas para intentar poner freno a todas aquellas actividades relacionadas con el cibercrimen y la ciberdelincuencia.

La primera solución

Desconectar al ordenador de la Red, aunque está parece totalmente imposible ante unas sociedades que también cada vez se hayan más hiperconectadas.

La segunda solución

Identificar las vulnerabilidades e individualizar los peligros existentes y potenciales que dichas debilidades permiten. Esto sólo se puede conseguir con la ciberinteligencia. El problema que se plantea es que Internet carece de fronteras y el contenido ilícito circula de un país a otro en milésimas de segundos; además existe una escasa o nula regulación de los cibercafés, locutorios, salas de informática públicas, bibliotecas, etc., máquinas populares de acceso a Internet y otras donde de forma anóni-

ma las personas puede conectarse y realizar actividades ilícitas. Lo mismo ocurre con las redes inalámbricas libres al alcance de equipos con conexiones capaces de conectarse a esas redes con el anonimato de la no pertenencia al grupo autorizado (Ruiloba, 2006; p. 53).

Pero éstas no son las únicas dificultades a las que deben hacer frente los policías cuando realizan investigaciones en la Red. Por ejemplo, cuando los posibles delincuentes saben que una máquina está comprometida por ser accesible a través de una conexión pueden convertirla en una *work station virtual* para navegar a través de su dirección sin ser detectados; o cuando utilizan las máquinas cachés de algunos proveedores de comunicaciones para optimizar su rendimiento, ya que garantizan el anonimato de los usuarios para delinquir (Ruiloba, 2006; p. 53).

En todo caso, para evitar estas posibles deficiencias jurídicas están tipificando gran cantidad y variedad de delitos informáticos. Por ejemplo, en nuestro país son considerados como delitos, el ataque a datos y a redes, así como la intercepción de datos. Además son castigados penalmente: la modificación, el borrado, la destrucción o la alteración y el acceso no autorizado a bases de datos, textos o programas mediante el *cracking* y la diseminación de virus. O en Estados Unidos la legislación federal, de fecha 15 de abril de 2002, establece penas para: el acceso no autorizado de sistemas informáticos, previendo específicamente el acceso a sistemas del Gobierno relacionados con la seguridad de Estado, por lo que se encuentra castigada la comunicación, la entrega, la transmisión e incluso el sólo intento de realizar los actos antes mencionados; el uso de cualquier computador de uso oficial o que se esté utilizando en algún momento como oficial que afecten al gobierno; y el acceso de computadoras sin la autorización, o quien tenga acceso a la misma se exceda del permiso que obtuvo (Orta Martínez, 2005).

El problema es que la mayoría de las legislaciones están vigentes en los diferentes países están dirigidas a proteger básicamente la utilización indebida de la Red, incluso algunas de ellas prevén la creación de órganos especializados que protejan los derechos de los ciudadanos, pero poco más. Ahora el Convenio sobre Cibercrimen (3) contiene contenidos de diverso carácter como, por ejemplo, delitos de intrusión en el que se integran infracciones penales contra la confidencialidad, integridad y dis-

(3) Convenio sobre Cibercrimen del Consejo de Europa, celebrado en Budapest, 23 de noviembre de 2001.

ponibilidad de datos y sistemas informáticos, delitos patrimoniales (falsificaciones y fraudes a través de Internet como *phishing* y *pharming*), delitos de contenidos en el que exclusivamente se incluyen delitos de corrupción de menores en su modalidad de pornografía infantil, y delitos de infracción de la propiedad intelectual y derechos conexos que comprende todos los delitos contra la propiedad intelectual y de los derechos afines según la legislación de cada parte, y otros delitos entre se produzcan en Internet.

La tercera solución

Dotarse de medios de seguridad, aunque siempre considerando que existe la posibilidad de que sean vulnerados. Pero establecer una buena política de seguridad en el ciberespacio exige constituir primero un lugar de partida, que debe consistir en analizar los riesgos y las amenazas, para después conocer sus puntos fuertes y sus vulnerabilidades. Después hay que construir un marco normativo que regule la seguridad en el ciberespacio, y en el que intervengan todas las partes. Posteriormente, debería centralizarse la gestión de la ciberseguridad con la creación de un organismo responsable que sea capaz de coordinar a todas las entidades públicas y privadas implicadas en esta materia. Y todo ello, sin olvidar la cooperación internacional a este respecto y fomentar una cultura de ciberdefensa y una promoción de la investigación en el sector de la ciberseguridad. El problema es que los Estados están haciendo más o menos eso, pero de una forma desorganizada y descoordinada, moviéndose a rachas, lo que está conduciendo a que cada país haga la guerra por su cuenta y de una manera precipitada, lo que reducen notablemente la eficiencia de sus estrategias de seguridad nacional e internacional.

La cuarta solución

Intentar adelantarse a cualquier acto delictivo mediante el control de los Sistemas de Información, como pueden ser: Echelon, Enfopol y Carnivore.

SISTEMA ECHELON

Un Sistema automatizado de intercepción global de trasmisiones operado por los servicios de inteligencia de cinco países: Estados Unidos, Gran Bretaña, Canadá, Australia y Nueva Zelanda. Su objetivo inicial era

controlar las comunicaciones militares y diplomáticas de la Unión Soviética y sus aliados durante la guerra fría. Aunque en la actualidad se emplea para interceptar todo tipo de transmisiones con el objetivo de localizar tramas terroristas y planes de narcotráfico, inteligencia política y diplomática. Su funcionamiento básico consiste en situar innumerables estaciones de intercepción electrónica en satélites y en otros puntos para capturar las comunicaciones establecidas por radio, satélite, microondas, teléfonos móviles y fibra óptica. Después cada estación selecciona, mediante la aplicación de unas palabras claves, toda aquella información que guarda relación con el fin que persigue el Sistema Echelon.

Además, cada uno de los cinco países que componen el Sistema facilitan a los demás «diccionarios de palabras claves» para que los incorporen como «filtros automáticos» a los aparatos de intercepción de las comunicaciones. Lógicamente estas «palabras claves» y «diccionarios» varían con el tiempo y de acuerdo con los intereses particulares de los países integrantes del Sistema.

SISTEMA ENFOPOL

Es consecuencia directa del deseo de los gobiernos europeos de no quedarse atrás en esta carrera de escuchas cibernéticas. Por esta razón, pusieron a funcionar su propio plan de interceptación de telecomunicaciones en: Europa, Estados Unidos y Australia, pero también en otros países. Enfopol intenta imponer sus normas a todos los operadores europeos de telefonía fija y móvil para que la policía secreta europea tenga acceso total a las comunicaciones de sus clientes, así como a la información sobre los números marcados y los números desde los que se llama. En el caso de Internet, los proveedores deben facilitar «una puerta de atrás» para que puedan penetrar a sus anchas por los sistemas privados.

Además, están obligados a informar sobre los datos personales de sus clientes (datos de correo electrónico y claves privadas) (Añover, 2001). Todo sin que sea necesaria una orden judicial (Añover, 2001). Pero todavía es más exigente para la criptografía. Se pide que sólo se permitan este tipo de servicios siempre que estén regulados desde un «tercero de confianza», que deberán entregar automáticamente cuando le sea solicitado: la identificación completa del usuario de una clave, los servicios que usa y los parámetros técnicos del método usado para implementar el servicio criptográfico.

SISTEMA CARNIVORE

Es la generación de los sistemas de espionaje de redes de la Oficina Federal de Investigación (FBI). Un sistema que ha sido diseñado por el FBI para capturar aquellos mensajes de correo electrónico que sean sospechosos de contener información útil para la Agencia. Se especula incluso que sea capaz de espiar el disco duro del usuario que se considere sospechoso y, todo ello, sin dejar rastro de su actividad. Para ello, se coloca un chip en los equipos de los proveedores de servicios de Internet para controlar todas las comunicaciones electrónicas que tienen lugar a través de ellos, así cuando encuentra una palabra clave, eso sí con el visto bueno de la Corte, revisa todos los datos del correo electrónico que circulan por el ordenador de esa persona, rastrea las visitas que hacen a sitios de la Red y las sesiones de *chat* en las que participa. Esto junto con el control de las direcciones de *IP* y de los teléfonos de conexión, permite la detección de lo que consideran «movimientos sospechosos» en la Red (Busón, 2009).

La quinta solución

La creación de ejércitos de cibersoldados para intentar garantizar los sistemas informáticos de sus respectivos países.

ALEMANIA

La Unidad Estratégica de Reconocimiento del Ejército alemán ha coordinado un equipo de soldados que están involucrados en el ensayo de nuevos métodos de infiltración, manipulación y explotación –e incluso de destrucción– de las redes informáticas. Por ello, este equipo está aprendiendo a instalar *software* maliciosos en ordenadores sin el conocimiento de los usuarios, robar contraseñas y datos confidenciales, etc.

ESPAÑA

El Ejército de Ciberdefensa de las Fuerzas Armadas españolas está compuesto por militares especialistas en telecomunicaciones e informática, que han hecho cursos avanzados, militares y civiles, en seguridad de las TIC, al mismo tiempo que se han incorporado ingenieros superiores civiles de la Ingeniería de Sistemas para la Defensa de España, S. A., especializados también en seguridad cibernética. Su entrenamiento con-

siste en asaltar los ordenadores enemigos, mientras que defienden los propios, dentro de una red creada expresamente para ello.

ESTADOS UNIDOS

Ha reunido un grupo de *hackers* de elite que se estarían preparado para luchar en caso de que se desencadenase una ciberguerra. Es lo que se conoce como JFCCNW *(Joint Functional Component Command for Network Warfare)*, una unidad que se cree que está integrada por personal de la Agencia Central de Inteligencia (CIA), la Agencia Nacional de Seguridad, el FBI, las cuatro ramas militares, algunos civiles expertos y representantes militares de naciones aliadas. Tiene la responsabilidad total de defender la Red de computadoras del Departamento de Defensa, destruir redes, entrar en los servidores de posibles enemigos para robar o manipular información, dañar las comunicaciones rivales hasta inutilizarlas y trabajar con una variedad de socios fuera y dentro del Gobierno de Estados Unidos. Un comando que tiene como contraparte el Grupo Especial de Tareas para la Libertad de la Internet Global, GIFTF *(Global Internet Freedom Task Force)* en sus siglas en inglés), una organización multiagencias subordinada al Departamento de Estado.

Además, con vista a la implantación de un sistema planetario de guerra ciberespacial y el lanzamiento del primer mando militar múltiple del mundo, el mando del Equipo Operativo Conjunto de la Red Global de Operaciones del Departamento de Defensa de Estados Unidos fue disuelto oficialmente para pasar a integrarse en el nuevo Cibermando (en inglés, CYBERCOM).

Éste servirá para fusionar el abanico de operaciones que lleva a cabo el Departamento de Defensa en el ciberespacio, y sus funciones serán liderar la defensa diaria, proteger las redes de información, coordinar las operaciones del Departamento de Apoyo a las Misiones Militares, dirigir las acciones y defensa de redes de información especificadas por el Departamento de Defensa, etc. Así, el USCYBERCOM centraliza el comando de operaciones ciberespaciales y fortalece las capacidades ciberespaciales del Departamento de Defensa. Además, el Cibercomando de la Fuerza Área (AFCYBER) ha creado también programas específicos de ciberguerra, entre los que se incluye: adversario, un sistema de objetivo de guerra de la información de la Fuerza Aérea; y ARENA, un programa de simulación «basado en objeto» para crear estudios por país; como casi tres docenas de otros programas y/o ejercicios de ciberguerra.

CHINA

En el pasado, el papel previsto para las fuerzas de reserva era el de apoyar al Ejército de Liberación Popular (ELN) en la defensa contra cualquier intervención extranjera. En cambio, hoy en día tienen la capacidad para emplear armas electrónicas y de información para alcanzar a un adversario en otro continente (Thomas, 2001). Por ello, entre sus funciones se encuentran: interrumpir el sistema de información, sabotear la estructura para la conducción de operaciones, debilitar la capacidad para contrarrestar una ofensiva, dispersar las fuerzas, armas y fuego del enemigo, logrando al mismo tiempo la concentración de las fuerzas, armas y fuego de las unidades propias, confundir al contrario y lanzar simultáneamente una ataque sorpresivo de información para que tome una decisión errónea o bien realizar una acción equivoca (Thomas, 2001; p. 76).

Además, el ELN ha incorporado tácticas de guerra cibernética en ejercicios militares y ha creado escuelas que se especializan en la guerra informática. También está contratando a graduados en informática para desarrollar sus capacidades en la guerra información y, así, crear un ejército de *hackers* civiles. Todo, tal vez porque los chinos se han dando cuenta que, de momento, no pueden ganar a Estados Unidos en un guerra convencional y, por tanto, están buscando nuevos campos de batalla donde puedan ser superiores, como en el ciberespacio (Brookes, 2007).

La sexta solución

El establecimiento de organismos gubernamentales destinados a luchar contra los posibles ataques cibernéticos. En este sentido, habría que mencionar que un gran número de gobiernos están creando Oficinas de Seguridad Informática para desde la legalidad combatir al cibercrimen, al ciberterrorismo y a la ciberguerra.

ESTADOS UNIDOS

Se creó la CIAO *(Critical Infrastructure Assurance Office)*, NIPC *(National Infrastructure Protection Center)* y el US-CERT *(United States-Computer Emergency Readiness Team)* para salvaguardar las redes de infraestructuras y los sistemas del país de los ataques cibernéticos, identificar las vulnerabilidades, difundir información sobre alertas de amenazas de seguridad, y coordinar las actividades de respuesta antes de incidentes

cibernéticos. Además, en el Departamento de Defensa existen muchas iniciativas tanto de los tres Ejércitos como de las agencias de inteligencia que tienen misiones en la protección de las redes sensibles y clasificadas como la Agencia de Seguridad Nacional. Esta Agencia, por ejemplo, tiene un departamento encargado del aseguramiento de la información, NSAIDA, que se centra en el análisis permanente de nuevas amenazas y vulnerabilidades, en el desarrollo de guías, productos y soluciones de seguridad, en el desarrollo de productos de cifra y gestión de claves de los mismos y en la formación y concienciación de seguridad. Además, el Departamento de Defensa financia el CERT-CC que tiene como misión principal establecer un foro de coordinación entre los CERT nacionales.

Asimismo, con la llegada de Obama se han reforzado todo este tipo de iniciativas relacionadas con la ciberseguridad. Por ejemplo, ha elaborado un informe sobre la seguridad cibernética que servirá para luchar contra los delitos informáticos y el robo de información confidencial, o ha anunciado el nombramiento de un responsable de ciberseguridad que formará parte del Consejo de Seguridad Nacional en la Casa Blanca, o ha ordenado al Pentágono que preparé la creación de un nuevo mando especializado en la ciberguerra (4).

Además, después del 11 de septiembre de 2001 (11-S) Estados Unidos cambió su estrategia de seguridad centrándola en: el establecimiento y reordenación relativas a la seguridad del territorio, el desarrollo de la legislación relativa a la Seguridad Nacional y la ciberdefensa, la implantación de planes y estrategias relativas a la Seguridad Nacional, y la ejecución de ejercicios periódicos en ciberseguridad. Además, se apuesta por la colaboración con otros Estados, tal es así, que Estados Unidos ya está enlazando algunos ordenadores de defensa con los de sus aliados, incluso se están llegando a acuerdos de intercambio de información, tecnología e inteligencia con sus aliados.

FRANCIA

Se ha creado la Autoridad Nacional de Seguridad de los Sistemas de Información para vigilar las redes informáticas gubernamentales y privadas, con el objetivo de defenderlas de ataques cibernéticos. Sus funciones

(4) «La Conferencia de Seguridad de Múnich», *Documento Informativo*, Instituto Español de Estudios Estratégicos (IEEE), febrero de 2011.

son: la detección y reacción urgente ante ciberataques mediante la vigilancia continua de las redes gubernamentales sensibles y la implementación de mecanismos de defensa en estas redes; el desarrollo de productos y servicios de confianza para su uso en los gobiernos y en los sectores críticos; el asesoramiento de seguridad a organismos gubernamentales y operadores de infraestructuras críticas; la difusión de información a empresas y ciudadanos sobre las nuevas amenazas a la seguridad de la información y el procedimiento de protección mediante una política activa de comunicación. Este organismo dependen la Subdirección de Estrategia y Reglamentación, el Centro de Formación y el Centro Operacional de la Seguridad de los Sistemas de Información (COSSI), que son los responsables de la realización de las inspecciones y auditorías de seguridad a sistemas gubernamentales, las misiones de desarrollo de productos de cifra, los ejercicios que evalúen la seguridad, el despliegue de los sistemas de detección, y la coordinación de la respuesta gubernamental.

En el COSSI se encuentra además, el Centro de Expertos del Gobierno en el Tratamiento de Ataques Informáticos (CERTA), creado en el año 1999, que facilita la aplicación de buenas prácticas y mejora la atención a los usuarios en todo el territorio. Pero el Gobierno francés también ha elaborado el *Libro Blanco de la Seguridad y Defensa Nacional* (5), donde se contempla cinco funciones estratégicas que las fuerzas de defensa y seguridad francesas deben dominar como son: el conocimiento y la previsión (con la necesidad de mejora de las capacidades técnicas de las agencias de inteligencia), la prevención (con la necesidad de una defensa proactiva en profundidad que realice una vigilancia permanente), la disuasión, la protección y la respuesta.

REINO UNIDO

Ha decidido crear el Centro de Operaciones de Ciberseguridad y la Oficina de Ciberseguridad, para supervisar la protección de importantes sistemas de tecnología de la información usados por el Gobierno británico y el sector privado, y para coordinar las medidas de ciberseguridad de todos los departamentos gubernamentales, respectivamente. El primero será una entidad multidepartamental con sede en Cheltenham, y ligado al GCHQ *(Government Communications Headquarters)*. Desde el que se

(5) *Livre Blanc Sur la Défense et la Sécurité Nationale*, en: *www.livreblancdefenseetsecurite.gouv.fr/information*

proporcionará protección coordinada a los sistemas de infraestructuras críticas del país. La segunda, coordinará las políticas y supervisará el programa de trabajo entre las distintas agencias gubernamentales. Estos dos Centros formaran parte del I Plan Estratégico de Ciberseguridad del Reino Unido, donde también se contemplará la creación de un grupo de asesores técnicos, y el establecimiento de las líneas estratégicas de seguridad cibernética del país: reducción del riesgo del uso del ciberespacio por el Reino Unido actuando sobre la amenaza, las vulnerabilidades y el impacto; aprovechamiento de las oportunidades en el ciberespacio mediante la obtención de inteligencia que apoye las políticas nacionales y que actué contra los adversarios, y, por último, el impulso de una doctrina sobre el ciberespacio.

ALEMANIA

Se ha creado la Oficina Federal de Seguridad de la Información, dependiente del Ministerio Federal de Interior. Sus funciones son la protección de las redes del Gobierno federal, el desarrollo de productos de cifra, el análisis de nuevas tecnologías, la seguridad de los productos *software*, la protección de infraestructuras críticas, y el soporte del CERT para ciudadanos y pequeñas y medianas empresas. Además se ha aprobado un Plan Nacional de Protección de Infraestructuras de la Información (6), donde se establece como objetivos la prevención (las actividades críticas son divulgar información sobre riesgos y posibilidades de protección o empleo de productos y sistemas confiables), la preparación (las actividades son recolectar y analizar la información para proporcionar alertas y avisos) y la reacción (mejorar las capacidades técnicas propias y desarrollar productos con tecnología nacional). Además, a partir de abril de 2011, el Gobierno alemán abrirá un Centro Nacional de Ciberseguridad para defenderse de los ataques cibernéticos externos a sus infraestructuras críticas. También podrá en marcha un Consejo de Ciberseguridad Nacional, para mejorar la cooperación entre el Estado y los representantes del sector financiero y económico.

---

(6) Federal Ministry of the Interior: «National Plan for Information Infrastructure Protection», Berlín, 2005, en: *www.bmi.bund.de/cln_012/nn_148138/Internet/Content/Common/Anlagen/Nachrichten/Pressemitteilungen/2005/08/National__Plan__for__Information__Infrastructure_Protection,templateId=raw,property=publicationFile.pdf/National_Plan_for_Information_Infrastructure_Protection.*

ESPAÑA

A lo largo de los últimos años, se han tomado acciones para incrementar la seguridad del ciberespacio. En nuestro país, el Centro Criptológico Nacional, dependiente del Centro Nacional de Inteligencia, tiene la responsabilidad de gestionar la seguridad del ciberespacio dependiente de cualquiera de los tres niveles de las Administraciones públicas (Fojón, 2010). Entre sus funciones cabe destacar: elaborar y difundir normas, instrucciones y recomendaciones para garantizar la seguridad de las TIC en la Administración; formar el personal de la Administración especialista en el campo de la seguridad de las TIC; constituir el organismo de certificación del Esquema Nacional de Evaluación y Certificación de aplicación a productos y sistemas de su ámbito; valorar y acreditar la capacidad de productos de cifras y Sistemas de las TIC; coordinar la promoción, el desarrollo, la obtención, la adquisición y la puesta en marcha de las tecnologías de seguridad de los sistemas antes mencionados; velar por el cumplimiento de la normativa, y establecer las relaciones necesarias con otros actores e instituciones.

A nivel nacional, también existen otros organismos con competencias en la materia: el Grupo de Delitos Telemáticos de la Guardia Civil y la Unidad de Investigación de Delincuencia en Tecnologías de la Información de la Policía Nacional, dependientes ambos del Ministerio de Interior, son responsables de combatir la delincuencia que se produce en el ciberespacio, etc. A nivel autonómico, existen centros homólogos a los referidos a nivel nacional, que igualmente tienen responsabilidades en la gestión de la ciberseguridad en su ámbito territorial. Además, a nivel internacional nuestro país forma parte de las organizaciones que promueven la defensa del ciberespacio, como, el Centro de Excelencia de Ciberdefensa Cooperativa de la Organización del Tratado del Atlántico Norte (OTAN) y en organismos como la Agencia Europea de Seguridad de las Redes y la Información (ENISA), *Antiphising Working Group* y *Data Protection Working Party.*

UNIÓN EUROPEA

Ha creado la ENISA, con sede en Heraklion (Grecia), para ayudar a los Estados miembros a obtener unos niveles altos de seguridad, asesorando técnicamente y prestando asistencia a los Estados miembros, así como a las instituciones de la Unión Europea sobre las cuestiones vin-

culadas a la seguridad de las redes y de la información, y fomentando la cooperación entre el sector público y privado. Para garantizar estos objetivos, las tareas de la Agencia (7) consiste, principalmente, en: acopio y análisis de datos relativos a aspectos vinculados a la seguridad y a los riesgos emergentes; cooperación con los distintos protagonistas, creando asociaciones entre el sector público y el privado con empresas que ejercen sus actividades en la Unión Europea y/o a nivel mundial; sensibilizar a los usuarios en la problemática de la seguridad de las redes y de la información, y promover métodos de evaluación de riesgos y mejores prácticas con el fin de encontrar soluciones interoperativas de gestión de los riesgos; el seguimiento del desarrollo de las normas sobre productos y servicios en la Sociedad de la Información y en las redes; asistir a la Comisión y a los países de la Unión en el diálogo que mantienen con las empresas para gestionar los problemas de seguridad; y presentar sugerencias.

Su estructura gira en torno al Consejo de Administración, el director ejecutivo, y el grupo permanente. La primera está compuesto por representantes de los Estados miembros y de la Comisión, así como de las empresas y expertos universitarios en la materia, y consumidores sin derecho al voto. A través de esta institución, los Estados miembros pueden formular sus necesidades en relación a esta materia. El segundo es nombrado por el Consejo de Administración a partir de una lista de candidatos propuestos por la Comisión. El tercero lo forman las partes interesadas, y es creado por el director ejecutivo y está compuesto por representantes de las empresas, los consumidores y expertos universitarios.

Así, viendo esta organización se podría concluir que ENISA es el centro neurálgico para fomentar el intercambio de información y cooperación entre todas las partes interesadas (organismos de la Unión Europea, miembros de la Unión Europea: Estados, la industria, el mundo académico y las organizaciones de consumidores de interés) en el campo de la seguridad en el ciberespacio. Además, en diciembre de 2002 la Unión Europea aprobó la Estrategia Europea de Seguridad, pero será en su revisión, en diciembre de 2008, cuando se recoja un apartado dedicado a las nuevas amenazas y riesgos, la seguridad de los sistemas de información.

---

(7) En: *http://europa.eu/legislation_summaries/justice_freedom_security/fight_against_organised_crime/l24153_es.htm*

Pero, además, para incrementar la ciberseguridad, la Unión Europea ha decidido crear un centro dedicado a la defensa frente al cibercrimen en el año 2013. Su misión será coordinar la cooperación entre los Estados miembros, las instituciones europeas y los socios internacionales (Cabanillas, 2010). También se está contemplando la puesta en funcionamiento de un sistema de alerta y compartición de información, cuyo objetivo será facilitar la comunicación entre los equipos de respuesta urgente y las autoridades policiales. Asimismo, se pretende poner en marcha en 2012, la Red de Equipos de Respuesta Informática Urgente, CERTS *(Computer Emergency Response Teams)*, de la que existirá una por país miembro. Por otra parte, la Comisión y la Unión Europea han anunciado la creación, junto con las autoridades estadounidenses, de un grupo de trabajo dedicado a la ciberseguridad, que empezará a proporcionar información al respecto a partir de 2010 (Cabanillas, 2010).

LA OTAN

Ha creado en Tallin (Estonia) el Centro de Excelencia para la Cooperación en Ciberdefensa, cuyo objetivo es estudiar ciberataques y determinar las circunstancias en las que se deben activar el principio de defensa mutua de la Alianza Atlántica. En la actualidad forman parte de él: España, Italia, Alemania, Eslovaquia, Estonia, Letonia, Estados Unidos, Hungría, Italia, Lituania y Turquía. Su misión será, según se manifiesta en su memorándum fundacional, proteger a los Estados de los ciberataques, entrenar a militares, investigar técnicas de defensa electrónica, desarrollar un marco legal para ejercer esta actividad, dar respuesta y soluciones globales a problemas concretos, y para ello, los proyectos son acometidos por equipos multidisciplinares, en los que se involucran al personal experto en ciberseguridad, y especializado en tres ramas: asuntos operativos, funcionales y militares; asuntos tecnológicos, académicos y científicos; y asuntos legales. Este Centro depende jerárquicamente de un Comité de Dirección compuesto por representantes de los países componentes y de la OTAN, y tiene el estatus legal de Organización Militar Internacional.

La séptima solución

La propuesta realizada por algunos investigadores estadounidenses de crear Internet 2. Una red separada de la Internet comercial, que une labo-

ratorios y universidades de todo el mundo, y que trabaja en el desarrollo de los sistemas de transmisión de información a grandes velocidades y a través de la fibra óptica (Sánchez Medero, 2009). Pero a diferencia del Internet comercial:

> «Internet 2 estará extraordinariamente regulado y una Comisión Federal de Comunicaciones o el propio gobierno aceptara solamente "contenidos apropiados". Además las directrices y las propuestas que están realizando, tanto la Unión Europea como Estados Unidos, para la retención de datos permitirán la regulación absoluta de la red» (Waston, 2007).

De esta manera, Internet 2 no escapará al control gubernamental, y por tanto, será menos permisible a las acciones delictivas.

Conclusiones

Internet se ha convertido en el espacio ideal para la ciberdelincuencia, ya que les ofrece fácil acceso, poco o ningún control gubernamental, anonimato, rápido flujo de información, altísimo impacto, escaso riesgo, barato y indetectable. Además, hay que tener en cuenta que por mucho que se empeñen las agencias o secretarias de seguridad de los Estados es imposible garantizar la seguridad plena de los sistemas informáticos. La única solución realmente efectiva y eficaz es apagar Internet o suprimirlo, pero esta alternativa no es, lógicamente, razonable en mundo como el actual, pese a las excepciones particulares como son las de los Emiratos Árabes Unidos, Corea del Norte o China.

También existe otra posibilidad, identificar las vulnerabilidades e individualizar los peligros existentes y potenciales que dichas debilidades permiten, y esperar a ver cual es el resultado final. Las otras soluciones aquí planteadas como han sido los sistemas de control de comunicación, la creación de agencias y de cibersoldados, de momento, no están resultado ser totalmente efectivas. Es cierto, que están contribuyendo a detectar a ciberdelincuentes, pero todavía no son capaces de controlar ni impedir su actividad en la Red. Por no hacer referencia a las precauciones que debemos tener cualquier ciberinternauta como son, por ejemplo, no abrir correos de procedencia desconocida, no hacer clic encima de un enlace, usar contraseñas, cifrar la red inalámbrica, realizar copias de seguridad, revisar con cierta frecuencia las cuentas bancarias, etc.

Bibliografía

Añover, J.: *Echelon y Enfopol nos espían,* 2001, en: *http://www.nodo50.org/altavoz/echelon.htm*

Brookes, P.: «Contrarrestando el arte de la guerra informática», *Grupo de Estudios Estratégicos,* número 201, octubre de 2007, en: *http://www.gees.org/articulo/4637/*

Busón Buesa, C.: *Control en el ciberespacio,* 1998, en: *http://www.uned.es/ntedu/espanol/master/segundo/modulos/poder-y-control/poder.htm*

— *Control en el ciberespacio,* conferencia en el Programa Modular en Tecnologías Digitales y Sociedad del Conocimiento, celebrada el 22 de agosto de 2009, en: *http://www.uned.es/ntedu/espanol/master/segundo/modulos/poder-y-control/poder.htm*

Cabanillas, M.: «Preparados contra el cibercrimen», *PCWorld,* noviembre de 2010.

Caro Bejarano, M. J.: «Nuevo concepto de ciberdefensa de la OTAN», *Documento Informativo,* número 9, Instituto Español de Estudios Estratégicos (IEEE), marzo, 2011, en: *http://www.ieee.es/Galerias/fichero/docs_informativos/2011/DIEEEI09_2011ConceptoCiberdefensaOTAN.pdf*

Fojón Chamorro, E. y Sanz Villalba, A. F.: «Ciberseguridad en España: una propuesta para su gestión», *ARI*, número 101, Real Instituto Elcano, junio de 2010.

Fuentes, L. F.: «*Malware,* una amenaza de Internet», *Revista Digital Universitario,* volumen 9, número 4, pp. 1-9, 2008.

Orta Martínez, R.: «Ciberterrorismo», *Revista de Derecho Informático,* número 82, mayo de 2005.

Pachón Ovalle, G.: «La red Echelon: privacidad, libertad y criptografía», *Virtualidad Real,* Programa de Doctorado en SIC, Universitat Oberta de Catalunya, Barcelona, 2004, en: *http://www.virtualidadreal.com/Red%20Echelon.pdf*

Rodríguez Pérez, C.: *Tecnologías de vigilancia e investigación: el caso Echelon. Informe: tecnologías de vigilancia e investigación,* Posgrado Conocimiento, Ciencia y Ciudadanía en la Sociedad de la Información, Universitat de Barcelona, Barcelona, 2008, en: *http://www.ub.es/prometheus21/articulos/obsprometheus/crodr_echelon.pdf*

Rogríguez Bernal, A.: «Los cibercrímenes en el espacio de libertad, seguridad y justicia», *Revista de Derecho Informático,* número 103, pp. 1-42, febrero de 2007.

Ruiloba Castilla, J. C.: «La actuación policial frente a los déficit de seguridad de Internet», *Revista de los Estudios de Derecho y Ciencia Política de la UOC,* número 2, 2006.

Sánchez Medero, G.: «Ciberterrorismo. La guerra del siglo XXI», *El Viejo Topo*, número 242, pp. 15-23, marzo de 2008.

— «21st Century to two new challenges: Cyberwar and Cyberterrorism», *Nómadas. Mediterranean Perspectives,* número 1, pp. 1-10, 2009.

THOMAS, TIMOTHY L.: «Las estrategias electrónicas de China», *Military Review,* pp. 72-79, julio-agosto de 2001.

TOFFLER, A.: «Onward Cyber-Soldiers», *Time Magazine,* volumen 146, número 8, agosto de 1995.

WASTON, S: «Científicos usamericanos quieren desembarazarse de la red de Internet», *Rebelión,* 2007, en: *http://www.rebelion.org/noticia.php?id=49932*

ACTIVIDADES DEL CENTRO

IX JORNADAS DEL CURSO DE GESTIÓN STIC

Entre los días 5 y 16 de marzo en el aula número 21 de este Centro, se celebraron las IX Jornadas del Curso de Gestión STIC, dirigidas por el Centro Criptológico Nacional a estas Jornadas asistieron aproximadamente 45 alumnos.

ACTIVIDAD ACADÉMICA

El día 8 de marzo en el aula magna de este Centro, dentro de las actividades académicas tuvo lugar la «mesa redonda» con el título: *Complementariedad de empresa y Fuerzas Armadas para la imagen de España en el exterior.*

ACTIVIDAD ACADÉMICA

El día 15 de marzo en el aula magna de este Centro, dentro de las actividades académicas tuvo lugar la «mesa redonda» con el título: *El espacio como fuente de oportunidad: ¿es necesaria una agencia espacial española?*

VISITA DEL NATIONAL LEMHANNAS *(RESILIENCE INSTITUTE DE INDONESIA)*

El día 21 de marzo en el aula número dos de este Centro, tuvo lugar la visita del LEMHANNAS compuesta por aproximadamente 12 personas, durante su estancia en el Centro se impartieron dos conferencias sobre la Escuela Superior de las Fuerzas Armadas y la Escuela de Altos Estudios de la Defensa.

VISITA DEL CURSO DE MANDO Y ESTADO MAYOR CONJUNTO DE LA ACADEMIA DE MANDO Y ESTADO MAYOR DE LAS FUERZAS ARMADAS FEDERALES ALEMANAS

El día 22 de marzo tuvo lugar la visita de los concurrentes del Curso de Mando y Estado Mayor Conjunto de la Academia de Mando de las Fuerzas Armadas alemanas durante su estacia en el Centro, se impartieron las conferencias: *La política de defensa en España, Las Fuerzas Armadas españolas* y *Organización, misiones y cometidos de la Escuela Superior de las Fuerzas Armadas.*

La delegación estuvo compuesta por 20 personas al mando del almirante Martín Krebs.

CONFERENCIA GENERAL

El día 22 de marzo tuvo lugar en este Centro, dentro del ciclo de conferencias de la Cátedra «Marqués de Santa Cruz de Marcenado» del CESEDEN-Fundación Sagardoy, la conferencia impartida por el general de Ejército, don Luis Alejandre Sintes con el título: *Enfoque Integral de las relaciones cívico-militares.*

VISITA DE LA UNIVERSIDAD DE LA DEFENSA NACIONAL DE COREA (KNDU)

El día 23 de marzo tuvo lugar la visita de una delegación de la KNDU, esta delegación estaba compuesta por 20 miembros de la Universidad al mando del profesor coronel, Ryu Jei-Hack

EXPERIMENTO MULTINACIONAL NÚMERO 7

Entre los días 10 y 12 de abril en las aulas números 20 y 21 de este Centro, tuvo lugar el Experimento Multinacional número 7, organizado por la Unidad de Tranformación de las Fuerzas Armadas.

PRESENTACIÓN DE LA PUBLICACIÓN *PANORAMA DE CONFLICTOS*

El día 10 de abril tuvo lugar en el paraninfo de este Centro, la presentación de la publicación *Panorama de conflictos* a cargo del Instituto Español de Estudios Estratégicos, en la cual participaron aproximadamente unas 200 personas.

ACTIVIDAD ACADÉMICA

El día 12 de abril en el aula magna de este Centro, tuvo lugar la «mesa redonda» con el título: *Posible evolución del escenario AF-PAK ante las nuevas estrategias.*

VISITA DE LAS ESCUELAS SUPERIORES DE LAS FUERZAS ARMADAS TURCAS

El día 17 de abril tuvo lugar la visita de una delegación de las Escuelas Superiores de las Fuerzas Armadas turcas, presidida por el brigada de división don Metin Gürak y compuesta por 70 personas.

Durante su estancia en el Centro, se impartieron las conferencias: *La política de defensa en España, Las Fuerzas Armadas españolas* y *La Escuela Superior de las Fuerzas Armadas: organización, misión y cometidos.*

SEMINARIO *LA INNOVACIÓN TECNOLÓGICA EN DEFENSA Y SEGURIDAD: APLICACIONES DUALES DE LAS TECNOLOGÍAS*

El día 18 de abril en el paraninfo de este Centro, tuvo lugar el Seminario *La innovación tecnológica en Defensa y Seguridad: aplicaciones duales de las tecnologías*, organizado conjuntamente por este Centro y la Universidad Politécnica de Madrid.

ACTIVIDAD ACADÉMICA

El día 19 de abril en el aula magna y dentro del ciclo de actividades académicas de este Centro, tuvo lugar la conferencia con el título: *Comunicación y defensa*, impartida por don Ángel Expósito Muñoz, colaborador de *ABC-Punto radio* y otros medios de comunicación.

VISITA DE LA UNIVERSIDAD DE NORWICH

El día 19 de abril tuvo lugar la visita de una delegación de la Universidad de Norwich (Estados Unidos), esta delegación estuvo presidida por su vicepresidente William H. Clements.

Durante su estancia tuvieron lugar las presentaciones: *El Sistema de Enseñanza Militar Superior y el CESEDEN* y *la Escuela de Altos Estudios de la Defensa en el Sistema de Enseñanza Militar.*

VISITA DEL COLEGIO REAL JORDANO DE DEFENSA NACIONAL

Entre los días 13 y 20 de abril tuvo lugar la visita de una delegación del Colegio Real Jordano de Defensa Nacional, esta delegación estuvo compuesta por 21 personas presidida el brigadier general don Ahmad Abdullah Al-Shibli.

Durante su estancia se impartieron las conferencias: *Política de defensa española* y *Las Fuerzas Armadas españolas*, realizaron visitas a la empresa EADS-CASA, a las instalaciones de la base aérea de Torrejón, a la Unidad Militar de Emergencias y al Museo Naval.

CONFERENCIA GENERAL

El día 24 de abril en el aula magna de este Centro, dentro del ciclo de conferencias de la Cátedra «Marqués de Santa Cruz de Marcenado» del CESEDEN-Fundación Sagardoy tuvo lugar la conferencia con el título: *La política del agua en España*, impartida por el catedrático de la Universidad Complutense de Madrid, don Ramón Llamas Marduga.

VISITA DEL COLEGIO NACIONAL DE DEFENSA DE TAILANDIA

El día 25 de abril tuvo lugar la visita de una delegación del Colegio Nacional de Defensa de Tailandia, esta delegación estuvo compuesta por 38 personas al mando de la general de brigada doña Siriprom Hitasari.

Durante su visita se impartió la conferencia: *Organización y funciones del CESEDEN y la Escuela de Altos Estudios de la Defensa* y recorrieron las instalaciones de este Centro.

- Se ruega a los suscriptores de este *Boletín de Información* que consignen los cambios de dirección postal que se produzcan a: Sección de Planes y Programas (Publicaciones) del CESEDEN en paseo de la Castellana 61, 28071-Madrid, o bien mediante fax a los números 91-3482553 o 91-3482554.
- Las personas interesadas en la adquisición de algunas *Monografías* del CESEDEN y *Boletín de Información* pueden hacerlo en la librería que para tal efecto dispone el Ministerio de Defensa, situada en la planta baja de la entrada al mismo por la calle Pedro Texeira, 15.