FORO PARA LA PAZ
EN EL MEDITERRÁNEO

ACTAS DE LAS XII JORNADAS DE SEGURIDAD, DEFENSA Y COOPERACIÓN

TOMO II

INFRAESTRUCTURAS CRÍTICAS Y GEOECONOMÍA

AUTORES

Francisco de la Torre Prados, Beatriz Rodríguez Díaz, Antonio Hernando Vera, Luis Miguel Salvador García, Fernando Sánchez Gómez, María del Pilar Rangel Rojas, Magdalena Martín Martínez, Fernando Morillas García, José María López Jiménez, Ignacio García Sánchez, Pablo Podadera, Anna Garashchuk, Lucas F. Martín Serrano y Rafael Vidal Delgado

Coordinadoras: Elena Ruiz Romero de la Cruz y Elena Cruz Ruiz

Colaboradora: Lara César López

Edita: Foro para la Paz en el Mediterráneo
ISBN: 978-84-09-13221-8

Depósito Legal:

Los autores y el editor autorizan la reproducción, el almacenamiento en un sistema informático y la transmisión parcial o total de esta obra por cualquier método o procedimiento mecánico o electrónico, siempre y cuando se reconozca de manera expresa la propiedad intelectual de los contenidos que la integran a los autores y la de edición del Foro para la Paz en el mediterráneo.
No se autoriza la elaboración de obra derivada.

INFRAESTRUCTURAS CRÍTICAS Y GEOECONOMÍA

ÍNDICE

AUTOR	TÍTULO	PÁG
Francisco de la Torre Prados	Prólogo	15
Beatriz Rodríguez Díaz	Fundamentos Matemático-Económicos del Bitcoin.	23
Antonio Hernando Vera	Situación en España de la lucha contra el terrorismo y el crimen organizado	47
Luis Miguel Salvador García	Lucha contra el terrorismo	65
Fernando Sánchez Gómez	El CNPIC en su lucha contra el terrorismo	81
María del Pilar Rangel Rojas	Geoeconomía, Geopolítica y Terrorismo en el Sahel	121
Fernando Morillas García	El libre comercio en el Mediterráneo en un contexto de guerra comercial	137
José María López Jiménez	El sistema financiero visto desde la perspectiva de la Estrategia de Seguridad Nacional 2017	157
Ignacio García Sánchez	Tendencias geopolíticas en el Mediterráneo y Atlántico: horizonte 2040	167

AUTOR	TÍTULO	PÁG
Pablo Podadera y Anna Garashchuk	Geoeconomía y Asociación Estratégica en el nuevo orden multipolar. Teoría y evidencia empírica en la Unión Europea	191
Lucas F. Martín Serrano	Boko Haram. Evolución de una amenaza	213
Rafael Vidal Delgado	El Servicio esencial del agua y el terrorismo	253

Prólogo a las Actas de las XII Jornadas de Seguridad, Defensa y Cooperación

Un año más me cabe la satisfacción de prologar la publicación que recopila el trabajo desarrollado en las Jornadas de Seguridad, Defensa y Cooperación, la actividad anual más importante que lleva a cabo el Foro para la Paz en el Mediterráneo.

Este año de 2018, ha sido crucial para la vida del Foro, al transformarse de una iniciativa constituida por un conjunto de entidades públicas y privadas, en una asociación, al amparo de la Ley Orgánica 1/2002, de 22 de marzo, reguladora del Derecho de Asociación, teniendo como objetivo primario que sea declarada de "utilidad pública", de acuerdo a lo establecido en el artículo 32 y siguientes de la misma.

Los Estatutos, aprobados con fecha 16 de noviembre, han recogido todo lo esencial del Acuerdo Marco de Colaboración, firmado en octubre de 2011, fundamentalmente en lo referente a las actividades que deben desarrollarse, las cuales permanecen inalterables, habiéndose demostrado a lo largo de los años que acertamos al relacionarlas, siendo una muestra de ello, las presentes Jornadas y las consecuentes actas de las mismas.

Otro aspecto a considerar en este año, ha sido la consecución práctica del Centro Internacional de Formación de Autoridades y Líderes (CIFAL), del cual el Foro para la Paz en el Mediterráneo, no ha sido solo uno de los pilares constitutivos, sino fuente de organización de cursos y jornadas formativas, como los de verano, conferencias sobre temas de interés e indudablemente, con estas Jornadas, que se han ganado un merecido prestigio en los ámbitos nacional e internacional.

Quisiera reconocer la labor intelectual y desinteresada del comité organizador de las Jornadas y del Comité Científico, así como al director y los coordinadores. No es fácil reunir a un conjunto de ponentes cualificados para tratar de forma precisa, cada uno de los temas de cada Jornada, dando en su conjunto una idea bastante precisa del tema central: Infraestructuras Críticas y Geoeconomía.

En esta ocasión las actas de las Jornadas, se han dividido en dos tomos, el primero con un análisis recopilatorio de la legislación que afecta al concepto de “infraestructuras críticas”, ponencia expuesta el día 15 de noviembre de 2018, y el segundo con el resto de las ponencias.

En definitiva, es un nuevo paso del Foro para la Paz en el Mediterráneo y un reforzamiento de la figura de la capital malacitana en el contexto europeo, mediterráneo y norteafricano, un espacio de gran importancia geoestratégica.

Francisco de la Torre Prados.
Alcalde de Málaga y Presidente del Foro para la Paz en el Mediterráneo

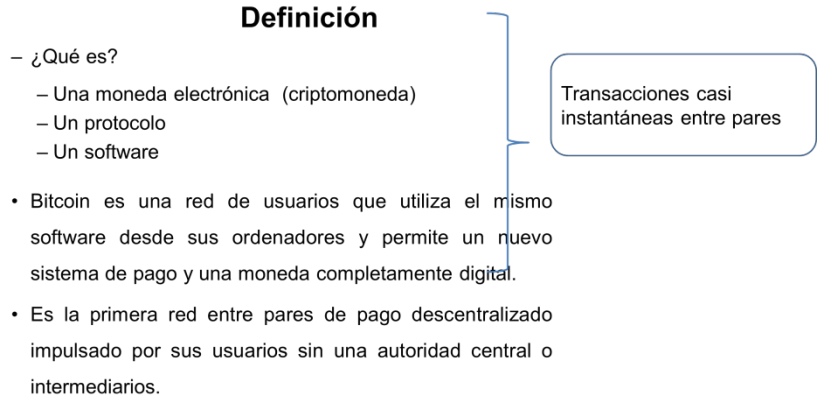
1ª Jornada: ¿El Bitcoin: Moneda Geoeconómica Mundial?

Fundamentos matemático-económicos del Bitcoin

AUTORA: Beatriz Rodríguez Díaz, profesora de Matemáticas de las Operaciones Financieras, de la Facultad de Ciencias Económicas y Empresariales de la Universidad de Málaga.

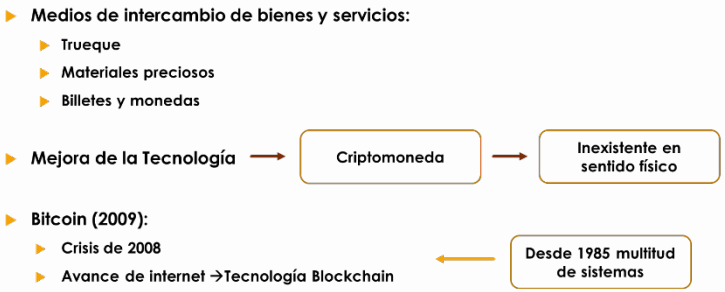
1. ¿Qué es el Bitcoin y cuál es su origen?

Bitcoin se define una moneda electrónica (criptomoneda), un protocolo o como un software. Podemos decir que es la conjunción de todos estos componentes, y que permite la realización de transacciones casi instantáneas entre pares. Se trata de una red de usuarios que utilizan el mismo software desde sus ordenadores para realizar transacciones permitiendo un nuevo sistema de pago. Es la primera red entre pares de pago descentralizado impulsado por sus usuarios sin una autoridad central o intermediarios.



A través de la historia, ha habido múltiples medios de intercambio de bienes y servicios. Todos ellos han ido sufriendo evoluciones y cambios o, directamente, han desaparecido. Es el caso del trueque o la utilización de materiales preciosos, los cuales dejaron paso al sistema que hasta la actualidad ha funcionado, los billetes y monedas. No obstante, en una época donde la tecnología cada día gana más y más terreno, se hace necesario un medio de intercambio más ajustado a los tiempos: la criptomoneda.

Origen de las criptomonedas



El Bitcoin es una criptomoneda, que ve la luz en el año 2009, debido a la necesidad de un nuevo sistema monetario paralelo al tradicional, entre otros, por dos motivos principales:

- Por la crisis que tuvo lugar en 2008, que hizo desconfiar del sistema de pagos tradicional.

- Por el avance que se había producido en Internet y las redes de comunicación, concretamente por la tecnología “Blockchain” (cadena de bloques).

Estos factores impulsaron a una persona o varias a crear Bitcoin con el pseudónimo de Satoshi Nakamoto. Aunque es la criptomoneda más conocida, Bitcoin no es el único sistema de dinero electrónico, ni fue el primero. Esta idea surgió en 1985 y se han propuesto multitud de sistemas mejorando distintos aspectos de los anteriores. Bitcoin destaca porque es el primer sistema que funciona sin una autoridad central.

2. Participantes.

Podemos destacar los siguientes participantes en este sistema:

Participantes

- **Usuarios normales: Compran y pagan bienes y servicios utilizando bitcoins →**

  Transacciones del sistema

- **Mineros: Dedican potencia de cómputo a validar nuevas transacciones (bloques) →**

  Recompensados por ello

- **Desarrolladores: Necesita un desarrollo y mantenimientos activos para el software**

Usuarios del sistema Bitcoin: aquéllos que compran y venden bienes y servicios utilizando bitcoins, produciendo así las transacciones del sistema.

Mineros: son unos usuarios especiales, éstos se dedican a validar las transacciones entre los usuarios a través de ordenadores, creando lo que se conoce como bloques de transacciones. Para ello tienen que realizar cálculos muy costosos, por tanto, van a ser recompensados por ello. Existen agrupaciones de mineros que trabajan conjuntamente para validar un mismo bloque de transacciones dado que la potencia necesaria es muy elevada.

Desarrolladores: este sistema necesita un desarrollo y mantenimientos activos para el software.

3. Características.

Este nuevo sistema monetario se creó como una alternativa al tradicional. Las principales características son:

- **Criptografía:** Utilizan técnicas de cifrado para realizar cobros y pagos seguros.
- **Descentralización:** No necesitan ser controladas por ninguna institución.
- **No hay posibilidad de falsificación o duplicación:** Gracias al sistema criptográfico que protege a los usuarios.
- **No hay intermediarios:** Contacto directo persona a persona.
- **Las transacciones son irreversibles:** Una vez se efectúe el pago, no hay posibilidad de cancelación.

- **Se pueden intercambiar por otras divisas.**
- **Privacidad de uso:** No es necesario revelar tu identidad al hacer negocios.

Las ventajas principales que lo caracterizan son:

- Bajos costes de transacción: Como consecuencia de la no presencia de intermediarios.
- Seguro: Cada moneda pertenece solo a su dueño.
- Transparente: Las transacciones se incorporan en un registro de acceso libre.
- Se acumula en un espacio ínfimo como es un USB.

Por su parte, las desventajas son:

- Volatilidad de sus precios.
- Falta de aceptación actual por algunas empresas
- Al no necesitar un regulador como el Gobierno o el Banco Central y proporcionar privacidad son utilizadas pueden ser utilizadas para transacciones ilegales.
- Vulnerabilidades: se han descubierto algunas vulnerabilidades en las diferentes implementaciones que han ido apareciendo, y que pueden ser utilizadas para el mal funcionamiento de la propia red, lo que puede producir caídas en el precio.
- Consumo de energía: para la minería se necesitan equipos conectados para las operaciones computacionales, lo que supone un consumo de energía cada vez más elevado.

4. Valor de los Bitcoins

La moneda Bitcoin se puede dividir hasta en 8 décimas, 0,00000001 BTC (Bitcoins), que equivalen a un Satoshi. Las unidades de medida más comunes que se suelen utilizar son:

mBTC = mili bitcoin = 1 milesima de Bitcoin = 0.001 BTC

uBTC = micro bitcoin = 1 million de bitcoin = 0.000001BTC

Se pueden dividir en unidades más pequeñas si es que así se requiere en el futuro.

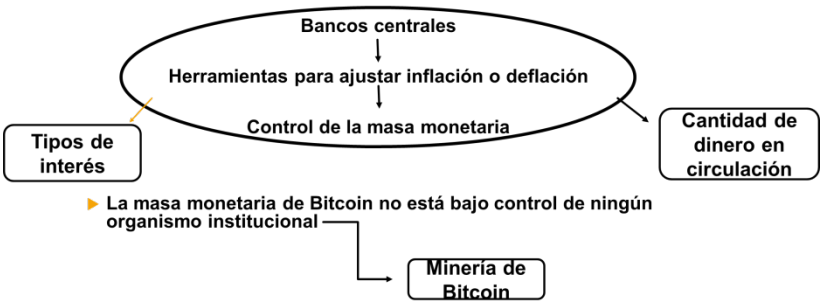
El precio de Bitcoin viene determinado por la oferta y la demanda; como en el mercado tradicional, cuando se incrementa la demanda el precio sube, y cuando cae la demanda, cae el precio. Hay un número limitado de bitcoins en circulación y los nuevos bitcoins son creados a una velocidad predecible y decreciente. Por tanto, el precio vendrá determinado en gran medida por la demanda de esta moneda virtual.

El valor del bitcoin ha ido cambiando a lo largo del tiempo y se basa, entre otros aspectos, en la confianza de sus usuarios, en su utilidad y en su popularidad. La demanda también puede verse afectada por la competencia entre criptomonedas o por otros problemas políticos o técnicos.

Durante más de un año, podemos decir que un bitcoin no valía absolutamente nada. Era una moneda que algunos usuarios se enviaban como recompensa de respuestas graciosas o útiles en algunos foros. La primera transacción en bitcoin fue en mayo del 2010, cuando un usuario compró dos pizzas a otro usuario a cambio de 10.000 bitcoins. Este hecho desató un proceso de revalorización, los poseedores de bitcoins se dieron cuenta de que podían acceder a bienes o servicios con esta moneda. Un solo bitcoin ha pasado de valer nada a casi 20.000 dólares americanos en diciembre de 2017.

El bitcoin y las criptomonedas tienen algunos problemas como medio de pago o de cambio dada la volatilidad de su valor. Al variar tanto el precio de la moneda, los usuarios no tienen certeza cuánto valdrán sus ahorros el día de mañana. Además, los empresarios tienen que actualizar los precios de sus productos cada momento.

Descentralización



Minería de Bitcoin

- **Cálculos matemáticos sobre un determinado bloque → Recompensa Bitcoins**
- **Se crean a velocidad predecible y decreciente. El número de bitcoins creados se reduce a la mitad a lo largo del tiempo → hasta que se detenga en 21 millones de bitcoins**
  - **2009-2012 → recompensa 50 bitcoins por bloque**
  - **28 de noviembre de 2012 se llegó al bloque 210.000 → recompensa 25 bitcoins**
- **2040 se llegará a los 21 millones de bitcoin**
- **Probablemente los mineros serán mantenidos por las tasas de transacciones**

Unidades de medida

- Bitcoin se puede dividir hasta 8 décimas, 0,00000001 BTC (Bitcoins) equivalen a un Satoshi.
- Las unidades de medida más comunes que se suelen utilizar son:
  - mBTC = mili bitcoin = 1 milesima de Bitcoin = 0.001 BTC
  - uBTC = micro bitcoin = 1 million de bitcoin = 0.000001BTC
- Incluso unidades mas pequeñas si es que así se requiere en el futuro.

Valor de los Bitcoins

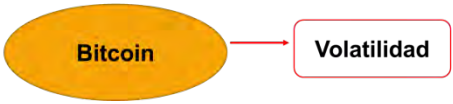
- **Los Bitcoins tienen valor porque son útiles como moneda.**
- **Tiene las características del dinero (durabilidad, portabilidad, fungibilidad, escasez, divisibilidad, reconocibilidad…)**
- **Valor basado en propiedades matemáticas en lugar de confiar en:**
  - **propiedades físicas (como el oro y la plata)**
  - **en autoridades centralistas (como las monedas fiduciarias)**
- **Necesita confianza**

Características del dinero	Oro	Efectivo (Euro)	Crypto (Bitcoin)
Fungible (Intercambiable)	Alto	Alto	Alto
No Desgastable	Moderado	Bajo	Alto
Portabilidad	Moderado	Alto	Alto
Durabilidad	Alto	Moderado	Alto
Divisibilidad	Moderado	Moderado	Alto
Seguro (No puede ser falsificado)	Moderado	Moderado	Alto
Fácilmente Manejable	Bajo	Alto	Alto
Escaso (Suministro Predecible)	Moderado	Bajo	Alto
Soberano (Emitido por el Gobierno)	Bajo	Alto	Bajo
Descentralizado	Bajo	Bajo	Alto
Inteligente (Programable)	Bajo	Bajo	Alto

Valor de los Bitcoins

Funciones del dinero

- **Medio de pago o de cambio: instrumento de pago aceptado.**
- **Depósito de valor: nos facilita desplazar capacidad adquisitiva al futuro.**
- **Unidad de cuenta o cambio: medir de forma homogénea el valor del resto de bienes.**
- **Patrón para pagos diferidos: diseñar pagos futuros en contrapartida de compras actuales.**

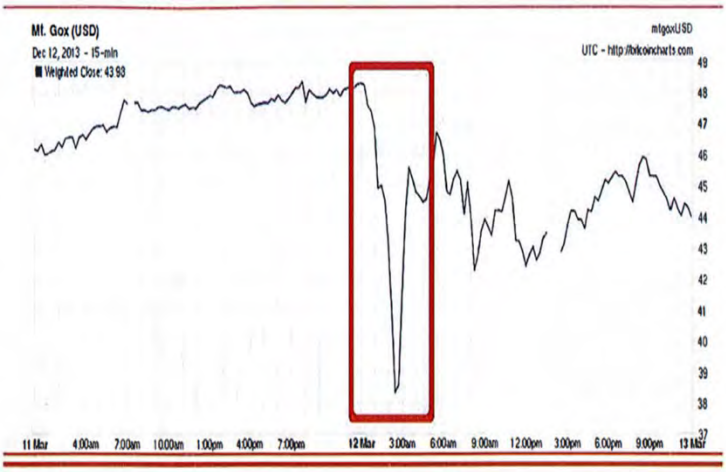


Determinación del Precio del Bitcoin

- **La oferta y la demanda**
- **Demanda ↓ Precio ↓**
- **Oferta predecible**
- **Demanda:**
  - **Confianza de sus usuarios, utilidad y popularidad**
  - **Competencia entre criptomonedas**
  - **Problemas políticos o técnicos**

Cotización

- **Grandes fluctuaciones**
- **Problemas técnicos (2013)**
- **Decisiones tomadas por países o grandes compañías**
- **Ataques de software malintencionado**
- **Mineros**



Evolución

- Enero, 2009 – Enero, 2010. Nada (0€)
- Mayo, 2010. Menos de $0.003
- Julio, 2010. $0.08
- Abril 2011. $1
- 8 Julio, 2011. $31
- Diciembre, 2011. $2
- Diciembre 2012. $13
- Abril, 2013. $266
- Enero, 2014. $750 – $1000
- Febrero 2017. $1222
- Diciembre 2017. $19499
- Mayo 2017. $9322

¿Burbuja?

- Rápido aumento en el precio
- Sobrevaloración que dará lugar a una repentina corrección a la baja
- Alta volatilidad → Mercado peligroso → especuladores profesionales

¿se corresponde el precio actual del Bitcoin con su valor real?

¿existen fundamentos económicos sólidos que puedan explicar tales niveles de cotización?

¿se trata de una demanda especulativa?

1. Uso actual y futuro.

El número de empresas que aceptan Bitcoin como medio de pago es cada vez mayor. Actualmente se puede contratar todo tipo de servicios: telefonía, internet, tarjetas regalo, asesoría legal, turismo, etc. Asimismo, está despertando el interés de diversas instituciones, múltiples bancos están trabajando juntos para crear una nueva criptomoneda.

Uso Actual y Aceptación

- **Nº de empresas que aceptan Bitcoin en constante aumento:**

  telefonía, hosting de internet, tarjetas regalo, asesoría legal, turismo, etc.
- **Algunos de los mayores bancos del mundo empiezan a bloquear la compra de Bitcoins con tarjetas de crédito**
- **El sector bancario trabaja en monedas virtuales, pero su emisión seguiría estando controlada por los bancos.**

Respecto al futuro de los bitcoins, algunos expertos estiman que entre 2.020 y 2.025 su precio podría estar entre los 100.000 y 1.000.000 de euros; otros expertos auguran escenarios más optimistas y colocan al bitcoin en un valor de 47 Millones de euros en las siguientes décadas y prevén una estabilidad de su precio tras la etapa de crecimiento. Sin embargo los detractores de Bitcoin consideran que es algo que podría desaparecer en cualquier momento.

Futuro del Bitcoin

- Optimistas: entre 2020 y 2025 → entre 100.000 y 1.000.000 de euros
- Más optimistas: 47 Millones de euros por cada Bitcoin en la siguientes décadas
- Detractores: puede desaparecer en cualquier momento.

De Izda. a dcha.: José Mª Hidalgo Martínez; Alberto Ruiz Ojeda; Beatriz Rodríguez Días; Eugenio J. Luque Domínguez; Rafael Vidal Delgado; Pedro Fernández y José Mª López Jiménez

2ª Jornada: TERRORISMO Y LAS INFRAESTRUCTURAS CRÍTICAS

FORO PARA LA PAZ
EN EL MEDITERRÁNEO

XII Jornadas de Seguridad, Defensa y Cooperación

Infraestructuras Críticas

GEOECONOMÍA

Días 14, 15 y 16 noviembre 2018
Jornadas de 18 a 21 horas. Diplomas
UNIA y CIFAL previa evaluación

Diploma de UNIA se encuentra en trámite

www.foroparalapazenelmediterraneo.es

“Situación en España de la lucha contra el terrorismo y el crimen organizado”.

PONENTE: D. ANTONIO HERNANDO VERA, Diputado al Congreso por el Grupo Socialista.

NOTA DE LA DIRECCIÓN DE LAS JORNADAS: La ponencia fue reproducida en video y audio y transformada mediante un programa informático a word, adaptándose el pensamiento y las palabras del ponente a un texto coherente. Puede que se hayan interpretados erróneamente algunos pensamientos, lo cual debe achacarse a la propia dirección del Foro y nunca al ponente.

Dar las gracias al Foro para la Paz en el Mediterráneo, a la Universidad Internacional por la invitación, a todos los organizadores y a los participantes y a las instituciones públicas y privadas que veo que apoyan la organización de estas Jornadas.

Tengo que decirles que cuando he visto el panorama y cuando les he visto a todos ustedes he dicho definitivamente yo no soy la persona adecuada para estar aquí, en este estrado, porque miren yo no soy un experto en terrorismo, no soy un experto en ciberdelincuencia y en ciberterrorismo no lo he sido nunca, tengo experiencia porque durante 6 años fui portavoz de la Comisión de Interior del Grupo Parlamentario Socialista cuando el ministro de Interior era Alfredo Pérez Rubalcaba

La primerísima experiencia inolvidable, ojalá no la hubiese tenido que vivir, fue mi participación en la comisión de investigación de los atentados del 11 de marzo.

RTVE-1

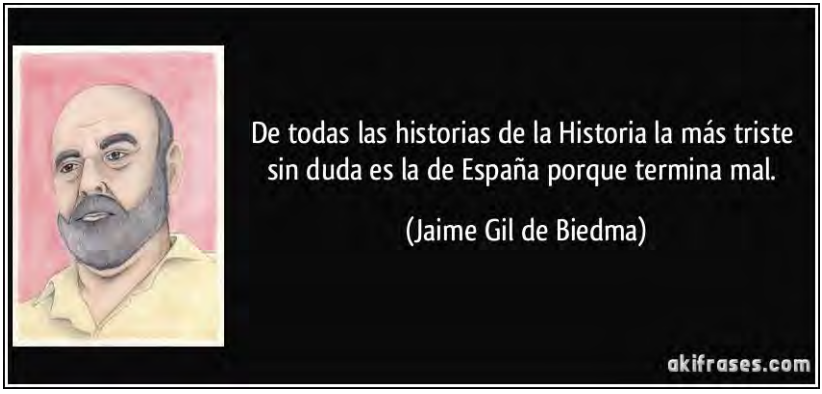
Bueno de ahí que luego haya seguido muy de cerca todos los temas relacionados con terrorismo y actualmente soy portavoz del grupo y he coincidido con alguno de ustedes en la comisión que se dedica a los temas de seguridad nacional: la Comisión de Seguridad Nacional que es fruto de la Ley de Seguridad Nacional. Hay una ponencia sobre ciberdelincuencia sobre ciberterrorismo en esa entidad seguridad en esa comisión y unas recomendaciones que esperamos que sean útiles y en las que muchos de ustedes de los cuerpos a los que ustedes representan están teniendo un papel importante por lo tanto insisto yo nunca he estudiado esto.

Actualmente doy clases en un máster de comunicación política y cuando voy a darles comunicación política digo que conozco el tema, por lo que he aprendido a base de golpes y 14 años en

el Congreso de los Diputados, no, no, y no lo he estudiado en la universidad; bueno pues exactamente lo mismo me pasa con el terrorismo y con las infraestructuras críticas no obstante el enfoque que yo había hecho me da la impresión que es un enfoque adecuado para enmarcar en términos históricos en términos políticos las jornadas porque luego veo que van a poder ustedes bajar mucho más al detalle, a la legislación, al desarrollo de lo que yo lo voy a hacer en esta intervención que está hecha en términos de perspectiva política e histórica sobre lo que ha sido, ha significado el terrorismo en nuestro país

Con todas esas prevenciones es por lo tanto poniéndome varios cinturones de seguridad para que ustedes no digan este señor que hace aquí pues voy a voy a leer lo que lo que he escrito.

En principio yo soy muy disciplinado para estas cosas, son 2100 palabras pues he calculado que aproximadamente serán 18 minutos o así y si me paso, usted (se dirige a la moderadora) me corta que estamos acostumbrados y no hay problema.



En el poema “Triste historia” dice Jaime Gil de Biedma en su primer verso de todas las historias de la historia la más triste sin duda es la de España porque termina mal como si el hombre harto ya de luchar con sus demonios quisiera terminar con esa historia de ese país, de todos sus demonios y en el último verso del mismo poema dice “pido que España expulsa esos demonios, que sea el hombre el dueño de su historia”, parafraseando podríamos decir que, de todas las historias de nuestra historia democrática, la del terrorismo es sin duda la más triste pero termina bien después de mucha muerte y de mucho sufrimiento y destrucción porque ha habido mucha muerte y mucho sufrimiento y mucha destrucción, hemos conseguido acabar con uno de nuestros terrorismos, con el terrorismo de ETA.

Nos hemos hecho dueños de nuestra historia, incluso del relato de la historia y hemos vencido a ese demonio que teníamos dentro de nuestras fronteras. Durante mucho tiempo y esto se lo he contado una vez a Ramón Jauregui, los cortejos fúnebres de víctimas de ETA discurrían en silencio.

Casi clandestinamente por las calles y pueblos y ciudades del País Vasco le seguían familias rotas de dolor miembros de las Fuerzas y Cuerpos de Seguridad del Estado, militares, miembros de la Judicatura, también compañeros de partido, pero en muchas ocasiones en demasiadas ocasiones, las persianas de las viviendas se bajaban al paso del cortejo, las puertas se cerraban y los comercios echaba en el cierre, muchas personas daban la espalda aquella realidad de violencia en la que vivía una parte importante de la sociedad del País Vasco. Las víctimas eran como piedras que impactaban contra las aguas del lago y que al principio en el

epicentro del impacto producen ruidos y olas, pero a medida que se alejan de ese lugar se va difuminando el efecto, el ruido, el oleaje y el dolor, hasta llegar a desaparecer, hasta recuperar la calma de las aguas del lago, en los tiempos en los que ir destinado como policía o Guardia Civil, funcionario de prisiones o juez al País Vasco, era sinónimo de poner en riesgo la propia vida y la de la familia, eran tiempos en los que los mítines o reuniones de mi partido y el Partido Popular, a la entrada de los edificios donde los hacíamos, había tantas personas como dentro de esos locales: eran los escoltas de los cargos públicos, desde humildes concejales de pueblos pequeños, hasta diputados senadores o miembros del Gobierno.

Atentado contra la Casa Cuartel de Zaragoza

Recordaran ustedes a humildes concejales de pueblos pequeños que, además eran los responsables de la limpieza de los mismos, acompañados a su lado por un escolta. Tiempos en los que Francia especialmente el País Vasco francés era considerado el santuario para los terroristas de ETA y tanto a

la justicia gala como sus fuerzas y cuerpos de seguridad les costaba mucho entender la magnitud y la trascendencia de la violencia terrorista del entonces denominado movimiento independentista vasco o del movimiento vasco de liberación, al que todavía rodeaba un inexplicable halo de prestigio por sus actos de terrorismo contra la dictadura franquista. Momentos en los que las asociaciones de víctimas especialmente la VT se sentían muy solos a la hora de dar sus primeros pasos en defensa de la vida de la libertad y la dignidad de las víctimas y de denunciar a los terroristas y a un entorno social y político que los legitimaba, acuérdese de aquella frase de "un político vasco que decía unos mueven el árbol y los otros recogemos los frutos" [1]

La estrategia de socialización de la violencia supuso la generalización de los actos terroristas a toda la ciudadanía que pasaban a ser objetivos potenciales de ETA. Ya no solo estaban militares, guardias civiles o policías y jueces, estaban los militantes y cargos de los partidos, empresarios, y ciudadanos anónimos inocentes, como las víctimas de Hipercor, los hijos, las hijas, las mujeres, los hermanos de los guardias civiles del cuartel de Burgos o de tantas otras dependencias de las Fuerzas y Cuerpos de Seguridad del Estado.

El secuestro y posterior asesinato de Miguel Ángel Blanco en el año 1997 marcó un antes y un después: primero social y luego político, constituyendo el denominado espíritu de Ermua

[1] EL PAÍS, edición impresa de 3 de abril de 1994: "Sacudir el árbol para que caigan las nueces".

-antes había nacido Gesto por la Paz- y después se constituye el Foro de Ermua.

Miguel Ángel Blanco

Luego vinieron “Basta ya” que, incluso llego a recibir el Premio Sajarov del Parlamento Europeo.

Pero el terrorismo seguía siendo uno de nuestros demonios patrios. Habían desaparecidos hacía tiempo las Brigadas Rojas, la banda Baader-Meinhof, pero el terrorismo en España seguía como un residuo violento del pasado, a pesar de que el nuestro era un país ya entonces, desde el principio, con una democracia sentada con libertades y derechos garantizados y un sistema político y social, homologable a los demás países de nuestro entorno, por eso el que Occidente empezase a recibir el zarpazo, el terrorismo yihadista islamista radical violento, supuso que muchos países y gobiernos tomaran conciencia de la gravedad del terrorismo y de la necesidad de prestar toda nuestra atención colaboración y medios para combatirlo

Antes del 11S y del 11M, el terrorismo yihadista había actuado contra intereses de países occidentales por ejemplo las embajadas de Estados Unidos en países africanos; en un

primer aislado atentado en el aparcamiento de las Torres Gemelas o en la Casa de España en Casablanca, pero sin duda es el 11S primero y el 11M después los que nos sitúan ante el nuevo escenario de la gravedad y ultraviolencia del terrorismo yihadista.

Informe de Incidentes de la Oficina de Explosivos ATF 1993. Atentado en los aparcamientos de las Torres Gemelas

El 11M nos pilla con mucha experiencia en materia de lucha contra el terrorismo etarra, pero con cierto desconocimiento frente a ese nuevo fenómeno terrorista yihadista.

Teníamos muchos policías especializados y muchos recursos volcados en el terrorismo de ETA, pero no los suficientes dedicados a combatir el terrorismo yihadista.

El 11M sirvió para que nos intentaremos poner el día, para que nos pusiésemos al día -ya nadie lo recordará- y no se suele hacer porque esa comisión, una comisión en la que hubo

mucha disputa política, yo creo que innecesaria disputa política, pero las conclusiones técnicas, las recomendaciones de aquella comisión de investigación sobre los atentados del 11M, que mi grupo por cierto redactó en un parador aquí cerca, en el Parador de Nerja, fueron votadas por todos los grupos parlamentarios, al menos por los dos grandes grupos parlamentarios, por Partido Popular y por el Partido Socialista, con recomendaciones de mejora coordinación, mayores medios, reformas legales y procedimental, control de explosivos, vigilancia en las prisiones, órganos más eficaces de coordinación entre Guardia Civil y Cuerpo Nacional de Policía y sus homólogos de otros países, coordinación entre servicios de inteligencia y servicios policiales, ampliación de los equipos contratación de traductores, etcétera.

Como resultado de todo ello se crearon el Centro Nacional de Coordinación antiterrorista [2] y el Centro de Inteligencia Contra el Crimen Organizado (CICO), que luego se fusionaron en el 2014 en el Centro de Inteligencia contra el Terrorismo y el Crimen Organizado (CITCO), se compartieron bases de datos, inteligencia, se reformaron leyes y transpusieron directivas

Avanzamos mucho y muy rápido a nivel internacional a partir del 11M, haciendo especial hincapié en descubrir los sistemas de financiación del terrorismo islamista, las cuentas ocultas entidades bancarias occidentales o los complejos sistemas a

[2] El **Centro Nacional de Coordinación Antiterrorista**, también conocido como **CNCA**, fue creado en el mes de mayo del año 2004 a raíz de los atentados del 11M para una mayor eficacia contra el terrorismo nacional e internacional. Quedó disuelto en octubre de 2014, integrándose con el Centro de Inteligencia Contra el Crimen Organizado (CITCO).

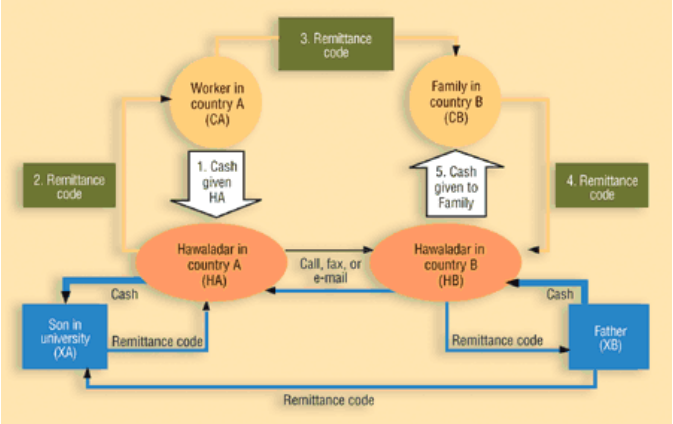
través de los que se veían cantidades ingentes de fondos seguir.

La pista del dinero era fundamental para acabar con los terroristas. ETA se financia a través del llamado impuesto revolucionario, los secuestros, las extorsiones, pero también con las aportaciones de los simpatizantes de la izquierda abertzale. Al Qaeda movía el dinero a través de un complejo sistema financiero [3], denominado la "Hawala" [4].

Y teníamos que saber qué era aquello de la "Hawala".

[3] CID GÓMEZ, Juan Miguel del, profesor de Economía y Contabilidad de la Universidad de Granada. *En busca de un perfil financiero del terrorismo de Al Qaeda y sus grupos afines*. https://www.ugr.es/~jmdelcid/Financiacion%20Al%20Qaeda.pdf. Consultado el 7 de abril de 2019.

[4] HAWALA: *Es una forma de mandar dinero a cualquier parte del mundo sin dejar rastro. Se basa en la confianza entre una red de familiares y compatriotas.* Teinteresa.es, de fecha 04.04.2014 y consultado el 04.07.2019, http://www.teinteresa.es/espana/funciona-metodo-financiacion-terrorismo-yihadista_0_1114089683.html



[5]

El terrorismo yihadista ha utilizado y utiliza las nuevas tecnologías para comunicarse, para coordinarse para instruir a sus comandos, hacer proselitismo, recaudar fondos, captar nuevos miembros, organizar comandos durmientes o lobos solitarios. La red internet es una plaza pública en la que los yihadistas se mueven con soltura. La red como instrumento, más que la propia red como objeto de las acciones terroristas o como medio para directamente a atentar, por ejemplo, contra las infraestructuras críticas, tema que tratarán estos días de las Jornadas.

Siempre me ha emocionado la madurez de la sociedad española cuándo ha sido brutalmente agredida por el terrorismo yihadista del 11M, Barcelona, Cambrils, … Son los ejemplos evidentes. En la Puerta del Sol de Madrid está la placa de agradecimiento.

[5] El sistema Hawala: http://www.gdrc.org/icm/hawala.html. Consultado el 07.04.2019,

De la ciudadanía madrileña todos los que colaboraron aquel infausto día de marzo: taxistas, bomberos, policías, funcionarios, sanitarios, personas anónimas, que pusieron sus coches al servicio de los heridos, vecinos que bajaron con mantas o donantes de sangre y no se produjeron actos de racismo-xenofobia, como los que han ocurrido en otros países, ni hubo una acusación de responsabilizar a las comunidades musulmanas y a los miembros de las mismas que hoy son nuestros vecinos, compañeros de trabajo o compañeros de nuestros hijos en las escuelas. Yo soy vecino de Roquetas de Mar en mi ciudad hay 110 nacionalidades. A la guardería de mi hija van niños de todas las nacionalidades y procedencias muchos de ellos musulmanes y no digo que no haya problemas de convivencia lo que digo es que cuando se han producido estos hechos de terrorismo de origen yihadista nunca he visto una reacción contraria hacia esa comunidad y sus miembros por parte de la población.

Mire la derrota sin paliativos de los terroristas, no hubiera sido posible sin el enorme sacrificio y entrega de los miembros de las Fuerzas y Cuerpos de Seguridad del Estado, su especialización y profesionalidad ha sido internacionalmente reconocidas, su eficacia y preparación la situaron a la cabeza de los cuerpos policiales mejor preparados para investigar combatir y prevenir el terrorismo, desgraciadamente a pesar de esa preparación y eficacia nosotros, como otras democracias, no somos inmunes al terrorismo, como escuche hace ya muchos años en la comisión de investigación de los atentados del 11M; nosotros los buenos, tenemos que acertar siempre y a ellos les basta con acertar una vez aunque lleguen en centenares de ocasiones. Mientras el terrorismo de ETA o del terrorismo de ETA podemos hablar en pasado, del terrorismo

yihadista, desgraciadamente, tenemos que hablar en presente en Occidente en Europa y en España. Los atentados de Barcelona y todo de hace poco más de un año son el vivo ejemplo de ello. Estamos con un nivel de alerta elevado porque las autoridades y los expertos lo consideran necesario y porque no podemos bajar la guardia. Los desafíos que representan las nuevas tecnologías, nos hacen más vulnerables, pero también más eficaces.

Soy portavoz de como he dicho, de la Comisión de Seguridad Nacional creada por el mismo nombre y en ella hemos examinado recientemente y algunos de ustedes ha comparecido, la nueva estrategia de seguridad nacional y además seguimos trabajando intensamente en la ponencia sobre ciberseguridad. Me gusta decir en esa comisión, en donde hay algunos clásicos modernos que se repiten en todas las intervenciones de los expertos que acuden a informarnos a los miembros de la misma: los diputados y las diputadas y que son:

Uno: Más inversión y mejores medios y cuando yo pregunto siempre me dicen para no quedar mal con sus jefes, los políticos de turno, no hombre no es que estemos mal, pero necesitaríamos más. Estoy convencido de que se necesita más de que todo lo que se invierta, y además debemos considerarlo bien invertido. Segundo: más coordinación entre los distintos servicios y especialmente entre los servicios públicos y el sector privado, más y mejor coordinación buscando las sinergias más medios humanos especializados. Tercero mayor especialización de los medios humanos, evitando perder el talento que se genera en España y que generan nuestras universidades que es mucho y a veces precisamente porque

les ofrecen ofertas interesantes desde el punto de vista profesional y desde el punto de vista académico y económico se van de España y prestan sus servicios para empresas en otros países. De esto especialmente alguno de ustedes puede tener algún ejemplo cercano dentro de sus propios cuerpos porque son expertos que se lo rifan en otros países y algunas empresas y, por último, y luego vendrá una de las personas, de los diputados que lo propuso y a mí me pareció bien y nos piden acuerdo nos piden que los partidos políticos en este tema nos pongamos de acuerdo y convirtamos la ciberseguridad en una auténtica política.

Con esto voy terminando, miren quizás comprendimos, más tarde de lo deseable que la política antiterrorista tenía que ser una política de Estado. En el caso del terrorismo no supimos verlo lo suficientemente rápido, si una política de Estado es aquella que afecta aspectos fundamentales de la convivencia, los derechos y la democracia esta lo es; si se debe planificar a largo plazo para evitar que los cambios de gobierno supongan vaivenes en la política, también lo es. Si hay que subirla por mutuo acuerdo y renunciar a la legítima confrontación política y partidista, debemos hacerlo. Sí debe gozar de un amplio consenso social y político, también debemos procurar que así sea. Pero es que, además, en el caso de la política antiterrorista, creo que lo que tiene que quedar claro es que la dirección de la misma corresponde al Gobierno.

Recientemente con motivo del 40 aniversario de la Constitución Española escuchaba a dos veteranos políticos; uno del Partido Socialista y el otro del Partido Popular. Decir que quizás, si nos hubiésemos puesto de acuerdo antes habríamos acabado antes con ETA, no sé si esto es así o política ficción. Como no

me gusta volver la vista atrás sobre nuestros errores o sobre lo que pudo ser y no fue, lo que tengo claro es que la experiencia del pasado nos debe servir para actuar en el presente y diseñar en el futuro.

Ernest Lluch, ministro de Sanidad

La unidad en la lucha contra el terrorismo, la hemos ido jalonando a través de diversos acuerdos: Acuerdo de Madrid sobre terrorismo de noviembre de 1987; el Pacto de Ajuria Enea, también denominado acuerdo para la normalización y la pacificación de Euskadi es del 88. El Pacto por las Libertades y contra el Terrorismo, de diciembre del 2000, que se suscribe después del asesinato poco después del asesinato de Ernest Lluch.

Un acuerdo para afianzar la unidad en defensa de las libertades y en la lucha contra el terrorismo: Pacto antiyihadista de enero del 2015. Lamento que no esté aquí Francisco Martínez porque tuvimos él y yo un papel importante en la redacción del pacto antiyihadista, junto con el entonces ministro Jorge Fernández Díaz y con otra persona de mi partido.

Cuándo se producen los atentados de París, yo le dije al entonces secretario general del Partido Socialista y hoy presidente del Gobierno que, era absolutamente necesario ampliar el Pacto por las libertades y contra el terrorismo que había sido concebido como un pacto para luchar contra ETA, al

terrorismo yihadista. No lo hicimos en su momento después del 11M, pero que era absolutamente imprescindible porque tarde o temprano nosotros nos terminaría tocando.

Como desgraciadamente fue así con los atentados de Barcelona y Cambrils y tengo que decir que a Pedro Sánchez lo vi inmediatamente esa misma tarde, anuló un viaje, llamó al presidente del Gobierno Mariano Rajoy, que se mostró inmediatamente receptivo a sellar ese acuerdo. Francisco Martínez tuvo un papel destacado en la redacción del mismo y yo humildemente también pude meter la pluma en aquel acuerdo. Nos pareció que será el camino, pero les he decir que no sin alguna crítica dentro de nuestro propio sector y dentro de nuestro propio partido, por renunciar a ese espacio y hoy sin embargo yo creo que nadie en su sano juicio estaría dispuesto a salirse del pacto a denunciar el pacto o a criticarlo.

Termino ya, quedan muchas cosas por hacer en relación con el terrorismo de ETA, quedan asesinatos por esclarecer y casos que no se han sido juzgados porque no se han encontrado los responsables. Nos queda ganar, estamos ganando la batalla del relato de las víctimas y los victimarios de los vencedores y los vencidos, porque si efectivamente hemos vencido y hemos derrotado al terrorismo de ETA, de esta relación al terrorismo yihadista, nos queda trabajo por hacer y no podemos, ni debemos bajar la guardia, tenemos que dedicar más recursos especializados cada día y dotarles de la más avanzada tecnología, será una guerra larga, pero tengo claro que la iremos ganando como creo que la vamos ganando para ella. Esa unidad de la que he hablado es fundamental, es una pieza insustituible en una sociedad democrática, lo demás cuesta, supone recursos y esfuerzos y no siempre los hay, son escasos

y hay que repartirlos, pero la unidad depende de nuestra voluntad política y esa existe de forma creo que a estas alturas inquebrantable al menos entre la mayoría de los partidos.

En el Parlamento hay algunos grandes discursos, algunos no tan buenos, pero jamás olvidaré el parlamento vibrante, poderoso, emotivo, indignado y a la vez valiente, de Pilar Manjón; la dignidad con la que aquella mujer emocionada representó a las víctimas del atentado del 11M, fue para mí una lección inolvidable que aún me genera emoción, exigía verdad, reparación, justicia y humildemente aunque quede camino por recorrer y a pesar de los errores creo que eso es lo que la democracia española con gobiernos del Partido Popular y del Partido Socialista ha procurado hacer, por eso y respondiendo finalmente a la pregunta del título de la ponencia que me han encargado los organizadores, Yo lanzaría un último mensaje de confianza de tranquilidad porque estamos en buenas manos, en manos de expertos de miembros de las Fuerzas y Cuerpos de Seguridad del Estado que tienen mucha experiencia mucho prestigio y que están muy preparados y porque estoy seguro que ya a nadie, a ningún gobierno, a ningún partido en España, se le ocurría cometer reincidir en los errores del pasado.

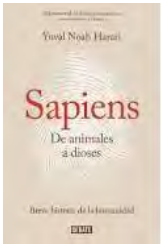
La lucha contra el terrorismo

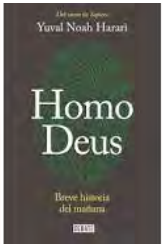
Ponente: Luis Miguel Salvador García (diputado en el Congreso por Ciudadanos)

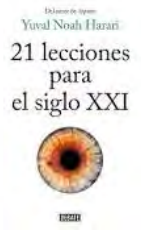
NOTA DE LA DIRECCIÓN DE LAS JORNADAS: La ponencia fue reproducida en video y audio y transformada mediante un programa informático a word, adaptándose el pensamiento y las palabras del ponente a un texto coherente. Puede que se hayan interpretados erróneamente algunos pensamientos, lo cual debe achacarse a la propia dirección del Foro y nunca al ponente.

Soy un amante del ajedrez, pero por lo que representa para la estrategia.

Terrorismo es una estrategia militar que espera cambiar la situación política extendiendo el terror en lugar de causar daños materiales. He empezado a ojear varios libros de Yuval Noah Harari: “Sapiens. De animales y dioses”, “Homo Deus” y ahora he hecho otro que es “21 lecciones para el siglo XXI”. He ido a ver lo que había puesto por la parte de terrorismo y asumo totalmente la definición, coincidiendo, además, en buena parte de los planteamientos que efectúa en el último libro:







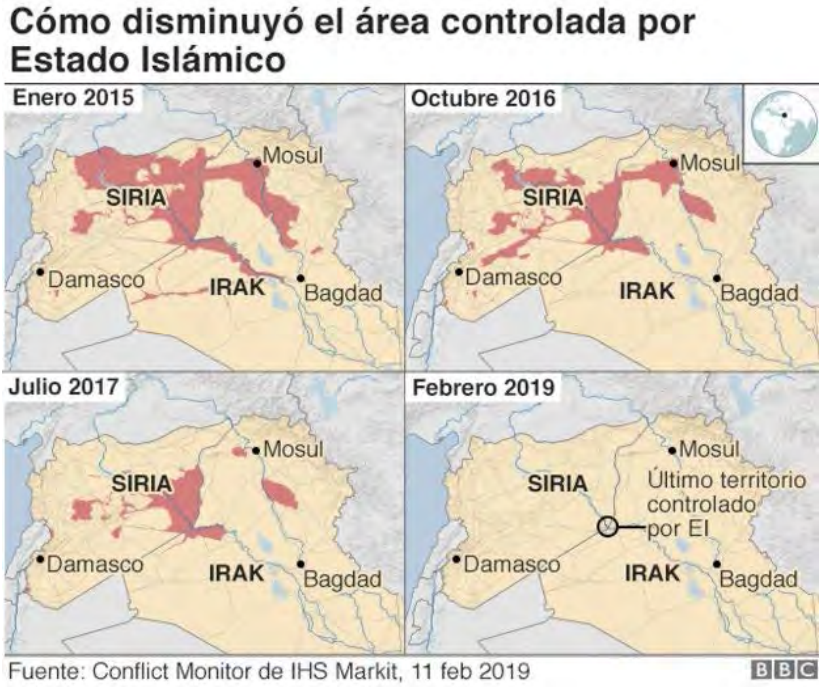
Si hacemos un cálculo rápido de las muertes por terrorismo, desde 2001 han muerto 50 personas al año en la Unión Europea, 50 en Estados Unidos y 7 en China.

Unas 25.000 en todo el mundo. En comparación con, por ejemplo, la diabetes, que mata a 3,5 millones de personas, Harari se pregunta, por qué tememos al terrorismo. En realidad, el terrorismo es «una estrategia militar que espera cambiar la situación política extendiendo el terror en lugar de causar daños materiales». En el terrorismo existe una desproporción «asombrosa» entre la fuerza real de los terroristas y el miedo que consiguen inspirar. «Los terroristas montan un espectáculo de violencia que se apodera de nuestra imaginación y la vuelve contra nosotros». De ahí que Harari afirme que los terroristas piensan más como productores teatrales que como generales del ejército: «Puesto que de forma intuitiva entendemos que el terrorismo es teatro, lo juzgamos más por su impacto emocional que por el material». Por eso, si queremos combatirlo de manera efectiva, afirma, hemos de ser conscientes de que nada que los terroristas hagan podrá «derrotarnos».[6]

El terrorismo yihadista ha seguido dos modelos: uno el referido por Hariri y otro, el militar, cuando contaba con un ejército regular fuerte, cuando iba conquistando territorios y cuando a partir de ahí, implantó su soberanía, dado que disponía de medios materiales, financiándose, a través de la venta de petróleo todo lo que iba construyendo.

[6] HARIRI, Yuval Noah. *21 Lecciones para el siglo XXI*. Parte Tercera. Desesperación y esperanza. DEBATE. https://diariojudio.com/opinion/21-lecciones-para-el-siglo-xxi-del-escritor-israeli-yuval-noah-harari-autor-de-de-animales-a-dioses-y-homo-deus/278702/ Consultada el 06.03.2019.

Constituyó el estado islámico, disponiendo de territorio, súbditos, soldados y finanzas, es decir los pilares en que se fundamenta un estado, aunque no llegara a ser reconocido por nadie .



7

Aparte de la forma de combatir en el “territorio ocupado” del llamado “califato”, está también el terrorismo tradicional, en donde hay menos personas y además están más perseguidos, con problemas para salir a la luz. Es el terrorismo tradicional, aunque posteriormente se tratará de nuevo este tema, en

[7] La conferencia se dictó en noviembre de 2018 y en marzo de 2019, el territorio que ocupaba DAESH ha vuelto a Iraq y Siria.

donde el miedo infundido era y es su principal arma, muy superior a su fuerza real, dado que el miedo que se pretende introducir en la sociedad, es como el motor para intentar desestabilizar las capacidades del Estado, pero en realidad éstas permanecen intactas.

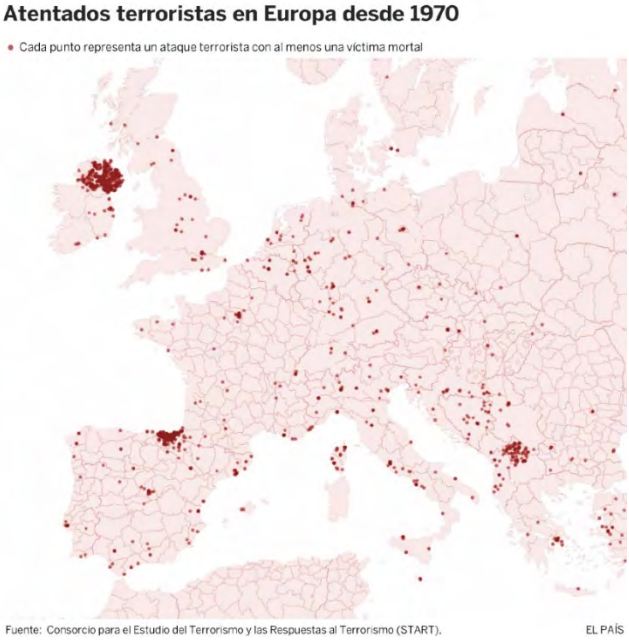
Esto no sucedía en Pearl Harbor donde un acto de guerra de Japón, efectuado sin una previa rotura de hostilidades y declaración oficial, provocó el hundimiento de la flota estadounidense del Pacífico, porque el objetivo en una guerra convencional es bajas, intentar destruir infraestructuras, intentar disminuir las capacidades de tu rival.

El terrorismo sabe que no puede hacer daño al Estado, como ahora veremos con estadísticas, pero busca algo que puede llegar a ser muy potente, si lo gestionan bien, y es la capacidad de influir en la opinión pública.

La fría estadística indica que el terrorismo causa pocas víctimas. En este sentido habría que hacer una anotación, para que no se me tache de “insensible”, ya que una sola víctima merece todo nuestro respeto y toda nuestra preocupación, pero el esfuerzo del sistema no está orientado precisamente hacia las víctimas, sino que está más a la reinserción de terroristas, suponiendo todo ello, miles de millones de euros. Por supuesto se han sucedido atentados terroristas con muchos muertos y afectados, como el 11S que supuso cerca de tres mil bajas y varios miles más de afectados, o el 11M y otros que hemos sufrido en los últimos años.

Veamos el número de bajas que hay anualmente en cada uno de estos países; en la Unión Europea en el entorno de las 50

personas cada año de media, desde 2001, 10 personas en Estados Unidos, 7 personas en China, unas 25.000 personas en todo el mundo. Cualquier causa de mortalidad que afecta a nuestras sociedades es infinitamente mucho más grande, pero, sin embargo, no despierta el temor y el miedo que despierta en este sentido el terrorismo. Algunos datos más, en Madrid el 11 marzo, casi 200 asesinados, en París, noviembre 130, Bruselas 32, en Manchester Arena 22, Barcelona y Cambrils 16… sabemos las cifras son cifras que a pesar de todo lo que son capaces de alterar la conciencia de toda la opinión pública repito, que no dejan de ser bajas si lo comparamos con cualquier otro tipo de accidentes de cualquier índole en esta sociedad moderna.



Esta semana pasada (5-9 de noviembre de 2018) estuvimos en una misión institucional. En el Congreso de los Diputados tengo una doble responsabilidad, siendo el portavoz, de mi grupo parlamentario, en las Comisiones Cooperación Internacional para el Desarrollo en el Congreso de mi grupo y en la Comisión Mixta de Seguridad Nacional, las cuales trata temas de interior, de ciberseguridad, del modelo policial del siglo XXI, etc., total que estoy dentro de las "patas" de la seguridad, por una parte, la cooperación y por otra la estricta seguridad.

Ambas están bastante relacionadas. Estuvimos en una misión en Honduras en dónde está organizada por el IFRC [9] de Cruz Roja, que son profesionales de la organización que intervienen en conflictos y nos comentaron muchísimas interioridades. Por ejemplo, del tema de los secuestros, o sea como normalmente países anglosajones no pagan rescate y, los países europeos que los pagan. Secuestran entonces a personas de Estados Unidos o de Inglaterra sabiendo que al final montan un teatro y terminan asesinándolos.

El objetivo para los que pagan, es que lo sigan haciendo, pero nos contaron intimidades de muchas negociaciones y distintos ámbitos, cuestiones que conocen muy bien al haber participado en más de 80 misiones en el mundo.

[8] EL PAÍS. Edición de 04.05.2018. https://elpais.com/politica/2018/05/02/actualidad/1525259651_003772.html Consultado el 06.04.2019.

[9] Internacional Federation of Red Cross

No hay que ir al terrorismo yihadista, porque cuando hablamos de terrorismo, estamos hablando de una acción terrorista y que provoca lo que se ha comentado hasta ahora.

La espiral de violencia en Latinoamérica es terrible

Si vamos a estos datos, en un país en que en este momento están imbuidos porque cuando hablamos de terrorismo estamos hablando de una acción terrorista que provoca lo que hemos comentado.

En 2017 el número víctimas en México fue de 29.168 asesinados violentamente, pero es que este año 2018, ya se ha batido el triste récord y estamos cerca de los 30.000 asesinatos. En Guatemala, hubo 4.110; en El Salvador otra cifra similar y en Honduras, lugar donde estábamos, 3.466, lo que para un país de nueve millones de habitantes y de extensión como Andalucía.

En estos países todos los habitantes están influidos por la violencia. Tu hijo, desde chiquitito, lo van a observar las “maras” [10] del territorio que controlan y en una edad determinada entra en una “mara” y ya no puedes salir de ella. En caso de que huyas a otros territorios, te perseguirán y te matarán y al final terminas dentro del sistema: los pobres roban a los pobres y todos tienen que pagar la extorsión.

Cabe preguntarse por el concepto de terrorismo, porque los países anteriores y otros de origen hispano, están dominados por la violencia, pero no los consideramos que son actos

[10] Grupo organizado de jóvenes, especialmente de origen salvadoreño, que se dedica a actividades delictivas y criminales

terroristas, aunque su violencia causa muchas más muertes que en territorios donde hay terroristas (oficialmente) armados. Comparemos las cifras de México, con los 10.507 de Siria o los 5.795 de Yemen.

En la Comisión de Cooperación Internacional para el Desarrollo, determinados partidos, están metiendo permanentemente iniciativas con el objetivo de que no vendamos las fragatas Arabia Saudí, eso en realidad es simplemente favorecer a uno de las partes en el conflicto para que, a partir de ahí, dificultarle a la otra, su dominio en la región.

Continuando con las cifras de la violencia, en Afganistán causaron 3.438 víctimas y en Libra 433.

Otro país, como Colombia está dominado por la violencia, porque de ella no se puede escapar nadie. Debemos pensar en todo lo que hay en muchos países: violencia, extorsión, secuestro, carteles de la droga, maras, las autodefensas, es decir un uso desproporcionado de la violencia, incluso por los propios órganos del Estado.

Hemos visto lo que está pasando en este momento con el gobierno de Guatemala, con el presidente de Filipinas. Estamos viendo a Bolsonaro, también con el discurso con el que ha ganado en Brasil o sea todo un endurecimiento de la violencia y al final lo que genera es más espiral de violencia.

Evidentemente, ¡claro que hay que combatir a la violencia y claro que hay que dotarlos de seguridad!, porque si no lo hacemos, estamos propiciando el caos; pero, por ejemplo en Honduras, las cifras cuando se han dedicado a hacer ciertos cambios han pasado de 150 asesinatos por cada 100.000

habitantes, y ahora están cerca de 50 fallecidos, ¡claro que se notan las medidas a corto plazo!, deben tomarse medidas por la seguridad, pero tienen que ser medidas que también acompañan para después, para el futuro del país porque, como se ha comentado antes, o sea cuando la captación, los jóvenes de estos países no tienen ninguna expectativa de futuro y por tanto, son caldo de cultivo de lo que les permita ganarse la vida más rápido, porque no hay otra opción aquí.

Vemos en los civiles desplazados en 2017 en México 354.000, en Guatemala 242.000, en Salvador 289.000, y en Honduras 90.000, y estamos viendo ahora las caravanas que se está produciendo [11], para protegerse de los coyotes que les cobran entre 7 y 10.000 dólares por hacer tres intentos para pasar la frontera. Encima, estos delincuentes lo hacen para protegerlos de los cárteles, que le secuestran, les roban, hacen trata de blancas, en definitiva, que intentan que trabajen para ellos y que al final seguramente, terminan en una fosa común.

Estuvimos en un centro de recepción y el 95% de los que llegaban eran del mismo país de donde habían salido.

Hemos visto también cifras sobre otras partes del planeta con conflictos muy grandes, siendo en resumen una completa espiral de violencia, precisamente cuando viajas a otros países, te das cuenta de que el nuestro, España, es uno de los más seguros del mundo, aparte de las libertades que están garantizadas por las Fuerzas y Cuerpos de Seguridad.

[11] La ponencia se impartió el 14 de noviembre, con una caravana centroamericana que quería entrar en Estados Unidos.

Tenemos un sistema en España que funciona mejor que la inmensa mayoría de los estados del planeta.

Decíamos anteriormente que los buscan los terroristas es incidir en la opinión pública, haciendo especial daño en aquellos países no acostumbrados a la violencia política. Por eso un atentado en Bruselas tiene mucha más repercusión que en Irak, en donde un atentado suicida, delante de la cola de un supermercado, provoca más de cien muertos y es una noticia que casi nos afecta.

Seguimos con el ejemplo. Un atentado con quince muertos en Bruselas nos hace temblar a todos, pero eso tiene que ver porque no estamos acostumbrados a que haya conflicto y violencia política, como en otros donde existen unidades de autodefensa, es decir grupos que se organizan para poder protegerse; pero existen otros grupos para comerciar de forma violenta, otros para atacar, es decir se produce una espiral que lo domina todo.

Lo que persiguen los terroristas es que todo el mundo tema por su vida, por eso ponía las estadísticas al principio, porque una cosa es lo que hacen, y otra cosa es la percepción del conjunto de la sociedad. ¡Cuánta gente después de haber visto el atentado de Cambrils o el que se produjo en Francia con los camiones circulando por un paseo lleno de personas, no han mirado con temor el pasar por una rambla, el pasar por una zona donde pudiera ver el peligro de que alguien volviera a meter otra furgoneta!

Por tanto consiguen que todo un país esté pendiente precisamente de eso, que el miedo y la confusión provoquen

una reacción desproporcionada de los gobiernos que permite a los terroristas alguna nueva oportunidad de su desesperación, *que nuestra relación sea nuestra peor enemiga*, decía el libro de la buena suerte, un librito chiquitito, la buena suerte no existe, lo que existen, son condiciones que en este momento no te favorecen, intentan alterarla y a partir de ahí, a ver si surge alguna que te pueda venir bien para aprovecharla, eso es lo que hacen los terroristas.

Cuando DAESH iba de conquista en Conquista y ampliando sus territorios imponiendo su ley, y creciendo y creciendo, estaba de una manera, cuando de repente repito tienen que esconderse, y tienen más dificultades tienen lo que tienen pues en ese momento o sea propia debilidad, que es muy distinta a la anterior, les hace también peligrosos precisamente por intentan conseguir lo que estamos mencionando en esta exposición.

Imagino que han leído, que se han informado, que han visto las productoras del terror de Al-Qaeda y DAESH. Cada atentado intenta ser una obra de arte que se escenifica y que se abre y se cuente durante mucho tiempo, por tanto, lo que pretenden realmente es que eso perdura en la opinión pública como algo que históricamente trascienda muchísimo. Vimos al principio del terrorismo de Al-Qaeda y DAESH a muchos asesinatos que fueron filtrando los medios de comunicación, que se veían en vídeos, en todos los sitios y no sé si algo no le llamaba la atención, era el ver la frialdad y la tranquilidad con la que estaba una persona cavando su propia tumba, se ponía de rodillas, se ponían con el cuchillo detrás, se ponían a recitar y después te cogían y te terminan cortando la cabeza.

Hacían esas prácticas tantas veces que ya había un momento en el que la persona pensaba que no iban a hacer nada contra él y cuando ya tenía la tranquilidad perfecta para la toma perfecta, en ese momento ya se lo cargaban.

¿Qué es lo que busca el terrorismo con ese tipo de acciones?: provocar una reacción desproporcionada de invasiones, de

guerras, de otro tipo de actuaciones que les dé pie precisamente para remover, toda la desigualdad, todos los problemas, todos los conflictos, y tener un caldo de cultivo también importante para estar en la zona como sujeto de la situación en la región.

Decía el semanario "Semana": "Nadie está a salvo" [12], esa es la percepción que queda. Es verdad que ha habido atentados en lo que han muerto gentes pero, la percepción y la idea que es lo que pretenden los terroristas es que todo el mundo tenga la conciencia de que nadie está a salvo, que todo el mundo piense que nos puede pasar algo, repito aunque cuando luego veamos otras cifras que afectan a nuestras sociedades modernas y que no le prestamos prácticamente atención.

El tema de los niños lo he puesto, primero porque todos los presentes son adultos y no se ve nada especial, porque lo que hacen es intentar hacer que se deshumanicen.

[12] https://www.semana.com/especiales/articulo/nadie-esta-salvo/47617-3 Consultado el 12.03.2019. Reportaje sobre los atentados de Nueva York en septiembre de 2001 (fecha del semanario 15.09.2001)

Forma parte de esa estrategia de terror, no el que te asesinen, sino lo que da pavor es la tortura que puede venir antes de la muerte. Tenemos que acordarnos de las películas de indios y americanos, en los cuales estos últimos, ante de ser atrapados y sabiendo que le iban a cortar la cabellera en vivo, se quitaban la vida.

Cómo actuar: compartiendo información inteligencia entre los estados que combaten; que los medios de comunicación no sirvan a esa propaganda, que ya de por si ellos están dando. yo creo que ha venido muy bien en los últimos tiempos el que se parara la espiral de estar divulgando constantemente estos contenidos, que desgraciadamente dominan enredes sociales y en las normas formas de comunicación.

Los terroristas saben que lo importante, más allá de tener una estrategia para comunicar, es tener buenos contenidos, y lo que hacen esta gente es proporcionar, divulgar buenísimos contenidos, pero tiene que haber alguien que te los divulguen. Ellos lo intentan por su cuenta, pero si encima, el adversario, también cogen buena parte del trabajo y que los gobiernos

actúen de manera proporcionada y fría con el único objetivo de derrotar al terrorismo, es un error, porque al terrorismo no se le derrota provocando una reacción furibunda desproporcionada que al final lo que hace es que crea un caldo de cultivo en la población civil en el conjunto de países, que lo que termina es, generando un semillero de odio que, posteriormente también habrá mucha más gente que esté trabajando en esa causa contra el propio país que en ese momento ha intentado defenderse.

Y ya para terminar, los riesgos actuales y teniendo en cuenta que entre los ponentes se encuentra el director del CNPIC, quisiera hacer una breve referencia a la ciberseguridad, que es uno de los temas que preocupa muchísimo a la Comisión y a mí especialmente.

Antes de darle paso, mencionar que los riesgos actuales de los terroristas son la posible adquisición de armas de destrucción masiva: nucleares y biológicas, pasando del terrorismo tradicional a otro de mucha mayor peligrosidad colectiva, de tal manera que unos pocos terroristas podrían causar daños incalculables.

Debemos también mencionar al crimen organizado, porque al fin y al cabo es una forma de terrorismo, porque genera violencia y todo lo que la genera es negativo, venga de donde venga.

Estos riesgos: terrorismo internacional, ciberataques, seguridad nacional, etc., no deben proporcionar una razón para reaccionar de forma desproporcionada contra esta violencia.

Por supuesto debemos tener muy en cuenta los objetivos ODS 2030, porque no podemos olvidar que, erradicando el hambre y la pobreza, actuando contra el calentamiento global, contra el SIDA, la malaria, la tuberculosis, etc., estaremos haciendo un mundo más justo.

Por tanto, que la lucha contra el terrorismo no nos haga olvidar estos objetivos, porque estaremos construyendo un mundo menos desigual, un mundo con más seguridad. Estos objetivos tienen que sobresalir, dentro de la respuesta contundente y resolutiva que necesitan estas amenazas para vivir en una sociedad libre y feliz.

El CNPIC en su lucha contra el terrorismo

PONENTE: D. Fernando Sánchez Gómez, Teniente Coronel de la Guardia Civil y Director del Centro Nacional de Protección de Infraestructuras Críticas y Ciberseguridad.

NOTA DE LA DIRECCIÓN DE LAS JORNADAS: La ponencia fue reproducida en video y audio y transformada mediante un programa informático a word, adaptándose el pensamiento y las palabras del ponente a un texto coherente. Puede que se hayan interpretados erróneamente algunos pensamientos, lo cual debe achacarse a la propia dirección del Foro y nunca al ponente.

Málaga es mi casa y es un lujo poder estar aquí ante todos ustedes. Los anteriores ponentes se han centrado en la visión sobre el terrorismo y creo que, dada mi condición de director del Centro Nacional de Infraestructuras Críticas y Ciberseguridad, centrarme más en el papel de estas infraestructuras críticas.

En primer lugar, debo indicar “quiénes somos:

El CENTRO NACIONAL DE PROTECCIÓN DE INFRAESTRUCTURAS Y CIBERSEGURIDAD (CNPIC) es el órgano responsable del impulso, coordinación y supervisión de todas las políticas y actividades relacionadas con la protección de las infraestructuras críticas españolas y con la ciberseguridad en el seno del Ministerio del Interior. El CNPIC depende del Secretario de Estado de Seguridad, máximo responsable del Sistema Nacional de Protección de las

Infraestructuras Críticas y de las políticas de ciberseguridad del Ministerio.

El CNPIC fue creado en el año 2007, mediante Acuerdo de Consejo de Ministros de 2 de noviembre, siendo sus competencias reguladas por la Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas y por el Real Decreto 704/2011, de 20 de mayo, por el que se aprueba el Reglamento de protección de las infraestructuras críticas.

El Centro Nacional de Protección de Infraestructuras y Ciberseguridad, tenemos una doble función, por un lado, en todo lo referente a infraestructuras críticas y por otro a la ciberseguridad, dependiendo en todo momento de la Secretaría de Estado de Seguridad del Ministerio del Interior.

Hace más de dos mil años, hubo un general en China, llamado Sum Tzu, cuyos preceptos sobre el "arte de la guerra", se encuentran vigentes y equiparaba a un ejército con un río, diciendo textualmente:

> *"Pues un ejército puede compararse con una corriente de agua, porque así como el caudal que fluye evita las alturas y corre presurosa hacia las tierras bajas, así un ejército evita la fortaleza y ataca los objetivos más débiles".*

El objetivo más débil, como nosotros, es decir la población y por ello, tal como se ha expuesto anteriormente, independientemente del número de bajas, lo que está causando otra serie de daños, el "soft target", creando inestabilidad en la esencia, en la convivencia, ciudadana.

En los países, estado y sociedades que, tienen siempre necesidades, siempre ha existido un término que ahora se llama “crítico”, y aunque sea un término moderno, ha existido a lo largo de la historia.

Para Málaga es crítico, el estadio de la Rosaleda, sede del Málaga y la vía de comunicación que se encuentra a su derecha. En la transparencia no he podido resistirme a poner el escudo del Málaga, primero, porque juega en casa y segundo porque mi tío diseñó este escudo y murió hace una semana en el hospital Carlos Haya.

También ha sido una infraestructura crítica a lo largo de la historia malacitana, el castillo de Gibralfaro y el puerto y, de hecho, hasta que Fernando el Católico no bloqueó ambas, no pudo tomar Málaga en 1487.

Con ello quiero expresar que las infraestructuras críticas siempre han existido.

Les voy a mostrar ahora, las amenazas en un mundo globalizado, en esta lámina, extraída de un estudio del Foro Económico Mundial de 2018, The Global Risk Report (apéndice 1 al presente trabajo).

Los ejes de coordenadas representan en las ordenadas (eje Y) el “impacto” y en las abscisas (eje X) la “probabilidad” y las dos líneas rojas, paralelas a los respectivos ejes, definen los riesgos a que nos enfrentamos a nivel global. Los ciberataques y los terribles ataques terroristas, están dentro del cuadrante claramente más probable. En 2017, el terrorismo estaba en el cuadrante superior derecho y ha bajado un poquito, pero no

quiere significar que ha habido menos atentados con menos bajas.

Hablamos de estos estudios por impactos directos, incluyendo los de origen humanos con el resto de riesgos de origen natural, eventos extremos como desastres naturales, migraciones, etc.

Si combinamos ciberataques y ataques terroristas contra infraestructuras, nos encontramos con el triángulo rojo de crisis: de agua, comida y migraciones.

Los objetivos han cambiado, porque a lo que nos enfrentamos es a un “impacto” tremendo, no tanto en el número de bajas, que también, sino el impacto que produce en la sociedad, dado que hemos pasado el atentado selectivo autóctono a asesinarnos en masa.

Las sociedades, principalmente las occidentales como la nuestra, tenemos un estado de vida y de salud, que nos hace fuertes, pero al mismo tiempo creamos una vulnerabilidad, porque dependemos de cosas que consideramos hoy en día vitales. Piensen un solo segundo que nos quedamos sin agua, sin electricidad y sin otras dinámicas que hemos vivido en los últimos años, cosas que hace cien o doscientos años, podíamos vivir perfectamente si ellas.

Sin embargo, hoy en día la sociedad se colapsa, es nuestro talón de Aquiles, y los “malos” lo saben y conocen donde nos pueden atacar, y la caída de estos servicios, de los que somos extremadamente dependientes, son los que se califican como operadores de servicios esenciales e infraestructuras críticas.

Además, todas esos servicios-infraestructuras, son interdependientes, porque si se nos va la energía eléctrica, se nos va el agua, no podremos sacar dinero de los cajeros automáticos, no podremos repostar combustible, no podremos circular porque los semáforos se apagarán, es decir se produce el caos.

La caída de una infraestructura crítica, puede generar un efecto dominó y al final generar un colapso, siendo esta la base sobre la que trabajamos desde el CNPIC. Las propias Naciones Unidas, en la Resolución 2341 (2017), aprobada por el Consejo de Seguridad en su reunión del 11 de febrero de 2017, reconoce la interdependencia entre varios sectores de infraestructuras críticas, precisamente porque incide en la acción de los Gobiernos [13]:

- *Reconociendo que, como consecuencia de la creciente interdependencia entre los sectores de infraestructura vital, algunas infraestructuras vitales pueden ser objeto de un número cada vez mayor y una variedad cada vez más amplia de amenazas y vulnerabilidades que plantean nuevos problemas de seguridad.*
- *Expresando preocupación por el hecho de que los atentados terroristas contra la infraestructura vital podrían perturbar considerablemente el funcionamiento del gobierno y del sector privado por igual y tener repercusiones más allá del sector de la infraestructura,*

[13] CONSEJO DE SEGURIDAD DE NN.UU. https://undocs.org/es/S/RES/2341(2017)

La sociedad moderna es extremadamente vulnerable, mucho más que algunas tribus de las selvas de Brasil o Centroáfrica y algo más que otras sociedades distintas de las occidentales.

El “efecto cascada”, de tal modo que la caída de un servicio esencial, arrastra al resto de los servicios y cuanto más tiempo estén caídos, mayor es la dificultad de reponerlos.

Las Tecnologías de la Información y las telecomunicaciones (TIC,s), actúan como hilo conductor, sin que exista hoy en día un servicio esencial o una infraestructura crítica, que quede inoperativo por estas tecnologías. Todos están monitorizados por un ordenador o sistema de información y de esta forma entramos en el ciberespacio y en los posibles ciberataques.

Entre 2005 a 2014 el tráfico de datos internacionales se multiplicó por 45, es decir que estamos totalmente conectados y nuestros servicios también.

El 12 de mayo de 2017 entre las 8 y las 17:08 horas UTC se registró un ataque a escala mundial que afectó a las empresas Telefónica, Iberdrola y Gas Natural, entre otras compañías en España, así como al Servicio de Salud Británico, como confirmó el Centro Nacional de Inteligencia. La prensa digital informaba aquel día que al menos 141 000 computadores habían sido atacados en todo el mundo.

Los expertos sostienen que WannaCry usó la vulnerabilidad EternalBlue, desarrollada por la Agencia de Seguridad Nacional estadounidense y filtrada por el grupo The Shadow Brokers, que permite atacar computadores con el sistema operativo Microsoft Windows no actualizados

debidamente. La compañía Microsoft había comenzado a distribuir actualizaciones de seguridad al día siguiente de conocerse esta vulnerabilidad, el 10 de marzo de 2017, a través de Windows Update, pero solamente para las versiones de Windows posteriores a Windows Vista. El 13 de mayo de 2017, ante la supuesta gravedad del ataque, publicó un parche separado para Windows 8, Server 2003 y XP. Muchos computadores que no tenían aplicadas las actualizaciones de seguridad MS17-010 de marzo de 2017 quedaron gravemente afectados, con sus archivos cifrados y mostrando un mensaje en pantalla que exigía un rescate de 300 dólares en bitcoins a cambio de descifrar los archivos.

En realidad, un experto de Reino Unido evitó en gran medida la expansión del ciberataque global. El autor del blog MalwareTech estaba estudiando el programa dañino cuando se dio cuenta de que el mismo intentaba conectarse a un dominio no registrado: si no lo lograba, cifraba el equipo; si lo lograba, se detenía. Una vez que este experto en seguridad registró el dominio, a las 17:08 UTC del 12 de mayo, cesó el ataque. Todas las medidas urgentes que se tomaron a partir de esa hora fueron prácticamente innecesarias. [14]

Fue un toque de atención para muchos gobiernos, impulsándoles a seguir trabajando, ya que le habían visto las orejas al lobo. El documental American Blackout, recrea un

[14] https://es.wikipedia.org/wiki/WannaCry

ataque cibernético contra la red eléctrica estadounidense que, en diez días, presenta una enorme crisis para la sociedad norteamericana.

Es interesante esta cita de Napolitano de hace ya unos años y básicamente viene a decir que un ciberataque puede causar un efecto parecido al del huracán Sandy. Es decir, no estamos hablando de ciencia ficción no estamos hablando de un juego efectivamente estamos hablando de la hipótesis más peligrosa y como los militares saben la hipótesis más probable se utiliza para la maniobra. Pero la hipótesis más peligrosa se utiliza para la seguridad y la labor que tenemos en el Centro Nacional de Infraestructura de ciberseguridad. Es precisamente esa intentar anticipar la situación a situaciones que posiblemente ahora mismo se ven como catastróficas.

El reto primero al que nos enfrentamos es identificar cuáles son las infraestructuras críticas y esa labor no es de un día, sino que es un estudio y análisis de muchos años. Nuestra función

es identificar qué servicio es crítico y cuáles son la interdependencia de que el mismo o la misma no funcione.

Prevenir, es decir gestionar los riegos y proporcionar a los órganos competentes del Ministerio del Interior y del Departamento de Seguridad Nacional, con la información e inteligencia disponibles a que puedan tomar las decisiones necesarios, es decir a intervenir y superar la situación.

La información no es solamente la obtenida por nosotros mismo, sino la que intercambiamos con otros órganos nacionales e internacionales, similares al nuestro. Este intercambio de información es absolutamente necesario porque los “malos” lo están haciendo continuamente. No podemos “tener el lujo” de retener información.

Tras la información y su intercambio, el segundo pilar es la construcción de un sistema de infraestructuras críticas, donde están, varios departamentos del Gobiernos, por supuesto las Fuerzas y Cuerpos de Seguridad, las comunidades autónomas y un sujeto muy importante: el operador crítico, que es la organización pública o privada que gestiona los servicios esenciales de agua, electricidad, gas, petróleo, telefonía, etc. Todos los anteriores son los que tienen que coadyuvar a defender estas infraestructuras-servicios esenciales, porque un objetivo prioritario de la Seguridad Nacional.

El CNPIC responde a una serie de iniciativas internacionales, centradas en infraestructuras críticas. Hemos ido modernizándonos y hemos asumido la “ciberseguridad”, sin que por ello hayamos cambiado el acrónimo ni el logo.

A la ciberseguridad le hemos dado gran peso y básicamente somos un órgano coordinador contra cualquier tipo de ciberataques de cualquier naturaleza.

Coordinamos distintos ministerios, las Fuerzas y Cuerpos de Seguridad y otros organismos, cada uno de los cuales ejerce su propia labor en el sector de la ciberseguridad. Nuestra función es intercambiar información y ayudar a identificar riesgos y amenazas y después tener un mecanismo de comunicación de alerta, ágil y computarizado, denominado AlertPic [15], basado en otra plataforma denominada AlertCops

[15] Ministerio del Interior dispone de una herramienta llamada AlertPIC, una aplicación con la que se intercambia información y ficheros de datos en tiempo real ante situaciones de crisis de carácter cibernético. Esta aplicación sirve como instrumento de comunicación para los incidentes que se producen entre los operadores de infraestructuras críticas y el Centro Criptológico

[16], de tal forma podamos prestar apoyo a operadores de la más variada procedencia y que manejen datos sensibles.

Acaba de ser aprobado el Real Decreto-ley 12/2018 de seguridad de las redes y sistemas de información, cuya sinopsis del Departamento de Seguridad Nacional, se recoge en el Apéndice 2. Con el sistema PIC operaciones apoyamos a aquellos que realmente tienen la competencia sobre el terreno y capacidades de ciberseguridad. Esta es la parte normativa decir que nos basamos lógicamente en la Estrategia de Seguridad Nacional en la Ley de infraestructuras críticas y en este sistema que acaba de salir que es trasladar todo lo anterior al campo del ciberespacio, fijando una serie de objetivos estratégicos con un final fundamental, que es disponer de un sistema coordinado que abarcar desde el Gobierno y las empresas porque estamos hablando de un 70 75 por ciento de infraestructuras críticas que son gestionadas por empresas privadas.

El CNPIC desarrolla de forma simultánea varias líneas de acción, la primera es proponer el desarrollo normativo, tanto legal como procedimental, al objeto que todos tengamos una base suficiente para actuar. La segunda es referente a la

Nacional asegurando que dicha comunicación sea fiable y segura. AlertPIC está basada, a su vez, en otra plataforma llamada Alertcops.

[16] AlertCops es el servicio de alertas de seguridad ciudadana que las Fuerzas y Cuerpos de Seguridad del Estado (FFCCSE) ponen a tu disposición para atenderte en situaciones de riesgo.

AlertCops es un canal complementario a los habituales con el que, entre otras funciones, podrás enviar alertas con imágenes o vídeos al centro policial más cercano, comunicarte por chat directamente y recibir avisos de seguridad enviados por los servicios de seguridad públicos, para que puedas recibir una atención más rápida y eficaz.

Además, si lo deseas, podrás compartir tu posición con los tuyos o con los centros públicos de rescate que presten el servicio.

implantación del sistema, tema que nunca poder entenderse como terminado, por la instauración de nuevos operadores y nuevas tecnologías.

La tercera son las operaciones propiamente dichas, es decir la implicación en lo que ocurre a diario en la protección de las infraestructuras críticas y ciberseguridad, uniéndose ésta a la cuarta, aumentando constantemente nuestras capacidades en ciberseguridad, única forma de disponer de un futuro más seguro, y por último y no menos importante son las relaciones institucionales, como la que hoy estamos desarrollando en estas Jornadas de Seguridad, Defensa y Cooperación, organizadas por el Foro para la Paz en el Mediterráneo.

Anteriormente se ha expuesto que el sistema PIC es coordinar las acciones del Gobierno y las empresas para una mejor

protección de las infraestructuras críticas y el mantenimiento de los servicios esenciales españoles, para ello, los operadores críticos, públicos y privados, deben de concienciarse en la necesidad de optimizar la seguridad de sus infraestructuras críticas y sus redes.

De hecho, el Real Decreto Ley 12/2008, especifica en su artículo 16:

> *Artículo 16. Obligaciones de seguridad de los operadores de servicios esenciales y de los proveedores de servicios digitales.*
>
> 1. *Los operadores de servicios esenciales y los proveedores de servicios digitales deberán adoptar medidas técnicas y de organización, adecuadas y proporcionadas, para gestionar los riesgos que se planteen para la seguridad de las redes y sistemas de información utilizados en la prestación de los servicios sujetos a este real decreto-ley.*
>
>> *Sin perjuicio de su deber de notificar incidentes conforme al título V, deberán tomar medidas adecuadas para prevenir y reducir al mínimo el impacto de los incidentes que les afecten.*

Con llevando sanciones en caso de no disponer de las medidas necesarias de seguridad.

Las Fuerzas y Cuerpos de Seguridad del Estado, deben disponer de una información actualizada y fiable, al objeto de poder prevenir, intervenir e investigar. Las Fuerzas Armadas (FAS) también se encuentran implicados por la Ley de Seguridad Nacional y por su propia normativa en la protección de los servicios esenciales.

Como último objetivo estratégico, el Sistema PIC debe adaptarse a los continuos cambios tecnológicos, intentando en todo momento ir por delante del "malo" y por supuesto evolucionar hacia nuevos modelos de seguridad, cada vez más eficientes y eficaces.

La pirámide de planes, en la cúspide de la misma disponemos del Plan Nacional de Protección de Infraestructuras Críticas, dividiéndose en los correspondientes planes sectoriales, en

consonancia con los sectores que se han declarado críticos por la Unión Europea y por España.

Como tercero y cuarto estadio se encuentran los planes responsabilidad del operador del servicio esencial o infraestructura críticas, denominados Plan de Seguridad del Operador, considerándolo en su conjunto y los Planes de Protección Específica, incidiendo en las instalaciones consideradas críticas, dentro del despliegue en el terreno del operador.

Como base de la pirámide tenemos los Planes de Apoyo Operativo, los cuales son los previstos por las Fuerzas y Cuerpos de Seguridad del Estado, para apoyar al operador.

Como ven es un sistema complejo, pero creo que podemos afirmar que estamos llegando a un buen ajuste en los tres niveles de Gobierno, Operador y FCSE, de tal manera que gozamos de un determinado prestigio, tanto en Europa como en América y en buena medida es debido a la elaboración que hemos hecho del Catálogo de Infraestructuras Críticas, al cual tienen acceso las Fuerzas y Cuerpos de Seguridad del Estado y los propios operadores.

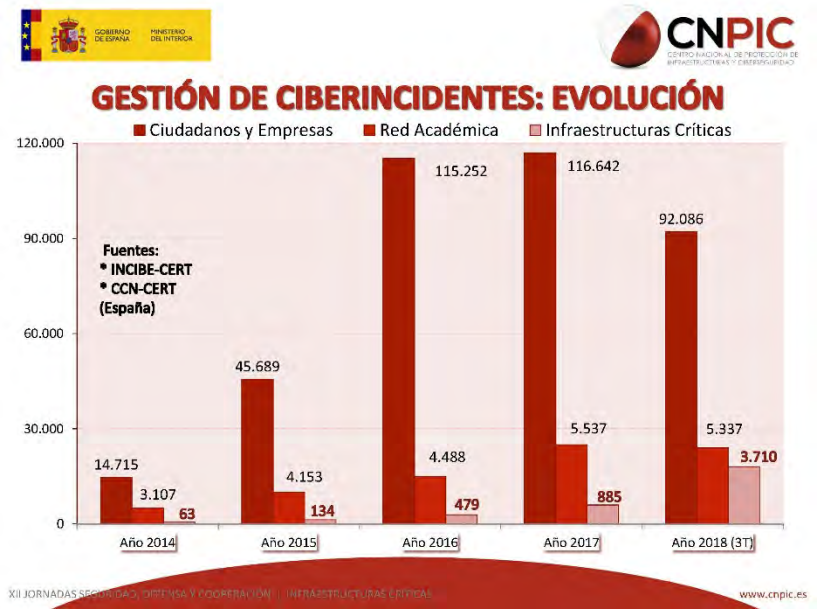
Hemos tratado anteriormente del Plan Nacional, en la cúspide de la pirámide, estando este plan hilvanado con el Plan Antiterrorista, como no podía ser de otra manera

Como ven en la imagen, nos encontramos en el nivel 4 de alerta, y como el Plan Antiterrorista establece cinco niveles, dependiendo del nivel en el que estemos, se van variando los

requerimientos que se hacen a nuestras unidades como el propio operador.

El Plan Antiterrorista está dirigido fundamentalmente a la policía, a la guardia civil y a otras fuerzas del Estado´. El Plan Nacional de Protección de Infraestructuras Críticas (PNIC) está dirigido, también, a otros colectivos, como son los operadores críticos y de servicios esenciales, con lo cual podemos afirmar que todos estamos trabajando conjuntamente por la Seguridad Nacional.

Como segundo sombre que nos toca ponernos es el de la ciberseguridad, y de la misma forma que en los expuestos para las infraestructuras críticas, trabajamos con los operadores y con las fuerzas de seguridad. Por eso estamos en el Ministerio del Interior y todos los que formamos el CNPIC procedemos del Cuerpos Nacional de Policía y de la Guardia Civil.



Miren en el gráfico cómo han evolucionado los ciberataques contra ciudadanos y empresas, pasando en 2014 de 14.000 a la actualidad que han llegado a 92.000, teniendo en cuenta que son los datos del tercer trimestre de 2018, probablemente sobrepasen los 116.000.

La segunda columna, es lo que nosotros llamamos "red académica"[17] en donde se colabora con muchas universidades

[17] El Instituto Nacional de Ciberseguridad de España (INCIBE), sociedad dependiente del Ministerio de Industria, Energía y Turismo (MINETUR) a través de la Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información (SETSI), es la entidad de referencia para el desarrollo de la ciberseguridad y de la confianza digital de los ciudadanos, **la red académica y de investigación española (RedIRIS)** y las empresas, especialmente para sectores estratégicos

en tareas de investigación. Empezamos con 63 y a día de hoy estamos en 1.710.

Dirán ustedes que se producen pocas incidencias, pero desde luego en las recogidas estadísticamente son las más graves y las que pueden hacer mella en un ámbito mayor. También hay que decir que los operadores, que antes eran reacios a informar sobre incidencias, ahora lo hacen de forma más fluida, debido fundamentalmente a los beneficios que le reporta.

Los “malos” intentarán siempre ir por delante de los “buenos” y por ello en la Estrategia Contraterrorista de 2005, se establecen cuatro pilares:

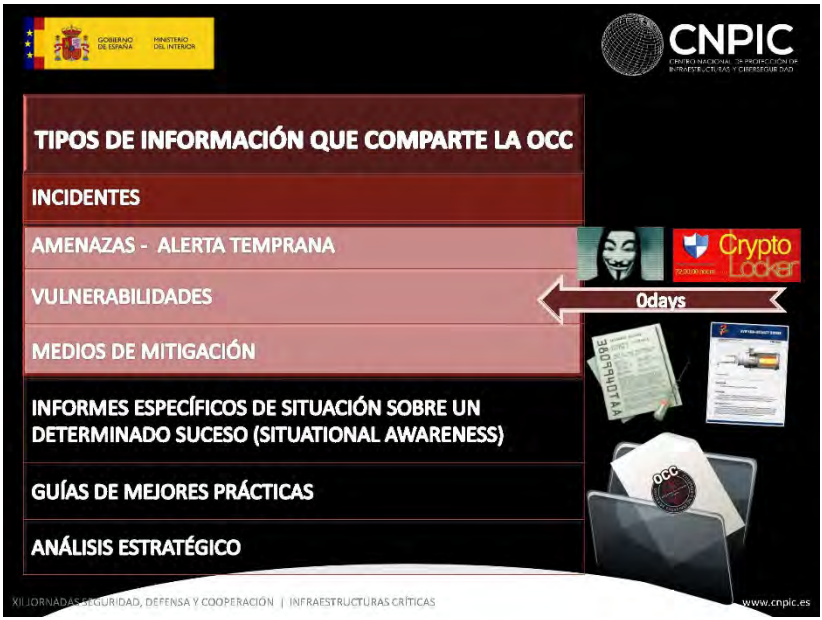
1. Prevención.
2. Protección.
3. Respuesta.
4. Persecución.

Estos cuatro pilares se trasladan de alguna manera al mundo cibernético y la prevención y la respuesta se ven bastante bien reflejados con los Centros de Respuesta de Incidencias (CERT) y con los Equipos de Repuesta (CERTS).

Lo anterior confluyen en dos altos organismos, uno el Centro Nacional de Inteligencia y el Centro Criptológico Nacional, el

INCIBE y otro el Mando de Ciberdefensa. Existe otros centros privados, conectados con los anteriores.

El último escalón la “persecución”, solo puede ser llevado a cabo por las Unidades Tecnológicas de la Guardia Civil y de la Policía Nacional, es decir, el único ministerio que está presente en los cuatro pilares de la ciberseguridad es el del Interior



Nos constituimos en correa de transmisión del ciclo de vida de la ciberseguridad, abarcando los cuatro pilares de prevención, protección, respuesta y persecución. ¿Cómo los hacemos?, pues coordinando y contactando con el mundo de los del CERTS, es decir con la “tecnología” y transmitiendo información e inteligencia a nuestras unidades, para que puedan perseguir delitos en todas sus variantes, y lógicamente transmitiendo también, información e inteligencia a nuestros operadores críticos, para que se prevengan sobre un ciberataque, aunque tenemos todavía ciertos problemas, porque falta algo de concienciación, porque existe una cierta

tendencia, cada vez menor, de que cuando una empresa o un banco sufre un ataque, se lo guarda, intenta solucionarlo como puede y no lo comunica. Esta postura es un error mayúsculo, porque ellos no pueden perseguir.

Si no se denuncia, si no se comunica al CERT, no se puede investigar y no se puede alertar a la empresa cercana, porque no lo olvidemos, no somos compartimentos estancos y si cae un servicio es más que probable que caigan otros, pero existe un miedo “a la reputación que puede quebrarse con repercusiones en el mercado”.

Dentro de la estructura orgánica del CNPIC se encuentra la OCC (Oficina de Coordinación Cibernética), y para eso se creó, para desempeñar la coordinación técnica y la comunicación con los CSIRT nacionales de referencia: CERTSI y CCN-CERT. Estos se ocupan de la resolución técnica de incidentes de ciberseguridad que puedan afectar a operadores privados de infraestructuras críticas (CERTSI) y operadores públicos (CCN-CERT).

Qué más cosas hace la Oficina de Coordinación Cibernética: Compartimos ciber incidentes, amenazas de alerta temprana, vulnerabilidades, medidas, etc., tenemos un equipo bastante potente de expertos en esta materia que saben de ciberseguridad y después se intercambian informes específicos, guías o análisis estratégico entre ellos, para rastrear las redes sociales, por ejemplo. Y entramos también a parte del terrorismo qué es lo que pasa con qué es lo que sucede cuando nos enteramos de eventos de este tipo que

contaba en la red directamente se lo pasamos a CITCO [18] o a La Policía Nacional o Guardia Civil dependiendo de en qué campo se encuentra cada situación para que ellos investiguen.

Básicamente nuestra función no es explotar esa información, pero sí que esa información le llegue a todos aquellos que la necesitan. Esa la función fundamental del CNPIC.

No somos operativos, nos quedamos en el escalón anterior, pero tenemos acceso a mucha información esa información.

En 2020 se implantará un sistema automático de integración normativa, dotándolo de capacidades de ciberseguridad y de gestión operativa. Cuando tengamos el sistema finalmente implantado, estaremos controlando más 250 operadores crítico, más de 700 infraestructuras críticas, más de 4.000 instalaciones estratégicas, más de mil planes. Toto lo anterior es lo que gestionaremos en el 2020, todo ello bajo la autoridad superior de la Secretaria de Estado de Seguridad, integrando la ciberseguridad, la seguridad física y la seguridad personal.

Eso es algo que también creo que vamos poco a poco calando sobre todo en nuestros operadores para que vean que no podemos separar seguridad física y ciberseguridad. La

[18] El CITCO es el órgano de recepción, integración y análisis de toda la información estratégica disponible referida al terrorismo, la criminalidad organizada y los radicalismos violentos, elaborando inteligencia estratégica y prospectiva, ofreciendo una valoración de estas amenazas permanentemente actualizada, proponiendo y coordinando estrategias nacionales para combatirlas, y estableciendo los criterios de actuación y coordinación operativa entre los distintos organismos en los casos de coincidencia o duplicidad entre investigaciones que se desarrollan contra estos fenómenos.

seguridad sólo es una, pero tiene apellidos o prefijos de la seguridad.

No es fácil todos los procesos que les he contado, pero tenemos que ser conscientes a lo que nos enfrentamos.

Apéndice 1

El informe *Global Risks Report* [19] es un documento publicado anualmente desde 2006 por el Foro Económico Mundial. Describe los cambios en el paisaje de riesgos globales y la interrelación entre los mismos. Los riesgos se analizan en base a su grado de impacto y probabilidad en un periodo de diez años y se clasifican en cinco categorías: económica, medioambiental, geopolítica, social y tecnológica. La identificación de los riesgos está basada en una encuesta a miembros del Global Risk Network, una red de alrededor de 1000 expertos.

La edición de 2018 señala como riesgos más probables: los fenómenos meteorológicos extremos, los desastres naturales, los ciberataques, el robo o fraude de datos y el fracaso en la mitigación y adaptación de los efectos del cambio climático.

En función del grado de impacto, los cinco riesgos identificados son: las armas de destrucción masiva, los fenómenos meteorológicos extremos, los desastres naturales, el fracaso en la mitigación y adaptación de los efectos del cambio climático y las crisis relacionadas con el agua.

El *Global Risks Report 2018* se estructura en seis partes: el paisaje de los riesgos globales, los desafíos económicos, choques futuros, cambios en el poder geopolítico, análisis retrospectivo y revaluación del riesgo.

---

[19] DEPARTAMENTO SEGURIDAD NACIONAL. El informe *Global Risk Report 2018* está disponible para su descarga en nuestra sección de "Documentos relacionados con la Seguridad Nacional".
https://www.dsn.gob.es/es/actualidad/sala-prensa/claves-del-%E2%80%9Cglobal-risks-report-2018%E2%80%9D

El paisaje de los riesgos globales

En el informe *Global Risks Report 2018* se señala que los desafíos identificados en 2017 se han intensificado y que la perspectiva de futuro según los expertos encuestados es generalmente pesimista. El informe resalta cuatro áreas de riesgos globales, para las que se precisa una acción urgente:

- ***Desigualdad e injusticia***: si bien los riesgos económicos son menos prominentes en el paisaje de riesgos de este año, la desigualdad persiste. Aunque a nivel global ha disminuido, a nivel interno de cada país parece acentuarse, y es un problema cada vez más corrosivo.

- Así, la creciente disparidad de ingresos y riqueza ha sido identificada como el tercer riesgo global más importante. Se identifica además la automatización y digitalización como un elemento disruptivo del mercado

laboral y que puede contribuir a una mayor desigualdad. Se señala que estos no son solo riesgos económicos, sino que sustentan sentimientos de injusticia social.

- ***Tensión política a nivel nacional e internacional***: El incremento de los riegos geopolíticos ha sido una de las tendencias más notables de 2017, particularmente en Asia y en focos de tensión como Oriente Medio. Los riegos geopolíticos se han visto exacerbados por la disminución del compromiso con un orden internacional multilateral basado en normas. Se identifican además la política de identidades y la personalización del poder (incluyendo en Arabia Saudí, China, Turquía o Rusia) como posibles catalizador de riesgos

- ***Riesgos medioambientales***: Los cinco riesgos en esta categoría se perciben con una probabilidad e impacto por encima de la media. Entre los más urgentes se encuentran los fenómenos meteorológicos y las temperaturas extremas, la aceleración en la pérdida de biodiversidad, la polución de la tierra, agua y aire, el fracaso en la mitigación y la adaptación de los efectos del cambio climático y los riesgos derivados de la transición hacia un futuro bajo en energía del carbón.

- ***Vulnerabilidad cibernética***: Los riesgos cibernéticos se han visto acentuados en 2017. Este año aparecen por primera vez los ciberataques y el fraude de datos entre los cinco riesgos más probables. Los ataques están incrementando tanto en número como en potencial disruptivo. Otra tendencia en aumento son los ataques sobre infraestructuras críticas y sectores

industriales estratégicos, con el consiguiente peligro de un ‘shock’ sistémico radical e irreversible.

- Este apartado concluye señalando nuestra vulnerabilidad a los riesgos sistémicos. Los riesgos hoy en día no son factores aislados que podamos gestionar con facilidad. Las sociedades, ecosistemas, economías y el sistema financiero global son sistemas complejos e interconectados, y cuando un riesgo se manifiesta en un sistema complejo puede desencadenar un colapso sistémico o una transición abrupta a un estatus peor.

Desafíos económicos

La segunda parte del informe *Global Risks Report 2018* se centra en las vulnerabilidades y desafíos económicos tradicionales y emergentes.

Si bien los indicadores económicos presentan un panorama global de recuperación de la crisis global que se desencadenó hace 10 años, persisten riesgos subyacentes. Entre los riesgos tradicionales están los precios insostenibles de activos, altos niveles de endeudamiento, en particular en China, y la presión continuidad sobre el sistema global financiero. Entre los desafíos más nuevos están las disrupciones causadas por la automatización y digitalización, y las crecientes presiones mercantilistas y proteccionistas.

Choques futuros

Está sección señala que los riesgos se pueden materializar de manera sorprendentemente rápida. Esto, unido a la

complejidad e interconectividad del mundo actual hace que se incremente la probabilidad de inesperadas y dramáticas crisis.

Con el fin de alentar a la reflexión sobre potenciales elementos desestabilizadores o disruptivos y cómo afrontarlos, se presentan 10 posibles choques futuros. Los choques señalados son: la insuficiencia del suministro de alimentos global, los efectos adversos de la Inteligencia Artificial sobre la eficiencia de internet, las guerras comerciales, las olas populistas que amenazan el orden social, la extinción de las reservas de peces de manera a manos de drones automatizados, una cascada de crisis económicas o financieras, el incremento de la desigualdad como resultado de la bioingeniería y de drogas que potencian las habilidades cognitivas, los ciberataques entre estados que se intensifican por la falta de protocolos, la geopolítica de la identidad y la fragmentación de internet por temas regulatorios, de ciberseguridad o proteccionistas.

Cambios en el poder geopolítico

Este apartado señala que el mundo se encuentra en una nueva y desestabilizadora fase geopolítica. No es solo multipolar, sino también multiconceptual. Esto está dando lugar a nuevos riesgos e incertidumbres: tensiones militares crecientes, disrupciones económicas y comerciales y disruptivos bucles que se retroalimentan. Cuatro tendencias que pueden causar disrupciones en el corto y medio plazo son: la intensificación de políticas de estado fuertes, la erosión de las normas globales y el aumento de la tensión, agendas geoeconómicas cada vez más agresivas y la creciente presión sobre los estados más pequeños.

Análisis retrospectivo

En esta nueva sección se resaltan tres riesgos que se habían señalado en ediciones pasadas del informe: la resistencia antimicrobiana, el desempleo juvenil y el fenómeno de la desinformación digital. El objetivo es analizar el progreso que se ha hecho desde su identificación. Se trata de analizar la evolución de estos riesgos y de las respuestas globales a los mismos.

Revaluación del riesgo

En este apartado algunos expertos aportan su percepción sobre el desarrollo de nuestro entendimiento de riesgos. En esta edición, Roland Kupers (consultor internacional independiente de alto prestigio en materia de complejidad, resiliencia, y transición energética) sobre la resiliencia en sistemas complejos y Michele Wucker (analista política y autora de publicaciones relacionadas con estrategia, economía mundial y gestión de crisis) hacen un llamamiento a que las organizaciones presten más atención en sus procesos de gestión de riesgos a los sesgos cognitivos.

Apéndice 2 [20]

Las redes y sistemas de información desempeñan un papel crucial en la sociedad. Su fiabilidad y seguridad son esenciales para las actividades económicas y sociales, y en particular para el funcionamiento del mercado interior de la Unión Europea y de nuestro país, siendo fundamental reforzar la seguridad de estas redes y sistemas.

Así se recoge en la Directiva de la UE 2016/1148 (conocida como Directiva NIS) relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión.

El Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información publicado en el Boletín Oficial del Estado, el pasado 8 de septiembre, que transpone al ordenamiento jurídico español la mencionada Directiva, tiene por objeto regular la seguridad de las redes y sistemas de información utilizados para la provisión de los servicios esenciales y de los servicios digitales, y establecer un sistema de notificación de incidentes en nuestro país.

Su contenido trasciende a la propia Directiva y aborda determinados aspectos que permitirán reforzar la ciberseguridad a nivel nacional, extendiendo su aplicación a ámbitos que se consideran fundamental para ofrecer un enfoque global y cohesionado, adaptado a las particularidades de nuestro país.

[20] https://www.dsn.gob.es/es/actualidad/sala-prensa/aprobado-real-decreto-ley-122018-seguridad-redes-sistemas-informaci%C3%B3n

El Real Decreto-ley aprobado determina la forma y criterios de identificación de los servicios esenciales y de los operadores que los presten, así como a los que se aplicará. Además recoge el marco estratégico e institucional de la seguridad de las redes y sistemas de información en España haciendo énfasis en la cooperación entre autoridades públicas. También se disponen las potestades de inspección y control de las autoridades competentes y la cooperación con las autoridades nacionales de otros Estados miembros, se tipifican una serie de infracciones y sanciones, y se establecen las obligaciones de seguridad de los operadores. Finalmente se regula la notificación de incidentes, con especial atención a los incidentes con impacto transfronterizo y a la información y coordinación con otros Estados de la Unión Europea para su gestión.

Cabe destacar, en este sentido, la creación de la Estrategia de Ciberseguridad Nacional para desarrollar el marco estratégico e institucional de la ciberseguridad recogido en el Real Decreto-ley, compuesto por los CSIRT de Referencia. Éstos son equipos de respuesta a incidentes que analizan los riesgos y que como puerta de entrada supervisan incidentes, difunden alertas y aportan soluciones para mitigar sus efectos. Las Autoridades Competentes supervisan el cumplimiento y reciben notificaciones de incidentes a través de los CSIRT.

Punto de contacto único

Según el Real Decreto-ley, el Consejo de Seguridad Nacional ejercerá, a través del Departamento de Seguridad Nacional, una función de enlace para garantizar la cooperación transfronteriza de las autoridades competentes designadas,

con las autoridades competentes de otros Estados miembros de la Unión Europea, así como con el grupo de cooperación y la red de CSIRT.

En particular, cuando las autoridades competentes o los CSIRT de referencia tengan noticia de incidentes que pueden afectar a otros Estados miembros de la Unión Europea, informarán a través del punto de contacto único a los Estados miembros afectados.

Además, el punto de contacto único se encargará de remitir a la Comisión Europea un informe anual resumido sobre las notificaciones recibidas de las Autoridades Competentes.

El Real Decreto-ley supone un importante avance para la ciberseguridad en nuestro país y establece una serie de mecanismos que, con una perspectiva integral, permitan mejorar la protección frente a las amenazas que afectan a las redes y sistemas de información, facilitando la coordinación de las actuaciones realizadas en esta materia tanto a nivel nacional como con los países de nuestro entorno, en particular, dentro de la Unión Europea.

Más información:

- Directiva de la UE 2016/1148 (Directiva NIS)
- Real Decreto-ley 12/2018, de 7 de septiembre
- Estrategia de Ciberseguridad Nacional

GEOECONOMIA, GEOPOLITICA Y TERRORISMO EN EL SAHEL

AUTORA: María del Pilar Rangel Rojas, Profesora de Derecho Internacional Público y Relaciones Internacionales de la Universidad de Málaga

MODERADORA: Dra. Magdalena Martín Martínez, catedrática de Derecho Internacional Pública de la Universidad de Málaga

A forma de introducción, María del Pilar Rangel es Profesora de Derecho Internacional Público de la Universidad de Málaga desde hace 24 años, tiene una dilatadísima experiencia docente e igualmente es una gran experta en lo que se refiere a la organización de Jornadas y Seminarios con una marcada especialización en el ámbito del Terrorismo y en particular en la cuestión que va a abordar esta tarde que es la del Sahel donde tiene también experiencias personales muy interesantes y además de eso, es amiga, así que ella va a ser en primer lugar la que nos va a ilustrar sobre la visión que va a plantear y cuyo

El Título es Geoeconomía, Geopolítica y Terrorismo en el Sahel, tema que de mayor actualidad yo creo que es imposible. Te doy la palabra Pilar.

INTRODUCCIÓN

En primer lugar, dar las gracias a la Universidad Internacional de Andalucía en su sede de Málaga, al Foro para la Paz en el Mediterráneo, especialmente al Coronel Rafael Vidal Delgado y también y especialmente a la Doctora Magdalena Martín quiero darle las gracias porque muchos de ustedes no lo saben, pero ella es mi jefa y además amiga. No voy a entretenerme más porque tenemos el tiempo limitado, decirles que la ponencia mía va a tratar sobre Geoeconomía, Geopolítica y Terrorismo en el Sahel.

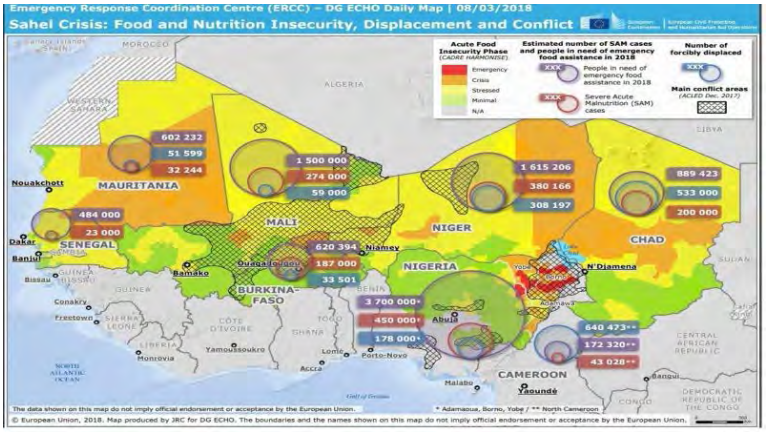
Hemos visto las dos primeras ponencias, la del Diputado Hernando que ha hablado desde su experiencia en la Comisión de Interior, también hemos visto la ponencia de Julio Andrade, director de CIFAL MALAGA que ha hablado de la lucha contra el terrorismo y la radicalización violenta desde el ámbito local y del ámbito internacional cómo se lleva a cabo la prevención en materia de radicalización violenta y ahora vamos a ver una ponencia totalmente distinta porque nos vamos a situar donde se centra actualmente el nuevo foco lucha contra el terrorismo y que es el Sahel.

¿QUÉ ES EL SAHEL?

Muchos de ustedes se preguntarán en este momento ¿qué es el Sahel? El Sahel es la zona o la región que se encuentra situada entre lo que es el Desierto del Sahara y la sabana africana. Está compuesto desde el punto de vista geográfico por distintos países como son Mauritania, Senegal, Mali, Níger, Nigeria, Burkina Faso, Chad, Sudan y Etiopia.

Estos países tienen una característica fundamental y es que son países que se encuentran dentro del ranking de los países más pobres del mundo, sin embargo, son muy ricos tanto en minerales como en recursos energéticos. Pero, ¿qué problemas existen aquí para que España esté muy preocupada con lo que ocurre en el Sahel? Si vemos la Estrategia de Seguridad Nacional una de las amenazas que existen es lo que está ocurriendo ahora mismo en el Sahel

En el Sahel al darse unos niveles de pobreza muy grande, existe una grave crisis de nutrición y de alimentación como vemos en esta Infografía.



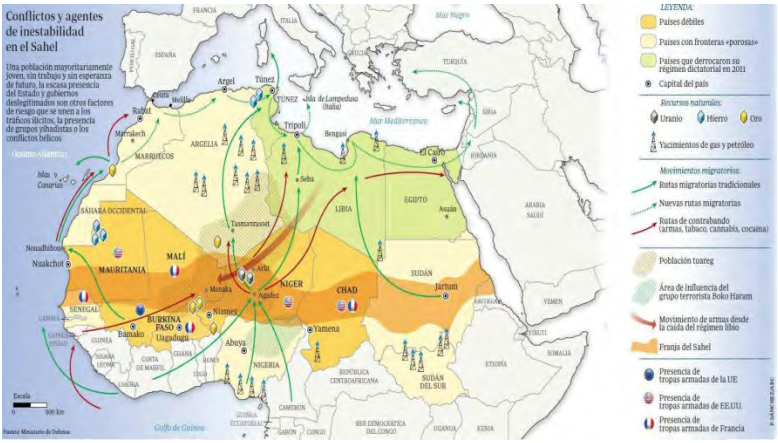
Esta crisis de alimentación va a hacer que confluyan otros factores como son especialmente el tema de los tráficos ilícitos, como el crimen organizado que se centra principalmente en lo que es el tráfico de armas, el tráfico de drogas, el tráfico de tabaco y el tráfico humano entre otros.

Estos países también forman las principales rutas de la inmigración que luego van a llegar a Europa a través de Libia y de Marruecos principalmente y luego otro de los problemas que tenemos es que al ser una zona tan pobre con estos grandes problemas es caldo de cultivo para lo que es el terrorismo yihadista

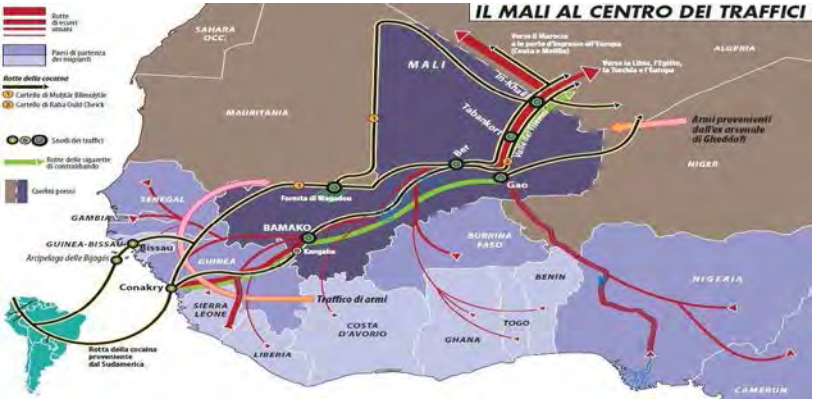
Además nos encontramos con países que tienen una característica geográfica especial y es que son países con una fronteras muy porosas, especialmente la frontera de Libia y de Mali y además que están formados en su mayoría por Estados fallidos donde sus gobernantes normalmente no pueden controlar la mayor parte del territorio o donde si existe muchísimo territorio por ejemplo el caso de Mali, todo lo que es la zona norte es desierto que está habitado por los tuaregs que lo que buscan la independencia de su territorio Azawad del gobierno de Bamako. Debemos de recordar que después de la caída de Gadafi todo lo que era el armamento libio llegó a Mali

Si unimos todos estos problemas a que nos encontramos una población mayoritariamente joven que no tiene trabajo, que no tiene esperanza de futuro, nos encontramos con la escasa presencia del Estado, de gobiernos deslegitimados, son factores de riesgo que se unen a todos estos tráficos ilícitos y que hace que la presencia de este grupo yihadistas o del crimen organizado se extienda por todo el territorio del Sahel

En cuanto a las rutas usadas en el Sahel nos vamos a encontrar distintas rutas que además van cambiando conforme son detectadas, desde las rutas migratorias, las rutas de contrabando, de armas, de tabaco, de cannabis, de cocaína. Así podemos observar por dónde llegan todos los tráficos ilícitos y se introducen en África.



Así podemos ver como el centro de todos los tráficos ilícitos y de crimen organizado se centran en Mali, la ruta de la cocaína proveniente de Sudamérica entra a través de Guinea y siguen hacia Bamako y aquí hay una ruta que llega a Europa a través de Libia y la otra llega a través de Marruecos.



Todos estos tráficos ilícitos llegan a Europa, nos encontramos como decía antes en una de las zonas más pobres de África. Mi experiencia en el terreno en países como Mali, Burkina y Gambia es que el sueldo medio de una persona son 50 €, el que tiene sueldo. Quiere decir que todo esto hace que estas personas que no tienen trabajo, son propicias para ser captados y puedan vivir a costa de estos tráficos ilícitos. El caso del Sahel existen personas que se han unido a los principales grupos terroristas simplemente por un plato de comida, estaríamos hablando más bien de mercenarios que de radicalizados.

Hay que recordar que en África la subsistencia es fundamental. Por ello, la primera organización que aparece y ofrece algo a estas personas, bien sea un tráfico ilícito o sea una organización terrorista se va con ellos por tal de poder sobrevivir. Estando allí en el Sahel les preguntábamos qué ¿porque venían a España si podía morir por el camino?, que el camino era difícil que muchos morían. Ellos me contestaban que si se quedaban allí sabían que morirían, pero si viajaban sabían que al menos tendrían alguna oportunidad.

Ante esta problemática, ¿cuál es la respuesta española tanto desde el punto de vista económico como desde el punto de vista del ámbito de la seguridad? Debemos decir que la presencia española en el Sahel principalmente está Mauritania, Mali, en Burkina Faso, en Níger y en Chad, donde existen distintos tipos de ayuda en lo que España contribuye y también lo hace a través de la Unión Europea como vemos en la siguiente Infografia, donde la ayuda como se puede ver es bastante pero no suficiente

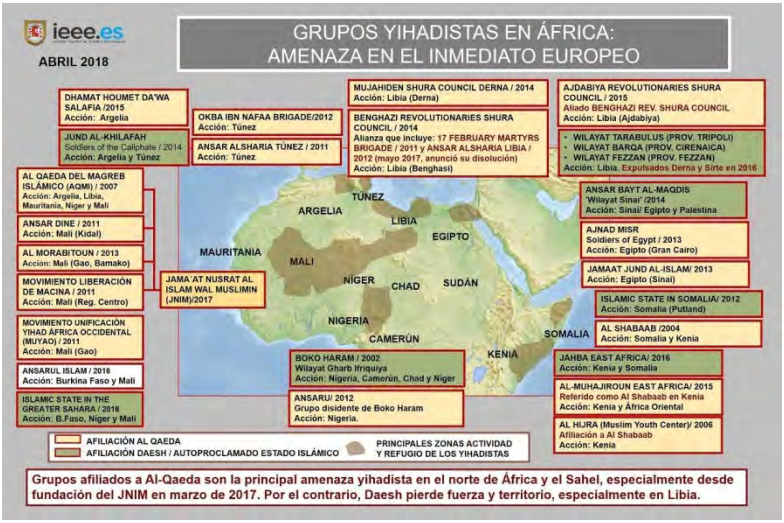
Y la respuesta española en materia de seguridad que luego veremos más específicamente son la EUCAP SAHEL MALI en 2012, la EUTM MALI en 2013 y la EUCAP NIGER en 2015.

Cuando hablamos de que el Sahel es nuestra frontera avanzada como nos recuerda el General Ballesteros nos preocupa especialmente la presencia terrorista y más concretamente lo que ocurrió en marzo de 2017 y que fue la fusión de 5 grupos terroristas que es lo que se llama el grupo

de apoyo al Islam y los musulmanes y que se puede ver en la siguiente infografía:

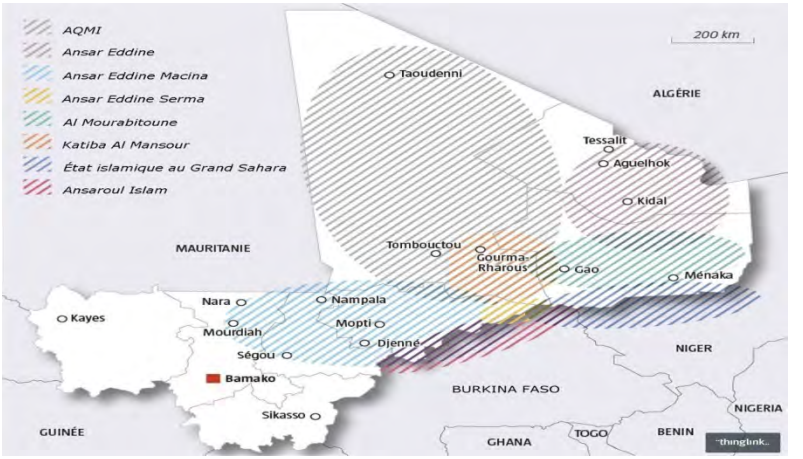
¿Quien es quien? De dcha a izda, Abderrahman al-Sanhaji (qadhi AQMI), Hassan al-Ansari (adjunto de Belmokhtar Morabitun), Iyadh Ag Ghali (emir AnsarDine) Yahiya Abu-l-Hammam (Emir de Aqmi en el Sahara) y Mohammed Kufa (Frente de Macina)

Además de este grupo terrorista existen muchos grupos terroristas más como aparecen en la siguiente Infografía del IEEE



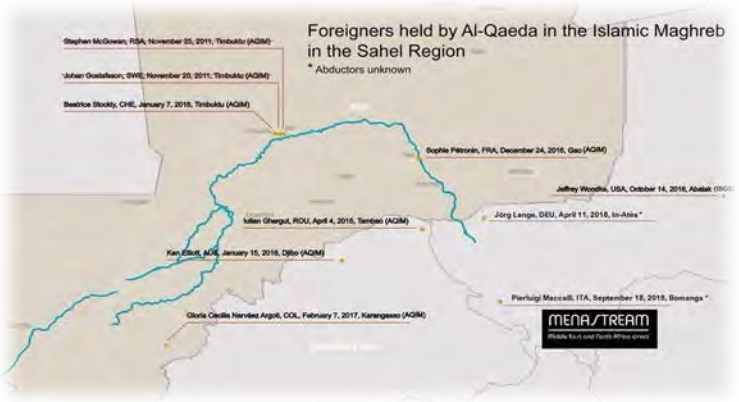
Todas estas amenazas son muy importantes pero la principal la tenemos en el norte de África. Si se dan cuenta existen grupos yihadistas afiliados a Daesh en el norte de Túnez y Argelia. ¿A qué distancia está Túnez o Argelia de España? A muy pocos kilómetros por lo que la amenaza la tenemos bastante cerca.

Pero si solamente nos centramos en Mali qué es dónde se encuentra el foco de todos los conflictos tanto de crimen organizado como de terrorismo nos vamos a encontrar que la amenaza se va extendiendo hacia Burkina Faso y Niger.



Todo esto, ¿qué repercusiones tiene para nosotros? En el caso del terrorismo además de la cercanía a España, nos encontramos también con todos los extranjeros de distintas nacionalidades que actualmente están secuestrados en el Sahel. El último secuestrado ha sido un sacerdote italiano, el Padre Pierluigi Macali que fue secuestrado el 18 de septiembre de 2018 y que como verán en esta infografía la zona principal

donde se producen todos los secuestros es la zona de Mali, de Burkina y de Níger.



Ante esta grave amenaza para la seguridad, ¿cuál es la respuesta militar?, ¿cuál es la respuesta en el ámbito de seguridad ante esta amenaza terrorista que nos encontramos?

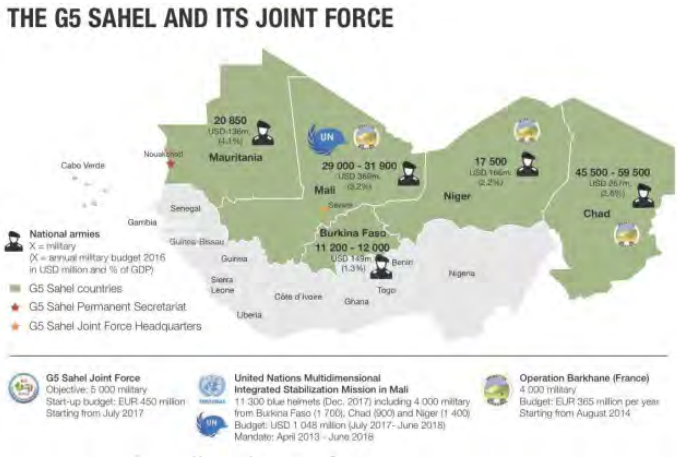
La primera operación francesa que se llevó a cabo fue la operación Serval, actualmente es la operación Barkhane que lleva a cabo Francia en la que intervienen 4000 soldados hay 300 vehículos de combate, 17 helicópteros, 8 aviones, de 6 a 10 aviones de transporte y 5 drones. Tienen lo que son bases permanentes y bases avanzadas. Francia invierte tanto en esta respuesta ante el terrorismo yihadista aparte de que porque fueron colonias francesas a parte porque tiene fuerte interés en estos países.

Existe otra respuesta por parte de la Unión Europea qué es la misión de la EUTM Mali en el que existe un total de efectivo de 580 de 27 países. España contribuye con 292 efectivos, el cuartel general se encuentra en Bamako aunque existen otros

centros de entrenamiento. Hasta hace unos meses España lideró la misión de la EUTM de Mali dirigida por el General Enrique Millán Martínez que decía que debemos ayudar a Mali y a defender su territorio y su población porque evidentemente de su de su seguridad depende la nuestra.

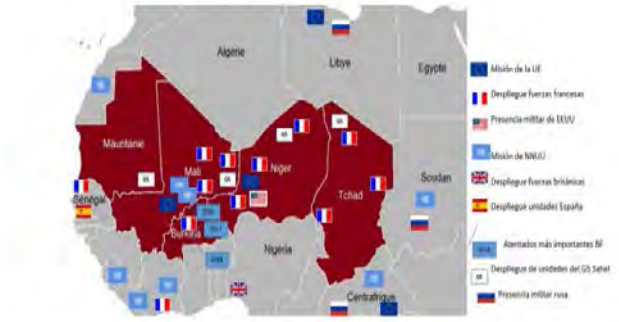
Por último, se encuentran las distintas Misiones de NNUU de mantenimiento de la paz que aparece en este mapa donde vemos el despliegue total de todas las operaciones que existen para dar respuesta a esta amenaza terrorista. Vemos también como está la misma que la misión de mantenimiento de paz de Naciones Unidas vemos donde está situada la misión de la EUTM Mali y el despliegue de la misión francesa con dónde son las zonas principales actividades terroristas y dónde tiene su presencia España principalmente como base operativa en Dakar, en Senegal y especialmente en Kulikoró y en Bamako.

Y la recién creada Fuerza G5 Sahel en el marco de la respuesta regional de los países de la zona al terrorismo yihadista



Quiero no obstante terminar diciendo que a pesar de todas las fuerzas militares que existen desplegadas en el terreno, no se ha conseguido frenar el terrorismo yihadista y lo que es aún peor, en estos años ha ido en aumento por lo que la respuesta a esta amenaza debe pasar por otras soluciones además de la militar que la vemos en la siguiente infografía.

LA FUERZA MILITAR EN EL SAHEL



2016: Ataque del 15 de enero de 2016 contra Hotel Splendid y restaurante Capuccino.
2017: Ataque del 13 de agosto de 2017 contra el Café Aziz Estambul y ataque patrulla TF Sabre (27 noviembre)
2018: Ataque del 2 de marzo de 2018 contra EMGA y Embajada de Francia.

3ª Jornada: PROTECCIÓN DE LAS INFRAESTRUCTURAS CRÍTICAS DEL SECTOR FINANCIERO

El libre comercio en el Mediterráneo en un contexto de guerra comercial

AUTOR: D. Fernando Morillas García, de Analistas Económicos de Andalucía

I. El espacio marítimo: el Mediterráneo

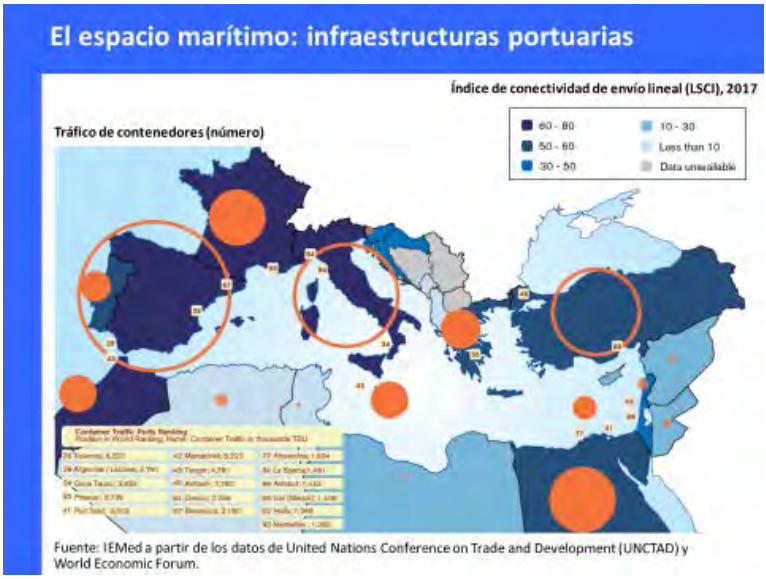
El espacio marítimo es un elemento clave para la convivencia entre los pueblos y, en este sentido, el Mediterráneo es un magnífico ejemplo de ello porque durante siglos ha sido el eje vertebrador que ha permitido establecer vínculos de muy diversa índole entre sus habitantes (culturales, sociales, comerciales, económicos, etc.). No cabe duda de que resulta indispensable garantizar la seguridad y la protección de ese espacio marítimo para facilitar las relaciones que se desarrollan en el mismo y alcanzar los objetivos de desarrollo económico y de prosperidad en la región. A tal efecto, resulta de interés referirse al contenido que, sobre esta materia, se recoge en la Estrategia de Seguridad Nacional, en la Estrategia de Seguridad Marítima Nacional y en la Estrategia de Seguridad Marítima de la Unión Europea y que señala la importancia del espacio marítimo y, de manera especial, de los aspectos que tienen que ver con la economía.

En estos documentos se definen una serie de amenazas y de desafíos que están presentes en los denominados espacios comunes globales, que son aquellos que conectan a personas,

bienes, servicios, ideas, datos, etc. Nos estamos refiriendo, por ejemplo, al espacio aéreo, al ciberespacio y, por supuesto, también al espacio marítimo. Por tanto, este espacio marítimo es vulnerable porque está sometido a una serie de amenazas, entre las que se pueden identificar aquellas de carácter fortuito (accidentes, catástrofes naturales que hay que prevenir o tratar de solventar una vez que se han producido) y otras de naturaleza delictiva, que surgen cuando de forma deliberada se producen determinadas acciones (terrorismo piratería, tráfico ilegal de mercancías de personas, sobreexplotación pesquera, el patrimonio subacuático). Asimismo, también se recoge como desafío explícito la inestabilidad económica y financiera, cuyas causas no son necesariamente de origen económico y financiero, sino que tienen que ver directamente con la seguridad (atentados contra infraestructuras portuarias, plataformas marítimas, pero también al poner límites a la libre circulación y navegación de buques y naves, etc.).

De este modo, se pone de manifiesto la necesidad de garantizar la seguridad en ese espacio marítimo en tanto que este tiene un importante valor estratégico a nivel económico, ya que las rutas marítimas son fundamentales para el transporte, para el comercio, para el aprovechamiento energético y también para el intercambio de información digital (a través de cables submarinos). Es decir, existe una vinculación muy estrecha entre la seguridad marítima y el desarrollo y el bienestar de la sociedad y la Estrategia de Seguridad Marítima de la Unión Europea define que la responsabilidad de salvaguardar y proteger el ámbito marítimo debe ser compartida, se trata de una cooperación transfronteriza de todos los pueblos que habitan en el Mediterráneo.

Concretamente, la región a la que nos estamos refiriendo, el Mediterráneo, abarca los países del sur de Europa, de Oriente Medio y del Norte de África, lo que configura un espacio en el tráfico marítimo de contenedores es uno de los más importantes del mundo y la actividad portuaria también es muy relevante. Además, la calidad de las infraestructuras portuarias ha evolucionado muy positivamente en la última década en términos de accesibilidad, conectividad y de desarrollo (número de naves, de los servicios que prestan los puertos, de las empresas están implantadas en los mismos).



Fuente: IEMed a partir de los datos de United Nations Conference on Trade and Development (UNCTAD) y World Economic Forum.

II. Hacia una zona de libre comercio en el Mediterráneo

En definitiva, un mar como el Mediterráneo, que comunica una red de países tan importante, representa una oportunidad para impulsar el desarrollo económico. En las últimas décadas se

han dado algunos pasos para avanzar en este objetivo, fundamentalmente a través de la iniciativa europea, que ha impulsado las relaciones comerciales con los países del sur desde la segunda mitad del siglo XX, a partir de la firma del Tratado de Roma y la aplicación de determinadas políticas posteriores. No obstante, el punto de inflexión fue la Declaración de Barcelona en 1995, cuando estas relaciones norte/sur empezaron a articularse en términos de igualdad, dirigidas hacia el desarrollo económico y una prosperidad compartida de la región euromediterránea. Es en este momento cuando surge la idea de crear una zona de libre comercio en la región. Posteriormente, esta iniciativa tuvo continuidad con la Política Europea de Vecindad (2004) y con la Unión por el Mediterráneo (2008).

La forma en que se desarrolló este proyecto fue a través de la firma de acuerdos entre la UE y los países del sur, acuerdos que, si bien respetaban las características propias de cada país firmante, tenían una serie de rasgos comunes que pretendían avanzar en diversas cuestiones básicas: primero, en la colaboración en política y seguridad; segundo, en términos de colaboración cultural, social y humana; y, por último, en la colaboración económica financiera, que se basa en la creación de una zona de libre comercio. En definitiva, en lugar de un acuerdo global para todos los países se ha desarrollado una red de acuerdos bilaterales país a país, aunque prácticamente alcanza a todos los del norte de África y Oriente Medio.

Asimismo, se pretendía impulsar las relaciones sur/sur para propiciar una mayor actividad comercial entre los países del norte de África y también entre las economías del norte de África con Oriente Medio, por lo que se ha tratado de promover

la firma de acuerdos entre ellos. Sin embargo, esta cooperación sur/sur ha sido menos relevante hasta el momento y apenas cabe destacar el acuerdo de Agadir (Marruecos, Túnez, Jordania y Egipto). También destaca el papel de Turquía, que prácticamente ha desarrollado un sistema de cooperación propio con la firma de un gran número de acuerdos bilaterales.

Libre comercio en el Mediterráneo: Acuerdos comerciales

ESTADO ACTUAL DE LA RED DE ACUERDOS DE LA ZONA DE LIBRE COMERCIO EUROMEDITERRÁNEA

Acuerdos de Asociación de la UE con Países Terceros Mediterráneos (PTM)

	Fecha de la firma	Fecha de entrada en vigor
Argelia	Abril 2002	Octubre 2005
Egipto	Junio 2001	Junio 2004
Israel	Noviembre 1995	Junio 2000
Jordania	Noviembre 1997	Mayo 2002
Líbano	Junio 2002	Acuerdo interino marzo 2003, abril 2006
Marruecos	Febrero 1996	Marzo 2000
Palestina (Acuerdo provisional)	Febrero 1997	Julio 1997
Siria	Octubre 2004	Pendiente a diciembre de 2008
Túnez	Julio 1995	Marzo 1998

Acuerdos de libre comercio entre PTM

	Fecha de la firma	Fecha de entrada en vigor
Agadir (Marruecos, Túnez, Jordania y Egipto)	Febrero 2004	Marzo 2007
Israel-Turquía	Marzo 1996	Mayo 1997
Turquía-Siria	Diciembre 2004	Enero 2007
Turquía-Marruecos	Abril 2004	Enero 2005
Turquía-Egipto	Diciembre 2005	Mayo 2007
Turquía-Argelia	Negociación concluida, a la espera de la firma	
Turquía-Túnez	Noviembre 2004	Junio 2005
Turquía-Jordania	En negociación	
Turquía-Líbano	En negociación	

En la práctica estos acuerdos se aplicaron de forma asimétrica, ya que la UE eliminaba los aranceles a la entrada de productos procedentes de países del sur desde su entrada en vigor, mientras que los países del sur tenían un periodo de 12 años desde la firma del acuerdo para eliminarlos progresivamente. Además, se establecía un trato preferencial para el comercio de productos agrícolas y también la liberalización progresiva de los servicios.

Con la creación de una zona de libre comercio se esperaba obtener una serie de efectos positivos sobre las economías de los países del sur, entre las que cabe reseñar las siguientes:

- Incremento del comercio entre los países de la región euromediterránea.

- Aumento de la competencia para las empresas locales, lo que incentivaría la búsqueda de una mayor productividad y, por tanto, de una modernización de los procesos y de la tecnología.

- Mejora del bienestar de la economía y de la sociedad, mediante el acceso a productos extranjeros (bienes de consumo y bienes de equipo) con precios más bajos.

- Crear unas condiciones que permiten establecer empresas extranjeras en estos países, lo que al final podría actuar como polo de desarrollo de estas economías.

Por otro lado, hay que considerar algunos inconvenientes:

- Desde el punto de vista de financiero, algunos países del sur son bastante vulnerables a prescindir de los ingresos que suponen los aranceles.

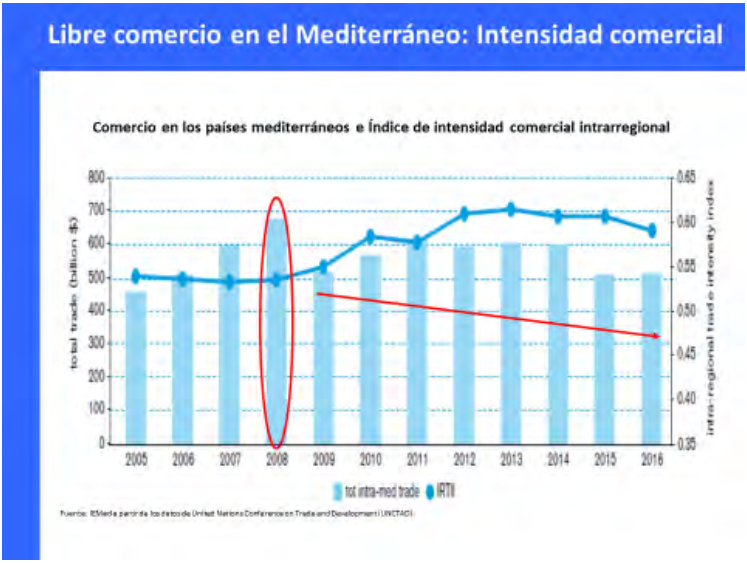
- A esto se une que la apertura comercial requiere la adaptación de las infraestructuras y genera un mayor gasto social, lo que conlleva grandes inversiones.

- Los aranceles no son las únicas barreras al comercio, ya que existen otras medidas que ponen límites al

comercio internacional que en principio no están tan recogidas en este tipo de acuerdos (prohibiciones directas de determinados productos, subvenciones a la exportación por parte del país de origen, etc.).

- El alcance del área de libre comercio es limitado porque la UE firma acuerdos con muchos otros países del mundo, por lo que no se garantiza un trato preferencial con los países del sur del Mediterráneo.

Cuando se planteó la creación de un Área de Libre Comercio Euromediterránea se fijó como objetivo que estuviera constituida en 1995 y que su entrada en vigor definitiva fuera en 2010. Sin embargo, hay que reseñar que este proyecto se desarrolla en un área bastante desigual, lo que también puede ser fuente de dificultades en la aplicación de las medidas y en el alcance de los objetivos propuestos. Así, estamos hablando de una zona de más de 500 millones de habitantes, donde el 55% se concentra en el norte y el 45% en el sur, aunque la evolución demográfica está siendo mucho más importante en la ribera sur, por lo que esta distribución tiende a igualarse o a incluso a invertirse a medio y largo plazo. En términos de generación de PIB la desigualdad es mucho más acusada, dado que el 86% del PIB se concentra en las economías de la orilla norte y apenas un 14% en el sur, mientras que la renta per cápita del norte es seis veces más elevada que la registrada en los países del sur. Por tanto, estas condiciones de partida pueden influir en las relaciones comerciales, pero no hay que olvidar tampoco que uno de los objetivos que se persiguen con la liberalización del comercio en la zona y la cooperación norte/sur es precisamente avanzar en la convergencia de estos indicadores.



Pero en un contexto como este, ¿qué ha sucedido desde la creación de una zona de libre comercio? Un breve repaso histórico permite apreciar que si bien durante los primeros años hubo un crecimiento importante de la actividad comercial intrarregional, alcanzándose la cota máxima en 2008 (unos 700 mil millones de dólares), desde ese momento se han producido ciertos altibajos, y el último dato disponible refleja una actividad algo inferior en 2016 (alrededor de los 500 mil millones de dólares). Entre las causas que podrían explicar este descenso de la actividad comercial pueden apuntarse las siguientes:

- Similitudes en la estructura productiva de los países que conforman la región, lo que genera una competencia entre los países del sur y del este (sobre todo en el sector agrícola y en el textil).

- La crisis económica (el comercio prácticamente cayó un 24% en 2009) y la Primavera Árabe (2011) han tenido un impacto negativo en los intercambios comerciales. De hecho, el impacto de la Primavera Árabe sigue presente en la zona, reduciéndose de forma muy significativa los intercambios comerciales y la apertura al comercio exterior de algunos países del sur.

- La superposición de acuerdos y un marco institucional complejo complican el proceso comercial: un mismo país estaba presente en varios acuerdos y, en ocasiones, las condiciones comerciales también son distintas con relación a otros socios.

- Políticas proteccionistas persistentes: desde 2012 se ha producido un aumento de las medidas proteccionistas destinadas a los propios países de la región.

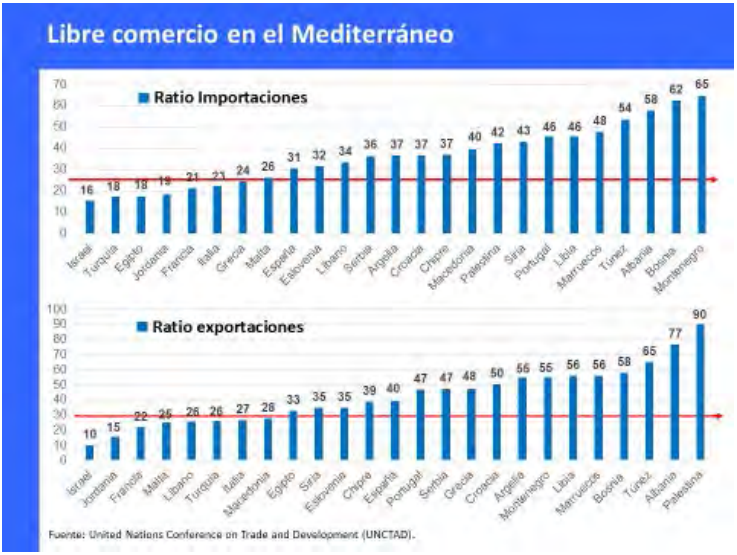
- Debilidad del entorno empresarial: dificultades de acceso a la información, excesivo tiempo en aduanas y lentitud en los trámites administrativos.

Así, la actividad comercial en la zona se caracteriza por un enorme peso de los países europeos, que concentran prácticamente tres cuartas partes del comercio intramediterraneo en origen o destino, seguido a mucha distancia de los países del norte de África (10%-12%), de los países que están ubicados en Oriente Medio (10%) y de los países localizados en los Balcanes (Bosnia, Montenegro y Albania), que han firmado acuerdos más recientes con la UE (4%-5%). En este sentido, conviene recordar que la Primavera Árabe ha hecho que países como Túnez, Argelia o Egipto

hayan visto reducido el grado apertura desde 2012 (suma de importaciones y exportaciones sobre el PIB).

En relación a la dependencia de las economías de región con el comercio mediterráneo, cabe reseñar que el 30% del comercio realizado por los países mediterráneos se destina a la propia región, una cuota que prácticamente coincide con la participación que representa el comercio europeo con el Mediterráneo, que acapara el grueso de la actividad comercial con la zona. En los países ubicados en Oriente Medio el peso que representa el comercio interior con la región es inferior a un tercio, constatando la importancia de otros socios comerciales para estas economías. Por otro lado, los países de los Balcanes y del norte de África muestran una elevada dependencia del comercio con intrarregional, ya que, teniendo una cuota de participación más pequeña sobre el total, realizan en torno al 50% de las importaciones y exportaciones con el Mediterráneo.

Los principales productos que se comercializan por parte de los países mediterráneos están relacionados con el sector de la energía (aunque ha perdido peso en los últimos años) y los productos agrícolas, el sector del automóvil y la industria química. Es preciso señalar la importancia de las nuevas rutas comerciales que han desarrollado países como Marruecos o Túnez, basadas en productos de alto valor añadido como por ejemplo del sector TIC.



No obstante, pese a los esfuerzos por impulsar el libre comercio, en los últimos años se aprecia un retroceso de la actividad comercial y un incremento de las medidas proteccionistas en la región del Mediterráneo en términos netos (medidas proteccionistas – medidas de liberalización). Desde 2009, a partir de la crisis económica, y los años posteriores a 2012, que recogen el impacto de la Primavera Árabe, se ha detectado un aumento de estas medidas proteccionistas que, en general, se han justificado como una estrategia para la protección de las economías nacionales. Estas medidas proteccionistas se han centrado fundamentalmente en los productos agrarios y en el sector del metal.

La propia UE ha tenido un papel protagonista en este sentido, ya que ha implantado el mayor número de medidas de protección, tanto a nivel mundial como con el propio Mediterráneo, aunque cabe reseñar que se han extendido más

las medidas no arancelarias que impiden la entrada de productos (cuotas, subvenciones a la explotación y las relacionadas con la exhaustividad en las inspecciones, en los controles sanitarios y en el incumplimiento de determinadas prácticas obligatorias para normativa europea).

III. Guerra comercial: efectos sobre la economía

Las relaciones económicas entre los países mediterráneos se están desarrollando en la actualidad en un contexto marcado por una creciente implementación de medidas proteccionistas a nivel mundial. Concretamente, a lo largo de 2018 la escalada proteccionista ha empezado a tomar tintes de "guerra comercial", promovida por las medidas impuestas por EE.UU. frente a otras potencias de la economía mundial como China, Rusia o la Unión Europea.

Recordando el esquema básico de lo que supone una guerra comercial, podemos resumirlo en que un país toma una serie de decisiones y de acciones para limitar la entrada de uno o varios productos procedentes de uno o de un grupo de países. Fundamentalmente estas limitaciones se concretan mediante la imposición de aranceles e impuestos a esas importaciones o bien limitando la cuota de importación de determinados productos. Como respuesta, los países afectados también aplican aranceles o cuotas sobre la entrada de productos del primer país, de manera que se inicia una espiral proteccionista entre ambos que va generando efectos nocivos para la economía.

Pero ¿a quién beneficia una guerra comercial?

- A priori, beneficiaría a los productores nacionales de los artículos cuya entrada se encuentra afectada por los aranceles, que mejorarán su competitividad al incrementarse el precio de los productos de sus competidores en el mercado.

- Asimismo, también sería positivo para el Gobierno que lo propone, que mediante estas medidas espera aumentar la recaudación fiscal.

Sin embargo, ¿a quién puede perjudicar?

- Por un lado, aunque resulte paradójico, puede perjudicar a los particulares y empresas del propio país que consumen esos productos, dado que se producirá un aumento de los precios finales de los mismos, lo que, en consecuencia, representará una merma de poder adquisitivo.

- Obviamente, también a los exportadores de esos productos, que verán interrumpido el tráfico comercial que venían realizando, o bien deberán soportar un encarecimiento de sus productos en el mercado de destino.

- Las propias empresas locales del país que ha puesto los aranceles también pueden sufrir estos efectos negativos, ya que, en un mundo globalizado como el actual, las barreras a la entrada posiblemente afecten a productos en los que estas empresas participen en la cadena de valor tanto antes de entrar al país como después de hacerlo.

- Por supuesto, también afecta a los mercados financieros, como ha podido constatarse en la evolución de los últimos meses.

- En términos de empleo podrán percibirse estos efectos negativos, con reducciones de plantillas de las empresas afectadas tanto del propio país como a nivel mundial.

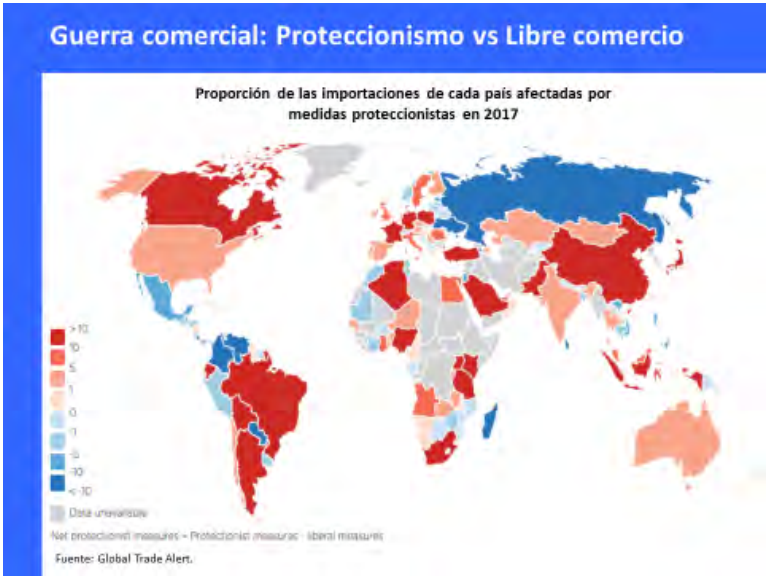
Pero las repercusiones de una guerra comercial no se limitan a las economías de los países directamente implicados. Los vínculos que se han establecido con el avance de la globalización se traducen en un impacto agregado severo, que puede concretarse en la ralentización de crecimiento económico mundial, en un descenso de las inversiones en un clima de incertidumbre, en efectos sobre las cadenas de producción y suministros, un aumento de los costes de producción de las empresas, pérdida de poder adquisitivo de los hogares y, sobre todo, el miedo al contagio y a que se extienda la espiral proteccionista.

En el ámbito europeo, las implicaciones de la guerra comercial podrían afectar también a las relaciones comerciales con el Mediterráneo, dado el peso que tiene la economía europea sobre la región. En este sentido, previamente a la decisión de EE.UU. de aplicar aranceles a los productos procedentes de la UE, se había interrumpido la negociación de un acuerdo bilateral que prácticamente se había cerrado con el Gobierno anterior. Como respuesta a estas medidas, Europa se había planteado tanto llevar a EE.UU. al tribunal de la Organización Mundial del Comercio como establecer aranceles compensatorios, aunque finalmente en los últimos meses se ha

podido llegar un acuerdo que ha permitido liberalizar la mayor parte de los productos industriales (con la excepción del sector del automóvil).

En cualquier caso, si bien estas implicaciones a nivel mundial y europeo son importantes, sin duda lo más relevante es dañar la credibilidad de los organismos que, como la OMC, se han creado precisamente para ejercer de intermediario en este tipo de conflictos y cuyas reglas es preciso cumplir. Ahora mismo este organismo queda en una posición difícil al tener que decantarse entre admitir las justificaciones relativas a la seguridad nacional a las que alude el Gobierno de EE.UU. para imponer estas medidas proteccionistas, lo que podría ocasionar que otros países empezaran a actuar de forma similar, o bien no aceptarlas y que EE.UU salga de la OMC. La posible solución pasará por intentar reducir al proteccionismo mediante acuerdos y negociación y volver a generar un clima de confianza.

Durante este año 2018, la opinión de los principales organismos e instituciones responsables de la economía mundial (FMI, Banco Mundial, OMC, OCDE y BCE) sobre los efectos que puede generar una guerra comercial auguran un futuro poco halagüeño en caso de persistir estas medidas. Así, algunos señalan los efectos nocivos para la propia economía estadounidense, una debacle del comercio y de la economía mundial e incluso se apunta la posibilidad de que se produzca una década perdida.



Por último, hay que considerar también que el mapa del proteccionismo en el mundo a fecha de 2017 (ver mapa adjunto), es decir, el que permite observar la situación previa a las decisiones del presidente Trump y de iniciarse la guerra comercial a la que estamos asistiendo, revela que la tendencia proteccionista ya había empezado con anterioridad (el color rojo señala los países cuyas importaciones sufren más proteccionismo), aunque se ha recrudecido durante 2018.

No obstante lo anterior, también se han podido constatar en los últimos meses algunas iniciativas para seguir promoviendo el libre comercio: contactos para establecer un tratado de libre comercio entre Reino Unido y China tras el *Brexit*; los países de economías emergentes como Brasil, Rusia, India, China, Sudáfrica (BRICS) hacen frente contra la guerra comercial; África impulsa una histórica área de libre comercio; el Acuerdo Transpacífico se mantiene con 11 países firmantes pese a la

salida de EE.UU.; e incluso existe disposición para alcanzar un acuerdo comercial entre EE.UU. y China en los próximos meses.

IV. Retos y perspectivas

A modo de conclusión, es preciso reiterar la importancia de garantizar la seguridad y la protección en el espacio marítimo que comprende la cuenca del Mediterráneo, ya que este es un factor clave para alcanzar los objetivos de desarrollo económico y de prosperidad y bienestar de los pueblos presentes en la zona.

Asimismo, se ha podido constatar que la implementación de una zona de libre comercio no ha sido suficiente para mejorar la convergencia entre las economías mediterráneas, e incluso se ha detectado un descenso de los flujos comerciales en la región debido a los factores que se han analizado anteriormente. En este sentido, es imprescindible promover e impulsar nuevos acuerdos y políticas en la zona que permitan seguir avanzando en los objetivos propuestos.

Además, pese a que la apuesta por el libre comercio, que se había generalizado en etapas precedentes, aún persiste a escala mundial, estamos asistiendo a una mayor implantación de medidas proteccionistas como instrumento para salvaguardar las economías nacionales, especialmente en momentos de crisis, lo que, sin embargo, se ha demostrado que puede ser en muchas ocasiones contraproducente para dichas economías, para las empresas locales y para los ciudadanos.

El sistema financiero visto desde la perspectiva de la Estrategia de Seguridad Nacional 2017[21]

PONENTE: Dr. José María López Jiménez, Coordinador de Responsabilidad Social Corporativa de UNICAJA Banco.

[21] Departamento de Seguridad Naciona (DNS). *La Estrategia de Seguridad Nacional es el marco de referencia para la política de Seguridad Nacional, una Política de Estado que concibe la seguridad de forma amplia al servicio del ciudadano y del Estado. La Estrategia actual, que cuenta con el informe favorable del Consejo de Seguridad Nacional de 1 de diciembre de 2017, profundiza en los conceptos y las líneas de acción definidas en 2013, y avanza en la adaptación de dicha Política y de los instrumentos y recursos del Estado que la conforman ante un entorno de seguridad en cambio constante.*

1. Introducción (1)

Fuente: El País, 11 de noviembre de 2018.

1. Introducción (2)

Fuente: Edufinet.

2. Otra visión del sistema financiero

Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas.

Sectores estratégicos

Sector estratégico:
«Cada una de las áreas diferenciadas dentro de la actividad laboral, económica y productiva, que proporciona un **servicio esencial** o que garantiza el ejercicio de la autoridad del Estado o de la seguridad del país».

Infraestructuras críticas:
«Las infraestructuras estratégicas cuyo funcionamiento es indispensable y no permite soluciones alternativas, por lo que su perturbación o destrucción tendría un grave impacto sobre los servicios esenciales».

CNPIC:
Centro Nacional de Protección de Infraestructuras y Ciberseguridad.

3. Cooperación entre los sectores público y privado (I)

- El desgaste de los Estados.
  - Referencia a la deuda pública.
- La aparición de nuevos actores no estatales, más flexibles.
- Un mundo globalizado…
- …donde el territorio y lo material no son lo esencial.

3. Cooperación entre los sectores público y privado (2)

- Una cooperación necesaria → Ejemplos recientes.
- La propiedad y la gestión privada de elementos estratégicos para la seguridad nacional.
- El interés privado por preservar información legítima y por mantener la posición competitiva.
- Ejemplos de composición accionarial de empresas energéticas:

Enagás

Denominación	% Total (A)	% Directo	% Indirecto
BANK OF AMERICA CORPORATION	3.614	0.000	3.614
BLACKROCK INC.	3.205	0.000	3.205
RETAIL OEICS AGGREGRATE	1.010	0.000	1.010
STATE STREET CORPORATION	3.008	0.000	3.008

Endesa

Denominación	% Total (A)	% Directo	% Indirecto
ENEL S.P.A.	70.101	0.000	70.101

Fuente: CNMV, datos a 13/11/2018.

3. Cooperación entre los sectores público y privado (3)

- Ley 36/2015, de 28 de septiembre, de Seguridad Nacional: «Las entidades privadas, siempre que las circunstancias lo aconsejen y, en todo caso, cuando sean operadoras de servicios esenciales y de infraestructuras críticas que puedan afectar a la Seguridad Nacional, deberán colaborar con las Administraciones Públicas» (art. 7.1).
- La necesidad de superar el «elemento nacional» y buscar otros valores compartidos por los actores públicos y privados.
- ¿Existe realmente una «Cultura de Seguridad Nacional»? ¿Y «Europea» u «Occidental»?

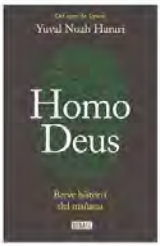
4. La Estrategia de Seguridad Nacional 2017 (1)

- «La Estrategia de Seguridad Nacional es el marco político estratégico de referencia de la Política de Seguridad Nacional. Contiene el análisis del entorno estratégico, concreta los riesgos y amenazas que afectan a la seguridad de España, define las líneas de acción estratégicas en cada ámbito de actuación y promueve la optimización de los recursos existentes» (art. 4.3).

- La «Estrategia de Seguridad Nacional 2017»: «Un proyecto compartido de todos y para todos».

4. La Estrategia de Seguridad Nacional 2017 (2)

- Aspectos generales:
  - Mundo hiperconectado.
  - Revolución tecnológica.
  - Hiperconectividad.
  - Internet de las cosas.
  - Inteligencia artificial.
  - Ingeniería genética.
  - Robotización.



4. La Estrategia de Seguridad Nacional 2017 (3)

- Estructura básica:
  - Amenazas: riesgos para las infraestructuras críticas.
  - Desafíos: inestabilidad económica.

➢ Ciberespacio
➢ Ciberriesgos

4. La Estrategia de Seguridad Nacional 2017 (4)

- La necesidad de contar con un sistema financiero sólido para:

Neutralizar las amenazas híbridas («acciones combinadas que pueden incluir, junto al uso de métodos militares tradicionales, **ciberataques, operaciones de manipulación de la información** o **elementos de presión económica**»).

Generar seguridad económica y apoyar la internacionalización de la actividad empresarial.

Favorecer la innovación de la economía y permitir la diferenciación de los productos y servicios españoles.

Llegar al «nuevo epicentro de la geopolítica global» → Asia-Pacífico (Banco Asiático para Inversión en Infraestructuras).

Controlar los flujos económicos relacionados con:

- El blanqueo de capitales y la financiación del terrorismo.
- Armas de destrucción masiva.

El desarrollo empresarial para rebajar la dependencia de terceros en los ámbitos de:

- La industria tecnológica.
- La industria de ciberseguridad.
- La industria de defensa.
- Los drones.

4. La Estrategia de Seguridad Nacional 2017 (5)

- Riesgos y desafíos relacionados con lo económico y lo financiero:
  - Reforzamiento de la UEM.
  - Ruptura del euro.
  - "Brexit".
  - Alto endeudamiento.
  - Retorno al proteccionismo.
  - Ciberataques.
  - Espionaje industrial contra entidades financieras estratégicas.

Conclusiones

- La seguridad nacional como valor a preservar.
- La necesaria alianza de los Estados con las empresas.
  - Alianza basada más en valores compartidos que en la nacionalidad formal.
- El establecimiento de vínculos adecuados entre los Estados y el sistema financiero como sector estratégico.
- La recuperación de la reputación del sistema financiero y el conocimiento por la ciudadanía de lo que este puede ofrecer desde el punto de vista de la seguridad y la defensa.
- Una realidad compleja y nuevos riesgos, que se podrán superar con el trabajo conjunto de todos.

4ª Jornada: GEOECONOMÍA Y GEOPOLÍTICA DEL MEDITERRÁNEO Y DEL ATLÁNTICO

Tendencias geopolíticas en el Mediterráneo y Atlántico: horizonte 2040

PONENTE: D. Ignacio García Sánchez, Director Operativo del Departamento de Seguridad Nacional.

NOTA DE LA DIRECCIÓN DE LAS JORNADAS: La ponencia fue reproducida en video y audio y transformada mediante un programa informático a word, adaptándose el pensamiento y las palabras del ponente a un texto coherente. Puede que se hayan interpretados erróneamente algunos pensamientos, lo cual debe achacarse a la propia dirección del Foro y nunca al ponente.

Estoy en un momento de cambio, ya que hace pocos días era el subdirector del Instituto Español de Estudios Estratégicos. He mantenido el logo del IEEE, al estar elaborada la ponencia con anterioridad, pero me debo a nuevo puesto en el Departamento de Seguridad Nacional (DNS) y es bueno que debatamos desde la mayor altura como es la Estrategia de Seguridad Nacional en el nivel político estratégico.

El DNS está enclavado en la Moncloa y Presidencia del Gobierno. El director Operativo con dependencia directa del director del DNS, con nivel de director general y dependiendo de don Iván Redondo, Secretario de Estado y luego lógicamente del Presidente del Gobierno.

En el departamento trabajamos siete personas. Somos como la “oficina técnica” del Consejo de Seguridad Nacional.

Quería explicar todo esto para dar a conocer que existe un extraordinario grupo de profesionales que velan y estudian por la seguridad de todos los españoles, desde las más altas instancias del Gobierno.

Por el Foro para la Paz en el Mediterráneo se me pidió que tratara sobre las tendencias geopolíticas en el Mediterráneo y en el Atlántico en el horizonte de 2040.

Para ello voy a dividir mi intervención en cuatro partes: un pequeño preámbulo, para entender el mundo que viene, pasando en segundo lugar a un análisis de los que está actualmente pasando en el mundo, hasta alcanzar el objetivo de determinar las tendencias geopolíticas en el horizonte del 2040, terminando con unas conclusiones.

PREÁMBULO: ENTENDER EL MUNDO QUE VIENE

De este preámbulo voy a extractar cuatro elementos que creo pueden ser definidores del futuro. Estos cuatro elementos escogidos del New York Time que, en 2017 publicó una serie de artículos, en donde se trataba de un nuevo concepto de "geopolítica líquida" [22], que es la incapacidad que tenemos hoy en día de concretar las cosas y de intentar comprender lo que está pasando.

El primer elemento es el "miedo líquido" es esa inmigración indeseada que está llegando a Europa, presentándonos dos vertientes, por un lado, la preservación de nuestra identidad y segunda, que la marea viene de países que están sufriendo, y que esa gente no tiene porvenir.

[22] IEEE. Monografía núm. 147
https://foroparalapazenelmediterraneo.es/?p=15611

También tenemos las redes sociales y el ciberespacio, con mucha gente sin rostro, a veces de culturas desconocidas y ello nos aterroriza. Además, a través de las redes sociales le mostramos al mundo nuestras ilusiones y nuestras capacidades, sin conocer quién está llamando a nuestra puerta. ¿Quién conoce hasta los más leves detalles de nuestras vidas?

El segundo elemento es la “banalidad del mal” como decía Hannah Arendt. El mal, para mí significa el daño realizado sobre un inocente, porque el daño se puede producir de diferentes maneras, como estando en conflicto o combatiendo, pero el que se ejerce a un inocente es maldad.

Como decía Stalin <<la muerte de una persona es una tragedia, la de un millón, una estadística>>. Diariamente vemos el sufrimiento de inocentes ¿Nos hacemos inmunes a ello?, simplemente normalizamos la situación. Kant y Hannah Arendt postulaban que el mal no se puede consentir, ni debe ser asumible, y que se deben poner remedios, tarea de la cual no podemos olvidarnos.

El tercer elemento es el Ecocidio, el juicio universal. Hemos pensado desde después de la Era Industrial, que el hombre tenía derecho sobre la naturaleza, a dominar el mundo, que todo está en nuestras manos. Pero no es verdad, nosotros somos una parte integrante del sistema y del universo, quizá más inteligentes y capaces. Nuestros hijos y nietos nos acusarán de culpables por pensar que este mundo, el cual nos ha puesto todos sus recursos y capacidades a nuestra disposición, no hemos hecho nada para mantenerlo, legarlo y preservarlo para nuestros sucesores.

Este cuarto elemento, el posthumanismo, es el más difícil de comprender y el más comprometido. Sigue la visión de que somos parte del sistema, y debemos respetar a la vida que nos rodea. Esta filosofía se debe a que actualmente nos creemos dueños y señores de todo (otros seres vivos, naturaleza…), este pensamiento lo hemos interiorizado y creyéndonos superiores, y por tanto dominadores, incluso de otros grupos humanos.

Voy a poner un ejemplo para darnos cuenta de que no es algo ilusorio. Europa ha tratado siempre de ser miembro del Consejo Ártico, en el cual España es observador. Europa siempre le ponía veto a Canadá porque comercializaba con carne de foca, y se piensa que la forma con la que tratan a esos animales no era moralmente aceptable. Canadá presentó queja a la Organización Mundial del Comercio, diciendo que no era serio el veto, diciendo que el comercio es el comercio, por lo cual la moralidad no debe interferir en los negocios. La OMC sostuvo que Europa tenía razón, no querían ese tipo de comercio.

Conocer es importante, por el Departamento de Seguridad Nacional fluye mucha información, y ¿cuál es nuestro problema? Tenemos muchas instituciones y organizaciones que velan por la seguridad del ciudadano español, nuestra misión es ser capaces de integrar y crear conocimiento de toda esa información, y dársela al poder decisorio, que es el que tiene la obligación de decidir y marcarnos el rumbo. Nuestro miedo es no ser capaces de analizar la maraña de datos e información, y clasificar lo que es importante y lo que no.

El escritor Joshua Cooper escribió en su libro “El séptimo sentido” las fuentes de poder que van a ser importantes en el futuro y cómo se están desarrollando. Sostenía que ese séptimo sentido se llama instinto, capacidad desarrollada entre tanto elemento de saber discernir el mundo y dirigir nuestras capacidades hacia la innovación.

Las 3 fuentes de poder son la densidad, entendidas como las ciudades y la masa, son un elemento clave. Otro de ellos es la velocidad, la capacidad de influir con rapidez; y la conectividad, porque para poder influir hay que conectar.

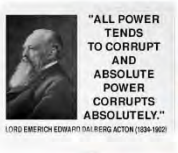
¿QUÉ ESTÁ PASANDO EN EL MUNDO?

Esta segunda parte es más teórica y conocida. ¿Qué está pasando en el mundo? En el Documento de la Estrategia Europea de 2013 de Javier Solana, decía que Europa nunca había sido tan próspera y tan libre, esto era lo que pensábamos todos los europeos, que éramos los líderes y la ejemplaridad de los valores. No teníamos ningún elemento que pudiera hacernos perder ese orgullo. Mogherini en 2016 decía que estos valores estaban en peligro, ya que no teníamos tanta capacidad de influir como creíamos y encima tenemos muchos problemas internos.

Siglos y siglos de conflictos entre las naciones europeas hasta que nos unimos en el proyecto europeo, el cual nos ha dado más de 70 años de paz completa. Yo he dado conferencias por todo el mundo, y me han llegado a preguntar cómo ha sido posible esta paz que nos ha proporcionado la Unión Europea.

El 14 de septiembre de 2008 sucedió la bancarrota de Lehman Brothers, causando la caída total del sistema financiero. El sistema político en el que estábamos basados, la democracia liberal, en el cual había un valor en alza e incorruptible se nos vino abajo, empieza a hacer aguas, y a partir de ahí todo ha ido rodado, causando el descrédito de organismos e instituciones. Hubo un intento de volvernos a colocar en la desconfianza que ha nacido en el mundo, esto es lo que decía el Foro Económico Mundial, el famoso Foro de Davos, el de los grandes sabios.

En el mapa de riesgo de 2012 lo más importante es la gobernanza global, elemento vital tanto universal como internacionalmente porque es un enlace de relaciones internacionales. ¿Cómo estamos ahora? Está perdido, el sueño se nos ha desvanecido en nuestras manos. ¿Dónde está esa posibilidad de crear un sistema que fuera capaz de establecer un marco con el mismo reglamento para todos por igual?



«EXISTEN FUNDADAS EVIDENCIAS QUE APOYAN LA FAMOSA SENTENCIA DE LORD ACTON:

"EL PODER CORROMPE Y EL PODER ABSOLUTO CORROMPE ABSOLUTAMENTE"

Y AMPLIOS ESTUDIOS DEMUESTRAN, QUE PARTICULARMENTE CORROMPE A AQUELLOS QUE, ADEMÁS, PIENSAN QUE SE LO MERECEN»

(Joseph Nye. *The Future of Power*. Pág. 207)

La visión de realistas e idealistas está en un difícil equilibrio donde el idealismo que marcaba el Documento Solana de la Unión Europea en 2003 ha dado paso al realismo, que tiene la visión de que el poderoso hace lo que puede y el débil sufre lo que debe, de que el hombre es un lobo para el hombre.

TENDENCIAS GEOPOLÍTICAS: HORIZONTE 2040

La definición de las tendencias del horizonte 2040 la voy a tener que cambiar, ya que antes se utilizaba la que se usaba en el instituto. Cuenta con cinco factores: la visión geopolítica, el

factor humano, económico, sociopolítico y militar, son cinco fuentes de poder por las que se debe establecer la definición de la política nacional en el ámbito internacional.

En la política nacional de seguridad basada en estrategia trabajamos con 15 ámbitos, porque al hacerlo sectorialmente es más fácil definir planes de acción, y realizar una estructura del sistema de seguridad para después globalizarlo. Dos de esos ámbitos son los más violentos y catastróficos, porque son los que impactan más en la vida humana, son: el conflicto armado y el terrorismo. El fundamento de la Seguridad Nacional es la defensa de las personas.

Después tenemos unos seis elementos que consideramos que hay que asegurar, tres son los espacios comunes globales en los que nadie tiene soberanía pero de los que todos dependemos, son la seguridad del ciberespacio y la marítima, ya que el 90% del comercio mundial se realiza vía marítima. La Organización del Marketing Internacional decía que si se cerrara el comercio marítimo, la mitad de la población se moriría de hambre, y la otra mitad de frio. El tercer elemento es el ámbito aeroespacial: el aire, el espacio ultraterrestre.

La energía y la economía son elementos muy importantes, y ahora ha salido un nuevo elemento en la última estrategia, diferente de la de 2015, que es el de la seguridad contra las epidemias y pandemias.

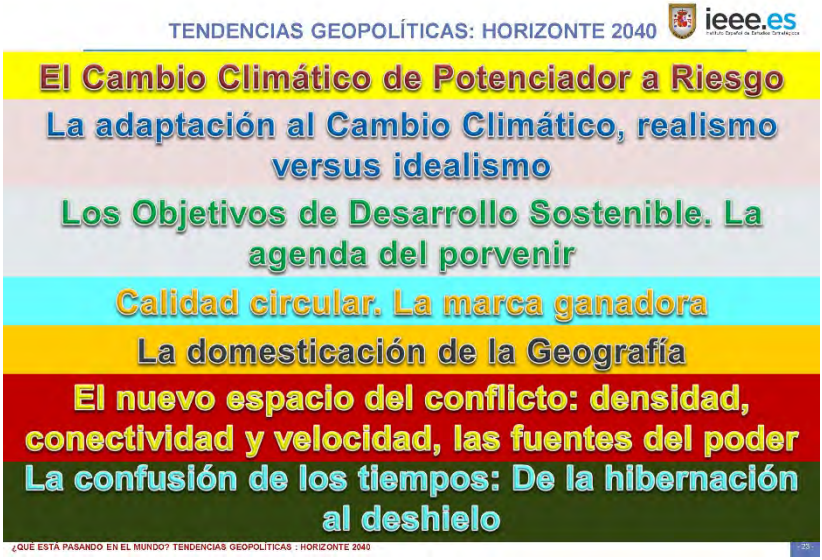
Tenemos 7 riesgos, de los cuales tres de ellos están evolucionando de una forma más desarrollada: los flujos migratorios, el crimen organizado y las catástrofes naturales, los fenómenos meteorológicos extremos. Hay dos protecciones

importantes, la protección de las infraestructuras críticas, y la protección del medio ambiente, que salió en la estrategia de 2017.

También tenemos otros dos elementos, quizá menos importantes y visibles, como es el caso de la contrainteligencia, sobre todo por el robo de patentes, toda esa capacidad de proteger nuestra propia inteligencia con las nuevas tecnologías e intentar detener la creación de armas de destrucción masiva.

Esto es un poco la visión que tenemos en el departamento de Seguridad Nacional, con una visión teórica como trabajábamos en el instituto.

La primera, el factor físico, resalto los espacios comunes. Traigo a Brzezinski porque además de todos los elementos anteriores, él habla del ámbito común medioambiental.



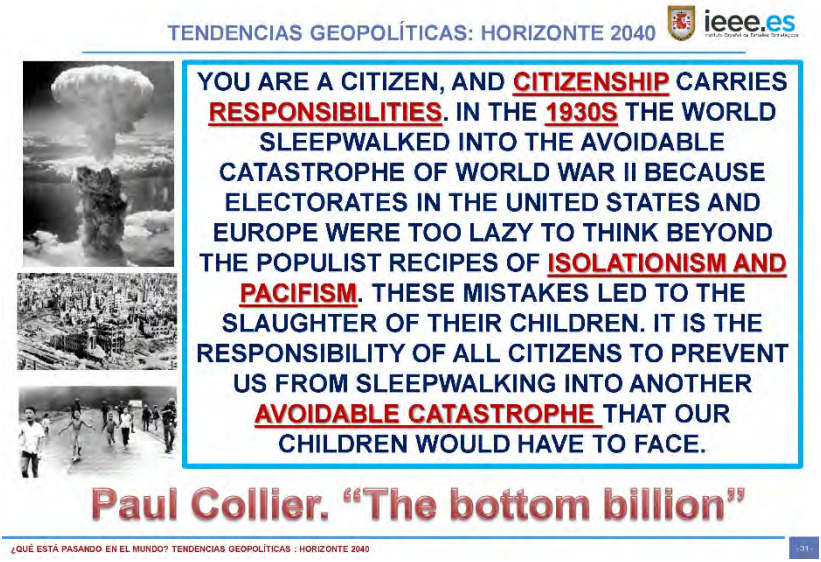
He cogido alguna de las tendencias geopolíticas que ha recogido el Instituto: la adaptación al cambio climático tiene una posición frontal, como riesgo; la Agenda 2030 de la Organización de Naciones Unidas tiene un amplio consenso, va a ser uno de los elementos claves en el futuro; la calidad circular es la calidad del futuro.

En el factor humano podemos ver que es cada vez más importante la importancia del liderazgo, lo podemos ver claramente con Putin y Trump, en el que la tecnología no ha podido modificar su papel de líder.

La tesis económica de Thomas Piketty es que el mundo de la economía va desequilibrándose, creando cada vez más desigualdades, hasta que en algún momento explote, no se sabe de qué manera, tal vez con una revolución. Hay muchas discusiones sobre esa desigualdad, hay muchos cambios entre

esos grupos, es decir, un flujo interno, lo que rompe un poco esa visión de la desigualdad.

Los fondos soberanos, en mi opinión es uno de los elementos más importantes, ¿dónde está el poder económico? Es difícil y complejo, no hay solución porque en cada momento va a ser diferente porque el mundo está en constante cambio. El factor sociopolítico son las instituciones, que es el fundamento de cualquier sistema estructurado y organizado.



Paul Collier en su famoso libro El Millón del fondo explica cómo es importante la ciudadanía. La seguridad es un elemento que debe estar siempre activo, que nunca se debe abandonar.

Traigo 2 de los libros más recientes e impactantes, por el mensaje que mandan Madeleine Albriht y Robert Kagan. El mundo está cambiando y se necesita un esfuerzo de la sociedad, de la ciudadanía, para no caer otra vez en tiempos pasados. La gráfica superior es sobre el populismo, justo antes de la Segunda Guerra Mundial.

La regionalización del mundo, hay una estrategia que dice <<señores, vamos a defendernos nosotros y a regionalizar el mundo>>, parece que es una tendencia que tenemos actualmente. El estado sigue siento la institución básica desde la Paz de Westfalia, y lo seguirá siendo, posiblemente en un futuro el actor principal ya no sean los estados, sino las ciudades.

El factor militar ¿qué estamos viendo para 2040? El diferencial de la capacidad convencional se nos está diluyendo, ha desaparecido la capacidad de desafío, y eso nos obliga a intentar buscar una nueva visión, como la de la inteligencia artificial, para ser más rápidos que el contrincante.

CONCLUSIONES

¿QUÉ ESTÁ PASANDO EN EL MUNDO? TENDENCIAS GEOPOLÍTICAS : HORIZONTE 2040 37

CONCLUSIONES

¿QUÉ ESTÁ PASANDO EN EL MUNDO? TENDENCIAS GEOPOLÍTICAS : HORIZONTE 2040 38

Nosotros en el instituto hacíamos escenarios, porque con los escenarios le das la palabra a la ciudadanía, el futuro nunca se

puede predecir aunque sí se puede hablar de tendencias. Hacemos tres, el malo, el status quo y el bueno, son un escenario mitológico para darle una visión más universal. El bueno: un desarrollo sostenible con la Agenda 2030, esa capacidad universal de progresar todos juntos y siendo muy respetuosos con el escenario en el que nos ha tocado vivir. El medio es la venganza de Agamenón: traiciones, delitos y grandes héroes, lo que sigue siendo, confrontaciones y conflictos pequeños. El malo es el mito de Casandra: a Casandra se le concedió la capacidad de ver el futuro, pero la incapacidad de convencer, ella veía los desastres que iban a pasar pero no convencía a los ciudadanos para que se salvaran. Nosotros tenemos complejo de Casandra, sabemos lo que va a pasar pero no somos capaces de reaccionar, no nos convencemos nosotros mismos, es el gran fracaso del escenario mundial del futuro.

Esto puede ser Europa, hacíamos también tres escenarios para Europa. De derecha a izquierda: La Travesía de Eneas, a pesar de las heridas y de la derrota de la guerra de Troya, pues esa podría ser la refundación de Europa después de la crisis del brexit, de los movimientos nacionalistas. El status quo sería la Doble cara de Jano, una Europa a dos velocidades, un no destruye pero no creo una nueva ilusión. El último, el mantón de Penélope, la pérdida de ilusión.

GEOECONOMÍA Y ASOCIACIÓN ESTRATÉGICA EN EL NUEVO ORDEN MULTIMPOLAR. TEORÍA Y EVIDENCIA EMPÍRICA EN LA UNIÓN EUROPEA

AUTORES: Pablo PODADERA Y Anna GARASHCHUK, de la Universidad de Málaga

Abstract

The EU has developed a 'three-step strategy', which pre-supposes strategic partnerships, firstly, with traditional post-Second World War Western partners, secondly, with the anticipated advantage of regional and inter-regional organization, and, thirdly, with the involvement of emerging powers in a new multipolar world order. However, there are some uncertainties with regard to the relationship between bilateral 'strategic partnerships' and the EU's regional and inter-regional 'strategies'.

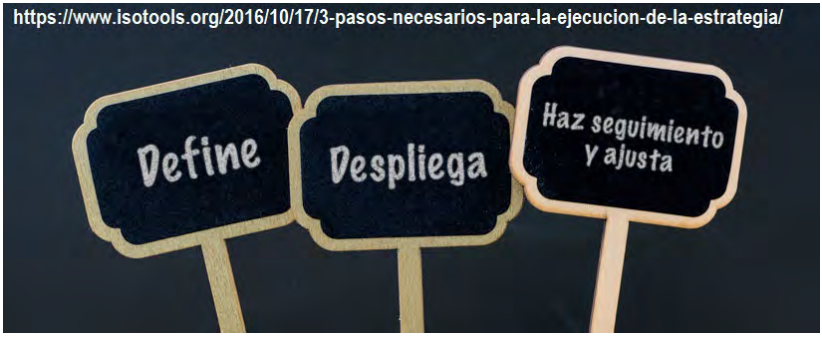
The present document, on the conceptual basis of "Geoeconomics", aims to present some conclusions about an ongoing research, carried out by the authors of this "paper", on the role of strategic partnership and international institutions in

the new multipolar world order, with special attention to the empirical evidence in the European Union and its interaction with other regional organizations.

Palabras clave: Asociación estratégica, multilateralismo, integración regional, modelo logístico binario, Índice sintético.

Resumen

La UE ha desarrollado una "estrategia de tres pasos", que presupone asociaciones estratégicas, en primer lugar, con los socios occidentales tradicionales posteriores a la Segunda Guerra Mundial, en segundo lugar, con la ventaja prevista de la organización regional e interregional, y, en tercer lugar, con la participación de las potencias emergentes en un nuevo orden mundial multipolar. Sin embargo, existen algunas incertidumbres con respecto a la relación entre las "asociaciones estratégicas" bilaterales y las "estrategias" regionales e interregionales de la UE.



El presente documento, sobre la base conceptual de la “Geoeconomía”, tiene como objetivo exponer algunas conclusiones en torno a una investigación en curso, llevada a

cabo por los autores de este “paper”, sobre el papel de la asociación estratégica y las instituciones internacionales en el nuevo orden mundial multipolar, con especial atención a la evidencia empírica en la Unión Europea y su interacción con otras organizaciones regionales.

Key words: strategic partnership, multilateralism, regional integration, binary logistic model, synthetic index.

1. Apuntes sobre Geoeconomía

Existen varios términos con esencia común e incluso inter incluyentes entre ellos, que debemos tener claros a la hora de hablar de Geoeconomía: entre ellos la Geopolítica, la Geografía Económica y la propia Geoeconomía.

http://lorenabaeztrejo.blogspot.com/2013/01/introduccion-la-geografia-economica.html

El estado más básico de los tres términos quizá lo ocuparía la *Geografía Económica,* que podemos definir como aquella disciplina que estudia las relaciones oferta-demanda desde una

perspectiva espacial. Para ello, analiza la localización y características de los "productores" y su relación espacial y temporal con los "consumidores". Estos procesos están relacionados con las leyes de mercado, comercio nacional e internacional, los procesos de mundialización de la economía y la situación económica propia de cada país. Por tanto, la Geografía Económica se interesa por el análisis de la combinación de factores naturales y espaciales en el estudio de las actividades económicas de una región o un país. Estudia la localización y naturaleza de las actividades económicas, los patrones de uso de la tierra, el valor de la misma en relación con las vías de transporte, la rentabilidad del suelo, la distribución espacial de las actividades productivas en las ciudades y el mundo.

Pero los términos de Geopolítica y Geoeconomía van más allá.

Según la RAE *Geopolítica* es “la ciencia que pretende fundar la política nacional o internacional en el estudio sistemático de los factores geográficos, económicos, raciales, culturales y religiosos.” Por ello se dice y admite que la *Geoeconomía* es hija de la Geopolítica y que consiste, por tanto, en evaluar las posibles consecuencias, riesgos y beneficios, no solo económicos, sino también culturales, teniendo en cuenta un factor clave como es la geografía, tanto política (países: fronteras, leyes, cultura, etc.) y física (accidentes geográficos: montañas, valles, composición de la tierra, ríos, posibles materias primas).

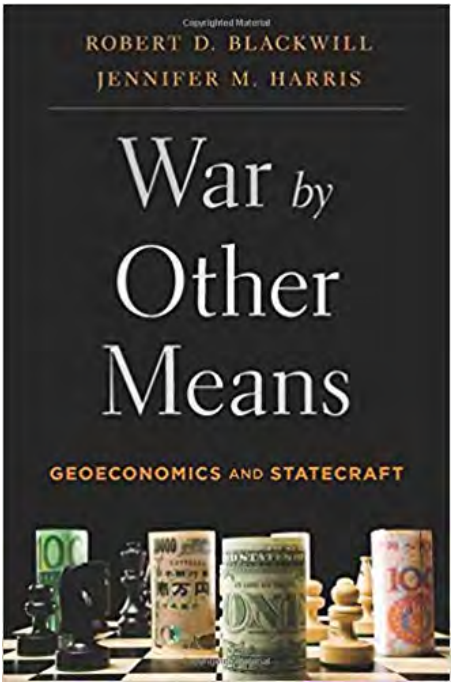
Se dice que esta disciplina nace en plena guerra fría con EE.UU. y la Unión Soviética disputándose una mejor posición frente al otro a través de mejores científicos, con relaciones

internacionales con países potentes tanto militarmente o como aliados.

El término geoeconomía fue acuñado por el militar estratega Edward Luttwark, de origen rumano, crecido en Gran Bretaña y

que posteriormente emigró a Estados Unidos. Luttwark definía la geoeconomía como “el mantenimiento de la antigua rivalidad existente entre las naciones, utilizando medios económicos en lugar de bélicos”.

En Francia, sobre los años ’90, Pascal Lorot fundó la revista Géoéconomie y definía la geoeconomía como: el análisis de las estrategias de orden económico, especialmente comerciales, decididas por los Estados en el contexto de las políticas para a proteger las economías nacionales, a adquirir el dominio de ciertas tecnologías claves, ciertos segmentos de mercado para la producción y/o comercialización de productos, que puedan considerarse un elemento de poder o de proyección internacional de la economía y sociedad nacional”.



Por su parte, Blackwill y Harris (2016) definen geoeconomía como “El uso de instrumentos económicos para promover y defender los intereses nacionales y producir resultados geopolíticos beneficiosos…” (donde adquieren especial importancia tres dimensiones: el rendimiento macroeconómico de una nación, la política económica internacional y los instrumentos económicos que se aplican en búsqueda de fines geopolíticos).

En definitiva, la Geoeconomía nos proporciona las herramientas necesarias para definir planes de expansión y posicionamiento en el nuevo orden mundial o en lo que ya algunos llaman “el nuevo orden geoeconómico” por lo que el término en sí mismo comporta seguridad nacional e internacional, proveniente no sólo de las fuerzas de seguridad, que nos protejan del terrorismo y de las organizaciones criminales transnacionales a que proporciona, sino de la necesidad de un constante aumento de la productividad, de la innovación tecnológica, de la sustentabilidad del desarrollo, de reformas económicas dinámicas que permitan adaptarse a escenarios que cambian a gran velocidad, de la integración a los mercados tanto regionales como internacionales y de la protección de las fuentes de ingresos.

Edward Luttwak precisa el progreso de la Geoeconomía como una competición definida por “la gramática del comercio, pero con la lógica de la guerra”.

2. Geoeconomía y Estrategia de la UE

La nueva etapa de desarrollo del orden mundial se puede caracterizar como transitoria. Para la mayoría de los Estados,

el multilateralismo se está convirtiendo en el principio de su política exterior. Los países en desarrollo intentan extraer más poder del sistema internacional mediante colaboraciones dentro de un grado menor de formalización e institucionalización, 'Grupos G' o el grupo BRICS y mediante la cooperación bilateral, regional e interregional. Las "asociaciones estratégicas", que no necesariamente son informales y dependen de relaciones de baja institucionalización, parecen coincidir con este nuevo escenario. Por lo tanto, no es de extrañar que, para muchos agentes poderosos, incluida la UE, tales alianzas estratégicas se hayan convertido en un medio bilateral importante para fomentar la cooperación internacional durante la última década.

La «estrategia de tres pasos» de la UE, que presupone estas asociaciones estratégicas, en primer lugar, con los socios occidentales tradicionales posteriores a la Segunda Guerra Mundial, como Canadá, Japón y EE. UU., en segundo lugar, con la organización regional e interregional y, en tercer lugar, con las potencias emergentes como los BRICS en un nuevo orden mundial multipolar, indudablemente provoca incertidumbres con respecto a la coherencia entre los enfoques bilaterales y multilaterales en las alianzas estratégicas.

2.1. Sobre la investigación en curso

2.1.1. El marco teórico

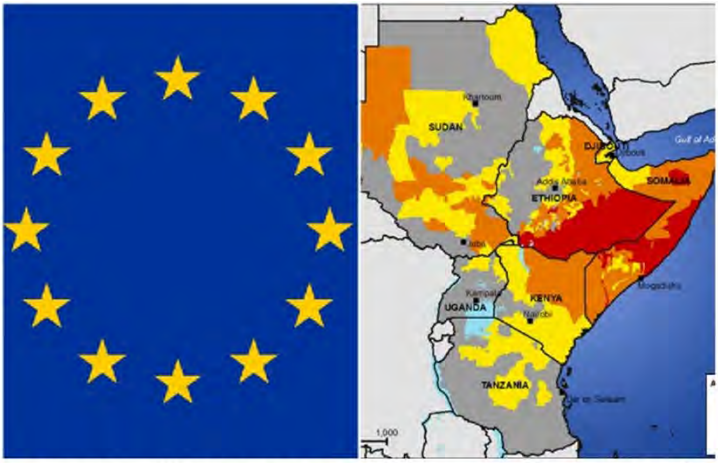
EL marco teórico de la investigación en curso, referida más arriba, pone interés en tres aspectos fundamentales: en el papel de las alianzas estratégicas y las instituciones internacionales en el nuevo orden mundial multipolar, en la

comparación de la asociación estratégica en relación con la integración regional, y en el análisis de la coherencia entre los enfoques bilaterales y multilaterales de la UE.

En este sentido, se han analizado las aportaciones de autores como North (1991), Bull (1995), Hernández et al. (2009), Peña (2010) o Philipovic (2011), entre otros, en torno al papel de las instituciones internacionales; las aportaciones de los neofuncionalistas, dirigidos por Haass (2008) y las de otros estudiosos como Balassa (1964) o Gratius (2011a), en lo referente a la relación entre los conceptos de asociación estratégica e integración regional; o las contribuciones de Barroso (2008), Solana (2003), Bendiek y Kramer (2010), Gratius (2010b), Grevi (2010) o Quevedo Flores (2012), entre otros, en lo que concierne a la asociación estratégica frente al multilateralismo.

En resumen, puede concluirse que la concepción de la UE de utilizar alianzas estratégicas como instrumento para lograr un

multilateralismo efectivo sigue siendo confusa y poco clara para una gran parte de académicos estudiosos del tema. Por lo tanto, la UE debería hacer su concepción más precisa sobre este tema, y debería tratar de llevar a cabo una estrategia coherente tanto con las instituciones internacionales como con respecto a sus relaciones bilaterales con Actores seleccionados; además, sería conveniente también explicar más claramente cómo se pueden conectar estos enfoques bilaterales y multilaterales.



Bruselas, 20 may.- La alta representante de la Unión Europea (UE) para Asuntos Exteriores y Política de Seguridad, Federica Mogherini, visitará desde hoy hasta el próximo miércoles países del llamado Cuerno de África, para fortalecer la asociación estratégica bilateral.
Como parte de su agenda de trabajo, se reunirá con el presidente de Kenya, Uhuru Kenyatta, y miembros del Gobierno, organizaciones juveniles y de la sociedad civil, informó la Comisión Europea.

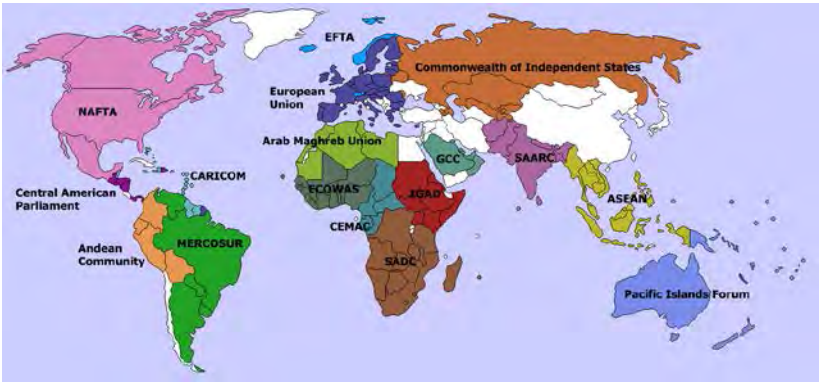
En cualquier caso, sin importar en qué dirección se desarrolle el sistema internacional, la posición de sus actores globales en la jerarquía internacional depende de la realización de sus potenciales económicos, militares y demográficos y de sus recursos. Hay dos opciones principales para desarrollar este potencial: fortalecerse a través de los otros participantes internacionales o unir constructivamente el propio potencial con el potencial de otro actor. Se puede decir que la segunda opción es la verdadera asociación estratégica. En el nuevo orden mundial multipolar, será importante ocupar una posición clave. Y en este caso, la asociación estratégica no solo es un instrumento para obtener todos los beneficios posibles de las relaciones bilaterales, sino también una medida para ocupar puestos superiores en el escenario internacional.

2.1.2. El marco analítico

Sobre dicha base teórica, la referida investigación pretende comparar las "asociaciones estratégicas" bilaterales y las "estrategias" regionales de la UE. Para ello se han aplicado una serie de técnicas analíticas, entre ellas: el modelo logístico binario, el Análisis de componentes principales Categórico (CATPCA- CATegorical Principal Components Analysis), el Análisis de Componentes Principales (PCA) y la extracción de un índice sintético de idoneidad del socio estratégico.

Con este objetivo se investigaron las siguientes organizaciones regionales: Asociación de Naciones del Sudeste Asiático (ASEAN: Indonesia, Filipinas, Malasia, Singapur, Tailandia, Vietnam, Brunei, Camboya, Laos y Myanmar), Comunidad del Caribe (CARICOM: Antigua y Barbuda, Bahamas, Barbados, Belice, Dominica, Granada, Guyana, Haití, Jamaica, Monserrat,

Santa Lucía, San Cristóbal y Nieves, San Vicente y las Granadinas, Surinam, y Trinidad y Tobago. Miembros Asociados: Anguila, Bermudas, Islas Caimán, Islas Turcas y Caicos, e Islas Vírgenes Británicas), Unión Económica Euroasiática (EAEU: Bielorrusia, Kazajistán, Kirguistán, Rusia, Tayikistán, Uzbekistán), Mercado Común del Sur (Mercosur: Argentina, Brasil, Paraguay, Uruguay, Venezuela y está en proceso de adhesión Bolivia.), Asociación del Asia Meridional para la Cooperación Regional (SAARC: Afganistán, Bangladés, Bután, India, Nepal, Maldivas, Pakistán, Sri Lanka) y el Sistema de Integración Centroamericana (SICA: Costa Rica, El Salvador, Guatemala, Honduras, Nicaragua, Panamá, Belice y República Dominicana).



Las organizaciones fueron elegidas de acuerdo con criterios que les exigían alcanzar un cierto nivel de integración, es decir, demostrar que al menos habían logrado crear una unión económica viable y limitar cada organización regional a tener como miembro no más de uno de los socios estratégicos oficiales de la UE. La aplicación de las técnicas analíticas anteriormente nombradas sobre la realidad de estas

organizaciones nos permitió investigar, primero, cuáles de estas organizaciones regionales eran atractivas para la UE como socios estratégicos y, segundo, saber si los grupos regionales eran más atractivos para la UE que para cualquiera de sus miembros reales.

Sobre la base de los indicadores sugeridos por el Observatorio Europeo de Asociaciones Estratégicas (ESPO) y otros indicadores relacionados con los valores de la UE (teniendo en cuenta la Estrategia de Seguridad Europea de 2003, donde la UE destaca las asociaciones estratégicas con países que comparten las normas y valores) como: raíces histórico-culturales comunes (considerando la Declaración de RIO de 1999 sobre la asociación estratégica entre la UE y ALC, que se basa en una profunda herencia cultural e intereses y valores comunes), la ausencia de acciones discriminatorias entre socios (teniendo en cuenta la experiencia negativa de la asociación estratégica europeo-rusa), la base jurídico-institucional del socio (sin perder de vista el enfoque neoinstitucional) y el factor frontera común, y utilizando el Análisis de componentes principales Categórico (CATPCA-CATegorical Principal Components Analysis), se identificaron las dimensiones sobre las que luego se aplicó el Análisis de Componentes Principales (PCA) y que condujo a tres principales componentes para 143 países analizados.

El primer componente (COM1) describe la posición económica y política de un país en el mundo, su patrón de desarrollo social y su interés comercial común con la UE, y por lo tanto se denomina Componente Estratégico; el segundo componente (COM2) describe la gobernanza sostenible, la libertad económica y los valores comunes del país con la UE y se

denomina componente de asociación espiritual; en el tercer componente (COM3), el mayor peso recayó en la base institucional y legal común, y se desarrolló particularmente con los países vecinos, por lo que el componente se conoce como el Componente del Buen Vecino. Sobre la base de estos tres componentes, se aplicó el modelo binario logístico, que había sido un modelo utilizado frecuentemente para predecir eventos en la economía (Karp, 2009; Boyacioglu, Kara y Baykan, 2009) y las ciencias políticas (King, Tomz y Wittenberg, 2000).

Las principales hipótesis de la investigación son las siguientes:

- Algunas organizaciones regionales son atractivas como socios estratégicos para la UE
- Las organizaciones regionales son más atractivas como socio estratégico para la UE que cualquiera de sus miembros sin la participación en la organización regional.

Algunos de los resultados arrojados por el proceso analítico son los siguientes. En primer lugar, se obtuvo una matriz de coeficientes de puntuación para cada uno de los tres componentes, sobre la base de la cual se calcularon las tres componentes principales para los grupos regionales considerados en el estudio.

Sobre la base del componente estratégico, que resultó ser el más significativo, se aplicó el Modelo Logístico Binario para los grupos regionales.

En este sentido, Mercosur, la UEEA y la ASEAN obtuvieron la mayor probabilidad de convertirse en los socios estratégicos más importantes de la UE. La SAARC alcanzó un potencial

considerable para convertirse en socio estratégico de la UE, mientras que SICA y CARICOM no son interesantes para la UE como socios estratégicos.

Se debe suponer que, de acuerdo con los resultados del Modelo Logístico Binario, los seis grupos regionales investigados son más atractivos como socios estratégicos para la UE que cualquiera de sus miembros ya establecidos, considerados por separado. La organización regional con el mayor potencial es Mercosur. Por lo tanto, Brasil, siendo un socio estratégico oficial de la UE con una alta probabilidad, junto con Mercosur se convierte en el socio estratégico más importante de la UE.

A pesar del hecho de que solo el primer componente fue significativo para el Modelo Logístico Binario, los otros dos componentes no son irrelevantes para nuestra investigación. La UE, al decidir qué socios estratégicos elegir, también debe tener en cuenta los valores comunes, así como el nivel de desarrollo de una base jurídica e institucional. De lo contrario, el concepto de Asociación Estratégica de la UE corre el riesgo de convertirse en una asociación programática más que estratégica. Por lo tanto, sobre la base de los tres componentes, se ha elaborado un índice sintético de Idoneidad.

Para construir el Índice de Idoneidad del Socio Estratégico (SPSI) para la UE, hemos otorgado peso a cada componente sobre la base de la varianza total, técnica que ya ha sido utilizada por muchos autores en diferentes campos económicos (Iglesias et al., 2000).

3. CONCLUSIONES

El concepto de asociación estratégica es imperfecto, pero es un instrumento esencial que permite el diálogo y la cooperación para un multilateralismo efectivo. Y en este caso, la asociación estratégica no es solo un instrumento para obtener todos los beneficios posibles de las relaciones bilaterales, sino también una medida para ocupar posiciones más altas en el nuevo orden mundial multipolar.

En comparación con la integración regional, las alianzas estratégicas no insisten en la existencia de un componente supranacional. En este sentido, la asociación estratégica permite la colaboración en una amplia gama de cuestiones, evitando al mismo tiempo la derogación de la soberanía de cualquier parte.

Sin embargo, debe concluirse que la concepción de la UE de utilizar las alianzas estratégicas como instrumento para lograr el multilateralismo efectivo sigue siendo confusa y poco clara para la mayoría de los expertos.

De acuerdo con los resultados de la aplicación del Modelo Logístico Binario, se puede suponer que las seis organizaciones regionales investigadas se hicieron más atractivas como socios estratégicos de la UE que cualquiera de sus miembros actuales. En este sentido, se puede concluir que para la UE es más efectivo desarrollar asociaciones estratégicas con organizaciones regionales que construir relaciones bilaterales con cualquiera de sus miembros actuales. Además, las organizaciones regionales dan la

posibilidad de que los miembros menos atractivos se vuelvan más estratégicos para la UE.

Si bien solo el componente estratégico fue significativo para el Modelo Logístico Binario, para llevar a cabo la Asociación Estratégica en la práctica también es importante tener una base jurisdiccional e institucional eficiente con un socio y, de acuerdo con el concepto de la UE, para que coincida con las normas y valores UE. En este sentido, teniendo en cuenta los tres componentes, se elaboró y se aplicó el Índice de Idoneidad del Socio Estratégico (SPSI) para la organización regional.

Según el SPSI, Mercosur es más adecuado como socio estratégico de la UE que cualquiera de sus miembros actuales en función de los resultados del Modelo Logístico Binario. Con respecto a ASEAN, se puede decir que su posición en el ranking se debe a la de su miembro Singapur. CARICOM también casi converge con la posición de uno de sus miembros, la de las Bahamas. En cuanto a la EAEU, la SAARC y el SICA, parecen ser menos aptos como socios estratégicos de la UE que cualquiera de sus miembros, en la medida en que probablemente fueron penalizados por no corresponderse con las normas y valores de la UE. Por lo tanto, se puede resumir que en el caso de la UE, al elegir sus socios estratégicos, debe tomar en consideración la coincidencia con sus valores y normas y el nivel de desarrollo de una base jurisdiccional e institucional con su socio. Al mismo tiempo, la idoneidad de la organización regional depende de cada caso individual.

Concluyendo, esto que acabamos de realizar es un simple ejercicio de análisis geoeconómico, lo cual pone sobre la mesa la importancia de la secuencia dato, información y

conocimiento, que casi seguro marcará la diferencia entre el éxito y el fracaso de muchas negociaciones en el futuro de la gobernanza global.

REFERENCIAS

BALASSA, B. (1964): Teoría de la integración económica. México: UTHEA.

BARROSO, S. (2008): Hacia una nueva redefinición del papel de la Unión Europea en situación de gestión de crisis: más allá de la paz estructural, en Navajas, Carlos e Iturriaga, Diego (eds.) Crisis, dictadura y democracias. Actas del I Congreso Internacional Historias de Nuestro Tiempo, Logroño, Universidad de la Rioja, pp.443-454.

BENDIEK, A.; Kramer H. (2010): The EU as a Would-Be Global Actor: Strategic Partnerships and Interregional Relations, in: Husar, Jörg/Maihold, Günther/Mair, Stefan (eds.): Europe and New Leading Powers. Towards Partnership in Strategic Policy Areas,Nomos, pp. 21-42.

BOYACIOGLU, M. A.; KARA Y.; BAYKAN, O K (2009): Predicting bank financial failures using neural networks, support vector machines and multivariate statistical methods: A comparative analysis in the sample of savings deposit insurance fund (SDIF) transferred banks in Turkey. Expert Systems Applications, 36, 3355–3366.

BULL, H.; (1995): The Anarchical Society: A Study of Order in World Politics. Macmillan.

DECLARATION OF RIO (1999), Available at:

https://eulacfoundation.org/en/documents/1999-rio-declaration (accessed 13 March 2017)

EUROPEAN SECURITY STRATEGY (2003), Available at:

http://www.consilium.europa.eu/uedocs/cmsUpload/78367.pdf (accessed 13 March 2017)

EUROPEAN STRATEGIC PARTNERSHIPS OBSERVATORY (2016), Available at: http://strategicpartnerships.eu/ (accessed 13 March 2017)

GRATIUS, S. (2011a): The EU and the 'special ten': deepening or widening Strategic Partnerships?", Policy Brief, FRIDA, a European Think Tank for Global Action, No 76, June, pp.1-5

GRATIUS, S. (2011b): ¿Profundizar el multilateralismo a través de las asociaciones estratégicas de la Unión Europea?, Documento de Trabajo FRIDE, Madrid, septiembre.

Grevi G. (2010) 'Making EU strategic partnerships effective' Documentos de Trabajos FRIDE, No 105

HAASS, R. N. (2008): Epoxa bespolyarnogo mira, Rossia v globalnoy politike, No. 4

HERNÁNDEZ, U.; LÓPEZ RAMÍREZ, A.; JIMÉNEZ ELIZONDO, A. (2009): Gobernabilidad e instituciones en las Cuencas transfronterizas de América Central y México, FLACSO, San José. Costa Rica.

KARP, A. H. (2009): Using logistic regression to predict customer retention. New York: Sierra Information Services, Inc.

KING, G.; TOMZ, M.; WITTENBERG, J. (2000): Making the most of statistical analyses: Improving interpretation and presentation. American Journal of Political Science, No. 44, pp. 341–355.

NORTH, D. (1991): Institutions. Institutional Change and Economic Performance. Cambridge University Press.

PEÑA, F. (2010): Capacidades en el caso del G20 y del grupo BRICS. Mercosurabc, March.

Philipovic M (2011): Exigency Politics or New World Order? Panoeconomicus, No. 3, pp. 373-391

REPORT ON THE IMPLEMENTATION OF THE EUROPEAN SECURITY STRATEGY (2008), Available at: http://www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/en/reports/104630.pdf (accessed 13 March 2017)

QUEVEDO FLORES, J A. (2012): Acción Exterior de la Unión Europea. European Scientific Journal, October edition vol. 8, No.24.

SOLANA, J. (2003) Multilateralismo eficaz: una estrategia para la Unión Europea. Política Exterior, No 95, España, pp.37-45.

Temas relacionados con los de Seguridad, Defensa y Cooperación

Boko Haram. Evolución de una amenaza

AUTOR: D. Lucas F. Martín Serrano, Teniente Coronel de Infantería y Jefe del Grupo de Obtención por Sistemas Terrestres.

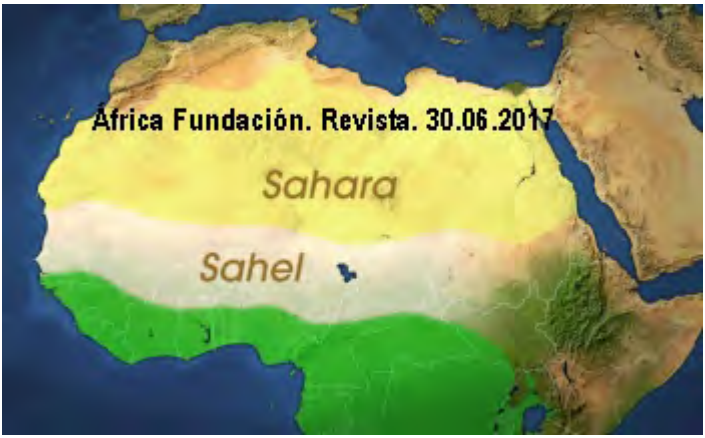
1.-INTRODUCCIÓN

Durante los últimos años, ha habido un notable incremento en los ataques terroristas perpetrados por grupos islámicos extremistas relacionados con Al Qaeda o el DAESH a lo largo del continente africano. Algunos de esos ataques, que han golpeado una extensa franja, desde Nigeria y Burkina Faso hasta Somalia, han captado la atención de los medios de comunicación y han sobrecogido, aunque sólo sea por unos días, a la opinión pública. Pero la mayoría han pasado desapercibidos y, a pesar de esa falta de atención por parte de los medios, la realidad es que la situación está empeorando. Y esto no significa necesariamente que los ataques se estén incrementando. Son otros muchos factores los que nos indican esa tendencia de deterioro en la situación.

No obstante, y dejando de lado otras consideraciones, este asunto cuestiona la capacidad real de los países africanos de contener la amenaza y combatirla de un modo eficaz y efectivo, lo cual tiene enormes implicaciones en lo que se refiere a la seguridad, no solo como muchos piensan, en los países del sur de Europa, sino en toda la UE y para su futuro y estabilidad.

La zona objeto de los ataques dibuja un arco a lo largo de toda

la región del Sahel, el cual se extiende desde las costas del Océano Atlántico, en el oeste, hasta el Mar Rojo, por el Este. Toda esa región está claramente controlada por una red de grupos islámicos que van desde al-Shabaab en Somalia hasta Boko Haram en Nigeria, pasando por Al Qaeda en el Magreb Islámico (AQMI), junto con el DAESH y sus franquicias en Libia.



De todos ellos, los que operan en ambos extremos, al-Shabaab en Somalia, y Boko Haram en Nigeria, son de lejos los más activos, pero tanto AQMI como el DAESH han sufrido una eclosión durante la cual, a la vez que han sido capaces de expandirse por ese inmenso territorio, han tomado como objetivo no sólo a occidentales, bien sean miembros de ONG,,s, militares de países intervinientes en la zona o miembros de la ONU, sino a los propios civiles, tanto por su no colaboración con ellos como por motivaciones religiosas.

Países como Nigeria, Somalia, Mali y Libia se han convertido en el nuevo epicentro del terrorismo internacional, un fenómeno que afecta y amenaza a otros estados de la zona como Kenia,

Egipto, Tunez, Argelia, Níger, Camerún y Chad, alguno de ellos pieza clave para la estabilidad no sólo de la región, sino del continente y de Europa misma, y que sufren un serio riesgo de pasar de “damnificados por el fenómeno” a “nuevos focos generadores del mismo”.

En junio de 2011, el anterior gobierno de Nigeria, liderado por el presidente Goodluck Jonathan, creó la “Joint Task Force” (JTF), una unidad militar especial compuesta por miembros de las fuerzas armadas y la policía con el objetivo de mitigar la amenaza del yihadismo radical violento.

Pero los resultados de esa iniciativa sobre el terreno fueron contradictorios, pues la actividad insurgente se recrudeció. Según afirmaciones de líderes de la sociedad civil, los abusos de la JTF crearon un profundo y creciente resentimiento en sus comunidades, provocando que sus miembros fueran reacios a proporcionar información que ayudara a combatir a Boko Haram. La actuación de esta fuerza no hizo sino aumentar la brecha entre el gobierno, ya de por sí con poca credibilidad en los estados del norte, y entre los habitantes de la zona.

Poco después de ser elegido, el presidente Muhammadu Buhari prometió que su nuevo gobierno erradicaría al grupo terrorista Boko Haram, dedicando a ello todos los esfuerzos necesarios de su administración y devolviendo la paz a las zonas afectadas y controladas por el grupo. Pero esa promesa no se ha cumplido, y a la vista de los acontecimientos y de los datos que nos proporciona la historia reciente en lo que a la guerra contra el terrorismo se refiere, está muy lejos de cumplirse. Los hechos nos dicen que el único caso de erradicación total de un grupo terrorista es el de la organización

“Tigres Tamiles de Liberación”, la cual operaba en Sri Lanka. Pero ese objetivo sólo se logró una vez que el gobierno decidió acabar con el grupo a cualquier precio y se lanzó a una brutal campaña de acciones militares que duró casi 30 meses.

El ejército de Sri Lanka consiguió eliminar a uno de los grupos terroristas más terribles y eficaces, que había perfeccionado enormemente la técnica de empleo de terroristas suicidas. La pregunta que nos hace plantearnos este hecho es, ¿podría lograrse lo mismo en Nigeria con Boko Haram?

Es evidente que el enfoque del presidente Buhari para lograr resolver la situación recae en el incremento del despliegue de tropas en el noreste del país y una mayor cooperación y coordinación con las fuerzas de seguridad de los países vecinos que permitan llevar a cabo operaciones más efectivas contra el grupo y aquellos que le apoyan. El ritmo de crecimiento de Boko Haram y sus acciones le han convertido en un factor desestabilizador para toda la región, y ello refuerza la necesidad de restaurar el orden no sólo de Nigeria, sino en todos los países vecinos.

Pero las raíces del problema son mucho más profundas y complejas, y este no puede ser resuelto totalmente sólo mediante acciones militares. Dichas acciones son necesarias, eso es un hecho objetivo, pero también lo es el que en paralelo deben llevarse a cabo otras en el plano civil, político y económico, enfocadas al desarrollo, el reasentamiento de los desplazados, la reconstrucción y fundamentalmente a la educación y formación de los jóvenes.

2.- EL ORIGEN

Los problemas del noreste de Nigeria no pueden considerarse únicamente problemas de seguridad. Varios son los retos que afectan no sólo a esa región sino a todo el país y que amenazan su estabilidad:

- Corrupción: Generalizada y extendida por todo el territorio e instituciones. Este es probablemente el más serio.

- Criminalidad y terrorismo: Con Boko Haram en el epicentro, pero hay que añadir las tensiones y violencia por problemas tribales, religiosos etc.

- Desempleo: Según informes del Banco Mundial, el 80% de la población por debajo de 24 años está en paro.

- Educación. El índice de analfabetismo ronda el 78% y la corrupción del sistema educativo incluyendo las universidades es endémica, convirtiendo el sistema en ineficaz.

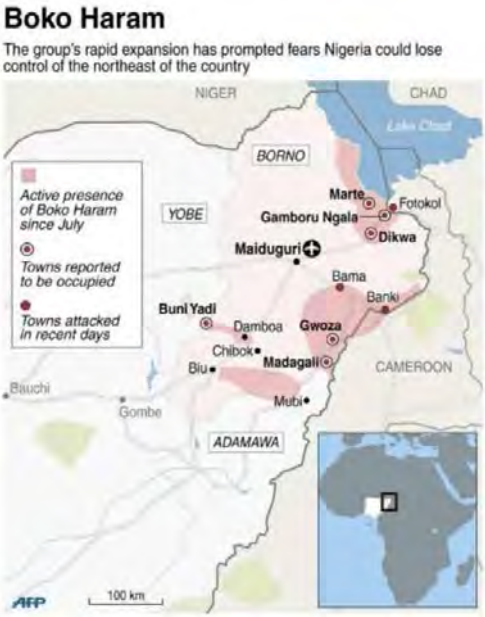
- Medio Ambiente: Nigeria sufre los problemas de medio ambiente clásicos en los países en desarrollo, como la pérdida de la fertilidad de la tierra a causa de la sobreexplotación, vertidos de petróleo, emisiones tóxicas, contaminación del agua debido a un inapropiado tratamiento de aguas residuales, etc.

- Infraestructuras: Nigeria adolece de un sistema de producción y distribución de energía eléctrica fiable, así como de un suministro adecuado y seguro de agua, lo

cual, unido a la falta de infraestructuras adecuadas de transporte, tiene un impacto negativo en el desarrollo económico y en la salud de sus habitantes.

- Disputas territoriales: Nigeria se ha visto envuelta desde su independencia en 1960 en 18 disputas fronterizas con Benin, Chad, Guinea Ecuatorial, Camerún y Niger

Todos los problemas relacionados dificultan cuando no imposibilitan la prestación de servicios básicos por parte del Estado como son la educación, la seguridad y la gobernanza, y ello nos lleva a formularnos dos preguntas: ¿Es esta situación una bomba de relojería que puede derivar en un conflicto social que termine en guerra civil? ¿Podemos considerar a Nigeria como un Estado fallido?



Según manifiesta en su libro “Cuando el Estado falla”, podemos considerar a un Estado fallido cuando éste es azotado por la violencia interna y no es capaz de desarrollar políticas positivas para sus ciudadanos. Es entonces cuando el gobierno pierde su legitimidad y la propia naturaleza del Estado de vuelve ilegítima a los ojos de la mayoría de sus ciudadanos. También afirma que en la mayoría de los Estados fallidos las fuerzas de seguridad han de hacer frente a rebeliones armadas lideradas por uno o más oponentes.

From left are Prof. Nimi Wariboko, Aminu Gamawa, Prof. Robert Rotberg, Prof. Okey Ndibe and Prof. Max Abrahms as Panelists at the recent Nigeria's Security Summit held at Harvard University in Cambridge, Massachusetts.
http://www.alltimepost.com/2014/08/from-left-are-prof-nimi-wariboko-aminu-gamawa-prof-robert-rotberg-prof-okey-ndibe-and-prof-max-abrahms/

Las afirmaciones de Robert Rotberg describen bastante bien la situación actual de Nigeria. Si añadimos la definición que hace el Crisis States Research Center (CSRS), que define como Estado fallido a aquel que sufre una situación de colapso tal que no puede desarrollar las funciones básicas de seguridad y desarrollo y no tiene control efectivo sobre su territorio,

podemos entonces aseverar, de acuerdo a los parámetros establecidos por el CSRS, que Nigeria corre un serio riesgo de pasar a formar parte de la lista de Estados fallidos.

Es una compleja combinación de factores la que ha favorecido que estos grupos de corte islamista hayan podido operar con relativo éxito, y entre ellos hemos de incluir la porosidad de las fronteras entre los países de la zona, la falta de instituciones de gobierno y control, unos estados débiles cuando no corruptos (o ambas cosas a la vez), el descontento y falta de desarrollo económico de la población, el desempleo, la pobreza y unas fuerzas de seguridad mal entrenadas y peor equipadas. Como puede verse, el abono perfecto para el arraigo de cualquier tipo de movimiento insurgente, radical o contestatario de cualquier tipo, especialmente porque la mayor parte de esos elementos tienen un hilo conductor común o llegan al mismo punto: la falta de desarrollo y la falta de esperanza. En esas circunstancias, cualquiera que ofrezca algo mejor a lo que tienen, aunque sólo sea la posibilidad de lograrlo, tiene garantizado el apoyo y el éxito.

Junto a lo ya mencionado, hemos de incluir otro aspecto no menos preocupante como lo son los tráficos ilícitos de todo tipo y las redes de crimen organizado que aprovechan la convulsa situación geopolítica de la zona, así como las facilidades que proporciona un territorio tan vasto, casi imposible de controlar. Estas organizaciones son parte esencial en la financiación de las acciones de los grupos yihadistas, cuando no su verdadera razón de ser, cubriendo o revistiendo de una motivación religiosa o “moral” la que es su verdadera actividad u ocupación, que no es otra que el lucrarse por medio de actividades delictivas.

Todo lo mencionado hasta ahora nos lleva a comprobar que estamos ante un fenómeno que tiene muchas aristas, una amenaza que muestra varias facetas, que no siempre la más visible es la real, y que nos sitúa ante lo que podríamos calificar de un nuevo tipo de guerra híbrida, ese concepto tan actual, pero que en este caso incluye aspectos socioeconómicos, culturales, religiosos y criminales.

Hasta no hace mucho, la tendencia general era la lucha entre los distintos grupos y facciones, agrupados principalmente en torno a Al Qaeda y el DAESH, por captar la atención tanto dentro como fuera del territorio, el ser vistos como actores principales e influyentes en el futuro de la zona con la finalidad de lograr adeptos, apoyos, reclutar combatientes y ganar territorio para demostrar así ante el mundo y “su mundo”, su fuerza y relevancia. Y no cabe duda de que los periodos de

mayor intensidad en sus acciones, tanto en número como en relevancia, hayan venido propiciados por dicha estrategia.

Los grupos adscritos a Al Qaeda, como al-Shabaab, emplean lo que podríamos considerar tácticas terroristas convencionales que incluyen acciones guerrilleras en las zonas de actuación, secuestros, colocación de artefactos explosivos y ataques suicidas. Por el contrario, la "marca" de actuación del DAESH y sus grupos asociados tienen una tendencia mucho más brutal si cabe y se caracterizan por una violencia extrema, que van desde la aplicación extrema de la sharía con su particular forma de castigar las faltas, como las decapitaciones, amputación de miembros y las lapidaciones, al empleo de acciones con el resultado de bajas masivas e indiscriminadas, la opresión sistemática de la mujer incluyendo la esclavitud, tortura, violaciones y desde luego los ataques suicidas.

Así, el gran reto en África es encontrar la forma de contener la rápida y profunda penetración de los grupos afines a ambas organizaciones, que han copado la región con grupos

terroristas afines. Ambos grupos son rivales, y compiten con hacerse con el territorio y el apoyo local, lo cual significa principalmente un mayor acceso a recursos materiales, económicos y de personal, pero tienen en común, aparte de la ideología y su objetivo final, el uso del terror como estrategia de movilización.

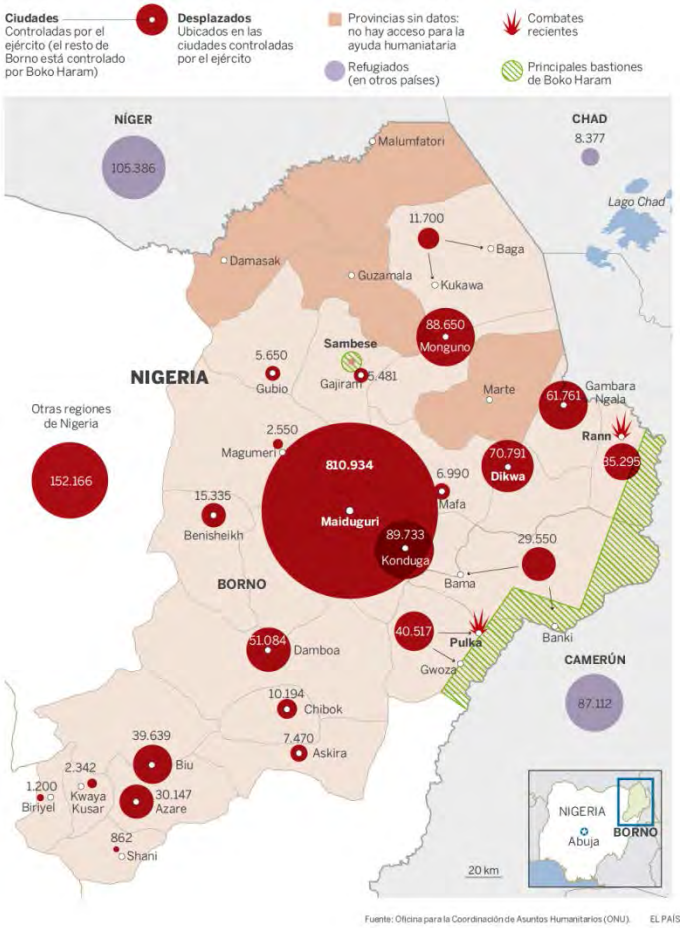
Pero, mientras que esa creciente rivalidad ha representado hasta ahora un importante desafío a la seguridad, la situación actual ha tomado una deriva que nos pone ante la que puede ser un reto aún mayor para la situación de seguridad en África y que tiene evidentes repercusiones en lo que se refiera a la seguridad de Europa. Esta amenaza no es otra que la ya más que evidente tendencia creciente de colaboración entre los diferentes grupos terroristas, sin importar cuál sea su afiliación, en lo que se refiere a reclutamiento de militantes, adiestramiento, financiación y acciones concretas en toda el área del Sahel.

Del mismo modo, y de una manera mucho más rápida de lo que se podría esperar, ya han comenzado a usar modernos sistemas de comunicaciones, redes de campamentos e instructores para el adiestramiento de combatientes, a través de las cuales comparten las tácticas militares aprendidas a lo largo de años de actividad, estrategias de comunicación y publicidad en lo que podríamos considerar a todas luces campañas de lo que se conoce como INFOOPS y métodos para mejorar su financiación y la circulación de sus recursos.

Y el ejemplo más patente de ello lo tenemos en la evolución durante los últimos seis o siete años de las actividades insurgentes de Boko Haram en Nigeria.

2.- ENTENDIENDO BOKO HARAM

Este grupo, el más numeroso y violento de la zona, ha mantenido su actividad durante décadas, pero no fue sino tras su afiliación a la marca de Al Qaeda en el Sahel, AQMI, en 2010, impulsada por su líder Abubakar Sheaku, cuando experimentó un claro crecimiento y mejora de su financiación y en el adiestramiento de sus miembros.



Pero en 2015 el grupo cambió de referencia, seguramente empujado por los éxitos del DAESH en Siria e Irak y la implantación efectiva del califato, viendo en ello una oportunidad de seguir creciendo, y prestó juramento de fidelidad al DAESH. Ello se tradujo inmediatamente en un cambio de estrategia y comenzó a llevar a cabo ataques brutales e indiscriminados en lugares como mercados y mezquitas contra aquellos que no profesaban la corriente sunnita del islam. A estos se añadieron acciones más allá de las fronteras de su país de origen, golpeando en países vecinos como Chad y Niger, aprovechando de ese modo sus conexiones con grupos de la zona y buscando la expansión del califato en el oeste del continente africano. De nuevo se materializaba así la teoría del "ink spot".

El caso de BH es seguramente el más claro ejemplo de cómo los grupos terroristas islamistas del Sahel comienzan a explotar sus lazos con las dos principales "franquicias" del terror. En su caso, para alcanzar sus objetivos en Nigeria. Pero no podemos obviar que esta comienza a ser la tendencia y que puede convertirse o podría estar convirtiéndose en el modo común de actuación en la zona, algo que tiene visos de ser la práctica común en el futuro más inmediato, materializando así la hipótesis de la opción más peligrosa en la evolución del terrorismo yihadista.

La realidad es que Nigeria ocupa a día de hoy el tercer puesto en el ranking de los países en lo que al número de ataques terroristas se refiere, sólo superado por Irak y Afganistán. Y para poder comprender el fenómeno en toda su extensión y el alcance de la amenaza, vamos a hacer un breve recorrido por la historia del grupo más numeroso, carismático y con más

potencial de la zona.

El nombre oficial de Boko Haram es Jama'atu Ahlus-Sunnah Lidda'Awati Wal Jihad, que significa "El pueblo dedicado a la propagación de las enseñanzas del profeta y la Yihad". Pero en el mundo se le conoce con su nombre reducido, Boko Haram, que significa en legua Hausa "La educación occidental es pecado". Este nombre fue el que le dio la población de Maiduguri, capital del estado de Borno, en el norte de Nigeria, en el cual se originó el grupo. Su objetivo es la creación de un Estado islámico donde sea la ley islámica o sharía la que regule la vida de sus habitantes, eliminando cualquier reminiscencia de influencia occidental, lo que desde luego no es lo que podríamos considerar un planteamiento original dentro de los grupos del mismo corte.

Su principal postulado es renegar de un país que consideran gobernado por infieles, incluso siendo el presidente del país

musulmán. En sus comienzos, y al contrario de la forma de actuar de al-Qaeda y sus franquicias, BH focalizó su actividad en Nigeria y en los países limítrofes Y ello, a pesar de que desde siempre ha mantenido fuertes lazos con otros grupos yihadistas sobre todo en lo que a ideología y apoyo logístico se refiere. Pero Boko Haram se ha ido moldeando a las peculiaridades de esa zona de África, donde se entrecruzan conflictos no solo religiosos, sino tribales, sociales y económicos, algunos de ellos con siglos de historia. Y ese contexto tan especial donde se ha desarrollado el islamismo extremista en Nigeria ha transformado a Boko Haram en lo que es hoy día.

https://www.hindustantimes.com/world-news/boko-haram-leader-abubakar-shekau-wounded-in-air-strike-nigerian-army/story-pbSKjzHeDvlkxJ0Y3ZTchJ.html

Hay dos opiniones encontradas sobre cuándo se puede establecer el comienzo de Boko Haram como grupo insurgente. Hay quien sitúa este momento en 2010, cuando llevó a cabo su

primera acción armada bajo el liderazgo de Abubaker Sheaku. Otra corriente, por el contrario, establece ese punto en el mismo momento de su fundación oficial por Mohamed Yusuf en 2002.

Lo que es un hecho evidente es que el contexto religioso en la zona norte de Nigeria es un factor más que determinante para entender la aparición de Boko Haram. De hecho, este no es el primer grupo yihadista o con una visión extremista del islam que aparece en el país africano.

La historia de Nigeria, y especialmente el norte del país, tiene una larga historia de movimientos islamistas que se remontan a la guerra Santa librada por Sheik Usman Dan Fodio a comienzos del siglo XIX.

La realidad es que desde que el califato de Sokoto cayó en manos de la dominación británica en 1903, la zona en la que este se asentaba, que comprendía parte de lo que hoy es el norte de Nigeria, Niger y el sur de Camerún, ha mostrado siempre una fuerte resistencia entre sus habitantes musulmanes a la adopción de las costumbres y educación occidentales.

Es por ello que, si echamos la vista atrás y hacemos un recorrido por la corta historia de Nigeria como país, la radicalización ideológica ha sido una constante. Antes de que Mohamed Yusuf emergiera como el líder de un grupo conocido como Boko Haram, los estados del norte y este del país como Borno, Yobe y Bauchi ofrecían un campo abonado y fértil para que su ideología radical se afianzara entre sus habitantes.

Los líderes de Boko Haram han demostrado una eficiente habilidad para manipular a una población ya de por sí radicalizada, sembrando su propia ideología para reclutar y transformar grupos socio-religiosos ya existentes en militantes violentos. Este hecho, la presencia previa de dichos grupos, fue la pieza clave sin la que Mohamed Yusuf no habría podido atraer a una cantidad tan significativa de seguidores en un periodo tan corto de tiempo. Una vez más vemos como las condiciones sociales y económicas adecuadas son la clave para el arraigo de la ideología radical yihadista, llevando a los habitantes de esas zonas a cruzar la línea que separa la radicalización de la violencia.

Pero esas depauperadas condiciones continúan presentes en el norte del país. Nigeria es un país totalmente polarizado en cuanto a la situación social, económica y religiosa, con un 50% de población de religión musulmana, la mayoría de los cuales pertenecen a la etnia Hausa-Fulani, que precisamente se asienta en la zona norte. Por el contrario, en el sur se concentra la mayor parte de las etnias Yoruba e Igbo, en sus mayores partes cristianos y animistas, significando el 40% de la población.

Ahondando más en las profundas diferencias de la sociedad

nigeriana se constata que el 75% de la población del norte vive en condiciones de pobreza, en muchos casos extrema, en contraste con el 27% de los habitantes del sur que comparten dicha situación. El factor clave para esta situación es el petróleo.

El delta del rio Níger es el pilar en torno al que gira la economía de Nigeria. Más del 80% de los ingresos del país proceden del petróleo. Esto se contrapone a la situación de la economía en el norte, dependiente principalmente de la agricultura y con una total falta de modernización.

Terminando de cerrar la ecuación, y como factor añadido causante también del ascenso de la violencia de Boko Haram, tenemos que señalar la constante marginación política que han sufrido las provincias del norte.

3.- EVOLUCIÓN Y ESCENARIOS

Tras su creación, y durante un primer periodo, los líderes de Boko Haram se centraron en aislar paulatinamente a sus seguidores de la sociedad, estableciendo pequeños asentamientos en torno a sus escuelas coránicas o “madrasas” en las remotas regiones de las provincias de Borno y Yobe. Todo esto sucedió entre 2002 y 2005 aproximadamente. Casi al final de esta fase, se inició lo que diferenció claramente a éste de otros grupos radicales presentes en Nigeria: sus acciones contra la policía.

Para esas fechas, el grupo evolucionó y junto con su crecimiento vino la transformación de éste en un fenómeno urbano. Fue en 2009, tras la operación que llevó a la muerte de su líder, Mohamed Yusuf, a manos de las fuerzas de seguridad nigerianas, y tras un periodo de inactividad que hizo pensar que el grupo estaba neutralizado, cuando resurgió bajo el liderazgo de Abubakar bin Mohamed Shekau.

Hasta ese momento las acciones del grupo se habían centrado en ataques a miembros de las fuerzas de seguridad o elementos como pequeños puestos o chek points, asalto a bancos, iglesias, sacerdotes cristianos y asesinatos selectivos. La mayor parte de ellos consistieron en tiroteos o emplazamiento de motos bomba.

Sin embargo, el cambio más significativo sobrevino con el empleo de terroristas suicidas en sus acciones. Salvo Al Shabaab en Somalia y AQMI (Al Qaeda en el Magreb islámico), ningún otro grupo yihadista en África había empleado dicha técnica hasta ese momento. Y la sofisticación y complejidad de las acciones denotaban la colaboración y asistencia de redes internacionales.

En 2014 sobrevino otro cambio significativo en su modo de actuar, ocupando amplias extensiones de territorio y manteniéndolas en lugar de replegarse tras cada ataque. Y a pesar de la colaboración con Al Qaeda y sus grupos afines, en agosto de ese mismo año, su líder declaró el califato en el territorio bajo su control, estableciendo la ciudad de Gwoza como capital del mismo al tiempo que proclamaba públicamente su lealtad al DAESH, dando la espalda a sus antiguos socios de Al Qaeda. Daesh aceptó esa adhesión dándole el nombre de “Estado Islámico de las provincias de África oeste”, como parte integrante del califato global que estaba tratando de establecer en esos momentos.

El área de actuación de Boko Haram incluye los estados de la frontera noreste de Borno, Yobe y Admawa, internándose en las zonas adyacentes de Camerún, Chad y Niger. La débil situación socioeconómica de la zona, la gran inseguridad, los lazos étnicos, la porosidad de las fronteras y las relaciones con otros grupos islámicos en los países vecinos, han sido aprovechados por el grupo para afianzarse firmemente y facilitar su expansión. Este hecho es una fuente de preocupación para esos países fronterizos, que ven como esa corriente radical islamista se interna en su territorio gracias, entre otros factores ya mencionados, a los lazos étnicos transfronterizos de la etnia

kanuri dominante en la zona y que proporciona refugio a los miembros del grupo terrorista a ambos lados de la frontera.

Un elemento fundamental para cualquier grupo de esta índole es el reclutamiento. La masa de militantes de Boko Haram procede de jóvenes desencantados y desafectos al sistema, jóvenes formados pero desempleados y antiguos “Almajiris”, niños de la calle, niños que en su momento fueron enviados a vivir y estudiar con reconocidos maestros coránicos. Esta es una práctica ancestral y habitual en algunas zonas del norte de Nigeria.

Otra fuente de reclutamiento, esta vez forzoso, la ha encontrado entre los jóvenes y niños que forman parte de los miles de personas que viven en campos de desplazados, que paradójicamente se encuentran en dicha situación a causa de la violencia y el deterioro de las condiciones de vida provocadas por Boko Haram. Los secuestros de niños y niñas se han convertido en algo recurrente, usando a éstas como esclavas sexuales y a ambos como punta de lanza en sus ataques a lo largo de la frontera, frecuentemente como atacantes suicidas. Del mismo modo, también es habitual que se utilice a estos menores para obtener información.

En este capítulo, tenemos un último grupo. Esta vez son jóvenes captados de entre las bandas criminales que se mueven por Niger y Camerún. Grupos de delincuentes empujados a dicho modo de vida por la falta de esperanza, por la imposibilidad de poder ganarse la vida de otra forma. Una vez más vemos como las condiciones de vida y económicas juegan un papel fundamental a la hora de incitar a los habitantes de una zona a abrazar un movimiento radical y

violento no por convicción, sino por necesidad. Una relación que podríamos calificar simbiótica, pero con resultado funesto.

En el caso concreto de Niger, el grupo ha ubicado algunas de sus bases en el sur del país, zona que considera no sólo segura sino una fuente de recursos humanos, llegando a significar para las autoridades del país una amenaza mayor que la de AQMI.

A pesar de los esfuerzos del gobierno nigeriano y de diversas agencias de inteligencia, actualmente no hay una estimación creíble de la entidad real del grupo. Shekau dirige a éste con mano de hierro, eliminando a cualquier posible rival dentro de la organización y no permitiendo a ninguno de sus mandos subalternos ganar la más mínima notoriedad o publicidad, llegando a no permitirles aparecer en ninguno de sus videos.

En lo que se refiere a su organización, Boko Haram opera como un movimiento insurgente al uso o una guerrilla subversiva, dividido en grupos más o menos homogéneos de entre 300 y 500 combatientes. Estos llevan a cabo actos de terrorismo, pero al mismo tiempo luchan por controlar el territorio y establecer su autoridad.

Las fuentes de financiación de la organización son muy diversas y van, desde las aportaciones de particulares, a timos por internet. Y aunque sorprenda, entre las aportaciones particulares encontramos a dirigentes o miembros de la administración de los estados del norte de Nigeria y a empresarios. Otra fuente recurrente es la actividad criminal, cubriendo el espectro que va desde el robo de bancos a la extorsión. Así mismo, su asociación con grupos como AQMI también le ha reportado el apoyo financiero de estos. Y aunque

resulte sorprendente por lo incongruente con su base religiosa, el tráfico de drogas también forma parte del espectro de recursos financieros, aunque no directamente, así como el tráfico ilegal de recursos naturales y el cobro de impuestos en los territorios que ocupa.

Boko Haram controla importantes tramos de la carretera que une Maiduguri, capital del estado de Borno, con el lago Chad, el punto en el que convergen las fronteras de Nigeria, Niger, Chad y Camerún y conocido por ser un nodo principal en las rutas de todo tipo de tráficos ilícitos que se dan en el Sahel. No hay evidencias de la implicación de Boko Haram en dichas actividades ilegales, salvo en lo que se refiere al tráfico de seres humanos, actividad en la que participa vendiendo como esclavas a jóvenes previamente secuestradas en el interior de Nigeria. Pero lo que sí hace al menos es cobrar a los diferentes grupos criminales por atravesar las zonas que domina.

Existe un amplio consenso entre analistas internacionales y expertos a la hora de exponer el enfoque sobre la posible

solución al problema que representa Boko Haram a largo plazo. Y este planteamiento conviene que los gobiernos regionales deben planear y ejecutar lo antes posible estrategias holísticas que mejoren las condiciones socioeconómicas de los más desfavorecidos y las comunidades marginalizadas. El desarrollo de infraestructuras, la revitalización económica, la transparencia y una gobernanza efectiva, así como medidas claras contra la corrupción, deben de ser las prioridades en el marco de esas estrategias. Y el eje central de todo ello debe ser proporcionar a la población más joven de esas zonas acceso a una educación de calidad y a oportunidades de mejora económica mediante el empleo. Pero es evidente, y a nadie se le escapa que, aunque se tuviera la capacidad de desarrollar esas acciones de un modo inmediato, los resultados tardarían en ser palpables, y lo que es igualmente importante, son estrategias que para que funcionen necesitan un nivel de seguridad y normalidad que a día de hoy son poco más que una utopía.

Por lo tanto, esa estrategia holística de medidas para el desarrollo y la gobernanza, encaminada a asegurar la paz, no es algo realista en las circunstancias actuales. Pero tampoco lo es una solución puramente militar para acabar con Boko Haram.

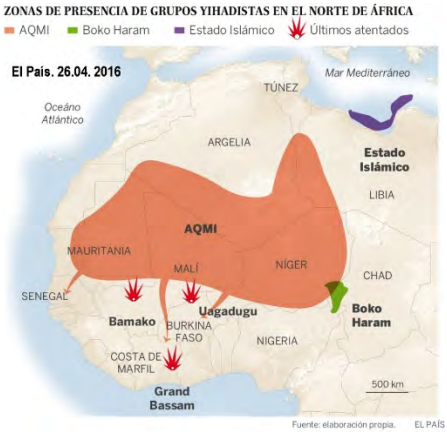
Se pueden identificar tres áreas prioritarias de actuación:

- **Evitar la regeneración de Boko Haram**

  El grupo ha demostrado tener una gran resiliencia. Limitar su capacidad de abastecimiento y de reagruparse utilizando sus redes y rutas de transporte en la región es crítico. Sus

miembros siempre se han movido sin dificultad alguna cruzando libremente las fronteras del norte de Nigeria: hacia Chad, a través del lago Chad y todas sus islas; hacia Níger y hacia Camerún, a través de los frondosos bosques, las zonas montañosas que jalonan gran parte de la misma. Un ejemplo de todo ello es lo sucedido después de la muerte de Mohamed Yusuf, cuando la mayoría de los líderes cruzaron esas porosas fronteras en busca de refugio. Se cree que Abubakar Shekau, durante ese periodo, viajó al norte de Mali, donde se adiestró con el Movimiento para la Unidad y la Yihad en África Oeste (MUJAO). Del mismo modo, otros miembros de BH viajaron a Chad y Níger, donde recibieron adiestramiento en diversos campamentos y se unieron a la lucha yihadista con diferentes grupos en Somalia, Argelia y Afganistán, adquiriendo una experiencia y formación más que notable.

En 2010 todos esos elementos regresaron a Nigeria y el grupo resurgió como un ente mucho más letal y sofisticado. La caída del régimen de Gadafi y el caos posterior significaron otro acicate en esta nueva etapa debido al flujo de armas procedentes de los arsenales libios y de combatientes nigerianos que servían en las fuerzas de seguridad de Gadafi que llegaron a través de las rutas procedentes de Chad.



La expansión del Daesh hacia Libia, después de su derrota en Irak, puede atraer a combatientes de Boko Haram, lo cual en principio puede parecer un respiro o un alivio de la actividad yihadista en la zona del lago Chad. Pero si la presión internacional tiene éxito y logra la derrota del Daesh también en este campo de batalla, estos elementos yihadistas retornarán a sus lugares de origen, mucho más entrenados, con experiencia y más radicalizados en el plano ideológico. Y si esto llega a suceder, la amenaza será de proporciones inimaginables.

- Mantener la presión diplomática para lograr una efectiva cooperación regional:

  Para evitar esa regeneración de Boko Haram, es esencial la cooperación entre Nigeria y sus vecinos para bloquear las rutas logísticas, erradicar los santuarios y los campos de entrenamiento e intercambiar inteligencia relativa al movimiento de los insurgentes y sus fuentes de financiación y abastecimiento. Con esa

finalidad se creó la Mutinational Joint Task Force (MNJTF), compuesta por fuerzas de Benin, Camerún, Chad, Niger y Nigeria. Pero esa fuerza no ha sido efectiva, pues la desconfianza entre Chad y Nigeria, sus diferentes visiones del problema, de la amenaza y sobre las prioridades han obstaculizado su acción. Esto ha dado como resultado que sólo se haya desplegado menos de la mitad de la fuerza prevista inicialmente. La solución a este problema concreto pasa porque elementos clave en la diplomacia internacional como Francia, Estados Unidos, la Unión Africana y Naciones Unidas eleven la presión para lograr esa fundamental cooperación regional y que los esfuerzos estén suficientemente financiados.

- Colaboración para cortar las vías de financiación de Boko Haram:

  Tan importante como acabar con el flujo físico de dinero y de combatientes es lograr un control efectivo y el posterior bloqueo a nivel internacional de las fuentes de financiación del grupo, tanto dentro de Nigeria como fuera del país.

- Favorecer la desmovilización de combatientes de Boko Haram:

  Una acción fundamental para debilitar a Boko Haram y socavar su capacidad de regeneración es establecer procesos de reintegración similares a los que ya se utilizaron en Afganistán y que hagan atractivo a sus miembros la opción de la entrega de las armas y

rendición. Los componentes del grupo no son una masa homogénea, y entre ellos se encuentran desde verdaderos yihadistas muy radicalizados a simples criminales oportunistas, adultos y niños, muchos reclutados por la fuerza, otros secuestrados y adoctrinados con posterioridad. Algunos se han unido buscando beneficio económico o simplemente como un empleo más. Muchos de ellos, sea cual sea su origen, se sienten atrapados en la organización. Incluso algunos de los que fueron forzados a unirse a ésta se sienten incapaces de volver a sus lugares de origen por la incertidumbre que rodea a ese posible regreso y con miedo a ser ejecutados si se entregan. Para una gran mayoría su visión del futuro permanece dentro de Boko Haram o huyendo a Libia llegado el caso como única opción.

Nigeria ha tratado de implementar un programa de reeducación y desradicalización en las prisiones, pero este está pobremente financiado y apoyado. Por ello, la potenciación de estos programas e incluso la implicación en los mismos de actores externos, es un paso clave en la derrota de la banda. Dichos programas también sería interesante implementarlos en Chad, Niger y Camerún para lograr una eficacia mayor, pues como se ha repetido en varias ocasiones el problema y la amenaza de Boko Haram es transnacional, y la solución debe tener el mismo carácter.

- **Aumentar las capacidades de protección civil y bienestar social**

La población del noreste de Nigeria y de la región del lago Chad es extremadamente vulnerable a los ataques de Boko Haram y a las privaciones e incertidumbre fruto del desplazamiento y abandono de sus pueblos y aldeas. Por ello, tantos las autoridades civiles como las fuerzas de seguridad tienen que priorizar la protección de esas comunidades y recuperar su confianza tras décadas de marginación. Ello requiere un cambio radical en su mentalidad, así como mejorar la capacidad de proporcionar no sólo seguridad, sino todo tipo de servicios comunitarios.

- Mejorar las capacidades y profesionalización de las fuerzas de seguridad:

  Prevenir y responder a los ataques de una fuerza insurgente, en un conflicto asimétrico a lo largo de un vasto territorio escasamente poblado y localizar unas células cada vez más fragmentadas es una tarea muy difícil y complicada. Para poder llevarla a cabo, las fuerzas de seguridad necesitan un equipamiento adecuado, así como elementos de obtención de información y transmisión de esta que les permita difundir la inteligencia que se obtenga en tiempo real, desplegar las unidades en tiempo oportuno y neutralizar los objetivos adquiridos con la mayor precisión. Esto sólo puede lograrse con la participación de mentores de terceros países que se involucren en esta lucha adiestrando a las fuerzas de seguridad, transformándolas en unas fuerzas capaces de afrontar las amenazas actuales.

  Desde la intensificación de las acciones de Boko Haram

en 2011, las fuerzas armadas nigerianas, mal entrenadas, pobremente equipadas y sobrepasadas por una amenaza sin precedentes hasta el momento para ellas, han sido responsables de abusos y un uso desproporcionado de la fuerza. Esto ha hecho que las relaciones con aquellos países involucrados en la ayuda a Nigeria no siempre hayan sido fluidas. No obstante, cuanto mejor adiestradas y equipadas estén las fuerzas de seguridad, menos casos de abusos se presentarán, como queda constatado por los hechos.

- Apoyo a los desplazados y a las víctimas:

  Las acciones de Boko Haram han provocado el desplazamiento de más de tres millones de personas en la región del lago Chad, la mayoría de estos dentro de Nigeria. Pero también son significativas las cifras en Camerún y Níger. Sólo una pequeña parte vive en campos construidos por el gobierno; el resto lo hace en

campamentos establecidos improvisadamente o acogidos en otras comunidades. Pero unos y otros, mientras la situación de violencia e inseguridad persistan, necesitan ayuda. La malnutrición infantil es una lacra permanente en los campos, provocando cifras de mortalidad alarmantes.

La esperanza de retorno a sus lugares de origen es casi inexistente, bien sea porque sus aldeas o pueblos han sido sencillamente destruidas o por el miedo a volver a ser atacados.

La comunidad internacional junto con los gobiernos de los países afectados debe volcarse en proporcionar no solo ayuda material, sino educación a esos niños y jóvenes atrapados en un limbo de incertidumbre, pues de lo contrario, la semilla de la desesperanza, clave para que surjan grupos de este tipo, se habrá sembrado de nuevo en un círculo vicioso sin fin.

- Mejorar la comunicación estratégica y la interacción con las comunidades locales:

  La comunicación, intercambio de información y colaboración entre las fuerzas de seguridad y las diferentes comunidades es de vital importancia frente a la amenaza asimétrica que significa Boko Haram. Crear un clima de confianza con comunidades que nunca han recibido apoyo alguno o ayuda de ningún tipo por parte del gobierno es un proceso largo, pero sentar las bases para esa confianza y avanzar en esa línea debe ser otra de las prioridades. Pero tan importante como tomar

esas medidas es difundir estas, por lo que una efectiva y completa campaña INFOOPS debe diseñarse e implementarse para que todos los afectados tengan conocimiento de los avances.

- **Considerar las alianzas y rivalidades entre grupos yihadistas**

Es fundamental considerar a Boko Haram, no sólo dentro del contexto local, sino como un fenómeno regional e incluso global. La región del Sahel corre el riesgo de convertirse en el campo de batalla que utilicen rivales ideológicos y geopolíticos que trascienden dicha región para dirimir sus conflictos.

La rivalidad entre Al Qaeda y Daesh, chiitas y sunnitas, incluso entre Arabia Saudí e Irán, podrían ser los catalizadores que fomenten la lucha entre grupos yihadistas en la zona.

Tanto Boko Haram como otros grupos yihadistas tienen una dilatada trayectoria de oportunismo. Las disputas internas sobre ideología, estrategia, liderazgo dentro de cada grupo y entre ellos, así como la lucha por la primacía, los recursos humanos y las fuentes de financiación, han provocado un continuo cambio de alianzas, uniones y rivalidades entre ellos.

La competencia entre Al Qaeda y el Daesh ha llevado en los últimos años los niveles de esa lucha entre grupos yihadistas a cotas muy elevadas. Desde el juramento de fidelidad de Boko Haram al Daesh, los grupos afiliados a Al Qaeda como AQMI, MUJAO, al Mourabitoum, etc han

redoblado su actividad en un intento de ganar notoriedad y recuperar la prevalencia sobre Boko Haram. Esta competencia ha resultado trágica en términos de acciones violentas y número de víctimas. Y a pesar de que ha derivado en acciones directas por parte de Boko Haram como grupo de inspiración sunní contra la mayor organización chiita de Nigeria, el Movimiento Islámico de Nigeria (IMN) y las complejas dinámicas ya reseñadas, podrían derivar en un escenario más preocupante aún si cabe y resultar en una amenaza incluso más grave para la estabilidad en toda la región que afectaría seriamente a Europa.

Este escenario no es otro que la colaboración o cooperación entre todos los grupos que actúan en el Sahel, algo que a priori puede parecer un imposible, si se tiene en cuenta la situación actual del extremismo islamista y las complejas dinámicas que hemos mencionado, y añadimos el interés común de todos los grupos en mantener el control de una zona por la que pasan todos los tráficos ilícitos que desembocan en Europa con el beneficio que ello supone, entonces comienza a parecer una situación más que factible.

Para valorar esta posibilidad hay que tener en cuenta la especial idiosincrasia de los grupos que tradicionalmente han actuado en dicho contexto. No importa a que imagen o motivación recurran para justificar sus acciones y "venderse" de cara a su "público". Si ahondamos un poco, siempre en todos encontramos un denominador común: el control de las rutas de tráfico de drogas, armas y seres humanos. Evidentemente hay alguna excepción, pero son

los menos.

Si nos detenemos en el Daesh, con la pérdida del control del territorio en Siria e Irak, ha perdido la mayor parte de sus fuentes de financiación, y lo convulso de la situación en Libia no le permite asentarse del mismo modo en que lo hizo en los dos países mencionados, por lo que su mejor opción para subsistir y volver a obtener recursos de todo tipo es adentrarse en el Sahel, territorio controlado en su mayor parte por AQMI. Siendo pragmáticos, una lucha no le conviene a ninguna de las dos facciones, y en cambio, si no la unión, la colaboración beneficiaría a ambos.

No obstante, es cuestión de tiempo la irrupción de un líder que vea más claramente los beneficios que esa unión de facto les reportaría. De tal modo que al igual que en su día las diferentes bandas de narcotraficantes, primero en Colombia y después en Méjico se organizaron y unieron en "cárteles" bajo una sola dirección, los grupos yihadistas del Sahel tomen su ejemplo y se unan en una suerte de "cooperativa" o "cártel" islamista. Todo es cuestión de que la persona con el ascendiente adecuado lo vea con claridad.

Si se permite que eso suceda entonces la amenaza a Europa será mucho más grave de lo que ya lo es.

4.- CONCLUSIÓN

Hemos de desterrar la idea de una victoria rápida y decisiva en la larga lucha contra Boko Haram.

Su evolución hasta convertirse en un grupo violento radical es

el resultado de un complejo entramado de dinámicas socioeconómicas y políticas en Nigeria, así como de la colaboración y apoyo de factores externos, particularmente sus lazos con otros grupos que operan en la zona del Sahel, principalmente en los aspectos ideológicos y apoyo logístico.

El resurgimiento del grupo en 2010 significó el inicio de una espiral de violencia muy significativa, llevando a cabo todo tipo de acciones a cuál más brutal, tanto en Nigeria como en los países vecinos. Pero a pesar de los progresos alcanzados por las fuerzas de seguridad nigerianas, que han sido capaces de desalojar al grupo de alguna de sus plazas fuertes, éste aun ha sido capaz de llevar a cabo acciones exitosas, debido a su carácter transnacional, Boko Haram significa una seria amenaza no solo para Nigeria, sino para toda la región y para la comunidad internacional, pues su capacidad es aún muy alta, sus miembros muy numerosos y su grado de adiestramiento y radicalización muy significativo. Y ello significa que puede desestabilizar una zona fundamental en clave geoestratégica para Europa y especialmente para España.

Hasta el momento, y salvo algunos avances puntuales o momentáneos, la lucha contra Boko Haram no ha dado los frutos deseados, y no se puede decir que su fin esté cerca.

El fracaso de todas las acciones llevadas a cabo hasta el momento puede explicarse por:

- Una patente falta de información/inteligencia sobre las actividades del Boko Haram, debido fundamentalmente a unos servicios de inteligencia poco formados y peor equipados.

- La politización del discurso sobre el extremismo violento y sus causas, lo cual hace que los líderes musulmanes y cristianos del noreste tengan serias diferencias sobre cómo afrontar el problema. Lo que domina el discurso a nivel nacional sobre la forma de actuar es precisamente eso, la falta de unidad.

- La violación de los derechos humanos por parte de unas fuerzas de seguridad que no distinguen en muchas ocasiones entre combatientes y civiles inocentes, fruto de su falta de preparación, formación y por supuesto de la enorme tensión a la que se ven expuestos sus miembros.

- La falta de implementación de medidas no coercitivas en el plano social, económico, político y de desarrollo.

A la hora de hacer frente a esta amenaza hay que tener en cuenta varios factores para que la respuesta sea verdaderamente efectiva:

- Las acciones en el campo de la seguridad, para que sean eficaces, deben estar perfectamente articuladas, coordinadas y medidas.

- Las políticas que se llevan a cabo en la región deben cambiar radicalmente, alcanzándose una plena cooperación entre la administración federal y del estado, en lugar de actuar la una contra la otra, definiendo una agenda precisa con las acciones que han de llevarse a cabo para corregir las graves deficiencias existentes. Al tiempo, esas medidas deben ser difundidas y publicitadas de tal modo que la

población sea consciente de esa colaboración y pueda constatar cada pequeño paso que se de en la buena dirección. El objetivo debe ser ofrecer esperanza a aquellos que actualmente ven como única salida enrolarse en Boko Haram no sólo porque es el "único trabajo" al que se puede optar, sino porque es el único referente de protección y desarrollo que existe en la zona

- Todas las acciones que se lleven a cabo, pero especialmente en el campo policial o militar deben enfocarse como contrainsurgencia, evitando ofrecer la imagen de una guerra contra una etnia o religión determinada, pues esa será la herramienta que usará Boko Haram para lograr apoyos, nuevos miembros y colaboración de todo tipo de otros grupos yihadistas. No hay mayor banderín de enganche que el victimismo, y esa es una de las partes de la ecuación que hay que controlar si se quiere tener éxito.

- La implementación de medidas de prevención contra la radicalización es otro factor fundamental. Para ello es crucial entender las raíces de este fenómeno en Nigeria. Hay que identificar los factores diferenciales con otras zonas para aplicar las medidas adecuadas. Si bien es cierto que hay unos factores comunes en todo proceso de radicalización, también lo es que este fenómeno presenta diferencias o rasgos diferenciales propios de cada lugar en el que aflora. Saber definir esos factores es clave.

En definitiva, hay que tratar de ver el problema a través

de los ojos de Boko Haram y de sus miembros, conocer sus motivaciones y construir una “contranarrativa”, no sólo en el campo de los hechos, sino ideológica que desmovilice a sus integrantes. Hay que tener presente que la ideología radical en sí misma no supone ningún problema, pero se convierte en una amenaza cuando ciudadanos, residentes o grupos organizados abogan por el uso de la violencia o la usan para imponer su visión política, su ideología o su religión. Cada actuación en el campo político, militar, de desarrollo, etc, tiene que estar reflejada en una minuciosa campaña de lo que llamamos INFOOPS para darles la apropiada visibilidad y contribuir al objetivo común. Actuar en los diferentes campos de modo aislado condena cada iniciativa al fracaso desde su inicio, y contribuye a la continuidad del caos en el noreste de Nigeria.

Almería, 27 de enero de 2019

BIBLIOGRAFÍA

- James Adewunmi Falode. *“THE NATURE OF NIGERIA´S BOKO HARAM WAR 2010-2015: A STRONG ANALYSIS”.* Perspectives on Terrorism Vol 10, Issue 1. Feb 2016

- Urko del Campo Arnaudas. *“BOKO HARAM Y LA PROLIFERACIÓN DEL ISLAMISMO YIHADISTA EN NIGERIA COMO AMENAZA PARA LA SEGURIDAD EN EL SAHEL”*. Campus Internacional para la Seguridad y la Defensa.

- Dr. Nivedita Ray. *“GROWING THREAT OF*

TERRORISM IN AFRICA: THE CASE OF BOKO HARAM". Indian Council of World Affairs. Feb 2016

- Jennifer G. Cooke. *"BOKO HARAM: THE ISLAMIST INSURGENCY IN WEST AFRICA"*. Center for Strategic and International Studies (CSIS). Feb 2016

“El Servicio esencial del agua y el terrorismo”[23]

AUTOR: Rafael Vidal Delgado, Coronel de Artª, Diplomado de Estado Mayor, de Estados Mayores Conjuntos e Inteligencia Militar Conjunta; Dr. en Geografía e Historia por la Universidad de Granada; Master Ejecutivo en Dirección de Servicios de Emergencias y en Dirección de Seguridad Global y profesor en ambos Master.

PREÁMBULO E INTENCIONES

El 7 de julio de 2016, el Foro para la Paz en el Mediterráneo, organizó en conjunción con la Asociación de Abastecimiento de Aguas y Saneamiento de Andalucía (ASA) y en colaboración con otras entidades, entre ellas AMASPLUS INGENIERÍA, una de las entidades constitutivas del Foro; del Centro Nacional para la Protección de las Infraestructuras Críticas del Ministerio del Interior y 4ª Zona de la Guardia Civil de la Comunidad Autónoma de Andalucía y otras empresas, una jornada informativa, con el objeto de concienciar a las empresas de agua de la necesidad de proteger su actividad de abastecimiento, suministro, saneamiento, depuración y reutilización del bien esencial del agua, asistiendo a dicho llamamiento numerosos directivos y

[23] El 14 de mayo de 2019, el autor dictó esta ponencia en las X Jornadas del Ciclo Integral del Agua, organizado en Baeza (Jaén), por la Universidad Internacional de Andalucía y la Diputación de la Provincia.

técnicos de las diferentes empresas públicas y privadas relacionadas con el agua en Andalucía.

La ponencia inaugural fue impartida por el autor del presente trabajo, el cual entre sus palabras recalcaba:

Es importante señalar que cuando se habla de TITULAR, se está hablando de la cúpula directiva de la empresa, es decir de su Presidente y de su Consejo de Administración, junto con Consejero Delegado, etc. Personas físicas, que, en caso de dejación de sus funciones como titulares de un servicio esencial,

les puede acarrear sanciones civiles, administrativas e incluso penales.

Este aserto fue comentado, por algunos de los asistentes, y consultado, posteriormente, con sus servicios jurídicos, los cuales asesoraron a su director o gerente, en el sentido, que en la Ley de Infraestructuras Críticas no se incluía ningún tipo de infracción, por lo su inobservancia no conllevaba sanciones administrativas ni de otro tipo, exponiendo como ejemplo, la Ley Orgánica de Protección de Datos de Carácter Personal que sí lo hacía.

Inauguración de la Jornada.
De izda. a dcha: Carlos Garcia del Rio (CNPIC),
TCOL André López Garcia (Zona Guardia Civil),
Pedro Rodriguez, presidente de ASA y Director Gerente de ALJARAFESA
y Rafael Vidal, director del Foro

Posteriormente se programó para octubre/noviembre del mismo año, una nueva jornada a celebrar en Granada, invitándose al director del Foro a pronunciar la ponencia inaugural, la cual versaría sobre la coercitividad de la Ley 8/2011 y de su Reglamento. La jornada iba a ser organizada conjuntamente por la Universidad de Granada y el Mando de Adiestramiento y

Doctrina, con sede en dicha ciudad, pero por circunstancias diversas, la jornada no pudo celebrarse, quedando el problema en el ambiente del sector del agua.

En 2017, impulsado por el Foro para la Paz en el Mediterráneo, la Asociación de Abastecimiento y Saneamiento de Aguas de Andalucía (ASA-Andalucía) y la Universidad Internacional de Andalucía (UNIA), se ha programado para el 25 de enero de 2018 un Seminario Académico, con expertos en las diversas materias a tratar, siendo objeto de ello la presente ponencia.

En los últimos 15 años, desde que se produjeron los atentados contra las Torres Gemelas. Norteamérica diseñó su Homeland Security, estableciendo los sectores estratégicos que había que proteger a ultranza. La Unión Europea ha ido a remolque de los acontecimientos.

En el año 2004, tras el atentado del 11 de marzo en España, la Unión Europea comprendió que el terrorismo yihadista era una amenaza que se debía tener muy en cuenta y debido a ello, el Consejo Europea en su reunión de junio de 2004, solicitó de la Comisión y del Alto Representante, en aquel momento Javier Solana, que prepararan una estrategia global contra el terrorismo.

COMUNICACIÓN DE LA COMISIÓN AL CONSEJO Y AL PARLAMENTO EUROPEA COM (2004) 702 FINAL DE 20.10.2004

Como resultado del encargo, la Comisión presentó una Comunicación con fecha 20 de octubre, en la cual se definía por

primera vez el concepto de Infraestructura Crítica (IC), el cual ha permanecido casi inalterable a lo largo de los años, efectuándosele exclusivamente ligeros matices:

Definición:

Las infraestructuras críticas son aquellas instalaciones, redes, servicios y equipos físicos y de tecnología de la información cuya interrupción o destrucción tendría un impacto mayor en la salud, la seguridad o el bienestar económico de los ciudadanos o en el eficaz funcionamiento de los gobiernos de los Estados miembros. Las infraestructuras críticas están presentes en numerosos sectores de la economía: actividades bancarias y financieras, transporte y distribución, energía, servicios, salud, abastecimiento de alimentos, comunicaciones, administraciones públicas clave.

Relacionaba los llamados posteriormente “Sectores Críticos”, encontrándose entre ellos:

Agua (por ejemplo, embalses, almacenamiento, tratamiento, redes).

Dentro de la brevedad de la Comunicación, marcó las directrices que iban a desarrollarse en el transcurrir de los años, tanto por la Unión Europea (UE) como por los países miembros.

Un aspecto importante de la Comunicación fue establecer los criterios para declarar que una infraestructura de un estado tuviera que conceptuarse como crítica.

Criterios:

- *Alcance - la pérdida de un elemento de infraestructura crítico se mide por el tamaño del área geográfica que pudiera verse afectada por su pérdida o indisponibilidad, internacional, nacional, provincial, territorial o local.*
- *Magnitud - el grado del impacto o de la pérdida puede evaluarse como nulo, mínimo, moderado o principal. Entre los criterios que podrían utilizarse para evaluar la magnitud potencial se encuentran los siguientes:*
  a) *Impacto público (cantidad de población afectada, pérdidas de vidas, enfermedades, lesiones graves, evacuación);*
  b) *Económico (efecto PIB, volumen de pérdida económica y/o degradación de productos o servicios);*
  c) *Ambiental (impacto en el lugar y sus alrededores);*

d) *Interdependencia (con otros elementos de infraestructura críticos).*
e) *Político (confianza en la capacidad de las administraciones públicas);*

- *<u>Efectos en el tiempo</u> - estos criterios determinan en qué plazo la pérdida de un elemento podría tener un impacto importante (inmediato, 24-48 horas, una semana, otros).*

Estos criterios se han mantenido a lo largo de los años. La normativa española añade un criterio nuevo, el de "redundancia", es decir cuando el problema de abastecimiento de agua no puede paliarse por otros medios.

Fuerteventura, durante muchos años y en temporada estival (década de los sesenta-setenta), se abastecía de buques aljibes de la Armada Española. Más recientemente, la ciudad de Ceuta, ante la avería de una Desaladora, se estuvo abasteciendo de agua desde la cercana Algeciras, con buques que transportaban más de ocho mil metros cúbicos de agua. También han sido abastecidas de agua potable, a través del mar, las ciudades de Barcelona, Tarragona y Cádiz, bien que no en la totalidad de sus necesidades.

También en el transcurso de los años se han abastecido a diversas poblaciones, como en el verano de 1986 a los municipios de la Costa del Sol, a base de camiones aljibes. Con este sistema no se cubrían todas las necesidades, sino de forma mínima y ante una avería en el sistema de abastecimiento de agua.

Con ello se quiere hacer ver que en el estudio y análisis de los "medios" disponibles, se deberá contar con estos medios adicionales.

Gestión compartida

La gestión de la seguridad de una IC, según la Comunicación, es responsabilidad del estado miembro, pero debido a que es imposible para las capacidades de los estados atender todas las vulnerabilidades, se recomienda que exista una "gestión compartida":

La protección de infraestructuras críticas (PIC) requiere un partenariado firme y cooperativo entre los propietarios y gestores de infraestructuras críticas y las autoridades de los Estados miembros. La responsabilidad principal de la gestión del riesgo en las instalaciones físicas, cadenas de suministro, tecnologías de la información y redes de comunicaciones corresponde a sus propietarios y gestores.

La responsabilidad compartida es recurrente en toda la normativa actual de seguridad, tanto europea, como la más reciente de seguridad nacional española.

Habría que preguntarse si una de las partes no asume su cuota de responsabilidad, estaría infringiendo la ley y por tanto podría ser sancionado administrativa e incluso penalmente, en este caso a los gestores de las infraestructuras hidráulicas por dejación de sus funciones

LIBRO VERDE [24] SOBRE EL PROGRAMA EUROPEA PARA LA PROTECCIÓN DE LAS IC. COM (2005) 576 FINAL DE 17.11.2005

En julio de 2005 se produce el atentado en el metro de Londres, pareciendo que, en aquellos primeros años, el Gobierno de la UE, se moviera a impulsos de estos ataques terroristas yihadistas.

El Objetivo del documento, presentado por la Comisión al Consejo, era establecer un Programa Europeo de Protección de Infraestructuras Críticas (PEPIC), con la colaboración de todas las partes interesadas, no solamente los estados miembros, sino incluso empresas y otras organizaciones.

Niveles de protección

Como tal libro verde, se plantea como un marco de reflexión, y de esta forma se exponen las amenazas posibles sobre las que debe precaverse el PEPIC:

1. Frente a todos los peligros, constituyéndose una amalgama entre terrorismo, catástrofes naturales, sabotajes, etc.
2. Similar al anterior, pero fijando como línea prioritaria la amenaza terrorista.

[24] Los Libros Verdes son documentos publicados por la Comisión Europea cuyo objetivo es estimular una reflexión a nivel europeo sobre un tema concreto. En ellos se invita a las partes interesadas (organismos y particulares) a participar en un proceso de consulta y debate sobre las propuestas que presentan.

3. Centrarse exclusivamente en la amenaza terrorista.

A la postre, el Programa Europea, se ha centrado en la tercera opción, aunque con el matiz, de que debe estar perfectamente coordinado con el resto de las amenazas a las IC, bien sea por causas antrópicas o naturales.

Principios

Aunque la UE es muy dada a establecer un buen número de principios, en este caso, se marcó únicamente cinco:

- **Subsidiariedad:** el principio de subsidiariedad estaría en el núcleo mismo del PEPIC; la protección de las infraestructuras críticas sería, ante todo, responsabilidad nacional. Las responsabilidades primordiales en cuanto a protección de estructuras críticas incumbirían a los Estados miembros y a los propietarios/ operadores, actuando bajo un marco común.
- **Complementariedad**: el marco común del PEPIC sería complementario con respecto a medidas ya vigentes.
- **Confidencialidad**: el intercambio de información sobre protección de infraestructuras críticas tendría lugar en un entorno de confianza y confidencialidad.
- **Cooperación de los agentes interesados**: todos los agentes interesados, incluidos los Estados miembros, la Comisión, las asociaciones sectoriales o profesionales, los organismos de normalización y los propietarios, operadores y usuarios (entendiéndose por «usuarios» las organizaciones que explotan y utilizan la

infraestructura para fines comerciales y de prestación de servicios) deben desempeñar un papel en la protección de las infraestructuras críticas.

- **Proporcionalidad**: las estrategias y medidas de protección serían proporcionales al grado de riesgo en cuestión, pues no todas las infraestructuras pueden protegerse frente a todas las amenazas

De estos principios se deducen dos actores primordiales:

1. Estado.
2. Operador Crítico.

Pero al mismo tiempo, se recomienda en este Libro Verde:

a) La necesidad de aprovechar los medios existentes, es decir que la seguridad que ya se dispone debe ser complementada.
b) Los agentes interesados, es decir las empresas, deben actuar, no por "imperativo legal", sino por propia convicción de la necesidad de su seguridad.
c) La proporcionalidad es necesaria, este principio va unido a un eficaz análisis de riesgos, de tal forma que no deben ser los mismos medios lo que deban de instalarse en un depósito de agua que se encuentra en lo alto de un cerro, a otro que está en el centro de un núcleo urbano, sin embargo, desgraciadamente, bastantes empresas, instalan las mismas medidas de protección en ambos depósitos, lo cual es un despilfarro económico.

En España nos movemos por “imperativos legales”, dado que no existe una “cultura” de seguridad [25].

Tal vez, la UE, debería de haber incidido en otro principio: el de la “economía de medios”, por la seguridad y las medidas a instalar, deben ser las suficientes, ni más ni menos.

El papel de los operadores críticos

Ya en el Libro Verde se señalan las responsabilidades de los operadores críticos, entre ellos, la designación de uno o varios funcionarios de enlace para la seguridad, entre el operador y la autoridad competente del estado miembro; el diseño, ejecución y actualización de un Plan de seguridad del operador y ***la participación en la elaboración de un plan de intervención*** *relativo a las infraestructuras críticas, conjuntamente con las autoridades competentes en materia de* ***protección civil de los Estados miembros****, así como las* ***autoridades represivas***.

Esta última responsabilidad se ha transcrito de forma textual, dada su referencia explícita a la Protección Civil y a las Fuerzas y Cuerpos de Seguridad. Posteriormente, en el desarrollo de la IC en España, y tras la aprobación en fechas recientes de la Ley

[25] Desde finales de la década de los ochenta he actuado como consultor-asesor de numerosas entidades públicas y privadas, y casi siempre los gestores de las mismas han querido circunscribirse únicamente a lo que se marca en la normativa “para que no me multen o no tenga responsabilidad judicial”. Judicialmente puede argumentarse que una empresa que presta un servicio público, como es el abastecimiento de agua, aunque por su entidad, no haya sido declarada como crítica, en caso de una manipulación del mismo, debido a agentes externos, podría el juez encontrar indicios penales en el gestor de la infraestructura.

que regula el Sistema de Protección Civil en nuestro país, se analizarán las connotaciones existentes.

En el Libro Verde habla de la posibilidad de que el operador crítico, no sea declarado como tal por una autoridad competente del estado miembro, sino que la empresa que tiene a su cargo un servicio esencial, proponga a dicha autoridad, esta declaración, cuestión que no se ha dado en España, en donde se espera que sea catalogada como tal para actuar en consecuencia.

En este sentido, el desarrollo normativo, podría haber seguido una línea similar a la de los “planes de autoprotección”, en donde se fijan unos mínimos, a partir de los cuales todas las actividades (empresas, centros, establecimientos, etc.), que entran dentro de esos mínimos, asumen su propio Plan de Autoprotección, presentándolo a la autoridad competente, como un documento más, para que se le autorice el inicio de la actividad.

Este procedimiento hubiera permitido una mejor concienciación y una progresiva asunción de responsabilidades por parte de las empresas de servicios esenciales, entre ellos el que nos ocupa, que es el de abastecimiento y saneamiento de aguas.

PRIMERAS ACTUACIONES ESPAÑOLAS

El 2 de noviembre de 2007, el Consejo de Ministros aprobó el marco estructural para la protección de las IC en España, basándose en la Comunicación de la Comisión de 2004 y en el Libro Verde.

Se crea el Centro Nacional de Protección de Infraestructuras y Ciberseguridad [26] (CNPIC), dentro de la Secretaría de Estado de Seguridad, debiendo ser custodio del Plan de Seguridad y del Catálogo Nacional.

De forma previa, con fecha 7 de mayo de 2007, el Secretario de Estado de Seguridad, aprobó el Plan Nacional de Protección de IC, creando además un esbozo de instalaciones sensibles contra atentados terroristas.

Define, por primera vez, que son las instalaciones críticas en España:

Son aquellas instalaciones, redes, servicios y equipos físicos y de tecnología de la información cuya interrupción o destrucción pueden tener una repercusión importante en la salud, la seguridad o el bienestar económico de los ciudadanos o en el eficaz funcionamiento de los gobiernos de los Estados miembros.

Se recoge entre las "instalaciones sensibles al agua, los embalses, el almacenamiento, el tratamiento y las redes".

[26] Anteriormente el CNPIC se denominaba al Centro Nacional de Infraestructuras Críticas, pero a raíz del Real Decreto 770/2017, de 28 de julio, por el que se desarrolla la estructura orgánica básica del Ministerio del Interior, se actualizan las funciones de la Secretaría de Estado de Seguridad (SES), asignándose al titular de dicho órgano, entre otras, la de la dirección y coordinación de las políticas de ciberseguridad, reforzándose de esta forma, la lucha contra las amenazas cibernéticas, añadiéndose al anterior CNPIC esta nueva función de seguridad.

También se fijó como una posible instalación sensible, determinados monumentos, que posteriormente no han pasado a la legislación, aunque en la actualidad parece que, desde el Gobierno de la Nación, se pretende tenerlo en cuenta.

DIRECTIVA 2008/114/CE DEL CONSEJO DE 8 DE DICIEMBRE DE 2008, SOBRE LA IDENTIFICACIÓN Y DESIGNACIÓN DE IC EUROPAS Y LA EVALUACIÓN DE LA NECESIDAD DE MEJORAR SU PROTECCIÓN

Un largo período de tiempo había transcurrido para que por fin la UE se decidiera a aprobar una Directiva, la cual tenía que ser obligatoriamente transpuesta a la legislación de todos los países miembros.

Aparte de todos los "considerando", propios de una directiva europea, es interesante remitirse a las definiciones:

«Infraestructura crítica», *el elemento, sistema o parte de este situado en los Estados miembros que es esencial para el mantenimiento de funciones sociales vitales, la salud, la integridad física, la seguridad, y el bienestar social y económico de la población y cuya perturbación o destrucción afectaría gravemente a un Estado miembro al no poder mantener esas funciones.*

«Análisis de riesgos*», el estudio de hipótesis de amenazas posibles, para evaluar las vulnerabilidades y las posibles repercusiones de la perturbación o destrucción de infraestructuras críticas.*

***«Protección»**, todas las actividades destinadas a garantizar la funcionalidad, continuidad e integridad de las infraestructuras críticas con el fin de prevenir, paliar y neutralizar una amenaza, riesgo o vulnerabilidad.*

***«Propietarios u operadores de infraestructuras críticas europeas»**, las entidades responsables de las inversiones en, o del funcionamiento diario de, un elemento, sistema o parte del mismo concreto, designado como ICE con arreglo a la presente Directiva.*

Del conjunto de definiciones, aunque se deberían destacar todas, se han seleccionado estas cuatro, para señalar no solamente lo que es una IC, sino que debemos siempre realizar un análisis de riesgos y de acuerdo con ellos, establecer unas medidas de protección, siendo los responsables los "titulares de la actividad" de que se trata.

No se harán más menciones a la Directiva base de toda la legislación española, precisamente, por la obligatoriedad de asumirla en su totalidad, pudiendo el estado miembro, en este caso, España, como así ha hecho, reforzar determinadas actuaciones y supuestos, dada la experiencia en la lucha y protección contra el terrorismo que desgraciadamente tiene nuestra Patria.

Este prolijo preámbulo sirve exclusivamente para entender que, al menos en el sector del agua, hay mucho recorrido que realizar.

El agua es un bien esencial, pero de la misma manera que es la energía o las telecomunicaciones, sin embargo, pagamos tres y

cuatro veces más por los dos últimos bienes que por los primeros que al contrario de ellos necesita muchas más inversiones en mejoras e instalaciones.

Para poder disfrutar del agua es necesario un tratamiento muy costoso llevado a cabo en las estaciones tratamiento de agua potable y desaladoras, necesita conducciones, depósitos intermedios, controles de la calidad del agua cada cierto recorrido de la misma, para que llegue en la cantidad y calidad suficiente, pero ahí no termina el proceso, sino que las aguas que desechamos y que han sido "ensuciadas" por nosotros, es preciso recogerlas, quitarle los residuos e impulsarlas a unas estaciones de depuración, en parte para que puedan ser reutilizadas para riegos y la sobrante que pueda verterse al mar o a algún río. Todo ello se denomina el "ciclo del agua", mucho más complejo y costoso que el suministro energético o el empleo de las redes de comunicaciones.

Las empresas energéticas y de telecomunicaciones son "rentables" económicamente, mientras que las de agua son "deficitarias" y si en alguna medida obtienen beneficios es a costa de una degradación de las aguas.

Periódicamente se producen graves inundaciones en el sur y levante español a causa de las intensas lluvias, mientras que, en el norte de la Península, acostumbrados a ellas, disponen de "tanques de tormenta" para que el agua de lluvia sea almacenada y no se expanda por el terreno circundante, pero

prácticamente no se dispone de esta obra hidráulica en ninguna de las empresas de aquellos territorios [27].

En las visitas realizadas a los directivos de las empresas públicas de agua, siempre surge el gran problema: "la insuficiencia de medios económicos" para "proteger adecuadamente el bien esencial del agua" y proporcionarla con plena seguridad a los ciudadanos en calidad y cantidad.

En unos cursos de verano de la Universidad de Málaga de hace bastantes años, dicté unas clases relacionadas con las "guerras por el agua" a lo largo de la historia, efectuando una prospección del futuro [28]. El agua es el "oro azul" y no es que "gastemos" más agua de la que necesitamos, sino que la "perdemos" entre los puntos de captación y hasta que llega a nuestras manos, calculándose en los países desarrollados que alrededor del 10% son pérdidas, alcanzando el porcentaje del 30 o 40 % en países africanos, americanos y asiáticos.

BASE LEGAL

Los últimos diez años han sido de intensa labor legislativa en los ministerios de Defensa e Interior, encontrándose en **toda la normativa promulgada un factor común: la de**

[27] EMASESA ha construido en los últimos años tanques de tormenta. En las inundaciones de Málaga de 2016, desde el Foro se advertía de esta necesidad: http://www.uma.es/foroparalapazenelmediterraneo/?p=7287

[28] Se puede consultar el trabajo completo en http://www.belt.es/expertos/HOME2_experto.asp?id=3490

responsabilizar de la seguridad a las distintas administraciones públicas y al sector privado.

Nos encontramos con las siguientes leyes:

a) Ley 9/68, de 5 de abril, Reguladora de los Secretos Oficiales
b) Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal.
c) Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal).
d) Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas (desarrollado por el Real Decreto 704/2011, de 20 de mayo, por el que se aprueba el Reglamento de protección de las infraestructuras críticas).
e) Ley 5/2014, de 4 de abril de 2014, de Seguridad Privada (se encuentra en trámite la elaboración del reglamento de ejecución, calculándose que será aprobado a principios de 2018).
f) Ley Orgánica 4/2015, de 30 de marzo, de Protección de la Seguridad Ciudadana.
g) Ley 17/2015, de 9 de julio, del Sistema Nacional de Protección Civil. Esta Ley se encuentra desarrollada por dos reales decretos, uno por Real Decreto 407/1992, por el que se aprueba la Norma Básica de Protección Civil; y el otro el Real Decreto 393/2007, de 23 de marzo, por el que se aprueba la Norma Básica de Autoprotección de

los centros, establecimientos y dependencias dedicados a actividades que puedan dar origen a situaciones de emergencia, así como las aprobaciones de las distintas Directrices Básica de Planificación ante riesgos especiales. La normativa de protección civil es probable que sea modificada en los próximos años, aunque seguramente para endurecer las medidas de protección.

h) Ley 36/2015, de 28 de septiembre, de Seguridad Nacional. Se encuentra a falta de un desarrollo, tanto reglamentario como de leyes, de acuerdo a lo que se expone en las Disposiciones Finales Segunda y Tercera.

Las cuales afectan plenamente al abastecimiento, distribución, suministro, saneamiento y reutilización del agua, como servicio esencial que es y en buena medida incurso como infraestructura crítica.

Por su parte en la página web del CNPIC se recoge la siguiente normativa que afecta al agua:

- **Orden de 12/03/96 Reglamento Técnico sobre Seguridad de Presas y Embalses.**
- **Directriz Básica Planificación Protección Civil ante el Riesgo de Inundaciones.**
- **Ley 10/2001 Plan Hidrológico Nacional.**
- **R.D. Ley 2/2004 que modifica Plan Hidrológico Nacional.**
- **Ley 11/2005 que modifica Ley 10/2001 Plan Hidrológico Nacional.**

- **R.D. 140/2003 sobre Criterios Sanitarios de la Calidad del Agua de Consumo.**
- **R.D. 1120/2012 que modifica R.D. 40/2003 sobre Criterios Sanitarios de la Calidad del Agua de Consumo.**
- **Libro Blanco del Agua en España.**
- **R.D. Ley 11/1995 Tratamiento de Aguas Residuales Urbanas.**
- **R.D. 509/1996 que desarrolla R.D. Ley 11/1995**.
- **R.D. 2116/1998 que modifica R.D. 509/1996 que desarrolla R.D. Ley 11/1995**.

Con respecto a depósitos:

Referencia b) de la relación anterior.

> En su apartado *2.1 TIPOLOGÍA DE LAS INUNDACIONES OBJETO DE LA DIRECTRIZ, se expone:*
>
> *A los efectos de la presente Directriz se considerarán todas aquellas inundaciones que representen un riesgo para la población y los bienes, produzcan daños en infraestructuras básicas o interrumpan servicios esenciales para la comunidad, y que puedan ser encuadradas en alguno de los tipos siguientes:*
>
> ***c) Inundaciones por rotura o la operación incorrecta de obras de infraestructura hidráulica***
>
> Un depósito de agua, es una obra de infraestructura hidráulica, por lo que queda afectado por la Directriz Básica.

RÉGIMEN SANCIONADOR DE LAS LEYES

Las leyes de Seguridad Nacional y de Infraestructuras Críticas no contemplan sanciones por su inobservancia, ¿quiere decir con ello que el infractor queda impune?

El poder sancionador del Estado se encuentra sujeto a los límites que emanan del artículo 25.1 de la Constitución Española, que incorpora una doble garantía: una formal y la otra, material. La primera exige que sea una ley, la que tipifique las conductas sancionables y las sanciones aplicables. La material, reclama que la ley describa directamente con claridad y precisión aquellas conductas.

En las anteriormente citadas leyes no existe ningún título de su articulado dedicado a sanciones y/o infracciones, fallos incomprensibles en leyes que quieren preservar la normalidad de la vida ciudadana contra cualquier ataque del exterior, incluyendo a la acción terrorista.

Si la Ley de Infraestructuras Críticas se encuentra plenamente desarrollada, no así la de Seguridad Nacional, la cual en sus disposiciones finales se recoge:

Disposición final segunda. Desarrollo reglamentario

> *Se faculta al Gobierno y a los titulares de los departamentos ministeriales, en el ámbito de sus respectivas competencias, para dictar cuantas disposiciones sean necesarias para la ejecución y desarrollo de lo establecido en esta ley.*

Disposición final tercera. Mandato legislativo

> *El Gobierno, en el plazo de un año desde la entrada en vigor de esta ley, deberá remitir al Congreso de los Diputados un proyecto de ley reguladora de la preparación y disposición de la contribución de recursos a la Seguridad Nacional.*

En esta Disposición Final Tercera la **ley reguladora de la preparación y disposición de la contribución de recursos a la Seguridad Nacional, deberá recoger las infracciones y sanciones tanto para entidades públicas como privadas que por acción u omisión no cumplan con las obligaciones que emanan de la Ley de Seguridad Nacional**, paliando de esta forma el "olvido del legislador" de no incluirlas en la misma.

La Estrategia de Seguridad Nacional (ESN) de 2017 ha entrado en vigor el 22 de diciembre de 2017, mediante el Real Decreto 2008/2017, de 1 de diciembre, en consonancia con lo especificado en el artículo 14 de la citada ley, resultando con ello el primer desarrollo de las disposiciones adicionales y la primera vez que la Estrategia de Seguridad Nacional se aprueba por este procedimiento.

La ESN es documento de planeamiento general para la acción del Gobierno, de las Comunidades Autónomas, Corporaciones locales e incluso para los propios ciudadanos, al relacionar las amenazas, desafío y vulnerabilidades que tenemos a nivel global y la necesidad de paliarlas. Las infraestructuras críticas están presentes en todo el documento, desde el resumen ejecutivo, el capítulo 4: *"Es igualmente relevante destacar la exposición de infraestructuras críticas a las amenazas dado el*

impacto que pueden comportar para la provisión de los servicios esenciales", reiterado en el mismo capítulo al tratar la amenaza terrorista de una forma mucho más amplia, significando: *"Puesto que la mayoría de estos servicios esenciales son proporcionados por operadores privados, resulta fundamental seguir potenciando la colaboración público privada en este ámbito en beneficio de la sociedad en su conjunto"*:

Al enumerar la ESN sus objetivo y líneas de acción estratégicas, las infraestructuras críticas y como muy importante el sector del agua, queda insertado en varios de ellos:

Inciden en el sector del agua

Entre los objetivos se encuentra protección de la información clasificada, teniendo el sector del agua, mucha documentación declarada como "CLASIFICADA"

APLICACIÓN DE LAS SANCIONES CON OTRAS LEYES SUPLETORIAS

Ley Orgánica de Protección de la Seguridad Ciudadana

La Ley Orgánica 4/2015, de 30 de marzo, de protección de la seguridad ciudadana, especifica en su *Disposición adicional segunda. Régimen de protección de las infraestructuras críticas. La protección de las infraestructuras críticas se regirá por su normativa específica y supletoriamente por esta Ley.* Es decir que la Ley 4/2015 es "supletoria" de la 8/2011, de 28 de abril de protección de las infraestructuras críticas [29].

El Artículo 26 de la citada LO, trata el tema de los *"Establecimientos e instalaciones obligados a adoptar medidas de seguridad":*

Reglamentariamente, en desarrollo de lo dispuesto en esta Ley, en la legislación de seguridad privada, en la de infraestructuras críticas o en otra normativa sectorial, podrá establecerse la

[29] DERECHO SUPLETORIO: lo forman aquellas normas de un ordenamiento jurídico que tienen la facultad de regir situaciones que no le son específicamente propias, pero obligadas por el hecho de que la rama específica del ordenamiento que debería haberla regulado no lo ha hecho. Por lo tanto, el Derecho supletorio suple la ausencia de una norma específica y sirve para cubrir la laguna jurídica. Se extiende a todos aquellos aspectos no regulados por un Derecho específico. Es normal que cada ordenamiento jurídico establezca un derecho supletorio básico. La principal utilidad de la existencia de los Derechos supletorios es cubrir las lagunas de las distintas ramas del derecho. En caso de ausencia de regulación, el juez se dirige al Derecho supletorio antes de acudir a otras fuentes del derecho como la costumbre o los principios generales del derecho. www.es.wikipedia.org

necesidad de adoptar medidas de seguridad en establecimientos e instalaciones industriales, comerciales y de servicios, así como en las infraestructuras críticas, con la finalidad de prevenir la comisión de actos delictivos o infracciones administrativas, o cuando generen riesgos directos para terceros o sean especialmente vulnerables.

Hemos subrayado lo relativo a infraestructuras críticas y de forma discontinua, las instalaciones de servicios que, en este caso de la seguridad nacional, tendría el calificativo de "esenciales", es decir necesarios para el normal funcionamiento de la convivencia ciudadana.

Al haberse aprobado el Reglamento de desarrollo de la Ley de Infraestructuras Críticas con la omisión de las infracciones y sanciones, quedaría por ser recogidas la mención en el de Seguridad Privada, que se desarrollará en el apartado siguiente. No obstante, también se intentará profundizar en la normativa sectorial específica, relacionadas con los distintos grupos de infraestructuras críticas, para comprobar de alguna manera si la omisión de medidas de seguridad pudiera ser motivo de sanción para el titular correspondiente.

En el Capítulo quinto, corresponde a "sanciones" y la Sección 1ª: *Sujetos responsables, órganos competentes y reglas generales sobre las infracciones y la aplicación de las sanciones.*

Artículo 30. Sujetos responsables.
1. La responsabilidad por las infracciones cometidas recaerá directamente en el autor del hecho en que consista la infracción.

Queda claro que la responsabilidad de la infracción es del autor en que consista la infracción. Si un establecimiento, espacio o actividad, está obligados a disponer de unas determinadas medidas de seguridad privada, y el titular no las adopta, habiéndose sido requerido para ello, queda inmerso en la presente Ley de Seguridad Ciudadana.

Además, las leyes de Infraestructuras Críticas y Seguridad Nacional, pretenden preservar los servicios esenciales de ataques de agentes externos que pretendan subvertir la normalidad y convivencia ciudadana, por lo que las infracciones contra las normativas anteriores, quedan bajo la autoridad competente del Ministro del Interior, Secretario de Estado de Seguridad o Delegado del Gobierno, según la importancia de la infracción cometida y de la sanción que le corresponda.

En lo relativo a sanciones, se dividen en “muy graves”, “graves” y “leves”. En el párrafo segundo del artículo 35 se señala que serán autores de una infracción grave: la *omisión, insuficiencia, o falta de eficacia de las medidas de seguridad o precauciones que resulten obligatorias, siempre que en tales actuaciones se causen perjuicios muy graves*. Es decir que un “Operador Crítico”, podría ser sancionado, desde luego siempre que se produzca un hecho contra sus instalaciones, con grave perjuicio para la comunidad a la que debe servir y se demuestre que ha omitido las medidas de seguridad exigibles en la correspondiente Ley, en este caso las de Infraestructuras Críticas y Seguridad Nacional.

Se omite el análisis de las faltas “graves” y “leves”, dado que la relación de las infracciones, se encuentra en la misma línea que las “muy graves”, aunque causantes de menor perjuicio a la comunidad.

Con respecto a la cuantía de la sanción, teniendo en cuenta que, para las infraestructuras críticas y servicios esenciales, casi siempre se incluiría en la relación de infracciones muy graves, conllevaría una multa de 30.001 a 600.000 euros (artículo 39).

En el supuesto que el acto vandálico o terrorista, cometido en la instalación crítica o servicio esencial, afecte gravemente a terceros, el titular de la instalación y/o servicio a reponer a su situación original los daños que hay podido causar. Por ejemplo, si se comete un acto terrorista en una instalación de agua y se provoca una inundación, siempre que la instalación no disponga de las medidas de seguridad que le correspondan, podría ser obligado a pagar los daños causados (artículo 42).

Ley de Seguridad Privada y su futuro reglamento [30]

En el preámbulo de la Ley ya advierte de infracciones y sanciones:

En el título VI se da solución a algunas de las principales carencias de la anterior legislación referidas al régimen sancionador. Así, se contemplan con la debida separación las

[30] Se dispone de un borrador de reglamento, en el cual se tipifican las sanciones, refiriéndose en múltiples ocasiones a infraestructuras críticas o a operadores estratégicos, a la postre “servicios esenciales” para el mantenimiento de la normalidad ciudadana.

infracciones que pueden ser cometidas por las entidades, el personal o los usuarios de seguridad privada, incluyendo junto a estos últimos, a los centros de formación en la materia.

Una instalación crítica o un servicio esencial son "usuarios de seguridad privada".

El artículo 12, *"Competencias de la Administración General del Estado y de las comunidades autónomas"* de la Ley 5/2014, de 4 de abril de 2014, de Seguridad Privada, relaciona entre las mismas, en su apartado 1, Subapartados:

i. La determinación reglamentaria de los establecimientos obligados a disponer de medidas de seguridad privada, así como la fijación del tipo y alcance de las medidas obligatorias que ha de cumplir cada tipo de establecimiento.

j. La autorización, inspección y sanción de los establecimientos e instalaciones industriales, comerciales y de servicios que estén obligados a adoptar medidas de seguridad, cuando el ejercicio de esas facultades no sea competencia de las comunidades autónomas.

A falta de la aprobación reglamentaria, uno de los puntos más conflictivos es la relación de los "sujetos obligados" a disponer de seguridad privada, encontrándose entre ellos las empresas e instituciones declaradas "operador crítico-infraestructura crítica" y las consideradas como "servicios esenciales", encontrándose afectadas las primeras por la Ley de Infraestructuras Críticas y los segundos por la de Seguridad Nacional.

De esta forma se paliaría la grave omisión de no recoger un título sobre infracciones y sanciones en las dos anteriores leyes.

No obstante, la propia Ley adelanta en su artículo 51, especifica:

Artículo 51. Adopción de medidas.

1. *Las personas físicas o jurídicas, públicas o privadas, podrán dotarse de medidas de seguridad privada dirigidas a la protección de personas y bienes y al aseguramiento del normal desarrollo de sus actividades personales o empresariales.*
2. *Reglamentariamente, con la finalidad de prevenir la comisión de actos delictivos contra ellos o por generar riesgos directos para terceros o ser especialmente vulnerables, se determinarán los establecimientos e instalaciones industriales, comerciales y de servicios y los eventos que resulten obligados a adoptar medidas de seguridad, así como el tipo y características de las que deban implantar en cada caso.*
7. *Los titulares de los establecimientos, instalaciones … serán responsables de la adopción de las medidas de seguridad que resulten obligatorias en cada caso.*

Los operadores críticos quedan inmersos en los apartados 2 y 7, ya que la propia Ley 8/2011 les ordena disponer de un Plan de Seguridad del Operador (PSO) para el conjunto de la actividad que realizan y Planes de Protección Específicos (PPE) para cada una de las instalaciones declaradas críticas. Por ejemplo, una empresa de agua, declarada “Instalación Crítica”, debe disponer de un PSO para el conjunto y de los correspondientes

PPE para las críticas, como pueden ser las Estaciones de Tratamiento de Agua Potable (ETAPs.), así como otras que se consideren. Aparte de los PPE, cada una de las instalaciones de dicha empresa, deben disponer de sus planes de seguridad y de autoprotección.

Con respecto a los operadores de servicios esenciales, aspecto mucho más amplio que el de infraestructuras críticas, tienen la opción de acogerse de forma voluntaria al primer apartado.

Con respecto a la regulación de las infracciones, en esta ley hay que trasladarse al artículo 59, relativo a los "usuarios de seguridad", es decir la empresa de abastecimiento y saneamiento de agua:

f) La falta de adopción o instalación de las medidas de seguridad que resulten obligatorias.

Como en el caso de la seguridad ciudadana, recogemos únicamente las infracciones "muy graves".

Por su parte el artículo 63 establece la cuantía de las sanciones a los usuarios de seguridad privada, volviendo a insistir en las empresas de agua:

Las autoridades competentes podrán imponer, por la comisión de las infracciones tipificadas en el artículo 59, las siguientes sanciones:

a) Multa de 20.001 a 100.000 euros

No pudiéndosele aplicar a un servicio esencial, como es el abastecimiento y saneamiento de agua, el apartado c), es decir la suspensión de la actividad.

Aspecto importante y que significaría una "multa a la reputación y/o política", es la publicidad de la sanción:

Artículo 71. Publicidad de las sanciones.
Las sanciones, así como los nombres, apellidos, denominación o razón social de las personas físicas o jurídicas responsables de la comisión de infracciones muy graves, cuando hayan adquirido firmeza en vía administrativa, podrán ser hechas públicas, en virtud de acuerdo de la autoridad competente para su imposición, siempre que concurra riesgo para la seguridad de los usuarios o ciudadanos, en infracciones de naturaleza análoga o acreditada intencionalidad.

Estando claro que la infracción en seguridad de una empresa de agua afecta totalmente a la seguridad de los ciudadanos a los que se presta el servicio esencial. Las empresas públicas de agua, la inmensa mayoría, se rigen por criterios políticos de representatividad, por lo que, al darle publicidad a la sanción, saldría perjudicada la opción política que en ese momento ostenta la presidente del consejo de administración, representante del "titular de la actividad".

Ley 17/2015, de 9 de julio, del Sistema Nacional de Protección Civil

Al centrar este trabajo en las empresas de agua, aplicaremos los preceptos a la misma, aunque son perfectamente extrapolables a otras actividades que pueden generar riesgos.

En primer lugar, en una de las disposiciones adicionales de esta Ley establece:

Disposición adicional segunda Sistemas de Seguridad Nacional, Defensa Nacional e Infraestructuras Críticas y los derivados de tratados internacionales.
Lo dispuesto en esta ley se entiende sin perjuicio de lo que establezca la normativa vigente para los sistemas de Seguridad Nacional, Defensa Nacional e Infraestructuras Críticas y los derivados de tratados internacionales suscritos por España.

En este sentido debe entenderse que en todo lo no regulado por las normativas anteriores, quedará sujeta su inobservancia a la de Protección Civil.

El artículo 2.7 define "servicio esencial", siendo todos ellos los afectados por las leyes de infraestructuras críticas y seguridad nacional:

7. *Servicios esenciales. Servicios necesarios para el mantenimiento de las funciones sociales básicas, la salud, la seguridad, el bienestar social y económico de los ciudadanos, o el eficaz funcionamiento de las instituciones del Estado y las Administraciones Públicas.*

En el artículo 3.3 se expresa la participación de las "personas jurídicas" (empresas de abastecimiento y saneamiento de agua)

en el Sistema Nacional de Protección Civil, encontrándose entre esta participación el "deber de colaborar a informar a los ciudadanos", tal como se recoge en al artículo 7.bis.7:

7. *Los titulares de centros, establecimientos y dependencias, en los que se realicen actividades previstas en el artículo 9.2.b) que puedan originar emergencias, deberán informar con regularidad suficiente a los ciudadanos potencialmente afectados acerca de los riesgos y las medidas de prevención adoptadas, y estarán obligados a:* … en definitiva informar.

El servicio esencial del agua es una "actividad" y un conjunto de instalaciones, en las cuales se pueden materializar unos riesgos para la población, unos provocados por la acción del hombre, como terrorismo, vandalismo o sabotaje y otros por causas naturales. Una empresa de agua se compone de un conjunto de obras hidráulicas [31], las cuales veremos con posterioridad al analizar el texto refundido de la Ley de Aguas, pero en las cuales pueden producirse contaminación, inundación, corte del suministro, sustancias peligrosas, etc., estando en consecuencia

[31] *A los efectos de esta Ley (de Aguas), se entiende por obra hidráulica la construcción de bienes que tengan naturaleza inmueble destinada a la captación, extracción, desalación, almacenamiento, regulación, conducción, control y aprovechamiento de las aguas, así como el saneamiento, depuración, tratamiento y reutilización de las aprovechadas y las que tengan como objeto la recarga artificial de acuíferos, la actuación sobre cauces, corrección del régimen de corrientes y la protección frente avenidas, tales como presas, embalses, canales de acequias, azudes, conducciones, y depósitos de abastecimiento a poblaciones, instalaciones de desalación, captación y bombeo, alcantarillado, colectores de aguas pluviales y residuales, instalaciones de saneamiento, depuración y tratamiento, estaciones de aforo, piezómetros, redes de control de calidad, diques y obras de encauzamiento y defensa contra avenidas, así como aquellas actuaciones necesarias para la protección del dominio público hidráulico (artículo 122).*

la empresa de agua, obligada a informar a la población circundante de estos riesgos que pueden afectarles, incidiendo además en las medidas de protección que se han impuesto para impedirlos, paliarlos o reducirlos, pero que en caso de que se materialicen, deben disponer de los medios y medidas de detección y de los medios, medidas y procedimientos de aviso a la población. En definitiva, deben disponer de un Plan de Seguridad del Operador, denominación del Plan de Autoprotección de la actividad "gestión del agua".

Por su parte el artículo 7, ter.2, expresa las obligaciones de los titulares de las actividades que pueden generar riesgos:

Los titulares de los centros, establecimientos y dependencias, públicos o privados, que generen riesgo de emergencia, estarán obligados a adoptar las medidas de autoprotección previstas en esta ley, en los términos recogidos en la misma y en la normativa de desarrollo.

Cuando analicemos la Norma Básica de Autoprotección, veremos que las actividades que pueden generar riesgos están obligadas a disponer de los correspondientes planes de autoprotección, con estudios, medios y disposiciones regulados en una serie de capítulos, aunque en caso de "sectores específicos", se atendrán a su propia normativa en materia de autoprotección y desde luego una empresa de agua, declarada infraestructura crítica, tiene para autoprotección y proteger a la población a la que presta servicio, el Plan de Seguridad del Operador (PSO) y los Planes de Protección Específico (PPE)

El artículo 7.bis.7 hace mención al 9.2.b) de la misma Ley, en la cual se expresa:

Los catálogos oficiales de actividades que puedan originar una emergencia de protección civil, incluyendo información sobre los centros, establecimientos y dependencias en que aquéllas se realicen, en los términos que reglamentariamente se establezcan.

Trataremos este catálogo de actividades en la Norma Básica de Autoprotección, pero no debemos olvidar que el catálogo genérico de infraestructuras críticas fue relacionado ampliamente por una directiva [32], una comunicación [33] y un "libro verde" [34] de la Unión Europea, abarcando los siguientes sectores estratégicos:

1. Centrales y redes de energía
2. Tecnologías de las comunicaciones y la información
3. Finanzas
4. Salud
5. Alimentación
6. **Agua (por ejemplo, embalses almacenamiento, tratamiento, redes).**
7. Transporte
8. Producción, almacenamiento y transporte de mercancías peligrosas

[32] DIRECTIVA 2008/114/CE DEL CONSEJO, de 8 de diciembre de 2008.
[33] COM (2004) 702 final de 20.10.2004
[34] COM (2005) 576 final, de 17.11.2005.

9. Estado (por ejemplo, servicios críticos, instalaciones, redes de información, activos, sitios y monumentos principales).

Tenemos pues que el agua y por tanto las empresas que la gestionan, está considerado dentro del concepto y grupo de "infraestructuras críticas", así como "servicio esencial", por manifestación explícita en la Ley de Seguridad Nacional.

En el artículo 45 se recogen las infracciones, declarando como "muy grave", la ya tipificado en el artículo 7.bis.7:

c) *El incumplimiento de los deberes previstos en el artículo 7 bis.7 de esta Ley, cuando suponga una especial peligrosidad o trascendencia para la seguridad de las personas o los bienes.*

Podrían ser declaradas "graves" e incluso "leves", la misma infracción, aunque son gran trascendencia para la población a la que presta servicio.

La sanción que podría conllevar el incumplimiento de las medidas de protección adecuadas, siendo requerido para ellos, al ser declarado "Operador Crítico una Empresa de Agua", según el artículo 46 de la misma ley, oscila entre 30.001 y 600.000 euros.

REAL DECRETO 393/2007, de 23 de marzo, por el que se aprueba la Norma Básica de autoprotección de los centros, establecimientos y dependencias dedicados a actividades que puedan dar origen a situaciones de emergencia.

Hay que señalar que el Real Decreto no establece un régimen sancionador específico, refiriéndose al propio del Sistema Nacional de Protección Civil, tal se observa en el artículo siguiente:

Artículo 9. Régimen sancionador.
El incumplimiento de las obligaciones de autoprotección será sancionable por las administraciones públicas competentes, conforme a la Ley 2/1985, de 21 de enero [35], las correspondientes Leyes de Protección Civil y Emergencias de las Comunidades Autónomas y el resto del ordenamiento jurídico aplicable en materia de autoprotección.

El título del Real Decreto puede parecer engañoso, dado que parece referirse a "centro, establecimientos y dependencias", pero si nos vamos al anexo III, "definiciones", veremos que su contenido en mucho más amplio y que lo que puede generar riesgos es la "actividad" que se realiza.

Vemos las definiciones que atañen al caso:

Actividad: Conjunto de operaciones o tareas que puedan dar origen a accidentes o sucesos generen situaciones de emergencia.

Autoprotección: Sistema de acciones y medidas, adoptadas por los titulares de las actividades, públicas o

[35] Habría que considerar que se refiere a la nueva Ley de Protección Civil 17/2015.

privadas, con sus propios medios y recursos, dentro de su ámbito de competencias, encaminadas a prevenir y controlar los riesgos sobre las personas y los bienes, a dar respuesta adecuada a las posibles situaciones de emergencia y a garantizar la integración de estas actuaciones en el sistema público de protección civil.

Autoprotección: Marco orgánico y funcional previsto para una actividad, centro, establecimiento, espacio [36], instalación o dependencia, con el objeto de pre- venir y controlar los riesgos sobre las personas y los bienes y dar respuesta adecuada a las posibles situaciones de emergencias, en la zona bajo responsabilidad del titular, garantizando la integración de éstas actuaciones en el sistema público de protección civil.

Plan de actuación en emergencias: Documento perteneciente al plan de autoprotección en el que se prevé la organización de la respuesta ante situaciones de emergencias clasificadas, las medidas de protección e intervención a adoptar, y los procedimientos y secuencia de actuación para dar respuesta a las posibles emergencias.

Titular de la actividad: La persona física o jurídica que explote o posea el centro, establecimiento, espacio, dependencia o instalación en que se desarrollen las actividades.

[36] Una empresa de agua despliega en un espacio de terreno, debiendo disponer todo ese espacio donde se desarrolla la actividad de un Plan de Autoprotección (Pan de Seguridad del Operador).

Vemos pues que es la “actividad” que puede generar riesgos el verdadero protagonista. Es decir, en la empresa de agua desarrolla su actividad de abastecimiento, suministro, saneamiento, depuración, reutilización y vertido de agua en un espacio de terreno, teniendo dicho conjunto que disponer de su propio Plan de Autoprotección (incluyendo en el mismo el Plan de Actuación en Emergencias), aparte del conjunto de instalaciones que deben disponer del suyo propio. Al primero, de acuerdo con la Ley 8/2011, se denomina Plan de Seguridad del Operador, para las instalaciones declaradas críticas, Plan de Protección Específico y para el resto “Plan de Autoprotección”.

Es importe reseñar el concepto de “titular de la actividad”, dado que una empresa municipal de aguas, consorciada o de otra naturaleza, el titular de la actividad es la propia empresa, representada por su “presidente” y su “consejo de administración”, siendo en el caso de una municipal, el “alcalde” de la localidad. Es decir que el incumplimiento de las obligaciones y las sanciones correspondientes se dirigen a los titulares de la actividad y no al director, gerente o similar, el cual no está sujeto a sanción administrativa, solamente a las de carácter interno, recogidas en el Régimen Interior de dicha actividad, pero no es responsable ante las delegaciones del gobierno, ni ministerio del Interior.

Es importante esta aclaración dado que los titulares son los responsables de que una actividad disponga del Plan de Autoprotección (PSO-PPE) y de su implantación (artículo 2.2. del Real Decreto), reiterado en el artículo 4.a) *Su elaboración, implantación, mantenimiento y revisión es responsabilidad*

del titular de la actividad, y no del director o gerente, debiendo ser firmado el documento del Plan o Planes por dicho titular o como mínimo el firmante del escrito con el que se remite a las autoridades competentes el Plan. Esta es una forma de reafirmar el compromiso del titular de la actividad con la autoprotección y con las consecuencias que puede generar la actividad ante terceros.

En las disposiciones generales de la propia Norma Básica de Autoprotección (NBA), en apartado 1.2 párrafo segundo se vuelve a incidir en esta cuestión:

Estas acciones y medidas deben ser adoptadas por los titulares de las actividades, públicas o privadas, con sus propios medios y recursos, dentro de su ámbito de competencia, reiterándose en varias ocasiones a lo largo de las disposiciones de la NBA.

En el apartado 3. de la NBA se señala:

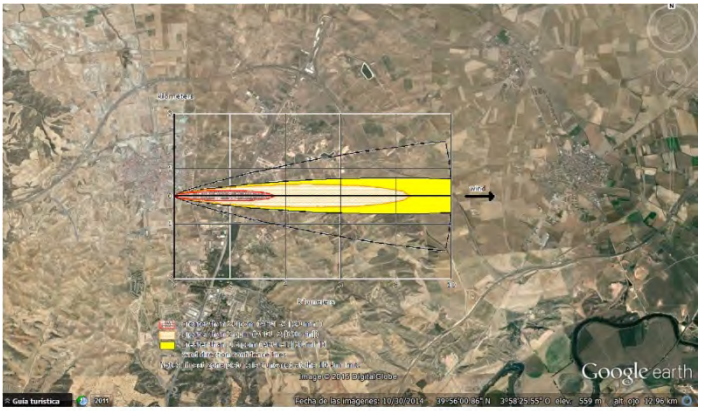
Órganos competentes en materia de Protección Civ il en el ámbito local, autonómico o estatal, según corresponda, sin perjuicio de las competencias atribuidas a los órganos a que se refiere el párrafo anterior, estarán facultados, para:

e) *Obligar a los titulares de las actividades que consideren peligrosas, por sí mismas o por hallarse en entornos de riesgo, aunque la actividad no figure en el anexo I, a que elaboren e implanten un Plan de Autoprotección, dándoles un plazo razonable para llevarlo a efecto.*

f) Ejercer la potestad sancionadora conforme a lo que prevean las leyes aplicables.

Los riesgos que afectan a las infraestructuras críticas, basados en vandalismo, sabotaje y terrorismo, entran en la categoría de emergencia de interés nacional, siendo el Ministerio del Interior, a través de la Secretaría de Estado de Seguridad (CNPIC) y con la remisión al titular por la Delegación o Subdelegación del Gobierno en la Comunidad Autónoma o provincia, el que debe exigir que una actividad que puede generar riesgos para la colectividad, como es la gestión del agua, disponga de Plan de Autoprotección, el cual al disponer de una normativa específica, en la ley y reglamento de IC, deberán tener el formato y denominación de PSO y PPE, ejerciendo sobre dichas actividades y sus titulares la potestad sancionadora que recoge la Ley de Protección Civil, entre otras.

Este artículo de la NBA es importante dado que cuando se habla de la necesidad de disponer de un plan de autoprotección, algunos titulares indican que su actividad no figura en el Anexo I, cuando precisamente, tal como vemos en el apartado citado, por orden de la autoridad administrativa una actividad debe disponer de autoprotección aunque no se encuentre relacionado en el anexo, siendo este el caso de las infraestructuras críticas y los servicios esenciales, los cuales pueden verse afectados en lo referente a sustancias peligrosas, dado que la cloración del agua, en muchos casos se emplea “cloro gas” en vez de “hipoclorito”, por ser más barato, pero que conlleva mucho más riesgo en caso de explosión de una bombona de forma accidental o premeditada.



SIMULACIÓN (FICTICIA) POR ESCAPE DE BOMBONA CLORO GAS

En el anexo II de la NBA figura una guía del Plan de Autoprotección, pero previamente en el apartado 3.2. se indica que la guía no es incompatible con otro formato, como pueden ser el PSO y PPE:

3.2 Contenido.– El Plan de Autoprotección se recogerá en un documento único cuya estructura y contenido mínimo se recoge en el Anexo II.

Éste u otros documentos de naturaleza análoga que deban realizar los titulares en virtud de la normativa sectorial aplicable, podrán fusionarse en un documento único a estos efectos, cuando dicha unión permita evitar duplicaciones innecesarias de la información y la repetición de los trabajos realizados por el titular o la autoridad competente, siempre que se cumplan todos los requisitos esenciales de la presente norma.

Aparte de lo anterior existen muchas actividades e instalaciones con normativas anteriores al Real Decreto 393/2007, en la cuales se diseccionaba lo que debería ser su Plan de Autoprotección a los que se les denominaba y se sigue haciendo "Plan de Emergencia Interior". Un ejemplo muy claro de ello es la actividad nuclear y sus centrales [37]. Pudiéndose decir lo mismo para las actividades en donde estén presentes sustancias peligrosas [38], las cuales deben disponer de Plan de Emergencia Interior, incluso en su artículo 25 se recoge un régimen de sanciones que no solamente hace referencia a la Ley de Protección Civil, sino también a la 21/1992, de 16 de julio, de Industria y la 26/2007, de 23 de octubre, de responsabilidad medioambiental.

La rotura de una tubería ha provocado una espectacular imagen en la Vía Helmántica a la altura del Puente Enrique Estevan provocando la inundación de aceras y calzada debido a la potencia con la que el agua salía del tubo dañado.

[37] Real Decreto 1836-1999, de 3 de diciembre, por el que se aprueba el Reglamento sobre instalaciones nucleares y radiactivas y GS 01-03 Plan de emergencia interior en centrales nucleares.

[38] Real Decreto 840/2015, de 21 de septiembre, por el que se aprueban medidas de control de los riesgos inherentes a los accidentes graves en los que intervengan sustancias peligrosas.

Conclusiones al Real Decreto y Norma Básica de Autoprotección:

1. Todas las actividades relacionadas con el agua, en su conjunto y en sus instalaciones deben disponer de Plan de Autoprotección.
2. Si han sido declaradas infraestructuras críticas, este Plan toma la forma de Plan de Seguridad del Operador y Plan de Protección Específico.
3. El Ministerio del Interior, Secretaría de Estado de Seguridad, a través de los Delegados del Gobierno en las Comunidades Autónomas o Subdelegados en caso de las provincias, podrán exigir que actividades que puedan generar riesgos, como la gestión del agua, y que no figuren en la relación del Anexo I, les obligue a disponer de Plan de Autoprotección, sea con el formato de la NBA o del PSO y PPE.
4. Es aconsejable que todas las empresas que gestionen agua, hayan sido declaradas críticas o no, deben disponer de PSO y PPE. Debemos tener en cuenta que todas las empresas de agua, son servicios esenciales y también infraestructuras críticas, aunque no sean declaradas oficialmente como tales [39].
5. El hecho que en las leyes de infraestructuras críticas y seguridad nacional no se incluya un título de infracciones

[39] Con respecto al agua se han declarado como críticos, aquellos operadores que abastecen a más de 500.000 habitantes o en donde no hay ninguna alternativa, caso de las ciudades autónomas y algunas islas españolas, pero a buen seguro, transcurridos unos años, se bajará el listón y se pasará a aquellas empresas que abastezcan a 250.000 habitantes y así sucesivamente, siendo por ello aconsejable que todas se adapten a la normativa de IC.

y sanciones, no significa que se encuentren ajenos los titulares a esta especificidad, dado que entran de lleno en la Ley de Protección Civil, que incluye sanciones.

LEY ORGÁNICA 10/1995, DE 23 DE NOVIEMBRE, DEL CÓDIGO PENAL. (Texto consolidado de abril de 2015)

El Código Penal es una "cajón de sastre", complementario de las infracciones y sanciones anteriores, cuando en grado superior se atente contra el medio ambiente (sustancias peligrosas), los recursos naturales (gestión del agua), información clasificada (difusión limitada declarada como tal por la Comisión Nacional Delegada para la seguridad de la información clasificada), etc.

Por ejemplo, en el delito contra los recursos naturales y el medio ambiente, se recoge en los artículos 325 y siguientes:

Artículo 325.

1. *Será castigado con las penas de prisión de seis meses a dos años, multa de diez a catorce meses e inhabilitación especial para profesión u oficio por tiempo de uno a dos años el que, contraviniendo las leyes u otras disposiciones de carácter general protectoras del medio ambiente, provoque o realice directa o indirectamente emisiones, vertidos, radiaciones, extracciones o excavaciones, aterramientos, ruidos, vibraciones, inyecciones o depósitos, en la atmósfera, el suelo, el subsuelo o las aguas terrestres, subterráneas o marítimas, incluido el alta mar, con incidencia incluso en los espacios transfronterizos, así como las captaciones*

de aguas que, por sí mismos o conjuntamente con otros, cause o pueda causar daños sustanciales a la calidad del aire, del suelo o de las aguas, o a animales o plantas.

2. *Si las anteriores conductas, por sí mismas o conjuntamente con otras, pudieran perjudicar gravemente el equilibrio de los sistemas naturales, se impondrá una pena de prisión de dos a cinco años, multa de ocho a veinticuatro meses e inhabilitación especial para profesión u oficio por tiempo de uno a tres años.*

3. *Si se hubiera creado un riesgo de grave perjuicio para la salud de las personas, se pondrá la pena de prisión en su mitad superior, pudiéndose llegar hasta la superior en grado.*

Aparentemente no es aplicable este artículo a los titulares de las empresas de agua, pero veamos lo que se indica en el artículo 326 bis.

Serán castigados con las penas previstas en el artículo 325, en sus respectivos supuestos, quienes, contraviniendo las leyes [40] u otras disposiciones de carácter general, lleven a cabo la explotación de instalaciones en las que se realice una actividad peligrosa o en las que se almacenen o utilicen sustancias o preparados peligrosos de modo que causen o puedan causar daños sustanciales a la calidad del aire, del suelo del suelo o de las aguas, o a animales o plantas, muerte

[40] Contraviniendo las leyes 8/2011, de infraestructuras críticas y 36/2015 de seguridad nacional.

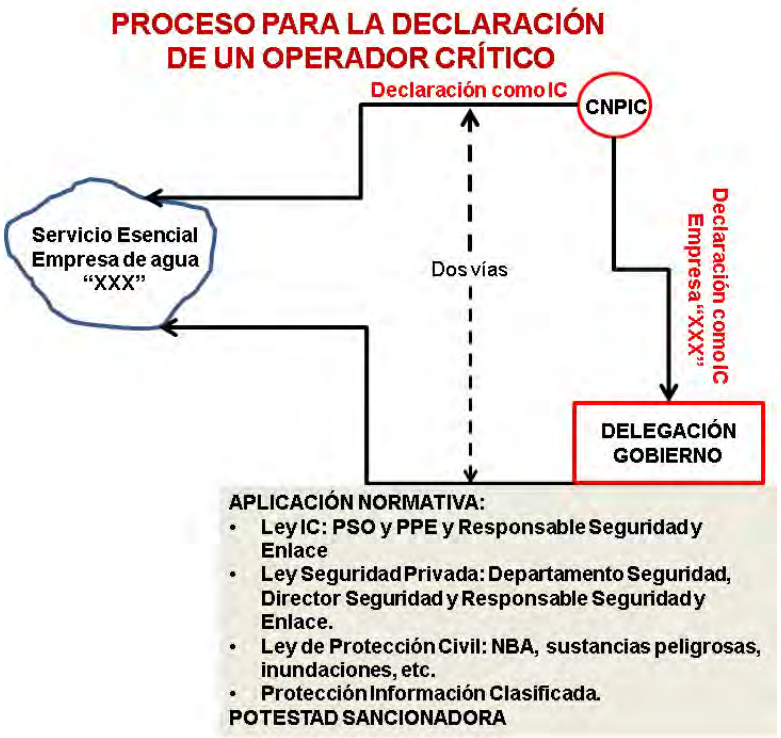
o lesiones graves a personas, o puedan perjudicar gravemente el equilibrio de los sistemas naturales [41].

En los artículos 343, 344 [42], 345 [43], 346 [44], 347 [45], se trata de "imprudencia grave" y esa situación podría darse cuando un operador de una infraestructura crítica o servicio esencial no tome las medidas apropiadas para que no se produzca un mal para la comunidad que pudiera verse afectada.

CONCLUSIONES

1. El proceso de declaración de una infraestructura como crítica, ante la ausencia sancionadora de las leyes de infraestructuras críticas y seguridad nacional, debe hacer a través de dos vías, una directamente por el Centro Nacional de Protección de Infraestructuras y Ciberseguridad (CNPIC) y el otro a través de las Delegaciones/Subdelegaciones del Gobierno, según el siguiente diagrama:

[41] Siempre que no se pongan los medios necesarios para impedir dichos riesgos, como son los Planes de Seguridad del Operador y de Protección Específicos.
[42] Cuando sea por "imprudencia grave", es decir no poner los medios adecuados de protección.
[43] Idem "imprudencia grave".
[44] En este caso por utilización de explosivos o artefactos de similar potencia, aplicándose en caso de acto terrorista, como mínimo.
[45] Idem "imprudencia grave"



2. La que genera riesgos es la actividad, independientemente de la instalación, por lo que esta actividad debe disponer de su propio plan de autoprotección, denominado Plan de Seguridad del Operador.
3. A su vez existen instalaciones que, por su incidencia en el conjunto, como por ejemplo una Estación de Tratamiento de Agua y Potabilización (ETAP), que dispone de sustancias peligrosas, siendo además un elemento vital para el mantenimiento de la actividad

como servicio esencial, debe disponer de un plan de autoprotección, denominado Plan de Protección Específico.

4. El resto de las instalaciones que pueden generar riesgos, como una tubería de agua, una depuradora, una estación impulsora, etc., deben disponer de un Plan de Autoprotección adaptado a lo que se especifica en la Norma Básica de Autoprotección.
5. Existen otras instalaciones, como presas, embalses, depósitos, y otras obras hidráulicas, las cuales deben disponer de plan de autoprotección y que según su reglamentación específica se denominan Plan de Emergencia Interior.
6. Cuando exista un Plan de Emergencia Interior, debe de redactarse por las autoridades de Protección Civil otro Plan denominado de Emergencia Exterior, elaborado con la información pertinente que le proporcione el operador.
7. Los planes relacionados con sustancias peligrosas, con inundaciones, etc., forman parte de los llamados “riesgos especiales”, sujetos a “planes especiales” y basados en las correspondientes Directrices Básica de Planificación de Protección Civil, emanadas en forma de Reales Decretos o de Órdenes Ministeriales según sea el riesgo. Los operadores de agua deben tener en cuenta si algunos de estos riesgos pueden producirse en el terreno donde se desarrolla su actividad.
8. La ley Orgánica de Protección de la Seguridad Ciudadana es supletoria de las leyes de Infraestructuras Críticas y Seguridad Nacional, aunque esta última se encuentra a falta de desarrolla en otras leyes que la

complementarán. Por ello en caso de producirse una emergencia por acción terrorista en una instalación declarada crítica, sin que el titular de la actividad haya tomado las medidas necesarias de protección, incurriría en sanciones como falta “muy grave”

9. Un atentado terrorista genera una catástrofe. La Ley de Infraestructuras Críticas atienden fundamentalmente a la “prevención” de que los hechos no se produzcan, pero acaecido, debe ponerse en funcionamiento los planes de protección civil, debiendo considerarse como tales los de autoprotección y en su especificidad en este tipo de actividad, de Planes de Seguridad del Operador, de Protección Específica y de Emergencia Interior. La Ley de Protección Civil, dispone de un título sancionador, aplicable a los operadores que no dispongan de las medidas de protección a las que están obligados.
10. La Resolución de 8 de septiembre de 2015 de la Secretaría de Estado de Seguridad, declara que los contenidos del Plan de Seguridad del Operador, tendrán la consideración de “Difusión Limitada” y sujeta a las Normas que emanan de la Autoridad Nacional para la Protección de la Información Clasificada del Centro Nacional de Inteligencia. ¿Quiere esto significar que si un operador crítico desoyendo la observancia de su declaración como tal, y por tanto no elabora el PSO, no se encuentra sujeto a esta restricción de la información? La ignorancia de la ley no exime de su cumplimiento y en este caso el operador ha sido informado fehacientemente, por lo que en caso de infracción y conocimiento a terceros de cuestiones que afecten a la

seguridad de la actividad, podría aplicársele el Código Penal.

En el presente trabajo, sujeto a crítica jurídica, se presenta la casuística sobre la obligación del cumplimiento de leyes que, aunque no hagan referencia a sanciones concretas, conllevan otras connotaciones en otras normativas, que pueden aplicárseles en caso de inobservancia.

26.12.2018

De izda. a dcha: Rafael Vidal; Francisco Javier Romero Bermúdez, Jefe del Servicio de Explotación de Presas de la Confederación Hidrográfica del Guadalquivir; y José Antonio Román Begines, Responsable de Seguridad de Servicios Esenciales de EMASESA