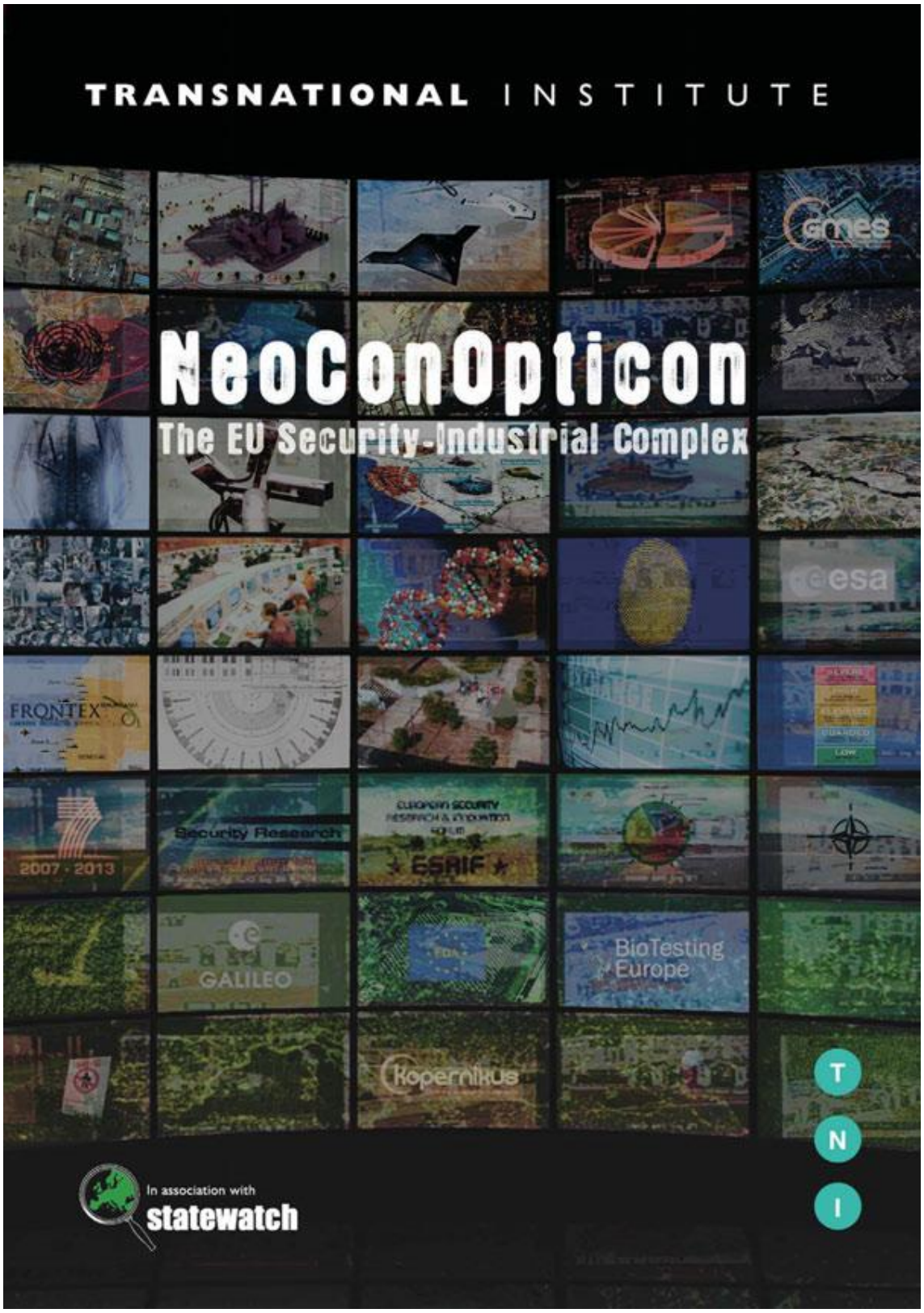

TRANSNATIONAL INSTITUTE
NeoConOpticon
The EU Security-Industrial Complex
gmes
esa
FRONTEX
2007 · 2013
Security Research
ESRIF
GALILEO
BioTesting Europe
Kopernikus
In association with
statewatch
T
N
I

Ben Hayes

Derechos de autor y detalles de la publicación

Agradecimientos

Este informe ha sido elaborado por Ben Hayes para Statewatch y el Transnational Institute (TNI). Max Rowlands y Fiona O'Malley de Statewatch han llevado a cabo la investigación adicional, mientras que Tnoy Bunyan y Trevor Hemmings (también de Statewatch) contribuyeron constantemente con valiosos comentarios, información y asesoramiento (varias secciones también le deben mucho a las columnas de opinión de Tony Bunyan publicadas en la página web *Liberty Central* del diario británico *The Guardian*). También resultaron de inestimable valor la información y los análisis que proporcionaron Frank Slijper (miembro de la campaña holandesa contra el comercio armamentístico y del TNI), Matthias (miembro de Gipfelsoli) y Kamil Majchrzak (ECCHR), así como el asesoramiento de Thomas Mathiesen en relación a las variaciones del "Panóptico" que se mencionan en este informe.

Los editores del informe fueron Nick Buxton y Fiona Dove, del TNI. Wilbert van der Zeijden y David Sogge (TNI) así como Eric Toepfer, (CILIP, Alemania), contribuyeron con comentarios y sugerencias. El autor también se enriqueció a partir de diversos debates llevados a cabo en varias conferencias y seminarios, de entre los que cabe destacar el Taller Internacional sobre Vigilancia y Democracia organizado por Minas Samatas en la universidad de Creta en junio de 2008 y los seminarios sobre la UE que se llevaron a cabo en la conferencia llamada "Militarismo: economía, seguridad y teorías políticas" en la universidad de Sussex, organizados por Iraklis Oikonomou y Anna Stavrianakis en mayo de 2009. Los comentarios de Kevin Haggerty (Departamento de sociología de la universidad de Alberta) sobre el primer borrador del ESRP que preparó para la conferencia llamada "Vigilancia y democracia" también resultaron de gran utilidad para la elaboración de este informe.

Índice de contenidos

PARTE I: INTRODUCCIÓN

> *Los gastos gubernamentales en productos y servicios destinados a la seguridad nacional deberían alcanzar los 141.600 millones de dólares en 2009... Según algunos expertos, la gran prioridad que se da a la seguridad nacional ha hecho de este mercado uno de los pocos sectores de la industria de la defensa que han aguantado la recesión económica.*
> Visiongain Market Research, 2009[1]

1 Resumen del informe

En 2006, Statewatch y el Transnational Institute publicaron *Arming Big Brother* (Armando al Gran Hermano), un informe en el que se examina el desarrollo del Programa Europeo de Investigación en Seguridad (ESRP). El ESRP es un programa de siete años y 1.400 millones de euros desarrollado en base a la necesidad de proporcionar nuevas tecnologías para aumentar la seguridad a los Estados miembro de la Unión con el fin de proteger a los ciudadanos de la UE de cualquier amenaza concebible a su seguridad (entendida aquí en términos de seguridad física).

El ESRP también tiene la intención explícita de fomentar el crecimiento de una industria de "seguridad nacional" lucrativa y competitiva a nivel mundial con base en Europa. A día de hoy, algunas empresas europeas de los sectores de la defensa y las tecnologías de la información y la comunicación han gozado de una implicación sin precedentes en el desarrollo de la agenda de "investigación" en materia de seguridad.

Arming Big Brother despertó inquietudes relacionadas con la puesta en marcha del ESRP, entre las que se encuentran la amenaza implícita que supone la "investigación" de la UE en vigilancia y otras tecnologías de seguridad para las libertades civiles y los derechos fundamentales. El informe también fue muy crítico con la influencia de las empresas en el programa de investigación en seguridad de la UE y advirtió de los varios peligros que supone la voluntad de establecer un "complejo industrial de seguridad" en Europa.

Arming Big Brother, publicado en 2006, se distribuyó ampliamente y generó una gran cantidad de debates.[2] La versión en línea ha sido descargada en más de 500.000 ocasiones.

[1] *Global Homeland Security 2009-2019*, ASD reports, véase: http://www.asdreports.com/shopexd.asp?ID=1442

[2] Hayes, B. (2006) *Arming Big Brother: The EU's Security Research Programme*. Amsterdam: TNI/Statewatch. Disponible en: http://www.statewatch.org/analyses/bigbrother.pdf.

Este informe de seguimiento contiene nuevos datos de investigación que muestran que el Programa Europeo de Investigación en Seguridad sigue siendo modelado en base al criterio de empresas de seguridad y defensa transnacionales y otros intereses personales. A pesar de que técnicamente es un programa de Investigación y Desarrollo (I+D), el ESRP está muy centrado en la aplicación de tecnología de seguridad (en lugar de centrarse en la investigación objetiva) y coincide cada vez más con la política de la UE en los ámbitos de Justicia y Asuntos Interiores (JAI, "el tercer pilar"), seguridad y defensa exterior (Asuntos Exteriores y Política de Seguridad, el "segundo pilar").

La investigación dirigida por empresas y llevada a cabo en el marco del ESRP coincide con los objetivos de la política de la UE y habla en favor de la obtención pública de nuevas tecnologías de seguridad y la implementación de nuevas políticas de seguridad en la UE que autoricen su implementación. Esta influencia tan encubierta tiene gran peso en la agenda de políticas de la UE, lo que está provocando la expansión de un ciclo de toma de decisiones particularmente tecnocráticas y muy poco justificables.

Este informe está compuesto por dos apartados sustanciales. El primero revisa el desarrollo del Programa Europeo de Investigación en Seguridad hasta el día de hoy. En él se muestra que el diseño del ESRP se ha externalizado precisamente a las empresas que se pueden ver más favorecidas por su implementación. El segundo se centra en la implementación del ESRP y en la consolidación del complejo industrial de seguridad de la UE, más allá de este programa. En él se examina el papel que desempeñan algunos elementos y la relación entre determinados proyectos de "investigación" y medidas políticas de la UE. En este informe se analizan los 95 proyectos financiados hasta la fecha en el marco del programa de investigación en seguridad (hasta finales de 2008) y se han consultado varios miles de proyectos de otros programas temáticos de I+D y financiados por la UE. Lo que se desprende de la apabullante selección de contratos, acrónimos y políticas de la UE es el veloz desarrollo de un poderoso nuevo sistema de vigilancia "interoperable" europeo que se utilizará con fines civiles, comerciales, policiales, de seguridad y de defensa.

A pesar de las intenciones, a menudo benignas, de la "investigación" europea colaborativa mediante sistemas de vigilancia terrestres, aéreos, marítimos, espaciales y cibernéticos integrados, la seguridad y la política de I+D de la UE están uniéndose en torno a un programa de tecnología punta para dar lugar a un nuevo tipo de seguridad. Este programa deja entrever un futuro mundo dividido en zonas rojas y zonas verdes; países cuyas fronteras estarán controladas por la fuerza militar, mientras que el control interno será responsabilidad de una extensa red de controles físicos y virtuales; espacios públicos, micro-estados y "mega eventos" en los que el control policial será responsabilidad de sofisticados sistemas tecnológicos de vigilancia y fuerzas de reacción rápida; métodos para mantener la paz y misiones de "control de crisis" que no harán diferencia entre los suburbios de Basra o la Banlieue; integración progresiva de las funciones de defensa y seguridad nacional tanto dentro de un mismo país como en el extranjero.

No se trata de un caso de "avanzar sin conocimiento" o "despertarse" en una "sociedad de la vigilancia", como ya alertó la autoridad británica de protección de datos[3], se trata

[3] *Waking up to a surveillance society*, Nota de prensa de la agencia de protección de datos británica, 2 de noviembre de 2006, véase: http://www.ico.gov.uk/upload/documents/pressreleases/2006/waking_up_to_a_surveillance_society.pdf.

más de apartar la mirada mientras da comienzo un nuevo tipo de carrera armamentística en la que todas las armas apuntan hacia dentro. Bienvenidos al NeoConÓptico.

Ben Hayes, Junio de 2009

2 ¿Por qué "NeoConÓptico? El trasfondo del título

> *En pocos años, la industria de la seguridad nacional, que apenas existía antes del 11-S, ha visto como se ha disparado su crecimiento hasta llegar a superar significativamente el tamaño de la industria de la música o de* Hollywood*. Con todo, lo que resulta más sorprendente es lo poco que se analiza y se debate el* boom *de la seguridad como economía, como una convergencia sin precedentes de poderes policiales y capitalismo sin comprobar, una mezcla de centro comercial y prisión secreta. Cuando la información sobre quién (y quién no) representa un riesgo para la seguridad es un producto que se puede vender con la misma facilidad que la información sobre quién compra libros de* Harry Potter *en* Amazon *o quién ha ido de crucero por el Caribe y puede estar pensando en hacer uno por Alaska, los valores de una cultura cambian. No solo resulta un incentivo para el espionaje, la tortura y la generación de información falsa, sino que también crea un poderoso impulso de perpetuar el sentido de peligro que la industria ha creado en primer lugar.*
>
> Naomi Klein[4]

Más allá del "Panóptico"

El "Panóptico" era un modelo de prisión diseñado en 1785 por el filósofo inglés Jeremy Bentham. También conocido como "casa de inspección", su diseño permitía a los vigilantes observar a todos los prisioneros (como indica la procedencia griega del término: *pan-opticon*) sin que estos supieran si estaban siendo vigilados en un momento dado. Como diseño penitenciario el ""Panóptico"" tuvo una vida corta[5], pero unos siglos más tarde, el filósofo francés Michel Foucault adoptó el término como una metáfora de las técnicas de vigilancia y control social en la sociedad moderna[6]. Su principal argumento era que el "panopticismo", el principio de la vigilancia omnipresente, había creado un *nuevo tipo de sociedad... transportada de la institución penal al conjunto de la sociedad.*[7] Desde centros de prevención de la delincuencia a hospitales, escuelas, lugares de trabajo o la vida doméstica, el hecho de ser observado (lo que Foucault llamaba el poder disciplinario de la mirada) demostró ser tan importante como el poder coercitivo del estado en el control de los comportamientos individuales.

El modelo de control y vigilancia de Foucault fue bien recibido por muchos intelectuales como un "modelo muy preciso y necesario del estado contemporáneo y de la tendencia innata en todos los poderes modernos".[8] La llegada de lo que ahora se denomina en todo el mundo "sociedad de la vigilancia" confirmó la hipótesis de Foucault y, a medida que aparecían sistemas internacionales para la vigilancia en masa,

---

[4] Klein, N. (2007) The Shock Doctrine. Londres: Penguin (página 306).

[5] Tan sólo existe media docena de prisiones que siguen el diseño "Panóptico" y la mayoría de ellas se construyeron antes de 1820.

[6] Foucault, M. (1979) Discipline and Punish: The Birth of the Prison. Harmondsworth: Penguin.

[7] Foucault, M. (1979: páginas 216 y 298)

[8] Bauman, Z. (1999) In Search of Politics. Cambridge: Polity Press (página 60).

muchos intelectuales llegaron incluso a proclamar la llegada de un "Panóptico" global, o súper "Panóptico".[9]

Sin embargo, el concepto de vigilancia se ha "salido de la antigua consideración de nación-estado y se ha convertido en una constante de la vida diaria, en el trabajo, en casa",[10] lo que ha llevado a muchos a la conclusión de que el "Panóptico" ha dejado de ser un marco teórico útil para la comprensión de las prácticas de vigilancia contemporáneas.[11] Los sistemas de vigilancia, que las empresas, las compañías comerciales, los consumidores y las redes sociales utilizan con tanta normalidad como las instituciones coactivas del estado, se están "convirtiendo rápidamente en la práctica de organización dominante en el mundo moderno."[12] Este proceso, que ha sido apuntalado por la revolución en las tecnologías de la información, también se ha denominado "el fin del olvido": una nueva era en la que la información se puede almacenar, recuperar y reproducir cuando se quiera. La cuestión que plantea esta nueva era no se limita a preguntarse quién lleva a cabo la vigilancia, sino quién se encarga de recordar.[13]

Algunas críticas se han dirigido a aquellos que se centran exclusivamente en las propiedades negativas de la vigilancia y en la imagen creada por el Gran Hermano de Orwell, mientras pasaban por alto el enorme impacto de la revolución tecnológica y en el hecho de que la vigilancia contemporánea se sufre a la vez que se utiliza. Estas críticas son válidas: una nueva generación en el mundo rico está encantada de empezar a depender de teléfonos móviles multimedia, navegación por satélite, *webcams*, *Facebook* y los demás sistemas de comunicación de última tecnología que adquieren. De esta manera, en una sociedad en la que todo el mundo, desde los distribuidores hasta los investigadores o las misiones de rescate, se benefician de las últimas tecnologías basadas en la vigilancia, es de esperar que los estados y los gobiernos intenten hacer lo mismo.

Este informe no parte del punto de vista de que la tecnología de seguridad es negativa. Al contrario; en principio, los esfuerzos genuinos y dirigidos por los ciudadanos de potenciar la capacidad de prevención y respuesta de los estados al crimen y a las catástrofes mediante la tecnología deberían ser bien recibidos. *Lo que debería determinar su aceptabilidad es el funcionamiento que van a tener en la práctica.* Aun así, a pesar de las críticas cada vez más sofisticadas a los viejos prejuicios sobre la vigilancia, sigue dándose el caso de que, como Thomas Mathiesen dijo, *nunca en la historia de la humanidad ha habido una tecnología con un "doble carácter" (utilizando la expresión de Marx) tan marcado; un "lado oscuro" que comprende "el uso de tecnología sofisticada y en renovación constante con fines de vigilancia, una vigilancia que se dirige rápidamente a un punto en el que supondría una amenaza para las bases democráticas de nuestra sociedad".*[14]

---

[9] Gill, S. (1995) 'The Global panopticon? The Neoliberal State, Economic Life and Democratic Surveillance', Alternatives, 1995 (2).

[10] Lyon, D. (ed) (2003) Surveillance as Social Sorting: Privacy, Risk and Digital Discrimination. Londres: Routledge, 2003 (página 11).

[11] Lyon, D. (ed) (2006) Theorizing Surveillance: The Panopticon and Beyond. Portland: Willan Publishing.

[12] 'Surveillance and Social Sorting', The New Transparency, véase:
http://www.surveillanceproject.org/projects/the-new-transparency/about.

[13] Bossewitch, J. & Sinnreich, A. (2009) 'Beyond the Panopticon: Strategic Agency in an Age of Limitless Information', Informe presentado en Media in Transition 6: Stone and Papyrus, Storage and Transmission, entre el 24 y el 26 de abril de 2009. Massachusetts Institute of Technology. Cambridge, MA USA, disponible en:
http://www.radarresearch.com/aram/index.php?view=article&id=62%3Abeyond-the-panopticon-strategic-agency-in-an-age-of-limitlessinformation&option=com_content&Itemid=57.

[14] Mathiesen, T. (1999) *On Globalisation of Control: Towards an Integrated Surveillance System in Europe*. Londres: Statewatch.

El "lado oscuro" de la vigilancia: el NeoConÓptico

Se han sugerido diversas alternativas al "Panóptico" para sustituir o poner a prueba las ideas de Foucault. Thomas Mathiesen introdujo el "sinopticismo" para explicar el proceso (dialéctico) de "las masas observando a los pocos", y el modo en el que la cultura popular ha ayudado a condicionar a la sociedad a aceptar nuevas técnicas de vigilancia y control;[15] Didier Bigo ha utilizado el concepto de "ban-opticon" para describir las prácticas excluyentes de perfilado y contención utilizadas por las fuerzas policiales europeas y en las fronteras del continente,[16] mientras que Michalis Lianos ha sugerido la idea de "periopticon" par describir un modelo gubernamental post-moderno de control más allá de la libertad, la democracia y la coacción.[17]

La idea básica del "NeoConÓptico" consiste en enfatizar tanto el papel central que desempeña el sector privado en la "creación" de políticas se seguridad basadas en la vigilancia como en el llamamiento inherentemente neoconservador a la "defensa del territorio nacional" en contra de las amenazas al "estilo de vida occidental" promovido por la UE y otros poderosos elementos.[18] La ideología neoconservadora se centra en el "derecho ilimitado a obtener beneficios",[19] que se encuentra en el epicentro de la voluntad de la UE de crear una industria de seguridad nacional. Las políticas de seguridad de la UE se basan en la filosofía neoconservadora de la política y el intervencionismo global en estados fracasados tanto para prevenir "amenazas" a su seguridad como para seguir extendiendo el mercado libre y la democracia occidental por el mundo.[20]

El "NeoConÓptico" también pretende captar la evidente relación que existe entre las políticas de "seguridad nacional" y una industria de seguridad nacional en crecimiento, otra tendencia que va de la mano de la administración Bush.[21] Los rudimentarios llamamientos a la seguridad nacional que se realizan en los discursos neoconservadores

---

15 Mathiesen, T. (1997), 'The Viewer Society: Michel Foucault's 'Panopticon' Revisited', *Theoretical Crininology*, 1(2). Discussing 'Big Brother's new avatar', Zygmunt Bauman también ha lamentado la banalización del término por parte de la television y ha comentado: "la generación actual ha olvidado su antiguo significado y las preocupaciones de los contemporaneous de Orwell. Bauman, Z. (2002) *Society Under Siege*. Cambridge: Polity Press (páginas 61-66).

16 Bigo, D. (2006) 'Globalized (in)Security: the Field and the Ban-opticon', *Harvard Conference Paper*, disponible en: http://www.ces.fas.harvard.edu/conferences/muslims/Bigo.pdf.

17 Lianos, M. (2008) '"Periopticon": Control Beyond Democracy', informe presentado en el Taller Internacional sobre Vigilancia y Democracia, Universidad de Creta, junio de 2008.

18 'Neocon' es un término inglés que se utiliza para describir la filosofía política neoconservadora. En un principio se utilizaba de forma despectiva para definir a aquellos que oscilaban entre posiciones políticas de izquierdas y de derechas, pero hoy en día se relaciona con la política de la administración Bush y sus intenciones de extender el liberalismo económico, la democracia y los derechos humanos a otros países mediante el poder militar estadounidense (estrategia representada en el proyecto neoconservador de 2000 'Project for the New American Century', véase Project for the New American Century, 2000. *Rebuilding America's Defenses: Strategy, Forces and Resources For a New Century*, disponible en: http://www.newamericancentury.org/RebuildingAmericasDefenses.pdf).
El término "neoconservador" también se utilice para describir movimientos políticos en países tan diversos como China, Irán y Japón y para algunos se ha convertido en una palabra tan "pobre, sobreutilizada, irreconocible y carente de significado" que debería dejarse de utilizar. Para más información sobre el tema consúltese la Wikipedia:
http://en.wikipedia.org/wiki/Neoconservatism. Para más información sobre el neoconservacionismo en todo el mundo, véase: http://en.wikipedia.org/wiki/Neoconservatism_(worldwide). Véase también Goldberg, J. (2007) 'Kill this word: poor, abused, unrecognizable, meaningless 'neocon'', *National Review* 2 de abril de 2007, disponible en:
http://findarticles.com/p/articles/mi_m1282/is_5_59/ai_n18744605/.

19 Klein, N. (2007) *The Shock Doctrine*. Londres: Penguin (página 322).

20 *A secure Europe in a better world: European Security Strategy*, documento del Consejo de la UE 15895/03, 8 de diciembre de 2003; disponible en: http://www.iss-eu.org/solana/solanae.pdf. Véase también: *Climate Change and International Security: Paper from the High Representative and the European Commission to the European Council*, documento del Consejo de la UE S113/08, 14 de marzo de 2008, disponible en: http://www.consilium.europa.eu/ueDocs/cms_Data/docs/pressData/en/reports/99387.pdf.

21 Véanse los capítulos 15 y 16 de: Klein, N. (2007) *The Shock Doctrine*. Londres: Penguin.

se plasman en esta aserción que se encuentra en el documento de la OTAN *Towards a Grand Strategy for an Uncertain World*, de 2008: "Los aliados occidentales se enfrentan a una defensa larga, sostenida y proactiva de su sociedad y su estilo de vida. Con ese fin, deben mantener los riesgos a distancia mientras protegen su territorio."[22]

Muchas críticos han descrito el "proyecto europeo" como neoliberal, una definición que se ajusta en gran medida a sus política social y económica. Mientras que la política exterior de la UE está estrechamente ligada a la globalización neoliberal (basada en el acceso a nuevos mercados para servicios y bienes materiales como parte de la estrategia "global europea"),[23] los procesos de militarización y titulación que se describen en este informe tienen muy poco o nada de liberales. Puede que la UE tenga algunos objetivos políticos liberales o incluso progresistas, pero la mayoría de sus políticas de inmigración, asilo, justicia criminal y contraterrorismo son conservadoras y reaccionarias. Una visión del mundo inherentemente conservadora, relacionada con los Asuntos Exteriores y la Política de Seguridad (PESC) de la UE,[24] que prometen "socios más fiables, inversiones más seguras y regiones más estables", está haciéndose con el consenso de la UE.[25]

Thomas Mathiesen, al observar paralelismos en el desarrollo de una *lex mercatoria* (el sistema internacional de leyes, normas y principios en los que se asienta la globalización económica neoliberal), ha sugerido la emergencia de una *lex vigilatoria* internacional para apuntalar el cada vez más avanzado sistema de vigilancia y control global (gran parte del cual está anclado en las leyes y políticas de la UE).[26] El "NeoConÓptico" es un simple intento de encapsular estas ideas: un proyecto entre el estado y las empresas que sea coherente, una visión potencialmente global y un diseño pensado para imponer un entramado de seguridad de nueva tecnología con el propósito expreso de mantener y extender el actual orden neoliberal en el siglo XXI.

La construcción del NeoConÓptico

Este informe hace uso de otros términos potencialmente polémicos para ayudar a explicar los avances al nivel de la UE. La idea de un "complejo industrial de seguridad" en la UE fue utilizada en nuestro informe previo en un sentido puramente descriptivo para definir la integración de la política de seguridad de la UE y la industria de seguridad nacional emergente. Hoy describe una realidad más literal en la que, en palabras de un ex Comisario de la UE, "la seguridad ya no es un monopolio que

---

[22] OTAN (2008) *Towards a Grand Strategy for an Uncertain World*, disponible en: http://www.csis.org/media/csis/events/080110_grand_strategy.pdf.

[23] Véase GLOBAL EUROPE: competing in the world, página web de la Comisión Europea: http://ec.europa.eu/trade/issues/sectoral/competitiveness/global_europe_en.htm

[24] Como ha explicado Bernd Hamm, "la visión del mundo conservadora es básicamente autoritaria y jerárquica. El estado es como la familia tradicional: el presidente gobierna y espera disciplina y obediencia de sus hijos. La desobediencia se enfrenta a castigos físicos. El mundo es malvado; el padre protege y necesita medios para proteger. Es la autoridad moral; todo lo que hace está bien… el territorio nacional se percibe como más moral que las demás naciones y, por tanto, se piensa que merece más poder. Tiene el derecho de ser hegemónico y nunca debe ceder su soberanía ni su tremendo poder económico y militar". Hamm, B. (2005) (ed) *Devastating Society: the neoconservative assault on democracy and justice*. Londres: Pluto (página 5).

[25] Solana, J. (2000) *The Development of a Common Foreign and Security Policy of the EU and the role of its High Representative*, disponible en: http://afa.at/globalview/052000/solana.html.

[26] Mathiesen, T. (2006) ''*Lex Vigilitoria*' – towards a control system without a state?' en: Bunyan, T. (ed) *The War on Freedom and Democracy: Essays on Civil Liberties in Europe*. Londres: Spokesman (páginas 38-42).

pertenece a las administraciones públicas, sino un bien común, para el que los cuerpos públicos y privados deben compartir responsabilidad e implementación."[27]

En ausencia de un escrutinio crítico, este nexo entre estado y empresas está cada vez más dirigido a la producción de un nuevo tipo de seguridad. Esta seguridad no se basa en las tradiciones de la sociedad liberal demócrata "libre" ni en las estructuras sociales que se encargaban de inculcar en la gente una sensación de seguridad (el estado del bienestar, el sistema de pensiones, las perspectivas de un trabajo seguro, etc.), sino en un autoritarismo cada vez mayor nacido de la irracional política de la inseguridad, la paranoia y el pánico moral. En 1980, Stuart Hall identificó como "populismo autoritario" el llamamiento del estado a los miedos populares sobre la inmigración, el crimen, el terrorismo y la subversión de la extrema izquierda.[28] Después de treinta años esta ha demostrado ser una técnica de gobierno duradera.

El modelo de "economía de la vigilancia" que se identifica en este informe, no es ni el del Reino Unido, que ha sido decisivo en muchas políticas de vigilancia en Europa, ni el de Estados Unidos, la tierra espiritual de la seguridad nacional, sino el de Israel, en el que el complejo militar-industrial ha ayudado a crear una de las principales industrias de la seguridad a nivel mundial.[29] A pesar de su "existencia híper-militarista" y de sus "gastos desmesurados en acuerdos ilegales, carreteras ilegales, el muro ilegal y, por supuesto, la ocupación ilegal",[30] Israel, al mantener los símbolos de la democracia liberal moderna, ha conseguido posicionarse como el estado de la seguridad nacional por *excelencia*, con los ingresos públicos aún pendientes de ajustarse.[31]

Control policial del NeoConÓptico

En este informe se utiliza el concepto de "dominio de espectro total" para explorar y conceptualizar el inevitable resultado de los enfoques autoritarios de la UE a la seguridad, al riesgo y al orden público. Este término se empezó a utilizar durante el reciente cambio de siglo en el Departamento de Defensa de Estados Unidos como eufemismo para el control sobre todos los elementos del "campo de batalla" mediante activos terrestres, aéreos, marítimos, espaciales y relacionados con la tecnología de la información.[32] La doctrina busca aprovechar la plena capacidad de la llamada "revolución en asuntos militares" engendrada por la revolución que ha experimentado la tecnología de la información.

---

27 Frattini, F. (2007) 'Security by design', *Homeland Security Europe*, basado en un discurso de Frattini en la Conferenica de Investigación en Seguridad de la UE en Berlín, 26 de marzo de 2007, disponible en: http://www.homelandsecurityeu.com/currentissue/article.asp?art=271247&issue=219.

28 Hall, S. (1980) 'Popular-Democratic vs. Authoritarian-Populism: Two Ways of 'Taking Democracy Seriously'', en: A.Hunt (ed), *Marxism and Democracy*. Londres: Lawrence and Wishart.

29 Gordon, N. (2009) 'The Political Economy of Israel's Homeland Security', *The New Transparency Project, Working Paper III, IRSP IV*, disponible en: http://www.surveillanceproject.org/files/The%20Political%20Economy%20of%20Israel%E2%80%99s%20Homeland%20Security.pdf

30 Rose, H. & Rose, S. (2008) 'Israel, Europe and the academic boycott', *Race and Class*, vol. 50, no. 1, pp. 1-20.(página 16).

31 Gordon, N. (2009) 'The Political Economy of Israel's Homeland Security', *The New Transparency Project, Working Paper III, IRSP IV*, disponible en: http://www.surveillanceproject.org/files/The%20Political%20Economy%20of%20Israel%E2%80%99s%20Homeland%20Security.pdf

32 Departamento de Defensa (2000). *Joint Vision: 2020*. Washington: USDOD.

En el contexto de la seguridad doméstica, el dominio de espectro total implica tanto un modelo intensivo de vigilancia internacional como un modelo policial basado principalmente en la fuerza militar. Steve Wright, un experto en tecnología de seguridad y tecnología militar, explica que "los sucesos del 11-S y la denominada revolución en asuntos militares solo han acelerado la ya existente tendencia a construir sistemas militares cibernéticos en los que las armas no son más que el músculo de un enorme sistema que se basa en un uso inteligente de la información mediante la comunicación, el mando y el control." Wright también prevé un despliegue de estos sistemas en ámbitos de seguridad doméstica a medida que "las doctrinas militares que no dejan ningún lugar sin vigilancia" empiezan a "tomar futuros espacios habitables" y los gobiernos "se alejan de la vigilancia de masas para centrarse en sistemas más preventivos de selección de objetivos".[33] Estos conceptos se verán con mayor detalle en la sección 10.

En el análisis final, el dominio de espectro total proporciona un nuevo modelo policial basado no en el "consentimiento", como sugiere el modelo democrático liberal, sino en continuos procesos de sumisión pública a las autoridades. Quizás es más importante que, como proyecto, este modelo implica el fin de la resistencia a este proceso (total dominio = total sumisión). Por lo tanto, si se trata de que prevalezca la libertad, no se puede permitir que este proyecto tenga éxito.

33 Wright, S. (2006) 'Report. Sub-lethal vision: varieties of military surveillance technology', *Surveillance & Society*, 4(1/2): 136-153, disponible en: http://www.surveillance-and-society.org/Articles4(1)/sublethal.pdf (página 137). El informe STOA es "una valoración de tecnologías para el control político", Investigación de la Dirección General del Parlamento Europeo, documento de trabajo (versión de consulta) 6, enero de 1998, disponible en: http://cryptome.org/stoa-atpc.htm.

PARTE II: EL GRAN NEGOCIO: EL PROGRAMA EUROPEO DE INVESTIGACIÓN EN SEGURIDAD

> *Durante la próxima primavera, un grupo de personalidades en el campo de la investigación en seguridad enviará un informe a la Comisión Europea que trazará las líneas básicas de un programa de investigación para la futura seguridad de Europa. Entones se efectuará una investigación de entre seis y ocho propuestas de proyectos financiados con 65 millones de euros durante un período de tres años. La suma resulta minúscula en comparación con el desembolso de 17.500 millones de euros para el sexto programa de investigación y desarrollo de la UE. Sin embargo, a largo plazo establecerá las claves de un sistema de seguridad nacional en Europa. Los miembros del grupo (legisladores, empresarios e investigadores) fueron elegidos en base a sus conocimientos y su experiencia en el sector de la seguridad.*
>
> Los expertos en busca de la seguridad de Europa,
> *Intelligence Online,* Enero de 2004[34]

3 La preparación del encuentro: el grupo de personalidades

La historia y el desarrollo del programa Europeo de Investigación en Seguridad se documenta en nuestro informe anterior, *Arming Big Brother*.[35] Por lo que respecta a la redacción de políticas de la UE, fue un proceso extraordinario. El "grupo de personalidades" en investigación en materia de seguridad se formó en 2003. Solo tuvieron dos reuniones previas, pero sirvieron para cimentar la estructura, los objetivos y la ideología del futuro ESRP. En el grupo había Comisarios europeos para la investigación y la sociedad de la información, además de Comisarios de asuntos exteriores y comercio, el Alto Representante de la UE para Asuntos Exteriores y Política de Seguridad, en condición de observadores, y representantes de la OTAN, de la Organización de Armamento de Europa Occidental y del Comité Militar de la UE (véase figura 1 más adelante). También había representadas ocho empresas multinacionales: las cuatro mayores empresas armamentísticas de Europa (EADS, BAE Systems, Thales y Finmeccanica) y algunas de las empresas de tecnología de la información más importantes del continente (Ericsson, Indra, Siemens y Diehl). Junto con estas, también estaban representadas siete instituciones de investigación entre las que se encontraba la Rand Corporation.

También había cuatro miembros del Parlamento Europeo, lo que daba un lustre democrático al proceso, a pesar de que uno de ellos, Karl Wogau, es conocido por ser el presidente del Comité de Seguridad y Defensa del Parlamento Europeo. El señor Wogau es además miembro de la junta de consejeros de la Security and Defence Agenda

[34] *Intelligence Online* n° 468, disponible en: http://www.intelligenceonline.com/NETWORKS/FILES/468/468.asp?rub=networks.

[35] Hayes, B. (2006) *Arming Big Brother: The EU's Security Research Programme*. Amsterdam: TNI/Statewatch. Disponible en: http://www.statewatch.org/analyses/bigbrother.pdf.

(SDA), que es un *lobby* y un *think tank*[36] de la industria armamentística.[37] Posteriormente, seis miembros del grupo contribuyeron en el libro de Wogau *The Path to European Defence*;[38] entre ellos se encontraba Burkhard Schmitt, el relator del grupo y ayudante de dirección del Instituto de Estudios de Seguridad de la UE, otro individuo descrito como "partidario del libre comercio en la industria de la defensa".[39]

En febrero de 2004 la Comisión Europea anunció que había establecido la "acción preparatoria para la investigación en seguridad" (PASR, véase la sección 4)[40] de 65 millones de euros, esgrimiendo como razón el frágil mandato de la reunión de los cabezas de estado de la UE en el Consejo Europeo de Tesalónica de junio de 2003.[41] No hubo ningún "libro verde" acerca de la investigación en seguridad, ni se establecieron posibles políticas, ni se realizó ningún debate público. La elección de una base legal para la PASR fue más polémica, puesto que finalmente se eligió el artículo 157 del tratado CE, sobre la "competitividad de la industria de la Comunidad", en lugar del artículo 163 sobre I+D. Esta decisión política significó que desde ese momento el ESRP se desarrollaría bajo el auspicio de la dirección general de la Comisión para las empresas, en lugar de la dirección general para la investigación, el brazo establecido de I+D de la Comisión. Esto implicó que los objetivos de la dirección general para las empresas (competitividad industrial y beneficios a largo plazo) prevalecían sobre los de su equivalente para I+D (la creación de una "sociedad del conocimiento").

Tabla sobre el grupo de personalidades en investigación en seguridad[42]

[36] *Think tank es un laboratorio de pensamiento o de ideas que pretendr ejercer presiónsobre instituciones y medios políticos.(N.T.)*

[37] Véase la página web de la SDA: www.securitydefenceagenda.org.

[38] Von Wogau, K. (ed) (2004) *The Path to European Defence*. Bruselas: Maklu-Uitgevers.

[39] Fuente: *US Army War College's Strategic Studies Institute*, véase: http://www.strategicstudiesinstitute.army.mil.

[40] *Decisión de la CE 2004/213/CE del 3 de febrero de 2004 sobre la implementación de la Acción Preparatoria en la Ampliación del potencial industrial europeo en el campo de la investigación en seguridad.*

[41] *Consejo Europeo de Tesalónica, 19 y 20 de junio de 2003: conclusiones de la presidencia, documento del Consejo 11638/03, 1 de octubre de 2003.*

[42] Véase también: 'The Experts Looking Out for Europe's Security', *Intelligence Online* n° 468, disponible en: http://www.intelligenceonline.com/NETWORKS/FILES/468/468.asp?rub=networks.

Organisations	Members	Their Sherpas
	European Commission	
DG Research	**Philippe Busquin** (BE) Commissioner	**Jack Matthey** (FR) Director Space/Transport
DG Information Society	**Erkki Liikanen** (FI) Commissioner	**Frans de Bruine** (NL) Director Communication Networks
	Companies	
EADS	**Rainer Hertrich** (GE) CEO	**Daniel Deviller** (FR) Chief Technology Officer
BAE Systems	**Mike Turner** (UK) CEO	**Bill Giles** (UK) Government Affairs
THALES	**Denis Ranque** (FR) CEO	**Dominique Nodet** (FR) Strategic Planning Director
FINMECCANICA	**Pier F. Guaguaglini** (IT) CEO/Chairman	**Giovanni Barontini** (IT)
ERICSSON	**Eric Lowenadler** (SW) President	**Svante Bergh** (SW) Strategic Marketing Director
INDRA	**Javier Monzon** (SP) CEO/Chairman	**Emma F. Alonso** (SP) International Affairs Director
SIEMENS	**Claus Weyrich** (GE) Head Corporate Technology	**Peter Dreyer** (GE) VP EU Affairs
DIEHL	**Thomas Diehl** (FR) CEO/Chairman	**Michael Langer** (FR)
	Research/Institutions	
TNO(1) (NL)	**Jan Dekker** (NL) CEO	**Cees Ebberwijn** (NL) Director Public Safety
FRS(2) (FR)	**François Heisbourg** (FR) Director	**Hélène Masson** (FR) Research Chief
RAND Corporation (SW)	**Carl Bildt** (SW) Member of Board of Trustees	**Frederik Johanson**
Greek Defence Ministry	**Ilias Pentazos** (GR) Defence Industry Director	**Panagiotis Gavathas** (GR)
ISCTE(3) (POR)	**Maria J. Rodrigues** (POR) Economy Professor	**Alvaro de Vasconcelos** (POR) President of IEEI(4)
Pasteur Institute (FR)	**Philippe Kourilsky** (FR) Director	**Michèle Boccoz** (FR) International Affairs Director
Belgian Defence Ministry	**Marc Vankersbilck** (BE) Military Rep. On EUMC	**Christian Micha** (BE) Planning Officer
	MEPs	
Christian Democrats	**Karl Von Wogau** (Ger)	**Christopher Raab** (Ger)
EuropeanSocialist Group	**Eryl Mc Nally** (UK)	**David O'Leary** (UK)
Christian Democrats	**Christian Rovsing** (DK)	**Steffen Brun Hansen** (DK)
European Liberal Group	**Elly Plooij–van Gorsel** (NL)	**Tineke Zuurbier** (NL)
	Observers	
EU COUNSIL	**Javier Solana** (SP) HR for CESP(5)	**Hans-Bernhard Weisserth** Head ESDP Task Force
EU COMMISSION	**Chris Patten** UK) Commissioner External Relations	**Kyriakos Revelas** (GR)
EU COMMISSION	**Pascal Lamy** (FR) Commissioner for Trade	**Paul Vandoren** (BE) Public procurements
WEAO(6)	**Ernst van Hoek** (NL) Chairman WEAO	**Hilary Davies** (UK) Manager, WEAO
OCCAR(7)	**Klaus von Sperber** (GE) Director of OCCAR	**Lucio Bianchi** (IT) Italian Defence Ministry
ESA	**Jean-Jacques Dordain** (FR) Director of ESA	**Michel Praet** (BE) Represents ESA in Brussels
NATO	**George Robertson** (UK)	**Bob Reedijk** (NL) Former NATO sec. General
	Rapporteur	
EU ISS(8)	**Burkard Schmitt** (GE)	Assistant Director EU ISS

(1) Netherlands Organisation for Applied Scientific Research – (2) Foundation pour la Recherche Strategiques – (3) Instituto Superior de Ciencias do Trabalho e da Empresa – (4) Instituto de Estudos Estrategicos e Internacionais – (5) Common European Security Policy – (6) Western European Armaments Organisation – (7) Organisation conjointe de cooperation en matiere d'armament – (8) EU Institute for Security Studies

El informe del grupo de personalidades

El grupo de personalidades propuso que la financiación de la investigación europea en seguridad estuviera al mismo nivel que la de Estados Unidos. El grupo sugirió que un gasto anual de "más de cuatro dólares por ciudadano en I+D relacionada con la seguridad en Estados Unidos significaría que en Europa sería deseable contar con un presupuesto total de I+D relacionado con la seguridad de 1.800 millones de euros por los 450 millones de ciudadanos". En su análisis final, el informe acordó un presupuesto mínimo de 1.000 millones de euros anuales para ESRP con el fin de "superar las distancias entre la investigación en defensa tradicional y la civil, fomentar la transformación de tecnologías tanto en el ámbito civil como en el de seguridad y el de defensa y mejorar la competitividad industrial de la UE".[43]

El informe que redactó en 2004 el grupo de personalidades se centró en la petición de la UE de promover el desarrollo de un complejo industrial de seguridad europeo mediante un programa de investigación en seguridad. El informe propuso cuatro argumentos principales que apoyaban estas recomendaciones. En primer lugar, afirmaba que la seguridad, el terrorismo, la proliferación de armas de destrucción masiva, los estados fallidos, los conflictos regionales, el crimen organizado y la inmigración ilegal son las principales preocupaciones tanto para los ciudadanos como para los políticos. En segundo lugar, afirmaba que la tecnología es indispensable para la seguridad: "La tecnología en sí misma no puede garantizar la seguridad, pero resulta imposible lograr esta última sin el apoyo de la tecnología. Nos aporta información sobre amenazas, nos ayuda a protegernos de ellas de manera efectiva y, si es necesario, nos permite neutralizarlas." En tercer lugar, afirmaba que existen "sinergias" entre el sector de defensa (militar) y el de seguridad (civil): "generalmente la tecnología tiene diversos propósitos. Las aplicaciones civiles y de defensa parten cada vez en mayor medida de la misma base tecnológica y se retroalimentan... Como consecuencia, la base tecnológica para las aplicaciones civiles, de defensa y de seguridad forma un *continuum*... a menudo pueden transformarse las aplicaciones de un área".[44] En cuarto lugar, afirmaba que existe una capacidad económica consistente para subsidiar el desarrollo del complejo industrial de seguridad en Europa.

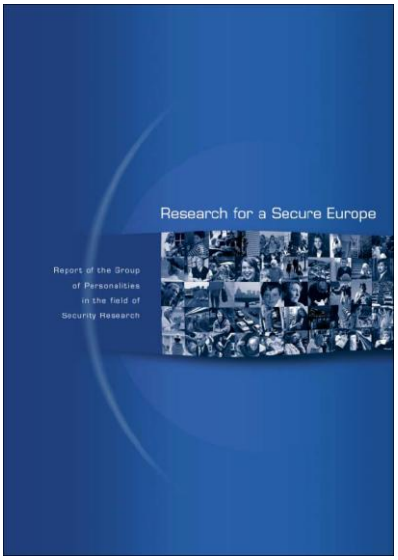
El grupo dejó constancia de que el presupuesto del Departamento de Seguridad Nacional de Estados Unidos "incluye un porcentaje notable destinado al equipo y alrededor de 1.000 millones de dólares dedicados a la investigación". La magnitud de las inversiones de Estados Unidos en investigación sobre seguridad nacional, según dijo el grupo de personalidades, significa que están "a la cabeza" del desarrollo de "tecnología y equipo que... podrían satisfacer las necesidades de Europa en gran medida". Este hecho se vio como algo problemático ya que la tecnología estadounidense iría "imponiendo progresivamente estándares normativos y operacionales a nivel mundial" y "su industria se situaría en una posición

[43] Grupo de personalidades (2004) *Research for a Secure Europe*, página 27, disponible en: http://ec.europa.eu/research/security/pdf/gop_en.pdf

[44] Grupo de personalidades (2004) *Research for a Secure Europe*, página 13, disponible en: http://ec.europa.eu/research/security/pdf/gop_en.pdf

tremendamente competitiva".[45] El personal relacionado con el ESRP ha estado recordando este argumento constantemente al autor del presente informe. Afirman que, si los gobiernos europeos tienen que gastarse miles de millones en tecnología de seguridad y en equipo, será más conveniente que compren materiales europeos. Y sería mejor si, además, las empresas europeas pudieran incorporarse al lucrativo mercado de la tecnología de seguridad.

Tras arduas negociaciones, al final el ESRP tuvo que conformarse con algo menos de 200 millones de euros anuales asignados al *Seventh Framework Programme* (VII Programa Marco de Investigación y Desarrollo, o FP7); la misma cantidad se asignó a la "investigación espacial". Sin embargo, si se tienen en cuenta los presupuestos adicionales de la investigación en seguridad y tecnología de la UE y de los programas de investigación en seguridad nacional, la suma total disponible se acerca mucho más a la petición original que el grupo de personalidades envió a la UE con el fin de equipararse a los miles de millones de dólares que se gastan cada año los EEUU en I+D en materia de seguridad.



"Research for a Secure Europe" (Investigación para un Europa segura), el informe definitivo del grupo de personalidades, se publicó en marzo de 2004 y estableció la ideología y objetivos del futuro Programa Europeo de Investigación en Seguridad.[46]

[45] Grupo de personalidades (2004) *Research for a Secure Europe*, página 21, disponible en: http://ec.europa.eu/research/security/pdf/gop_en.pdf

[46] Grupo de personalidades (2004) *Research for a Secure Europe*, disponible en: http://ec.europa.eu/research/security/pdf/gop_en.pdf

4 Acciones preparatorias: investigación en seguridad en la UE entre 2004 y 2006

> *¿Cuáles eran las expectativas iniciales?... Hay que entender que la investigación en seguridad en la Comisión es responsabilidad de la dirección general para las empresas y la industria (lo que nos da la respuesta inmediatamente). Necesitábamos crear un programa de investigación en seguridad capaz de realizar contribuciones reales y significativas a las diversas áreas de política de seguridad y, así, ayudar a mejorar la seguridad de los ciudadanos europeos (si se demostraba el valor de esas contribuciones, crecería un mercado europeo de material de seguridad). Teníamos que hacer esto sostenible, teníamos que reforzar la base industrial y la tecnológica de la seguridad europea y su cadena de suministros. Si les parece que esto está relacionado con la defensa, están en lo cierto.*
>
> Portavoz de la Comisión Europea en una convención sobre investigación en seguridad en la UE, 2008.[47]

La Acción Preparatoria para la Investigación en Seguridad de la UE (PASR) se llevó a cabo de 2004 a 2006 y ofreció un total de 65 millones de euros a 39 proyectos durante los tres años.[48] Las "áreas de prioridad" para la investigación en seguridad decididas por la Comisión Europea en base a las sugerencias del grupo de personalidades, fueron:

(i) El estado de la cuestión.
(ii) Optimizar la seguridad y la protección de sistemas en red.
(iii) Ofrecer protección contra el terrorismo.
(iv) Mejorar la administración de las crisis.
(v) Conseguir interoperabilidad y sistemas integrados en la información y la comunicación.

En 2004, se financió uno de cada trece proyectos solicitados. El reducido número de proyectos aceptados aumentaría cuando se sustituyera la oferta "de calderilla", en palabras de un funcionario británico, por los sustanciosos fondos del FP7.[49]

La característica más sorprendente de la acción preparatoria para la investigación en seguridad fue la extensión de la participación de la industria de defensa. De entre 39 proyectos de investigación en seguridad, 23 (el 60%) estaban encabezados por compañías que se dedican principalmente al sector de la defensa. Una tercera parte de los proyectos de la PASR (13) estaban encabezados por Thales (Francia), EADS (Países Bajos), compañías de Finmeccanica (Italia), SAGEM Défense Sécurité (parte del grupo SAFRAN, Francia) y la Asociación Europea de Industrias Aeroespaciales y de Defensa (ASD, el *lobby* de industria de defensa más grande de Europa). Junto con BAE Systems

47 Blasch, B (2008) 'Welcome on behalf of the European Commission and the European Programme', STACCATO [*plataforma de stakeholders para la realización de mapas en cadena de suministros, análisis de la condición del mercado y oportunidades tecnológicas*] *Foro final, 24 de abril de 2008, ASD Europe, disponible en:* http://www.asd-europe.org/Objects/2/Files/blasch.pdf.

48 Las listas de los proyectos financiados bajo la PASR entre 2004 y 2006 están disponibles en la página web de la investigación en seguridad de la Comisión Europea: http://ec.europa.eu/enterprise/security/index_en.htm.

49 Fuente: *Defensenews.com*, 26 de febrero de 2006.

(Reino Unido), estas compañías participaron en 26 (el 67%, o dos tercios) de los 39 proyectos.

El Programa Europeo de Investigación en Seguridad se basa en la necesidad de apoyar a la base tecnológica de la industria europea, pero solo en 2006, los ingresos en defensa de Thales, EADS, Finmeccanica, SAGEM y BAE Systems (empresas muy involucradas en la PASR) sumaron más de 60.000 millones de dólares. No parece que estas multinacionales estén en una mala situación en el lucrativo mercado global de la seguridad nacional. Todas ellas ofrecen "soluciones globales" a problemas de seguridad globales desde diversos lugares del mundo. EADS es uno de los diez principales proveedores del Departamento de Seguridad Nacional de Estados Unidos y BAE Systems se encuentra entre los diez proveedores más destacados del Pentágono.[50]

Además de los 39 proyectos financiados por la PASR, la UE también estaba financiando proyectos de investigación relacionados con la seguridad desde su principal programa marco de investigación desde 2002 hasta 2006 (el programa FP6, de 16.300 millones de euros). En un informe para el Parlamento Europeo, Didier Bigo y Julien Jeandesboz, estimaron que para el final de 2006, se han financiado 170 proyectos (relacionados directa o indirectamente con los temas y prioridades identificados por el grupo de personalidades y la Comisión Europea) con el FP6.[51] Entre las prioridades de investigación relevantes del FP6 se encontraban la seguridad en la tecnología de la información, la aeronáutica y la vigilancia y monitorización espacial vía satélite.

Si unimos el programa FP6 y la PASR, hacia finales de 2006 la UE ya había financiado al menos 50 proyectos de investigación que trataban aspectos relacionados con la vigilancia: sistemas de identificación biométricos, tecnologías de vigilancia y detección, control de bases de datos e información y sistemas de perfilado de riesgo. En la mayoría de los casos, estos proyectos se centraban en la aplicación de tecnologías de seguridad existentes con el fin de reforzar las leyes y el control policial, en lugar de investigar propiamente las tecnologías de seguridad *per se* (en la Parte III de este informe se examinan con más detalle algunos proyectos específicos).

Otra observación importante de la PASR es que ocho de los 39 proyectos no estaban relacionados con I+D sino con el desarrollo a largo plazo del Programa Europeo de Investigación en Seguridad y con la estructura necesaria para su implementación. Como veremos en la siguiente sección, al aumentar la "capacidad institucional" de la UE sobre la investigación en seguridad (la justificación oficial para estos proyectos), las empresas vuelven a cobrar protagonismo. Evidentemente, no hay nada nuevo en el hecho de que los gobiernos consulten sus políticas con la industria, particularmente al nivel de la UE, pero mientras que las empresas están incluidas en el ESRP, los parlamentos y la sociedad civil (con algunas excepciones) han sido excluidas en gran medida. Como se puede ver, el proceso ha sido completamente antidemocrático.

---

50 Fuentes: 'FACTBOX – Los 10 principales contratistas del Pentágono', *Reuters*: http://www.reuters.com/article/companyNewsAndPR/idUSN0739108620070507; página web de EADS: http://www.eads-nadefense.com/news/press_re/ngc_tankerpr.htm.

51 Bigo, D. & Jeandesboz, J. (2008) *Review of security measures in the 6th Research Framework Programme and the Preparatory Action for Security Research*. Bruselas: Parlamento Europeo, disponible en: http://www.pedz.uni-mannheim.de/daten/edz-ma/ep/08/EST21149.pdf.

Red de investigación en seguridad y plataforma de stakeholders[52] *de la UE*

El proyecto SeNTRE de 2004 (Red de Seguridad para la Investigación Tecnológica en Europa, PASR) estuvo encabezado por el *lobby* ASD (Asociación Europea de Industrias Aeroespaciales y de Defensa), con el apoyo de 21 organizaciones, dos tercios de las cuales provenían del sector de la defensa.[53] Su principal objetivo era "apoyar a la Comisión Europea para definir la agenda de investigación estratégica en seguridad con el fin de servir de enlace con la European Security Research Advisory Board (Junta de Asesores para la Investigación en Seguridad en Europa) y respaldarla". Entre los hallazgos del consorcio SeNTRE se encontraban "una metodología de investigación en seguridad" basada en "clasificación de misiones y amenazas", un refuerzo legal y gubernamental basado en "encuestas sobre necesidades de los usuarios", una encuesta tecnológica dentro del consorcio SeNTRE y la "identificación de prioridades e innovaciones tecnológicas". El consorcio SeNTRE también puso en marcha una "plataforma organizada de usuarios y expertos en tecnología para futuras consultas" que muy probablemente estableció las bases sobre las que se constituyó el "Foro Europeo para la Seguridad e Innovación" (ESRIF, véase sección 7).[54]

La STACCATO (siglas en inglés de la plataforma de *stakeholders* para la realización de mapas en cadena de suministros, análisis de la condición del mercado y oportunidades tecnológicas), establecida en el 2005, siguió al proyecto SeNTRE. También se financió bajo la PASR y estuvo encabezada por el *lobby* ASD. La STACCATO produjo un informe (no publicado) titulado "Cómo promover el mercado de la seguridad europeo", realizó mapas sobre las competencias de investigación en seguridad existentes en los 27 Estados miembro y propuso "métodos y soluciones para la creación de un mercado de la seguridad y una cadena de suministros estructurada en Europa".[55]

Estudio de alto nivel sobre "amenazas" y respuestas

El consorcio ESSTRT ("seguridad, amenazas, respuestas y tecnologías relevantes europeas) se encargó en el marco de la PASR para llevar a cabo un "estudio de alto nivel sobre la seguridad europea" encabezado por Thales UK, con el apoyo del Institute for Strategic Studies (Instituto internacional de estudios estratégicos) y la Crisis Management Initiative (Iniciativa para el Control de Crisis). El informe definitivo del ESSTRT, "Nuevos enfoques del contraterrorismo", no solo se centró en contraterrorismo, sino en toda la gama de seguridad interna, con la justificación de que "muchas de las respuestas que se han discutido son relevantes en la lucha contra el

[52] *Stakeholders* son todas aquellas personas y colectivos que se encuentras influídas por las decisiones de las empresas.

[53] El consorcio del SENTRE incluía a *IABG*, *QinetiQ*, *IPSC*, *ARC* (Centro de investigación austríacos), *FhG* (Fraunhofer-Gesellschaft), *EADS Astrium*, *Finmeccanica*, *Dassault Aviation*, *Sagem*, *Rheinmetall*, *EADS*, *Thales Avionique*, *Herstal Group*, *Saab Ericsson Space*, *BAE Systems*, TNO, el Centro de Investigación Conjunta de la UE (Instituto para la protección y la seguridad de los ciudadanos), Istituto Affari Internatiozionale, Délégation Générale de l'Armement (Centre d'Etude du Bouchet), VTT (Centro de investigación técnica de Finlandia).

[54] Véase también Blasch, B (2008), nota 45.

[55] El STACCATO estaba compuesto por cuatro paquetes: una plataforma de stakeholders (encabezada por EADS), análisis de condición de mercados (Finmeccanica), integración de prioridades y recomendaciones (Thales) y análisis de competencias de la cadena de suministros (Centro de investigación conjunta de la UE). Para más información consúltese la página web de ASD: http://www.asd-europe.org/content/default.asp?PageID=34.

crimen, los accidentes graves y los desastres naturales."[56] Al igual que el grupo de personalidades, el ESSTRT sostenía que los estados europeos deberían hacer lo posible por utilizar la tecnología para contrarrestar estas amenazas y mejorar la seguridad haciendo uso de servicios de inteligencia dentro y fuera de a UE, reforzando los controles fronterizos, sometiendo a la población a una vigilancia generalizada y protegiendo posibles objetivos terroristas (esto es lo que el estudio de "alto nivel "denomina " el modelo de las cuatro vallas").

Al contrario de las repetidas afirmaciones de la Comisión Europea de que el ESRP solo está relacionado con la tecnología de seguridad (y no con las políticas sobre seguridad), el estudio del ESSTRT contenía unas 70 recomendaciones detalladas (incluyendo 32 "acciones políticas" específicas de la UE). Además del informe definitivo, el ESSTRT facilitó un conjunto de 24 informes y anexos a la Comisión Europea, entre los que se incluían "Amenazas a la seguridad europea", "Encuesta sobre tecnología", "Aspectos políticos, legales y éticos de la seguridad", "Vacíos tecnológicos" y "Respuestas a amenazas terroristas". Las recomendaciones del ESSTRT concluían con un extraordinario "propósito estratégico unificado para controlar futuras actividades a todos los niveles", cuyo borrador estaba escrito al estilo de un tratado, provisión o declaración de la UE y llamaba a los Estados miembro a "evitar políticas que pudieran suponer nuevos obstáculos para las medidas y políticas relacionadas con el contraterrorismo" (véase el cuadro a continuación).[57]

¿Estableciendo la agenda?

Los Estados miembro y sus instituciones:

- *de manera coherente con los tratados europeos y con el espíritu de solidaridad entre ellos, se asegurarán de que cumplen los objetivos fundamentales de la Unión Europea respecto a la lucha contra el terrorismo, ya se generen de forma interna o externa, incluyendo:*


ESSTRT Deliverable D6-1
FINAL REPORT
New European Approaches to Counter Terrorism
21 MARCH 2006
PRINCIPAL AUTHORS
CRISIS MANAGEMENT INITIATIVE IISS THALES

- *El flujo continuo y libre de personas, bienes, servicios y capital; y el flujo libre de información.*
- *La protección de la sociedad civil y de los derechos individuales, manteniendo justicia, armonía y estabilidad social.*
- *El mantenimiento del crecimiento en la actividad económica.*
- *La mejora de las relaciones políticas con las contrapartes externas.*

- *como condición básica para conseguir este propósito, establecerán un conjunto de criterios generales mediante los cuales se puedan juzgar las próximas acciones de la UE, ya sean los Estados miembros o sus instituciones; estos*

56 ESSRT (2006) *Final report: New European Approaches to Counter Terrorism*. Londres: Thales Research and Technology, International Institute for Strategic Studies, Crisis Management Initiative (CMI) & Thales e-Security (TeS),disponible en: http://www.iiss.org/programmes/defence-analysis-programme/analysisarchive/european-security-high-level-study/.

57 ESSTRT, 2006: 6-7, véase nota anterior.

criterios deben incluir ***evitar políticas que pudieran suponer nuevos obstáculos para las medidas y políticas relacionadas con el contraterrorismo***.

(Recomendación del ESSTRT a la UE, énfasis añadido).

El "estudio de alto nivel sobre seguridad, amenazas, respuestas y tecnologías relevantes europeas" fue financiado por la PASR y encabezado por Thales UK con el apoyo del Institute for Strategic Studies y la Crisis Management Initiative.

Además de los proyectos ESSTRT, SeNTRE y STACCATO, había otros cinco proyectos de la PASR enfocados hacia el desarrollo estratégico del ESRP: el proyecto IMPACT, un programa de la UE sobre adquisición e investigación en contraterrorismo de armas químicas, biológicas, radiológicas y nucleares; PETRANET, que establece una "red de usuarios para adoptar la investigación en seguridad"; SECURESME, sobre la creciente participación de pequeñas y medianas empresas en el ESRP; y por último los proyectos USE-IT y SUPHICE, sobre las redes de comunicación seguras para la investigación en seguridad.

Solo uno de los 39 proyectos de la PASR (el PRISE, encabezado por la Academia de Ciencias Austríaca) se centraba específicamente en la privacidad y las libertades civiles en el contexto de la investigación en seguridad europea. El consorcio PRISE se estableció para desarrollar "principios aceptables y aceptados para las industrias de seguridad y las políticas europeas" basándose en "tecnologías de seguridad para mejorar la privacidad". En su informe definitivo, el PRISE ofreció criterios detallados y bien razonados además de recomendaciones, entre las que se incluía el afianzamiento de los estándares de protección de datos y privacidad de la UE en todas las tecnologías de seguridad.[58] Desafortunadamente, parece ser que estos estándares tuvieron poca influencia en el desarrollo del ESRP o en la más amplia agenda política europea. Así pues, en estos momentos los políticos de la UE están debatiendo sobre limitar la disponibilidad de tecnologías para mejorar la privacidad al pueblo europeo afirmando que pueden ser "explotados" por terroristas y criminales" (véase la sección 25).

[58] Todos los detalles del proyecto y los informes están disponibles en la página web del PRISE: http://www.prise.oeaw.ac.at/.

5 La preparación de la agenda: la junta de consejeros de investigación en seguridad europea

> *Resulta muy extraño a nivel nacional, pero más a nivel europeo, que los usuarios a los que se destinan los resultados de la investigación en seguridad definan el desarrollo de la investigación a medio plazo requerido en los términos que los proveedores y los encargados de llevar a cabo la investigación en seguridad. Esto es exactamente lo que la Comisión Europea ha logrado con la creación y la implementación de la junta de consejeros de investigación en seguridad europea...*
>
> *Su preparación pone de manifiesto la importancia de la investigación y las tecnologías de seguridad. Sin ella no podría haber ningún progreso ni hacia las aspiraciones sociales por una Europa más libre, segura y abierta, ni hacia los beneficios de una cadena de suministros tecnológicos más competitiva. Todas estas esperanzas para el futuro dependen del desarrollo y la implementación de nuevas tecnologías y por extensión, de que Europa disponga de la capacidad tecnológica necesaria.*
>
> Prefacio; informe de la junta de consejeros de investigación en seguridad europea, 2006.[59]

El 22 de abril de 2005 la Comisión Europea estableció la junta de consejeros de investigación en seguridad europea (ESRAB) con el fin de "asesorar acerca de los contenidos del ESRP y su implementación, prestando especial atención a las propuestas del grupo de personalidades".[60] Al igual que este grupo, la ESRAB contaba con "expertos de varios grupos de *stakeholders*: usuarios, industria y organizaciones de investigación". No se realizaron consultas en los parlamentos nacionales ni en el europeo sobre el nombramiento de los miembros de la ESRAB; los 50 puestos de la junta fueron designados por embajadores de la UE (las representaciones permanentes de los Estados miembros), la Agencia de Defensa Europea creada recientemente y otros "grupos de *stakeholders*" no especificados.

La ESRAB tenía el deber de asesorar a la Comisión Europea en cualquier cuestión relacionada con el desarrollo del ESRP y de emitir recomendaciones acerca de:

- las misiones estratégicas y las áreas de prioridad en la investigación en seguridad;
- asuntos de implementación como el intercambio de información clasificada y los derechos de propiedad intelectual;
- el uso de infraestructuras de investigación y evaluación públicas;
- una estrategia de comunicación de investigación en seguridad.

A la ESRAB se le permitió adoptar sus propias normas de procedimiento. Había dos grupos de trabajo dentro de ella, cada uno de los cuales contaba con 25 representantes.

---

[59] ESRAB (2006) *Meeting the challenge: the European Security Research Agenda – A report from the European Security Research Advisory Board*. Bruselas: Comisión Europea, disponible en: http://ec.europa.eu/enterprise/security/doc/esrab_report_en.pdf.

[60] *Decisión de la Comisión Europea 2005/516/CE del 22 de abril de 2005que establece la ESRAB.*

El grupo 1, "el grupo de la tecnología", se encargó de los "requisitos de la demanda de investigación en seguridad", mientras que el grupo 2, el "grupo de los activadores", se encargó de los "requisitos de la cadena de suministros tecnológicos". En lugar de la investigación, esta estructura parece haber tenido más relación con las necesidades comerciales y con el objetivo de integrar mejor la cadena de suministros (empresas) con la cadena de demanda (gobiernos). [61]

Las industrias de defensa y de seguridad, que ocupaban 14 de los 50 asientos, estaban bien representadas. Siete de las ocho empresas del grupo de expertos (EADS, BAE Systems, Thales y Finmeccanica, Ericsson, Siemens y Diehl) contaban con asientos en la ESRAB. La junta estuvo presidida por Markus Hellenthal de EADS y Tim Robinson de Thales, cada uno de los cuales tuvo un "periodo presidencial". El resto de asientos de la ESRAB se destinó a los Estados miembros (18), a académicos e instituciones de investigación (14), a la UE, representada por Agencia de Defensa Europea y la EUROPOL, y a dos "grupos de libertades civiles y *think tanks*". [62]

La Comisión Europea fue la principal responsable de la inclusión de dos "organizaciones y *think tanks* de la sociedad civil", si bien parece ser que considera la Crisis Management Initiative (establecida por el antiguo primer ministro de Finlandia, Martti Ahtisaari) una "organización de libertades civiles". [63] Por lo que respecta al *think tank* al que se refería la Comisión Europea, se traba o bien del Instituto de Estudios de Seguridad (relator del grupo de personalidades) financiado por la UE, o bien el Instituto Affari Internazionali (Instituto de asuntos internacionales italiano), ambos con agendas de línea conservadora.

El informe de la ESRAB

El informe definitivo de la ESRAB, *Meeting the challenge: The European Security Research Agenda* (Afrontar el reto: la agenda de investigación en seguridad europea), se publicó en septiembre de 2006 y estableció las prioridades de investigación del

61 La lista de los 50 miembros de la ESRAB está incluida en el informe final del grupo, disponible en: http://ec.europa.eu/enterprise/security/doc/esrab_report_en.pdf.

62 La ESRAB estaba apoyada por 14 servicios de la Comisión distintos y por cinco miembros del Parlamento Europeo. No se ha proporcionado información acerca de la razón por la cual estos constituyentes no participaron como miembros completos de la ESRAB. Véase Gasparini, G. y Leone, C., *'Meeting the challenge: the European Security Research Agenda', the final report of the European Security Research Advisory Board*, IAI/Finmeccanica [informe sin referencia sobre la ESRAB], disponible en: http://www.iai.it/pdf/ESRAB/ESRABGasspariniLeone.pdf.

63 La iniciativa para el control de crisis es una "organización independiente sin ánimo de lucro que, de manera innovadora, promueve la seguridad sostenible y trabaja para conseguirla y para fortalecer la capacidad de la comunidad internacional de resolver conflictos y de gestionar crisis de forma eficaz. Su trabajo se basa en extensas redes de stakeholders y combina análisis, acción y apoyo". Véase la página web de la iniciativa: http://www.cmi.fi /.

programa 2007-13 del FP7.[64] El informe tomó el mismo enfoque respecto a la seguridad que el grupo de personalidades, es decir, dirigido por la tecnología y la economía, si bien es cierto que incorporó gran parte de las reflexiones que se desprendieron de los estudios "de alto nivel"encargados en el marco de la PASR (especialmente los proyectos ESSTRT y SenTRE).

El informe proponía un definición extremadamente amplia de la "investigación en seguridad" que abarcaba todas las "actividades de investigación que pretendan identificar, prevenir, disuadir, preparar y proteger de actos maliciosos ilegales o intencionales que dañen a las sociedades europeas, seres humanos, organizaciones o estructuras, bienes materiales o inmateriales e infraestructuras, incluyendo la continuidad mitigadora y operacional tras una ataque de estas características (también aplicable tras catástrofes naturales o industriales)". La ESRAB desarrolló las 5 "áreas de misión" centrales del ERSP: "seguridad fronteriza", "protección contra el terrorismo y el *crimen organizado*" (nótese la ampliación de la misión), "protección de infraestructuras críticas", "restauración de la seguridad en caso de crisis" e "integración, conectividad e interoperabilidad".

Para cada una de estas "áreas de misión" aparentemente distintas la ESRAB propuso la misma respuesta: imponer una total vigilancia (la llamada "conciencia y evaluación de la situación") mediante los siguientes métodos: uso de toda la tecnología de vigilancia disponible en el mercado; introducción de comprobaciones de identidad y protocolos de autentificación basados en sistemas de identificación biométricos; despliegue de una serie de tecnologías y técnicas de detección en todos los puntos de control de identidad; uso de sistemas de comunicación de tecnología punta para asegurar que los agentes del refuerzo de la ley tienen un conocimiento total de la información; uso de análisis de perfil, de obtención de datos y de conducta para identificar a individuos sospechosos; uso de evaluación y modelado de riesgos para predecir (y mitigar) comportamientos humanos; asegurar una rápida "respuesta a incidentes" y la consecuente intervención para neutralizar la amenaza, de forma automática siempre que sea posible; finalmente, asegurar que todos los sistemas son completamente interoperables de manera que las aplicaciones tecnológicas que se usan en una misión puedan utilizarse en otras. Este modelo extremo de seguridad se trata con más detenimiento en la Parte III de este informe.

"Implicaciones éticas"

Scientists for Global Responsibility (SGR, un grupo de académicos críticos del Reino Unido) informan de que la "lucha contra el terror" ha "alimentado el incesante aumento de la carga que supone la militarización mundial" y ha "contribuido a causar una serie de cambios en la manera que tienen los políticos de enmarcar la seguridad (muchas de las cuales resultan muy polémicas)". Según el SGR, entre los cambios más significativos se encuentra "el creciente énfasis en la intención de usar armas de tecnología punta para afrontar los problemas de seguridad".[65]

64 ESRAB (2006) *Meeting the challenge: the European Security Research Agenda – A report from the European Security Research Advisory Board*. Bruselas: Comisión Europea, disponible en: http://ec.europa.eu/enterprise/security/doc/esrab_report_en.pdf.

65 Langley, C., Parkinson, S. & Webber, P. (2008) *Military influence, commercial pressures and the compromised university*, Scientists for Global Responsibility, disponible en: http://www.sgr.org.uk/ArmsControl/BehindClosedDoors_jun08.pdf.

El informe de la ESRAB dedicó solo una de sus 84 páginas a la "ética y la justicia", en la que observaban que "las tecnologías de seguridad, además de las políticas que las acompañan, despiertan diversas inquietudes éticas y legales entre los ciudadanos europeos".[66] En este punto la ESRAB reconoció el "animado debate público sobre las libertades civiles" y "la pérdida de privacidad potencial" asociados con las medidas de seguridad y contraterrorismo y afirmó que "el respeto de la privacidad y las libertades civiles debería ser el principio básico (del ESRP)". Esta fue una de las diez "conclusiones clave" del informe, pero al margen de la recomendación de que la investigación en seguridad debería "tener en cuenta el triángulo de dependencia mutua formado por tecnología, dinámica organizacional e impacto humano", no se volvía a hacer mención al modo en que se podrían proteger las libertades civiles y los derechos humanos, ni se tuvo en cuenta su protección en casos de tecnología punta como los que se destacan más adelante.

A pesar de que los tratados de la UE establecen obligaciones legales claras para los políticos acerca de la protección de los derechos fundamentales, la ESRAB adoptó un punto de vista más adaptable respecto a los derechos y las libertades, ya que los veía como un "reto político", un experimento para encontrar un equilibrio "socialmente aceptable". En este escenario de compensación, se ha conseguido reducir las libertades civiles a "implicaciones éticas" que deben "equilibrarse" con las necesidades de la seguridad y que, por lo tanto, pueden restringirse cuando esta última lo precise. El hecho de que tanta gente piense que este "equipaje", que está cubierto por el maquillaje constitucional de la democracia europea, representa la libertad fundamental conseguida después de tantos siglos, también resulta un cambio de paradigma.

Mientras que el informe de la ESRAB dedicó una gran cantidad de páginas a convencer al lector de que la tecnología puede ayudar de muchas maneras a protegerle de amenazas como el crimen y el terrorismo, no mostró ningún interés en las causas que originan estos fenómenos ni en las políticas sociales que pueden ayudar a resolverlos, exceptuando una sola referencia al programa de investigación en "ciencias sociales y humanas" de la UE (que recibiría una fracción del total de los fondos disponibles para la seguridad y el espacio, como se verá más adelante). En lugar de ello, la ESRAB promovió una nueva disciplina académica de "economía de seguridad", que incluye análisis de riesgos, análisis de finanzas públicas y estiramiento de los "costes económicos" que conlleva la financiación de la inseguridad y la investigación para combatir el terrorismo.

[66] Informe de la ESRAB (página 60), disponible en: http://ec.europa.eu/enterprise/security/doc/esrab_report_en.pdf.

ESRAB: “tecnología en distintas áreas de misión”[67]

Dominio tecnológico	Áreas de prioridad tecnológica
Tecnología de señal e información	Técnicas de fusión de datos, recolección y clasificación de datos, tecnología de procesado de imágenes y patrones, tecnología de fusión de información, tecnología de control de datos e información
Inteligencia artificial y apoyo de decisiones	Obtención de textos y datos, técnicas de sistemas inteligentes basados en el conocimiento e inteligencia artificial, control del conocimiento, modelado y simulación, tecnología de apoyo de optimización y decisión
Equipo con sensores	Cámaras, equipo con sensores para radares, sensores con fines nucleares, radiológicos, biológicos y químicos (especialmente en tecnología para la detección de amenazas biológicas y químicas), equipo con sensores infrarrojos pasivos
Tecnología de sensores	Sensores hiperespectrales y multiespectrales, procesado hiperespectral y multiespectral, sensores autónomos pequeños, tecnología de polvo inteligente, tecnología de sensores infrarrojos, sensores de terahercios, tecnología de sensores ópticos, sensores acústicos (pasivos)
Equipo de comunicación	Comunicaciones reconfigurables, comunicaciones móviles aseguradas, control de redes de comunicación, equipo de control, supervisor de red, comunicaciones independientes aseguradas de red y protocolo, enlaces de datos asegurados inalámbricos de banda ancha para comunicaciones aseguradas, protección de las redes de comunicación contra entornos rigurosos
Ciencias humanas	Análisis y modelado de comportamientos humanos, comportamiento poblacional, factores humanos en el proceso de decisión, equipos, organizaciones y culturas
Tecnología de seguridad de la información	Encriptado y control clave, obtención de datos, control de acceso, tecnologías de filtrado, tecnologías de autentificación, tecnologías de encriptado (criptografía)
Tecnología informática	Tecnología de protocolo, arquitectura de software, técnicas informáticas seguras, informática de alto rendimiento, informática crítica de alta integridad y seguridad, ingeniería de software
Sistemas de información de guerra e inteligencia	Infraestructuras para apoyar el control y la diseminación de información, herramientas de control de las políticas de seguridad cibernética, optimización, sistemas de apoyo de planificación y decisión
Simulación de escenarios y decisiones	Conceptos de análisis y reducción de impacto, simulación y modelado avanzados de comportamiento humano, simulación para la toma de decisiones (en tiempo real), predicción de vulnerabilidad de estructuras, técnicas de control de evacuación y consecuencias, simulación de misiones
Sistemas de la información	Infraestructuras para apoyar el control y la diseminación de información, herramientas de control de las políticas de seguridad cibernética, optimización, sistemas de apoyo de planificación y decisión
Navegación, guía, control y rastreo	Etiquetas de identificación de radiofrecuencia, GPS, radionavegación, búsqueda de direcciones y guía con mapas, seguimiento mediante códigos de barras
Tecnología forense (biometría)	Reconocimiento mediante huellas dactilares, reconocimiento facial, reconocimiento mediante iris, retina, voz, escritura y firma
Plataformas integradas	Vehículos no tripulados (tierra, mar y aire), plataformas más ligeras que el aire, satélites de navegación y vigilancia
Tecnología de supervivencia y endurecimiento	Evaluación y endurecimiento del código de fabricantes de equipo, ropa y equipo inteligentes, blindado de cristales y cementos, arquitectura específica de edificios críticos, consecuencias de los choques y estallidos
Autentificación electrónica	Sistemas de etiquetado electrónicos, tarjetas inteligentes
Biotecnología	Análisis rápido de agentes biológicos y de susceptibilidad humana a enfermedades y sustancias intoxicantes, técnicas de descontaminación, análisis y técnicas de purificación hídricos, análisis y técnicas de control alimenticios
Simuladores, entrenadores y entornos sintéticos	Realidad virtual y aumentada, sistemas de entrenamiento tácticos y del equipo, sistemas de entrenamiento de los mandos y el personal, entornos sintéticos
Materiales químicos, biológicos y médicos	Técnicas de detección químicas y biológica
Protección de señales (en entornos bélicos)	Reconocimiento de objetivo no cooperativo, sistemas de información geográficos
Sistemas espaciales	Observación de la Tierra (imagen y comunicaciones)
Materiales ligeros y fuertes, cubrimiento...	Materiales ligeros para la protección humana, material textil inteligente, materiales ligeros para la protección de emplazamientos, tecnología de materiales auto protectores resistentes a explosiones, tratamiento de superficies para aumentar la duración, reducción de la corrosión
Generación, almacenamiento y distribución de energía	Generadores eléctricos, baterías eléctricas, distribución de la energía

67 Cabe destacar que las “tecnologías de control de masas”, “los aparatos de detención de masas” y las “armas no letales” se encontraban entre las tecnologías de seguridad incluidas en el borrador del informe de la ESRAB que obtuvo el autor de este documento, pero se omitieron en la versión definitiva (versión no publicada sobre el informe mencionado, v. 2.7, con fecha de septiembre de 2006, página 52). Para más información acerca de las “armas no letales” consúltese el apartado correspondiente de este informe.

6 El programa FP7 y más allá: investigación en seguridad entre 2007 y 2013

> *(El programa FP7) no invita al debate político. De hecho, no estamos ante opciones que puedan discutirse, sino ante lo que se presenta a sí mismo como una mera representación de la "agenda de Lisboa", que respalda totalmente sus eslóganes, como "sociedad del conocimiento", "economía del conocimiento", "el conocimiento y su explotación" como "la clave para el crecimiento económico" y la "competitividad de las empresas"... estamos ante un conjunto de lo que en francés se conoce como "mots d'ordre". Los "mots d'ordre" no están hechos para inducir a la reflexión ni al debate, sino para crear acuerdo y una percepción consensual, lo que pone a la defensiva a aquellos que piensan "sí, pero...". Sí al empleo, sí al modelo europeo, sí a todas esas mejoras y, desde luego, sí al progreso del conocimiento. Pero... ese "pero" llega demasiado tarde, después de muchos acuerdos y será fácil caer en la trampa en lugar de tratar medios de los que se dispone y ratificar los objetivos consensuados percibidos. El funcionamiento y el objetivo de los "mots d'ordre" consiste en capturar e inhibir la capacidad de pensar.*
> Catedrática Isabelle Stengers, filósofa en el ámbito científico[68]

El FP7 es el séptimo Programa Marco de Investigación y Desarrollo de la UE.[69] Se desarrolla entre los años 2007 y 2013 y tiene un presupuesto total de 51.000 millones de euros divididos entre diez ámbitos de investigación colaborativa (véase el diagrama correspondiente más adelante) y tres temas: "ideas", personas" y "capacidades".[70] "La seguridad y el espacio" tienen un presupuesto conjunto de 2.800 millones de euros, que se dividen a partes iguales entre ambos ámbitos.

El componente de investigación en seguridad del FP7 constituye una clase magistral acerca de cómo prevenir el debate sustituyendo propuestas específicas por generalidades y adaptando los objetivos en base a los medios disponibles.[71] Las áreas racionales y prioritarias de la investigación en seguridad del FP7 son *idénticas* a las establecidas por la ESRAB, pero están condensadas en unas pocas páginas que carecen de la sustancia. Al leer el programa del FP7 con su compromiso explícito con las libertades civiles, la privacidad, los derechos fundamentales y la democracia, los lectores poco observadores no encontrarán muchas razones para preocuparse.

---

68 Stengers, I. (2005) *Speech to the "What Science, What Europe?" conference in the European Parliament*, 2-3 de mayo de 2005, disponible en: http://www.peoplesearthdecade.org/articles/article.php?id=381.

69 Véase *Seventh Framework Programme*, página web de la Comisión Europea: http://cordis.europa.eu/fp7/.

70 El Consejo de la UE (los Estados miembro) aceptó en un principio un presupuesto total de 72.000 millones de euros. Si bien la suma definitiva era bastante inferior, el presupuesto del FP7 sigue siendo un 60% más elevado que el del FP6.

71 *Decisión número. 1982/2006/CE del Parlamento Europeo y el Consejo del 18 de diciembre de 2006 relacionado con el FP7 de la CE para la investigación, el desarrollo tecnológico y las actividades de demostración (2007-2013)*, OJ 2006 L 412/1.

La petición de propuestas del primer año del ERSP (2007) recibió 325 respuestas elegibles, con un fondo solicitado de más de 1.000 millones de euros. La Comisión Europea aportó 156,5 millones de euros a 46 proyectos exitosos (lo que hizo que el programa estuviera sobre suscrito siete veces).[72] Estos proyectos se analizan con más detalle entre los apartados IV y VI de este informe.

De los 46 proyectos de investigación financiados bajo las peticiones del 2007, 17 (el 37%) están encabezados por organizaciones que sirven principalmente al sector de la defensa, mientras que otros cinco están encabezados por empresas de la industria de la seguridad. Si bien el sector de la defensa parece tener menos presencia que en la PASR (entre 2004 y 2006), la abrumadora mayoría de los proyectos contaban con una o más "personalidades" procedentes de este sector.

De los gigantes de la seguridad europeos, las compañías Thales (que encabeza tres de los proyectos y participa en otros cinco) y Finmeccanica (que encabeza dos proyectos del ESRP y participa en otro seis) están especialmente bien representados. EADS también tiene una gran presencia, al igual que Saab, Sagem y BAE Systems. De las organizaciones representadas en el grupo de personalidades y en la ESRAB, las agencias de investigación en seguridad sueca (FOI) y Holandesa (TNO) encabezan cuatro proyectos y participan en otros siete cada una.

A pesar de que, de manera instintiva, puede resultar incómodo que los fabricantes de armas se dediquen al sector de la seguridad nacional, su dominio en este mercado emergente también refleja un sustancial esfuerzo por su parte de replantearse sus estrategias de negocio básicas tras los atentados del 11-S. Mientras que antes del 2001 el concepto de seguridad nacional no había entrado a formar parte del léxico común, tras los atentados en Nueva York las multinacionales no tardaron en establecer divisiones similares al aparato de estados federales reestructurados de los EE.UU. y al recientemente establecido Departamento de Seguridad Nacional. Las compañías de defensa europeas siguieron rápidamente la estela de sus homólogas estadounidenses, lo que les dejó en buena posición para explotar la seguridad nacional europea.

Las organizaciones y compañías de Israel, cuyo desarrollo en materia de seguridad nacional es anterior al 11-S y procede de la política de ocupación y el intento de vigilar y controlar a la población palestina, siguieron el ejemplo de las europeas. Hay integrantes israelíes participando en diez de los 46 primeros proyectos del ESRP y liderando cuatro de ellos. También es destacable que actualmente el programa de investigación en seguridad del FP7 incluya proyectos de demostración (en los que se fabrican y se ponen a prueba prototipos de sistemas de seguridad) y proyectos de infraestructuras (por ejemplo sistemas de comunicaciones y capacidad de control de crisis de infraestructuras críticas). Estos proyectos están claramente dirigidos a la obtención pública (tanto a nivel nacional como de la UE) de tecnologías de seguridad más que a llevar a cabo una investigación objetiva tradicional.

---

72 A causa de los retrasos en la puesta en marcha del FP7 y del tiempo que se tomó la CE para evaluar las propuestas, completar las negociaciones contractuales y publicar la información pertinente, en el momento de escribir este informe (junio de 2009) solo se disponía de los resultados de la petición de propuestas de financiación de 2007 (que se publicaron en mayo de 2009). En ese momento la CE seguía evaluando las propuestas aspirantes a la financiación de la petición de 2008. La petición de propuestas de 2009 se prevé para septiembre de 2009. La lista de proyectos financiados de la petición de 2007 se encuentra disponible en la página web de la CE: http://ec.europa.eu/enterprise/security/index_en.htm. Todos los proyectos financiados bajo los programas marco de la UE se pueden encontrar realizando búsquedas en la página web de CORDIS: http://cordis.europa.eu/search/index.cfm?fuseaction=proj.advSearch.

Investigación para la competitividad industrial de la UE[73]

Investigación para inversores de capital a nivel mundial[74]

Ampliación del programa de investigación en seguridad de la UE

También se dispone de sustanciosos fondos para la "investigación en seguridad" bajo una serie de líneas presupuestarias alternativas de la UE, lo que hace suponer que la "investigación en seguridad" total de la UE será notablemente superior a los 200 millones de euros anuales asignados al ESRP. El Centro Común de Investigación de la UE inició un "programa de protección de infraestructuras críticas" (PIC) independiente. Además, se ha emitido una petición de propuestas conjunta bajo los componentes de investigación en seguridad y las tecnologías de la información y la comunicación (TCI) del FP7. El programa de PIC tiene su propio presupuesto para desarrollar "las piezas clave de tecnología para crear infraestructuras de la información seguras, adaptables, con capacidad de respuesta y disponibilidad absoluta" así como "infraestructuras de transporte y energía capaces de soportar ataques maliciosos o fallos accidentales y de garantizar una continua provisión de servicios" (para más información consúltese la sección 20).

También se dispone de fondos para tecnología de seguridad en los 4.000 millones de euros dedicados al Fondo Europeo para la Solidaridad y el Control de Flujos Migratorios, del cual se destinan 1.800 millones de euros a fronteras exteriores y unos 676 millones al Fondo Europeo para el Retorno, relacionado con la expulsión y la repatriación de "inmigrantes ilegales".[75] En el futuro se ampliarán los fondos dedicados

---

[73] Resumen de los 45 primeros proyectos financiados bajo el ESRP en 2007, disponible en: http://ec.europa.eu/enterprise/security/doc/fp7_project_flyers/securityresearchlowdef.pdf.

[74] Estudio de Mercado de Visiongain (2009) *Global Homeland Security 2009-2019* ($2,481.00), véanse los informes de ASD: http://www.asdreports.com/shopexd.asp?ID=1442.

[75] Véase *Solidarity and Management of Migration Flows*, página web de la CE: http://ec.europa.eu/justice_home/funding/intro/funding_solidarity_en.htm. Los Estados miembro también disponían de fondos adicionales

a la investigación en seguridad a nivel nacional. Al menos siete Estados miembro ya han establecido programas de investigación en seguridad nacional de acuerdo con las recomendaciones previas del grupo de personalidades y la ESRAB (Reino Unido, Francia, Alemania, Austria, los Países Bajos, Suecia y Finlandia) y la UE ha puesto en marcha una "red nacional de puntos de coordinación del ESRP" a través del SEREN, un proyecto financiado por el FP7.[76] La "fase uno" del proyecto SEREN consistirá en el desarrollo de una red de puntos de contacto nacionales en la investigación en seguridad entre los estados participantes, tanto los que pertenecen a la UE como los que no.

Puesto que la investigación relacionada con la seguridad empezó a abrirse paso en el FP6,[77] que era más extenso, es probable que el grado de convergencia entre el ESRP y el resto de elementos del FP7 (enumerados más adelante). El programa espacial europeo ahora tiene un destacable componente de seguridad y defensa (véase sección 18 más adelante), mientras que la investigación financiada por la UE en alimentación, energía, medio ambiente, transporte y tecnologías de la información y la comunicación incluyen forzosamente seguridad alimentaria, seguridad energética, seguridad medioambiental, y así sucesivamente. Si la nanotecnología, de la que tanto se habla y a la que se va a destinar la asombrosa cifra de 3.500 millones de euros bajo el FP7, se traslada a las ciencias aplicadas, también tiene la capacidad de impactar en gran medida en la investigación militar y en seguridad puesto que revolucionará las posibilidades de vigilancia, la guerra química y bacteriológica, la munición y el armamento.[78] Según Steve Wright la nanotecnología cambiará la manera de construir armas "para mejorar en el seguimiento y la destrucción de objetivos". La "súper miniaturización permitirá que los soldados individuales se conviertan en partes más eficientes en el campo de batalla mientras sus comandantes usan métodos de vigilancia para ver a través de los cascos de sus hombres.[79]

El presupuesto de cooperación del FP7[80]

---

para material y tecnología de control fronterizo bajo el Acuerdo de Schengen (con un valor aproximado de 1.000 millones de euros). La disponibilidad de éstos para Bulgaria y Rumanía estaba garantizada por la 'Transition Facility' (con un valor aproximado de 100 millones de euros anuales), fuente: Frattini, F. (2007), Security by design', *Homeland Security Europe*, disponible en: http://www.homelandsecurityeu.com/currentissue/article.asp?art=271247&issue=219.

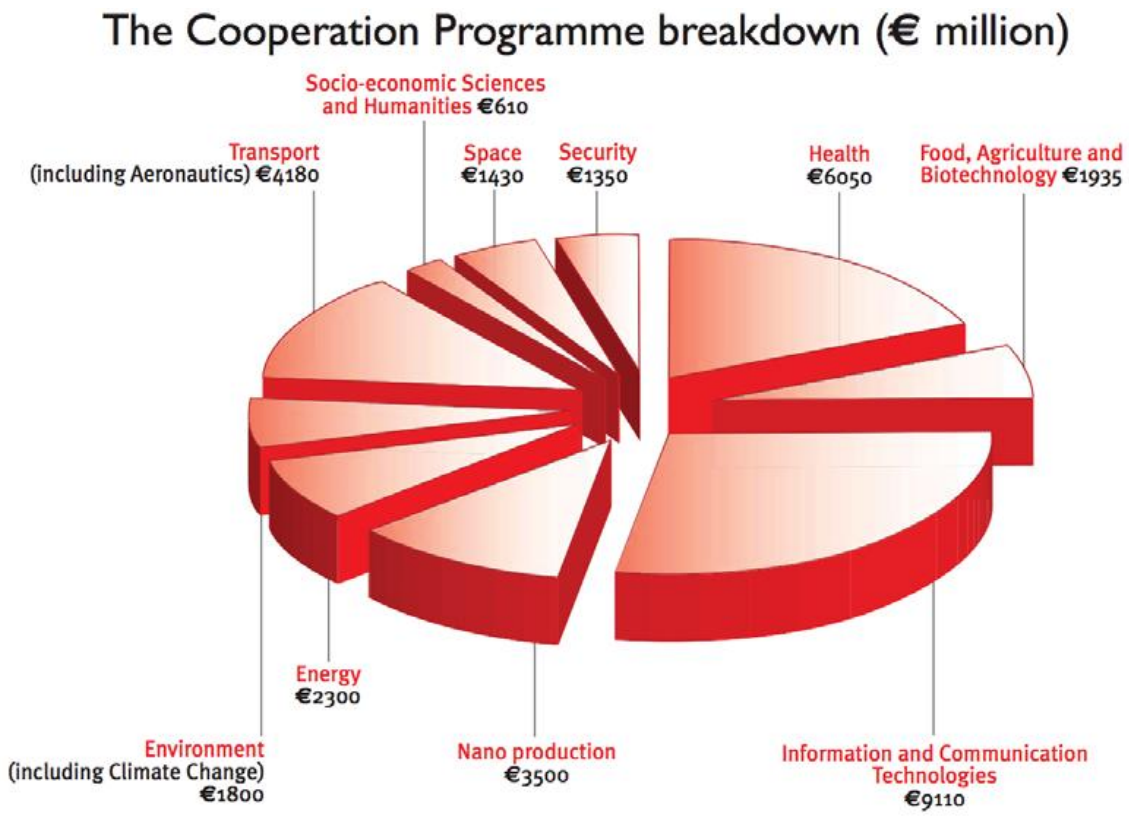
[76] Véase página web del proyecto SEREN: http://www.seren-project.eu/.

[77] Bigo, D. & Jeandesboz, J. (2008) *Review of security measures in the 6th Research Framework Programme and the Preparatory Action for Security Research*. Bruselas: Parlamento Europeo, disponible en: http://www.pedz.uni-mannheim.de/daten/edz-ma/ep/08/EST21149.pdf.

[78] Langley, C. (2005) *Soldiers in the laboratory: Military involvement in science and technology - and some alternatives*, Folkstone: Scientists for Global Responsibility (páginas 54-55), disponible en: http://www.sgr.org.uk/ArmsControl/MilitaryInfl uence.html. Véase también 'Industry, NGOs at odds over nanotech regulation', *Euractiv* 4.3.2009, disponible en: http://www.euractiv.com/en/science/industry-ngos-odds-nanotech-regulation/article-179936.

[79] Wright, S. (2006) 'Report. Sub-lethal vision: varieties of military surveillance technology', *Surveillance & Society*, 4(1/2): 136-153, disponible en: http://www.surveillance-and-society.org/Articles4(1)/sublethal.pdf (página 136).

[80] Fuente: folleto sobre el FP7 de la CE.



¿Investigación en el servicio del ESRP?

Bajo el ESRP, el proyecto FORESEC sobre la "seguridad europea en proceso de evolución: responsables, tendencias y escenarios" aportará "una dirección, una orientación y una estructura convincentes a todas las actividades de investigación futuras (de la UE) relacionadas con la seguridad. Además, este proyecto "ampliará la visión compartida y facilitará la emergencia de un enfoque coherente y holístico de los retos y amenazas actuales y futuros para la seguridad europea en el marco de la comunidad de constituyentes oficiales y no oficiales involucrados".

El proyecto FORESEC está encabezado por la Crisis Management Initiative con el apoyo del FOI (la agencia de investigación en seguridad sueca), el International Institute for Strategic Studies (IISS), el Austrian Research Centres GMBH, el Centre for Liberal Strategies (Bulgaria) y el Centro Común de Investigación de la Comisión Europea. En las conclusiones preliminares del FORESEC se plantea la pregunta de si a medida que "crece el alcance del riesgo para la sociedad", "habrá que gastar cada vez una mayor cantidad de nuestras riquezas en seguridad".[81] A aquellos que estén familiarizados con la Constitución Europea recordarán una cláusula similar relacionada con el gasto militar.

81 Eriksson, A. (2008) 'First ESRIF results – Long term threats and challenges and needed capabilities', *FORESEC 2008 Workshop on "Europe's evolving security: drivers and trends", 2-3 July 2008*, disponible en: www.foresec.eu/wp3_docs/anders.ppt. Véase también: Rintakoski, K. (2008) 'European Security Research Challenges for Foresight and risk assessment', seminario sobre seguridad y evaluación de riesgos, 13 de noviembre de 2008, disponible en: www.operaatiotutkimus.fi/seminaarit/108/Kalvot/Rintakoski.pdf.

Otros dos proyectos de investigación del FP7 trataban la naturaleza de las "amenazas" a la seguridad europea. El proyecto CPSI sobre "cambiar la percepción de seguridad e intervención" está encabezado por el TNO (el laboratorio de ciencias aplicadas a la investigación de los Países Bajos, que tiene una división de defensa y seguridad) y analizará "qué intervenciones son efectivas para aumentar la seguridad" y proporcionar "herramientas prácticas y listas para ser utilizadas" a "políticos y otros posibles usuarios, con el fin de elaborar políticas relacionadas con la seguridad".

El proyecto FESTOS sobre la "previsión de las amenazas de la seguridad en proceso de evolución que suponen las tecnologías emergentes" está encabezado por la Universidad de Tel Aviv con el apoyo de la Turku School of Economics, la Technical University of Berlin, la European Foundation for Scientific Cooperation (una ONG polaca) y Efp Consulting Ltd (una asesoría de especialistas basada en el Reino Unido e Israel que ofrece servicios de aplicaciones y dirección de proyectos para los programas marco de investigación de la UE). El objetivo del FESTOS consiste en "identificar y evaluar amenazas de la seguridad en proceso de evolución producto del abuso o del mal uso de las tecnologías emergentes" y "proponer medios para reducir la medida en que se producen". Según lo que "se espera para el año 2030", el estudio de previsión identificará "amenazas para la seguridad que podrían derivarse de futuras tecnologías entre las que se incluirían la robótica, la cognición, los nuevos materiales, la nanotecnología y la biotecnología" y "construirá situaciones de amenaza a partir del análisis del impacto de las amenazas identificadas en el trasfondo de climas de seguridad previstos". Es de suponer que en la estructura del ESRP se haya pasado por alto la ironía que supone el uso de la investigación en seguridad para analizar las amenazas de la propia investigación en seguridad.

Mientras tanto el consorcio EUSECON cuenta con 14 de los "principales líderes europeos en investigación" en el "nuevo campo emergente de la seguridad económica europea", entre los que se encuentran la RAND Corporation, la Universidad de Jerusalén y la Universidad de Oxford y tiene el fin de desarrollar "nuevos entendimientos analíticos y conceptuales" de la seguridad. El EUSECON establecerá una red de investigadores para proporcionar "asesoramiento político (basado en la investigación) acerca de los aspectos económicos de la seguridad".[82] "El tema unificado de la investigación propuesta son los causantes humanos de la inseguridad moderna, es decir, el terrorismo y el crimen organizado".

"Planos" para la investigación: la futura dirección del FP7

Al menos otros nueve proyectos prometen facilitar "planos" para establecer futuras nuevas agendas para la UE y para el componente de investigación en seguridad del programa FP7. Entre ellos se encuentra el proyecto CRESCENDO (acción de coordinación de riesgos, evolución de amenazas y análisis de contextos por parte de una red ampliada para la creación de un plano de I+D), que básicamente es una continuación de los proyectos SeNTRE y STACCATO (véase la sección 4).[83] De forma similar, el

[82] Véase la página web del proyecto EUSECON: http://www.economics-of-security.eu/eusecon/index.html.

[83] El proyecto CRESCENDO cuenta con muchos de los participantes del SeNTRE y el STACCATO. Su objetivo consiste en "fortalecer, ampliar y hacer sostenibles las redes creadas por estos" con el fin de "elaborar recomendaciones para algunso temas importantes en el ESRP

proyecto STRAW proporcionará una "taxonomía revisada de la seguridad (básicamente inspirada en el STACCATO) enlazada con una base de datos con información de proveedores, usuarios y tecnología", manteniendo la plataforma de *stakeholders* desarrollada bajo la PASR. El consorcio STRAW está encabezado por el gigante de la tecnología de la información Atos Origin y cuenta con los *lobbys* de seguridad y defensa AESD y EOS (la Organización de Seguridad Europea) junto con Thales y Elsag Datamat (una compañía de Finmeccanica). Además, la investigación en seguridad de la UE contará con "planos" para el medio ambiente (SECURENV), el sistema de transportes (DEMASST), las tecnologías de la información y otros sistemas cibernéticos (ESCORTS), los controles fronterizos (GLOBE), las fronteras marítimas (OPERMAR), el control policial en protestas y eventos públicos de masas (EUSEC II), el material químico, biológico, radiológico y nuclear (CREATIF) y los sistemas de respuesta de emergencia (NMFRDISASTER).

¿Investigación ética?

El programa FP7 ha demostrado un mayor compromiso en la reflexión ética relacionada con la investigación en seguridad. El respetado Instituto Internacional de Investigación por la Paz de Oslo está coordinando el proyecto INEX sobre "valores éticos convergentes y enfrentados en el *continuum* de la seguridad interior y exterior en Europa". Su investigación dirigirá las "consecuencias éticas de la proliferación de tecnologías de seguridad", los "dilemas legales producto de los acuerdos en seguridad transnacional", "las cuestiones éticas y de valores que surgen de los cambios en el papel que desempeñan los profesionales de la seguridad" y "las consecuencias de los cambios en el papel que desempeñan las políticas de seguridad exteriores en una era en la que las diferencias entre fronteras interiores y exteriores son cada vez más pequeñas". De manera similar, el proyecto DETECTER, encabezado por el departamento de filosofía de la Universidad de Birmingham (Reino Unido) sobre "tecnologías de detección, terrorismo, ética y derechos humanos" analizará "el cumplimiento del contraterrorismo con los derechos humanos y con los estándares éticos en el campo de las tecnologías de detección".

Por valiosos que puedan ser estos proyectos, la pregunta crucial que se plantea en este informe es si pueden llegar a tener un impacto significativo en la amplia trayectoria del ESRP y en el desarrollo y la implementación de las tecnologías específicas analizadas más adelante. Puesto que, en lugar de situar las "dimensiones éticas" de la investigación en seguridad en el núcleo del ESRP (tal y como prometieron la ESRAB y la Comisión Europea) y por extensión en el centro de todos los proyectos de investigación en seguridad, lo que se ha hecho ha sido separarlas, da la sensación de que, en el mejor de los casos se dará carpetazo a "la ética y la justicia" y, en el peor de ellos serán directamente ignoradas.

y analizar la evolución de la evaluación de amenazas (agresiones) y riesgos (accidentes) teniendo en cuenta el equilibrio entre la seguridad y las libertades civiles".

7 Visión del 2030: Foro Europeo de Innovación e Investigación en Seguridad

> *La ESRAB recomienda la creación de una junta de seguridad europea para fomentar el diálogo y compartir la visión de las necesidades de seguridad europeas. La junta debería reunir de manera no burocrática a representantes de gran autoridad de* stakeholders *públicos y privados para desarrollar conjuntamente una agenda de seguridad estratégica y actuar como posible cuerpo de referencia para la implementación de programas e iniciativas existentes... El consenso en la junta debería ayudar a compartir las distintas tareas y a mejorar las relaciones entre los programas y las políticas nacionales y las de la UE así como a influenciar el despliegue de fondos.*
>
> Junta asesora de la investigación en seguridad europea: puntos clave

La creación del "Foro Europeo de Innovación e Investigación en Seguridad" (ESRIF) se anunció en la "2ª Conferencia Europea de Investigación en Seguridad", en Berlín el 26 de marzo de 2007. El ESRIF no se desveló al público hasta seis meses más tarde (curiosamente un 11-S) en un comunicado de prensa de la Comisión Europea titulado "diálogo sobre investigación en seguridad entre los sectores público y privado".[84] Sin embargo, en todo menos en el nombre, el ESRIF sigue con el gobierno corporativo del ESRP propuesto por el grupo de personalidades y la ESRAB, pero con una mayor variedad de destinatarios.

Según su página oficial, "el ESRIF irá más allá de la investigación en seguridad del FP7; se dirigirá a satisfacer necesidades de investigación en seguridad y desarrollo tecnológico a largo plazo por toda la UE para estar cubierto por inversores de la UE, nacionales y privados".[85]

El ESRIF está compuesto por un plenario de 65 miembros y unos 660 asesores de investigación en seguridad divididos en 11 grupos de trabajo. Un "equipo de integración" se encarga de coordinar el trabajo del plenario y los grupos de trabajo. Los mandatos del ESRIF son:

- identificar los retos y amenazas a largo plazo, principalmente a partir de técnicas de previsión y escenarios
- relacionar las predicciones y las expectativas sobre futuras creaciones
- relacionar los requisitos de investigación
- hacer el mejor uso posible de los diversos instrumentos de financiación
- desarrollar el "marco de apoyo" para la investigación en seguridad ("relacionado con la sociedad, el mercado y la forma de gobierno")

El ESRIF está adoptando "una perspectiva a medio y largo plazo (de hasta 20 años)... dirigida no solo a nivel europeo, sino también a nivel nacional y, en ocasiones, regional". El "plano" del ESRIF para la investigación en seguridad se presentará en la

84 *The European Security Research and Innovation Forum (ESRIF) - Public-Private* 82 *Dialogue in Security Research*, Nota de prensa de la CE publicada el 11 de septiembre de 2007.

85 Véase la página web del ESRIF: http://www.esrif.eu/.

conferencia anual de investigación en seguridad de la UE en Estocolmo, el 29 de septiembre de 2009.[86] Como ya hizo la ESRAB, es de esperar que se base en los resultados de los estudios de alto-nivel encargados por el ESRP y en las contribuciones de sus miembros.

Los 65 miembros del plenario del ESRIF se seleccionaron y designaron de la misma manera que los de la ESRAB: nombrados por la UE y por funcionarios de los Estados miembro sin llevar a cabo consultas ni en el Parlamento Europeo ni en los parlamentos nacionales. El primer presidente del plenario fue Gijs de Vries (antiguo coordinador de contraterrorismo de la UE), al que ha sustituido el que fuera ministro de interior de Eslovenia, Dragutin Mate, que ha designado como "segundos" a Giancarlo Grasso (Finmeccanica) y a Jürgen Stock (Deutsches Bundeskriminalamt). De los 65 miembros del plenario, 30 representan el "lado de la oferta" de la investigación en seguridad y 33 el "lado de la demanda", con cinco de la "sociedad civil".[87] Diecisiete de los miembros del ESRIF también estaban representados en la ESRAB, entre los que se encuentran Thales, EADS, Finmeccanica y Sagem.[88]

Los cinco *think thanks* de pensamiento, organizaciones por las libertades civiles y otros "expertos relevantes" representados en el ESRIF son el ministerio de protección de la población y ayuda en catástrofes del Gobierno Federal alemán (BBK), el Instituto Europeo para el Control de Riesgos, Seguridad y Comunicación (EURISC), la Asociación de Empresas de Seguridad Europea, el Centro de Ingeniería Biomédica de la Academia Búlgara de Ciencias y la siempre presente Iniciativa para el Control de Crisis. De nuevo, no hay ni organizaciones privadas ni de libertades civiles, de la misma manera que no hay miembros del Parlamento Europeo en el plenario del ESRIF. Sin embargo, hay representados varios elementos de estados no miembros, entre los que se encuentra el ministerio de contraterrorismo del consejo de seguridad nacional de Israel ("lado de la demanda").

Los stakeholders del ESRIF

El ESRIF está subdividido en 11 grupos de trabajo compuestos por los 65 miembros del plenario y por otros 595 *stakeholders* seleccionados de la investigación en seguridad. A cada grupo de trabajo se le ha asignado un "líder" y un "relator" (que podría ser una de las posiciones más influyentes dentro de la estructura del ESRIF). La mitad de estos 22 elementos clave proceden del sector de la defensa y las posiciones más importantes las ocupan organizaciones muy conocidas.

Grupos de Trabajo del ESRIF

Grupo de trabajo	**Líder**	**Relator**
WG1 Seguridad de los ciudadanos	Cees Van Duyvendijk TNO [NL]	Jean-Marc Suchier SAGEM Securité [FR]
WG2 Seguridad de las	Eleanor Travers	Holger Mey

[86] Véase la página web de la conferencia SCR09: http://www.src09.se.

[87] Nótese que varios de los miembros del plenario del ESRIF representan más de una de las tres categorías

[88] La lista completa de los miembros del ESRIF está disponible en su página web: http://www.esrif.eu/documents/members_22012009.xls.

infraestructuras críticas	Dublin Airport Authority [IE]	EADS [DE]
WG3 Seguridad fronteriza	Erik Berglund FRONTEX [EU]	Giovanni Barontini Finmeccanica [IT]
WG4 Control de crisis	Christoph Unger BBK Bundesamt für Bevölkerungsschutz und Katastrophenhilfe, DE	Johannes Prinz FREQUENTIS [AT]
WG5 Previsiones y escenarios	Kristiina Rintakoski Iniciativa para el Control de Crisis [FI]	Anders Eriksson FOI [SE]
WG6 CBRNE	John Erik Stig Hansen National Centre for Biological Defence [DK]	Ruud Busker TNO [NL]
WG7 Conciencia de la situación y ámbito espacial	Utimia Madaleno EMPORDEF [PT]	Massimo Comparini Thales Alenia Space, IT
WG8 Identificación de personas y activos	Thierry Delville Direction de l'adminsitration de la police nationale, FR	Martin Walsh European Biometrics Forum, IE
WG9 Innovación	Alois Sieber Joint Research Centre, Ispra, EU	Luc Desimpelaere Barco, BE
WG10 Forma de gobernar y coordinación	Lucio Accardo Ministerio de Defensa, IT	Sandra Bell RUSI, UK
WG11 Dinámicas de seguridad humana y social	Liviu Muresan EURISC Institute [RO]	Bengt Sundelius SEMA [SE]

[Figura de Euractiv, página web de noticias de la UE][89]

> *"Tenemos que escuchar la opinión de los expertos en tecnología sobre lo que es técnicamente factible. Después será necesario escuchar a los expertos en derechos fundamentales para ver si el uso de esas tecnologías tendría consecuencias que los pudiera poner en peligro. Solo cuándo se puede dar con una respuesta equilibrada y cuándo se tienen en cuenta todas las posibilidades.*
> Franco Frattini, antiguo comisario de Justicia y Asuntos Internos de la UE[90]

Según las cifras facilitadas por la Comisión Europea como respuesta a una solicitud de libertad de información realizada por el autor de este informe, de los 660 *stakeholders* de la investigación en seguridad que participan en los grupos de trabajo del ESRIF, 433 (66%) proceden del "lado de la oferta" (contratistas de defensa y seguridad). Este porcentaje aumenta hasta el 69% si se tienen en cuenta los que tienen múltiples

89 "La investigación en seguridad de la UE busca el respeto de las librtades civiles", *Euractiv* 30.9.2008: http://www.euractiv.com/en/science/eu-security-research-seeks-respectcivil-liberties/article-175851.

90 Frattini, F. (2007), 'Security by design', *Homeland Security Europe*, disponible en: http://www.homelandsecurityeu.com/currentissue/article.asp?art=271247&issue=219.

intereses.[91] Algunas compañías están especialmente bien representadas en la base de datos de *stakeholders*, como es el caso de EADS (43 registros), Finmeccanica (29 registros), Thales (19 registros) y AeroSpace and Defence Industries Association of Europe (ASD, 11 registros).

Los *stakeholders* del "lado de la demanda" cuentan con otras 200 (30%) plazas en el ESRIF. Estas incluyen 62 representantes de agencias e instituciones de la UE: 28 de la dirección general de la Comisión Europea para las empresas, que supervisa el ESRP, nueve de la dirección general de Justicia, Libertad y Seguridad (asuntos internos de la UE), nueve de la Agencia de Defensa Europea, tres de la EUROPOL, dos de FRONTEX, ocho de otras juntas directivas de la Comisión y tres miembros del Parlamento Europeo. Solo nueve de los 660 *stakeholders* del ESRIF (1,4%) proceden de la categoría de la "sociedad civil". Estas son las organizaciones representadas en el plenario del ESRIF, comentado previamente, junto con el Instituto de Asuntos Europeos, la Asociación George C. Marshall y un asesor irlandés. Una vez más, no se establece ninguna organización a favor de preservar las libertades civiles ni garantizar la privacidad de las personas.

Responsabilidad del ESRIF

Dada su composición, es muy difícil imaginarse cómo llegará el ESRIF a dar con la "respuesta equilibrada" que la UE ha afirmado estar buscando en tantas ocasiones. Más bien al contrario, al establecer tres "grupos asesores" de investigación en seguridad (el grupo de personalidades, la ESRAB y el ESRIF), la Comisión Europea ha fracasado por completo en conseguir la representación equilibrada de *stakeholders* que prometía. Mientras que las compañías han desempeñado un papel principal en el desarrollo del ESRP, con muy contadas excepciones (específicamente escogidas), se ha excluido y marginado a los parlamentos europeos así como a las organizaciones a favor de las libertades civiles y los derechos humanos. No se trata solo de una cuestión de fracasar en la tarea de "equilibrar" los derechos y las libertades con la seguridad. Para el Corporate Europe Observatory y otros elementos de la sociedad civil, el nombramiento de grupos de *stakeholders* dominados por la industria para desarrollar las políticas de la UE representa un acto ilícito de mala administración.[92]

Según la Comisión Europea, el ESRIF es un "grupo informal de titularidad compartida y establecido conjuntamente por sus *stakeholders* de los ámbitos de la oferta y la demanda de soluciones y tecnología de seguridad"; no es "ni un cuerpo de la Comisión ni un ejercicio dirigido por la misma".[93] Esta es una afirmación sorprendente en la medida en que da a entender que la Comisión Europea ha externalizado el desarrollo estratégico de un programa de investigación de la UE de 1.400 millones de euros a un grupo informal e irresponsable. En el caso de que no fuera cierta, y queda claro que el ESRIF está, si no "totalmente dirigido", "parcialmente controlado" por la Comisión Europea, esta habría fracasado espectacularmente en la tarea de asegurar mecanismos

91 Algunos de los 660 stakeholders están representados en más de uno de los 11 grupos de trabajo del ESRIF. Cuando se analiza el total de 889 registros, la representación del lado de la oferta (industria) en el ESRIF aumenta hasta el 72%.

92 Queja del Observatorio de empresas europeo al defensor del pueblo en contra del BIOFRAC (Consejo asesor en investigación sobre biocombustibles) y de la EBFTP (Plataforma europea de tecnología de biocombustibles). Abril de 2008.

93 Véase la página web del ESRIF: http://www.esrif.eu/.

adecuados para la responsabilidad y habría informado de la liquidación de sus responsabilidades de manera bastante deshonesta. Ambas posibilidades son del todo inaceptables.

La verdadera razón por la que el ESRIF se ha establecido como un grupo informal es la ausencia de una base legal adecuada en los tratados de la UE para la Comisión Europea con el fin de establecer una junta de asesores que se encargue tanto de las políticas de seguridad como de los asuntos relacionados con la tecnología. Esto dice mucho del estado de la cuestión. En lugar de intentar legitimar las actividades de la Comisión en este ámbito, la UE y sus Estados miembros han elegido conceder un dudoso mandato a un cuerpo informal.

Dirigir el ESRIF y sus predecesores cobre una base específica sin formalizar el papel que desempeñan los *stakeholders* escogidos también hace muy difícil para los observadores externos comprender la formación y la implementación de la política de investigación en seguridad de la UE. De manera crucial, la ausencia de financiación legítima para las actividades del ESRIF también favorece a las organizaciones que son lo suficientemente grandes para proporcionar experiencia, consejos y asistencia de manera gratuita, lo que explica el gran exceso de representación de la industria de la defensa. Según el nuevo registro de intereses de los grupos de presión (*lobbys*) de la Comisión Europea, compañías como EADS, Thales y el *lobby* ASD gastan miles de euros cada año solo en presionar a la UE.

Su invitación para ayudar a dar forma a la agenda de investigación en seguridad de la UE le da a estas organizaciones una ventaja competitiva en lo relacionado con la solicitud de fondos ofrecidos por la UE. Además, puesto que el proceso de aplicación del FP7 será duradero y, por tanto, caro, las organizaciones que puedan permitirse desarrollar sus ideas convirtiéndolas en distintas aplicaciones están mejor posicionadas que las organizaciones pequeñas, que se ven obligadas a desempeñar papeles de colaboración con los "grandes negocios" (y las "grandes academias"). No es casual que haya aparecido toda una industria en torno a las aplicaciones del programa marco de investigación de la UE (servicios disponibles al mejor postor).

La confusión en torno al fracaso en el intento de separar claramente el diseño del programa (y establecer sus prioridades) de los posibles postulantes (y su clamor por la financiación), ha dado lugar a un conflicto de intereses estructural y puede incluso haber contaminado el proceso de evaluación. Para la Comisión Europea la práctica estándar de evaluación de propuestas de investigación consiste en el uso de evaluadores independientes, externos y con experiencia en el campo en cuestión. En la investigación en seguridad, esto significa que hay que recurrir a expertos en tecnología de seguridad. Sin embargo, cuando se estaban evaluando las propuestas de la PASR, la Comisión Europea parecía contar con tan pocos expertos relevantes, que sus propios funcionarios tuvieron que dedicarse al proceso de evaluación (una clara violación de las normas que rigen la investigación financiada de la UE). La Comisión reclutó como es debido a un número suficiente de expertos en investigación en seguridad independientes para el programa FP7, pero muchos de ellos tuvieron que proceder necesariamente del mismo grupo de *stakeholders* relacionado con el desarrollo del propio ESRP.[94]

[94] Para cuando el FP7 se había puesto en marcha la CE ya había reclutado a sufientes evaluadores con la experiencia en investigación en seguridad necesaria. La lista de los 143 evaluadores que se utilizó en 2007, a la que ha tenido acceso el autor de este informe, contiene 21 "cuerpos públicos que no se dedican a la investigación" (incluyendo 14 ministerios de interior y de defensa y agencias nacionales depolicía),

8 El sueño de los miembros de un *lobby*

> *La EOS se constituyó a partir de recomendaciones de la ESRAB, que abogaba por la interacción cercana entre los sectores público y privado en el momento de implementar la investigación en seguridad de la Comisión Europea bajo el VII Programa Marco de Investigación. Durante su fase inicial, la Organización de Seguridad Europea gozará de apoyo organizativo y estructural por parte de la Asociación Europea de Industrias Aeroespaciales y de Defensa (ASD).*
>
> *A pesar de trabajar de cerca con la Comisión Europea y el Foro Europeo para la Seguridad e Innovación" (ESRIF), la Organización de Seguridad Europea también deberá actuar de enlace entre la Comisión Europea, las instituciones europeas y nacionales y los miembros de la propia EOS, así como entre los miembros mismos.*
>
> Luigi Rebuffi, presidente de la Organización de Seguridad Europea[95]

La Organización de Seguridad Europea

La Organización de Seguridad Europea (EOS), un nuevo *lobby* que representa los intereses de la industria de la seguridad y la defensa, se estableció en mayo de 2008.[96] El director ejecutivo de la EOS es Luigi Rebuffi, antiguo director de Thales; el presidente es Markus Hellenthal de EADS, que también presidió la ESRAB. La EOS se describe a sí misma como "una organización que puede conseguir y controlar con facilidad todo tipo de contratos, que puede establecerse de forma más rápida que las asociaciones tradicionales y que puede proporcionar sin problemas a sus miembros una serie de recursos para dirigir proyectos y estudios con efectividad".[97] La EOS sigue el modelo del "ERTICO", "la asociación multi-sector pública y privada que busca el desarrollo y el despliegue de sistemas de transporte inteligente en Europa", que se fundó como una iniciativa de los miembros de la UE encargados de elaborar políticas de transporte.[98] La EOS es una "organización sin ánimo de lucro" en la que todos los miembros poseen partes iguales y está financiada mediante cuotas de socio de entre 4.000 y 7.000 euros (la cifra alta corresponde a los miembros de la junta directiva).

Cuando se escribió este informe, la EOS tenía 26 miembros entre los cuales se encontraban: ASD, BAE, Dassault, Diehl, EADS, Fincantieri (una compañía de Finmeccanica), Indra, Sagem, Smiths, Saab, Thales y TNO. Un tercio de los socios de la EOS también estaban representados en el plenario del ESRIF. Si bien sería una

---

28 "cuerpos privados que no se dedican a la investigación" (principalmente asesores de dirección, gobierno y tecnología de la información junto con algunos especialistas en investigación en seguridad), 41 "organizaciones de investigación" (la mayoría de las cuales son compañías privadas y 17 de las cuales están relacionadas con la investigación en materia de seguridad, militar, aeroespacial o nuclear), un gran grupo de profesores y doctores de 35 universidades (departamentos generalmente no especificados) y "otros" 18 (incluyendo nueve agencias de defensa y aplicación de la ley). Al menos 20 de los evaluadores proceden directamente de organizaciones representadas en la ESRAB o en la organización que la sucedió, el ESRIF. El nivel de independencia de esta selección levanta serias dudas.

95 Véase informe sin referencia sobre la EOS: http://www.isi-initiative.eu.org/getdocument.php?id=210.

96 Véase la página web de la EOS: http://www.eos-eu.com/.

97 Véase informe sin referencia sobre la EOS (página 12), disponible en: http://www.isi-initiative.eu.org/getdocument.php?id=210.

98 El ERTICO y la EOS están registradas como 'SCRL' bajo la legislación belga y se gestionan como entidades independientes sin ánimo de lucro. Véase la página web del ERTICO: http://www.ertico.com/.

exageración insinuar que la ESRAB recomendó la creación de la EOS, la nueva organización comparte los mismos objetivos básicos que el ESRP, es decir, "promover un mercado de la seguridad coherente en Europa" y contribuir a la definición de una política de seguridad civil europea que lo abarque todo". La EOS afirma estar apoyando la creación, el desarrollo y las operaciones del ESRIF y su secretariado, de la Comisión Europea, del trabajo y la dirección del ESRIF y del equipo de integración del ESRP de la CE, además de representar el "interés y las posiciones de una gran parte de los *stakeholders* de la seguridad privada" en el ESRIF. La EOS también proporciona "funciones de apoyo en asuntos clave (como coordinar trabajos, proyectos y actividades en sectores específicos, facilitar el diálogo entre usuarios y operadores y relacionar las pequeñas y medianas empresas) y apoyar "la implementación de las recomendaciones del ESRIF a largo plazo".

La EOS también pretende "asesorar en materia de definición e implementación de políticas de seguridad en otro foros relevantes de la UE", participar en proyectos y tareas conjuntas de la Comisión Europea y actuar de enlace con varias direcciones generales de la Comisión Europea. Con este fin, la EOS ha establecido siete grupos de trabajo que básicamente se encargan de los mismos objetivos que el ESRIF: fronteras verdes y azules, vigilancia, seguridad y protección; protección civil (incluyendo dirección de las crisis); infraestructuras de energía; seguridad y capacidad de recuperación; redes de tecnología de comunicación de la información, protección de datos, seguridad de la sociedad de la información; seguridad en el transporte de superficie.

Correspondencia entre la oferta y la demanda

No hay nada nuevo en el hecho de que los intereses empresariales intenten describirse como una ONG: el término BONGO (ONG con orientaciones empresariales) se creó para designarlas,[99] pero todos los días no se da la situación de que uno de los *lobbys* de defensa crea una nueva organización basada en una determinada medida política de la UE, tal y como han hecho los miembros de la ASD con la Organización de Defensa Europea. La EOS une un gran número de publicaciones, *think tank* financiados por las industrias de la seguridad y la defensa, grupos de relaciones públicas, compañías de dirección de eventos, de entre las cuales puede que la más conocida sea la Security and Defence Agenda. La SDA es otro *think tank* con sede en Bruselas entre cuyos miembros se encuentran los contratistas de defensa más grandes de Europa, la OTAN y la Agencia de Defensa de la UE, con patrocinadores como Karl von Wogau (miembro del Parlamento Europeo), George Robertson y Javier Solana, que recibió con alegría el relanzamiento de la SDA y dijo que es "el tipo de plataforma capaz de proporcionar las nuevas ideas que necesitamos en Bruselas para ayudar a forjar un consenso en las políticas comunes". [100]A pesar de que la gran mayoría de sus fondos proceden de las cuotas de socios de las industrias y de las compañías patrocinadoras, la SDA se describe como "una organización independiente sin vínculos institucionales ni empresariales".

---

99 Para más información acerca de BONGOS, GONGOS, QUANGOS etc. En el contexto de la UE, véase: Cutrin, D. (2003), 'Private Interest Representation or Civil Society Deliberation? A Contemporary Dilemma for European Union Governance', *Social & Legal Studies*, Vol. 12, No. 1, 55-75 (2003).

100 La SDA se conocía antes como la "Agenda para la Nueva Defensa" que Solana mencionó en el lanzamiento de la SDA, véase: http://www.securitydefenceagenda.org/.

Además de una multitud de ONG con orientaciones empresariales (BONGO) tanto nueva como ya establecida, existen ONG con orientaciones gubernamentales (GONGO) en materia de seguridad nacional e internacional, que se hacen pasar por *think tank* u organizaciones independientes. Un ejemplo es el Instituto de Estudios de Seguridad de la UE, un cuerpo creado bajo el "segundo pilar" de la Unión Europea que se define como "una agencia autónoma con total libertad intelectual que investiga asuntos relacionados con la seguridad relevantes para la UE y proporciona un foro de debate".[101] La Asociación de Seguridad Nacional Europea (otra ONG belga),[102] la Asociación de Empresas de Seguridad Europea y el Foro Europeo de Biométrica son otras GONGO y BONGO que han emergido en esta área. Estas asociaciones *think tank* elaboran o contribuyen a la elaboración de diversas revistas académicas, seudo-académicas y con orientaciones empresariales. Un ejemplo es *Homeland Security Europe*, una publicación en línea e impresa hecha por GDS Publishing, una división de GDS International especializada en "revistas de dirección industrial y empresarial para los mercados más apasionantes del mundo".[103] Entre los colaboradores de la revista HSE se encuentran Franco Frattini, antiguo vicepresidente de la Comisión Europea (*Security by design*; seguridad mediante diseño), Max-Peter Ratzel, director de la Europol (*United we stand*; permanecemos unidos) y Christian Sommade, director ejecutivo de la Asociación de Seguridad Nacional Europea (*We must be ready for the worst at anytime*; debemos estar listos para lo peor en cualquier momento), con lo que se asegura que los puntos de vista de los políticos y de los profesionales se presentan a una gran variedad de destinatarios en forma de "perspectivas de vendedor".[104] La misma confabulación de "correspondencia entre el lado de la oferta y el de la demanda" que ha calado en el ESRP resulta evidente en multitud de conferencias internacionales sobre seguridad en las que los políticos y profesionales de la seguridad más experimentados debaten acerca de la futura trayectoria de la seguridad europea con representantes del gran negocio. En este circuito de conferencias se incluyen las "jornadas de corretaje" de investigación en seguridad de la UE (en las que funcionarios de la Comisión Europea, consejos de investigación nacionales y grandes potenciales receptores debaten acerca de las posibilidades de financiación para el desarrollo de sus proyectos), jornadas de *think tank*, "jornadas de mesas redondas", foros de QUANGO (organizaciones no gubernamentales casi autónomas) y exhibiciones de hardware y software abiertamente comerciales.

[101] Véase: http://www.iss.europa.eu/index.php?id=103

[102] Véase: http://www.e-hsa.org/home_english.php.

[103] Véase: http://www.homelandsecurityeu.com/aboutus.asp. HSE es aprte del GDS, un grupo de medios cuyo portafolios *Food Safety Europe, Next Generation Pharma Europe, HR Management EU, Financial Services Technology EU* y títulos similares producidos para el mercado estadounidense, véase: http://www.gdsinternational.com/.

[104] Véase: http://www.homelandsecurityeu.com/index.asp.

PARTE III: DE INVESTIGACIÓN EN SEGURIDAD A POLÍTICAS DE SEGURIDAD

> *El contraterrorismo es más que una respuesta a un acto de terrorismo; es un escenario de suministro autónomo que necesita una cierta demanda para sobrevivir y tener éxito. Pero la demanda de contraterrorismo y la protección que aparentemente ofrece no son automáticas; tienen que ser creadas y mantenidas. La división de tareas dentro del escenario del contraterrorismo implica que, al igual que sucede con la pasta de dientes, los cereales y los vehículos deportivos utilitarios, distintos productos necesitan distintas estrategias de venta.*
> Lipschultz & Turcotte, *The political economy of Threats and the Production of Fear*.[105]

9 Hacia una política económica del ESRP

Este informe ha analizado el desarrollo político del ESRP desde su concepción en 2003 hasta su plena implementación bajo el programa FP7. Lo que resulta más chocante es lo lejos que está dispuesta a llegar la UE para establecer una industria de la seguridad nacional competitiva en Europa, lo cercano que está siendo el trato con la industria para hacerlo y lo poco que se tienen en cuenta las consecuencias de este proyecto. Sin embargo, sería demasiado simplista insinuar que la UE es una mera carcasa para los intereses empresariales. El desarrollo del ESRP es el resultado de factores políticos, económicos, sociales y culturales específicos. Al tomar la decisión política de fomentar una industria de la seguridad nacional competitiva a nivel mundial, los Estados miembros de la UE han puesto en marcha un conjunto complejo de factores y organizaciones. Las compañías transnacionales están pugnando entre sí para determinar la agenda de investigación en seguridad de la UE "vendiendo" ideas a los funcionarios de la Comisión Europea con el fin de aumentar los fondos que se pueden dedicar a actividades de I+D, mientras que los Estados miembro están compitiendo para intentar recuperar los fondos de sus contribuciones al presupuesto del FP7. Los estados más competitivos (ellos dirían "astutos") han establecido agencias gubernamentales y no gubernamentales dedicadas a ayudar a sus factores nacionales a competir por los fondos de la UE (lo que también sirve para explicar el relativo éxito de los estados más grandes de la UE además de países como Irlanda e Israel a la hora de asegurarse contratos de seguridad de la UE).

En el marco del ESRP, los Estados miembros también han utilizado su influencia política para asegurarse de que sus intereses empresariales nacionales estén representados en posiciones clave en organismos como el ESRIF o la ESRAB. Tal y como dijo un miembro anónimo del ESRP: "Si el gobierno italiano piensa que los intereses de Finmeccanica y los intereses nacionales de Italia están al mismo nivel, la

105 Lipschultz, R. D. & Turcotte, H. (2005) 'Duct Tape or Plastic? The political economy of Threats and the Production of Fear' in Hartman, B., Subramaniam, B. & Zerner, C. (2005) (eds) *Making Threats: biofears and environmental anxieties*. Nueva York: Rowman & Littlefi eld (página 26).

Comisión Europea no puede hacer gran cosa".[106] Esta proposición también ayuda a explicar el prominente papel que desempeñan Thales (Francia), EADS (consorcio franco-germano-español) y las agencias de investigación en seguridad de los Países Bajos y Suecia en el ESRP.

La UE contemporánea es, por tanto, una unión creada a la imagen de los Estados miembros más importantes, en la que los intereses nacionales y comerciales, al menos en lo relacionado con las "inversiones", suelen ir de la mano. Tal y como explicó Iraklis Oikonomou, las labores organizadas a nivel Europeo han apoyado las políticas de la UE en favor de su desmilitarización, mientras que la industria de la defensa es una gran fuente de trabajos que ha utilizado las perspectivas de pérdida de empleo con el fin de justificar su continuo apoyo por parte del estado.[107]

Los intereses empresariales en vender tecnología de seguridad y los intereses de seguridad nacionales en la compra de tecnología de seguridad están impulsados por una nueva política del miedo y la inseguridad y convergen a nivel de la UE. Sin embargo, los adornos de los gobiernos democráticos siguen estando firmemente arraigados en el concepto nación-estado. A partir de este punto, en este informe se analiza la visión del nuevo complejo industrial de seguridad de la UE, su posible impacto en las políticas y prácticas estatales y sus implicaciones en materia de libertades civiles y justicia social.

Ahora contamos con un mayor presupuesto para investigación, desarrollo político y atención de solicitudes. La investigación no debería llevarse a cabo *per se*, sino que debería estar relacionada con las necesidades y desplegada con el fin de beneficiar a los ciudadanos y a la economía. La seguridad ha dejado de ser un monopolio que pertenece a la administración pública y ha pasado a ser un bien común, en el que los cuerpos públicos y privados deben compartir responsabilidad e implementación.
Franco Frattini, antiguo comisario de Justicia y Asuntos Internos de la UE[108]

10 Dominio de espectro total: explicación de la misión

La importancia del Programa Europeo de Investigación en Seguridad solo se puede apreciar en el amplio contexto de las políticas de seguridad de la UE. En los siguientes apartados se analiza la influencia del ESRP en la política de seguridad de la UE y viceversa. Se pone atención en lo que está siendo "investigado" (y a veces gestionado), quién está investigándolo y con qué fin lo hace. La investigación también indica un cambio de paradigma en la estrategia de seguridad de la UE, un cambio que se caracteriza por buscar un doctrina militar como la de Estados Unidos, es decir, de "dominio de espectro total", eufemismo utilizado para referirse al control sobre todos los elementos del "campo de batalla" mediante el uso de bienes terrestres, marítimos aéreos y espaciales.

106 Fuente: conversación con el autor de este informe.

107 Oikonomou, I. (2009), 'Kopernikus/GMES and the militarisation of EU space policy', informe presentado en la conferencia *Militarism: Political Economy, Security, Theory* Universidad de Sussex, el 14 y el 15 de mayo de 2009.

108 Frattini, F. (2007), 'Security by design', *Homeland Security Europe*, disponible en: http://www.homelandsecurityeu.com/currentissue/article.asp?art=271247&issue=219.

La UE no ha adoptado formalmente una estrategia de dominio de espectro total. Sin embargo, sus políticas relacionadas con un conjunto de temas que anteriormente eran distintos (como las actividades de las fuerzas del orden, el contraterrorismo, la protección de infraestructuras críticas, los controles fronterizos, la dirección de las crisis, la seguridad exterior y las políticas marítimas, espaciales y de defensa) están convergiendo en torno a dos objetivos interrelacionados. El primero es la amplia implementación de tecnologías y técnicas de vigilancia para mejorar la seguridad, la aplicación de la ley y las competencias de defensa en estas "áreas de misión" centrales. El segundo es la búsqueda de la "interoperabilidad", es decir, la integración de las herramientas de vigilancia con otros sistemas de información y comunicaciones gubernamentales de manera que puedan utilizarse en múltiples tareas relacionadas con la seguridad y el cumplimiento de la ley. Otro concepto que sirve para describir esta tendencia es el de "unión de tipos de vigilancia" para una "unión de gobiernos".

La búsqueda de una política doméstica de dominio de espectro total tiene consecuencias especialmente profundas en las libertades civiles, el seguimiento de la ley y otras tradiciones democráticas. Magnus Hörnqvist, un académico sueco, ha descrito la manera de eclipsar el seguimiento de la ley mediante la "lógica de la seguridad".[109] Según su hipótesis, "el principio básico que dicta la conveniencia de la aplicación de la fuerza física y de otras medidas coactivas no es la ley sino la seguridad". Durante este proceso "la ley se ha separado en dos tendencias de forma simultánea: una consiste en la supresión de las diferencias entre crímenes y actos de guerra, mientras que la otra se basa en la equiparación de delitos y pequeñas alteraciones del orden público". Por consiguiente, "la ley se vuelve superflua... se necesitan otros medios que se correspondan con más precisión a la lógica militar: neutralizar, noquear y destruir al enemigo".[110]

La seguridad fronteriza no solo se basa en el control de las personas que cruzan fronteras nacionales e internacionales, sino también en la vigilancia sofisticada de la población interior (para identificar y prevenir la entrada de los llamados "ilegales") y del resto del mundo (por ejemplo en el Mediterráneo o en las costas del norte y el oeste de África). La "lucha" contra el crimen y el terrorismo ya no se centra solamente en la investigación policial de delitos, sino más bien en la identificación, la interrupción y la destrucción de redes criminales y terroristas y sus apoyos. Actualmente hay un gran número de agencias del orden público que vigilan a poblaciones enteras con el fin de identificar individuos sospechosos antes de que cometan delitos o atentados terroristas (o incluso si intentan entrar en el territorio del "mundo libre"). La protección de infraestructuras críticas y el control policial de los llamados "grandes eventos" (competiciones deportivas, cumbres, protestas, etc) están cada vez más orientados hacia la tecnología militar, la vigilancia con tecnología punta y los puntos de control de seguridad.

Como se mencionó anteriormente, el ESRP tiene cinco "áreas de misión" clave: "seguridad fronteriza", "protección contra el terrorismo y el crimen organizado", "protección de infraestructuras críticas", "restauración de la seguridad en caso de crisis" e "integración, conectividad e interoperabilidad". Para cada una de estas aparentemente distintas "áreas de misión" se observa que se propuso la misma respuesta: maximizar el uso de la tecnología de seguridad; utilizar métodos de evaluación y modelado de riesgos

[109] Hörnqvist, M (2004) The Birth of Public Order Policy, *Race & Class*, Vol. 46, No. 1, páginas 30-52.
[110] Hörnqvist, M (2004: página 35).

para predecir (y mitigar) comportamientos humanos; asegurar una rápida "respuesta a incidentes"; intervenir para neutralizar la amenaza, de manera automática siempre que sea posible. La ESRAB también recomienda el desarrollo de sistemas de seguridad totalmente interoperables para que las aplicaciones tecnológicas que se usan en una "misión" puedan utilizarse fácilmente en las demás. Los diagramas obtenidos del informe de la ESRAB y reproducidos en las páginas 32, 42, 57 y 62 de la versión original de este texto ayudan a comprender lo que se propone exactamente.

El modelo de dominio de espectro total, que está promovido por el sector privado, también se basa en una serie de distintas tendencias en políticas de defensa y seguridad de los estados occidentales más poderosos. La primera de estas tendencias es la llamada revolución en asuntos militares y la investigación para conseguir sistemas armamentísticos de tecnología punta orientados hacia la superioridad militar. Las tácticas de impacto e intimidación de la segunda guerra del golfo y el "SeaPower21", el plan de estrategia naval estadounidense de 2005, también son manifestaciones del paradigma que representa el dominio de espectro total. Lo mismo sucede con la afirmación de que "a día de hoy, dominar el espectro de información es tan esencial en los conflictos como lo era antes la ocupación del territorio o el control del espacio aéreo".[111]

La segunda tendencia clave es la integración de las funciones de seguridad y defensa y la eliminación de las distinciones "tradicionales" entre el control policial interno (tradicionalmente una empresa civil) y la seguridad y la defensa exteriores (tradicionalmente reservadas a los servicios militares y de inteligencia). En la UE este es un proceso a largo plazo y el fruto de la integración europea en este campo (hasta la fecha ha creado zonas de seguridad común interiores y exteriores) y del solapamiento de mandatos, poderes y equipo suministrado a las agencias estatales en el siglo XXI. Por ejemplo, los sistemas de justicia criminal utilizan sistemas de GPS para realizar seguimientos vía satélite de los "delincuentes"; actualmente los ejércitos ayudan a controlar las fronteras y a proteger los aeropuertos; la policía utiliza vehículos aéreos no tripulados en tareas de vigilancia doméstica; la guerras contra el narcotráfico, el terror y los estados fallidos están convergiendo y se ha organizado a toda prisa una nueva armada internacional para combatir la piratería en las costas de África. Mientras tanto, las cumbres del G8 se llevan a cabo en "zonas verdes" al estilo de Bagdad, con los manifestantes siendo controlados en el exterior como si un grupo paramilitar estuviera intentando "mantener la paz"; a día de hoy, las fronteras electrónicas internacionales realizan seguimientos de viajes intercontinentales, de principio a fin; la vigilancia de las telecomunicaciones se está convirtiendo en un privilegia internacional en lugar de en un poder policial controlado de manera judicial. Lejos de la "sociedad abierta" brevemente prometida una vez finalizada la guerra fría, los movimientos interestatales e intraestatales, así como los que se producen en el mundo cibernético, están siendo cada vez más controlados y vigilados por vías policiales.

La tercera tendencia clave es el desarrollo de marcos internacionales para el "control policial global" basado en los objetivos de las políticas exteriores occidentales y la definición expansiva del concepto de "seguridad nacional", que ahora abarca desde epidemias hasta la piratería pasando por los efectos del cambio climático (los cambios en las definición de este concepto se tratan más ampliamente en la sección 24, página

111 Cita de Wright, S. (2006) 'Report. Sub-lethal vision: varieties of military surveillance technology', *Surveillance & Society*, 4(1/2) , disponible en:http://www.surveillance-and-society.org/Articles4(1)/sublethal.pdf.

72, según la numeración de la versión original de este informe). Una cuarta tendencia es el desarrollo y la consolidación del complejo de seguridad industrial (descrito anteriormente) y la novedosa idea de que hoy en día la seguridad es "un bien común, para el que los cuerpos públicos y privados deben compartir responsabilidad e implementación".

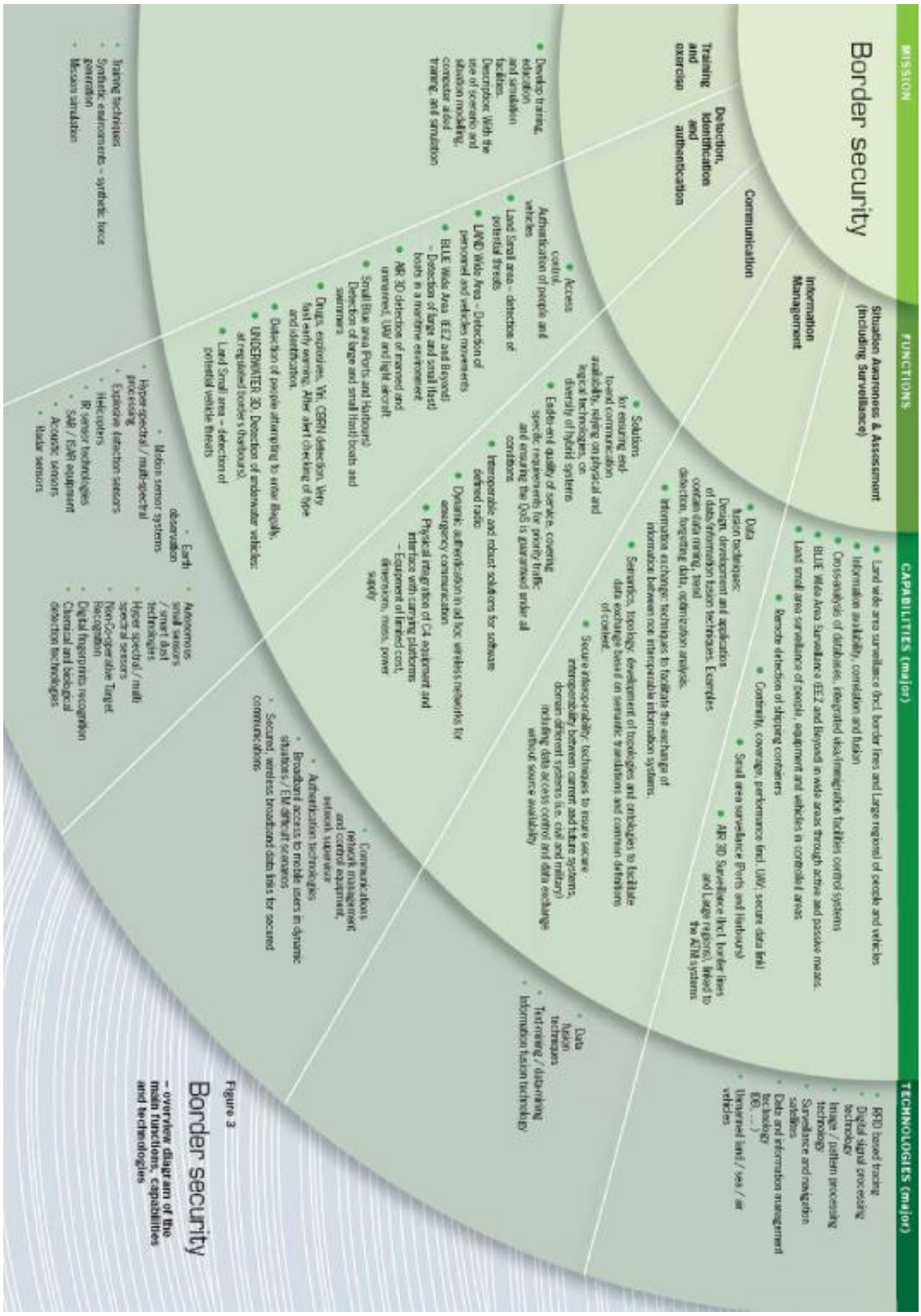


Figure 3

Border security

– overview diagram of the main functions, capabilities and technologies

PARTE IV: DOMINIO DE ESPECTRO TOTAL EN LAS ZONAS FRONTERIZAS

> *Además de sus características geofísicas tradicionales, las fronteras han adquirido también una serie de atributos desterritorializados. Los castillos, las ciudades enmuralladas y las almenas que se situaban a lo largo de las fronteras han sido reemplazadas por comunidades separadas por puertas, puestos fronterizos y por el "control remoto" como medio de dirección. Las fronteras contemporáneas están constituidas tanto por flujos de datos, zonas artificiales y espacios cercados que llegan hasta las ciudades y barrios como por las antiguas fronteras geográficas.*
> Editorial de *Smart Borders* (fronteras inteligentes), *Surveillance & Society*[112]

11 Puntos de partida: de los controles de inmigración a los sociales

La política de control fronterizo de la UE se remonta a medio siglo, cuando se llevaron a cabo los primeros intentos de los entonces miembros de la CEE de controlar la inmigración y, especialmente, de prevenir la inmigración no autorizada o "ilegal", mediante la cooperación intergubernamental. Estas aspiraciones se plasmaron en el Acuerdo de Schengen de 1990 y en una serie de medidas consiguientes. Los intentos más estrictos que se han llevado a cabo hasta la fecha y que consisten en controlar la inmigración y en asegurar las políticas en esta materia han transformado de manera fundamental la naturaleza de los controles fronterizos. Desde los puntos de control entre países y en los puertos de origen, actualmente estos controles no son más que meras partes de un mecanismo que se encarga del cumplimiento de la ley y que se encuentra en expansión tanto "hacia dentro" como "hacia fuera".

A medida que la UE ha refinado sus intentos de prevenir la llegada y la entrada de "inmigrantes ilegales", sus controles fronterizos se han extendido más allá de su territorio. Puesto que en la práctica los Estados miembro no suelen hacer distinciones significativas, es inevitable que estos controles se apliquen también a los refugiados que huyen de las guerras y la pobreza. Esto ha permitido a los países europeos seguir manteniendo el Tratado de Génova sobre la protección de refugiados y el derecho al asilo, a la vez que niegan el acceso a territorio europeo a cada vez más posibles refugiados.[113]

Este proceso empezó en la década de los 90 con la creación de una "zona de separación" para la inmigración para los países del centro y el este de Europa que querían entrar a formar parte de la UE. Su acceso hizo cambiar la "zona de separación" por una

112 Amoore, L, Marmura S. & Salter, M.B. (2008) 'Smart Borders and Mobilities: Spaces, Zones, Enclosures', *Surveillance & Society*, vol 5 no 2, disponible en: http://www.surveillance-and-society.org/journalv5i2.html.

113 Por ejemplo, en junio de 2009 el UNHCR afirmó que no participaría en el nuevo procedimiento de asilo griego a menos que se realizaran "cambios estructurales". Véase la nota de prensa emitida por el UNHCR el 17 de Julio de 2009: http://www.statewatch.org/news/2009/jul/greece-unhcr.prel.pdf.

"vecindad" de la UE que va desde África Occidental hasta Asia Central.[114] Esto es parte del "enfoque global" de la UE en materia de inmigración, que se centra en países de origen y tránsito de inmigrantes que limitan con Europa. El marco de trabajo de sus políticas incluye financiación para controles de inmigración en países colaboradores, una preferencia por la "protección regional" (es decir, fuera de Europa) de los refugiados que se dirigen a Europa y el despliegue de agencias europeas de "control fronterizo en terceros países.

Una vez que se han fortalecido la mayoría de puntos de entrada a Europa, la "lucha contra la inmigración" ha pasado a centrarse en las islas del Mediterráneo y la costa de África y Oriente Medio. Para FRONTEX, la nueva agencia de control fronterizo creada por la UE, esta "frontera marina meridional" es la "primera línea de defensa" de las "fronteras Europeas".[115] Desde 2003 FRONTEX ha coordinado una serie de misiones de colaboración policial y naval para combatir la inmigración "ilegal" por mar y actualmente está estableciendo una red de patrulla europea permanente en el Mediterráneo y un cuerpo de equipos de intervención fronteriza rápida para ser desplegados los "puntos calientes de la inmigración ilegal".[116]

Este enfoque militarizado del control de la inmigración forma parte de una estrategia más amplia de seguridad y defensa marítimas. EN 2005, siguiendo los pasos de la estrategia "SeaPower21" de Estados Unidos, el CHENS (Chiefs of European Navies) lanzó una "visión para el futuro papel de las fuerzas marítimas europeas" con un plazo de 20 años para responder a las necesidades de la Estrategia de Seguridad Europea (2003) y a las operaciones marítimas conjuntas ampliadas de la OTAN.[117]

La razón que sustenta la estrategia del CHERNS es que el mar "ya ha sido utilizado para llevar a cabo ataques terroristas con barcos armados con misiles y pequeñas armas" y "para dar apoyo logístico al terrorismo". El mar es también es una posible ruta para trasladar materiales químicos biológicos radiactivos y nucleares y para llevar a cabo "actividades criminales como el narcotráfico, el tráfico humano y la piratería"; además, estas actividades están "creciendo en sofisticación y volumen".

En noviembre de 2008, la UE acordó lanzar su primera misión naval bajo el auspicio de las relaciones internacionales de la UE y encabezada por el Reino Unido, para combatir la piratería en las costas de Somalia. De esta manera se unió a las fuerzas de la OTAN, de Estados Unidos, de Japón, de China, de Arabia Saudita, entre otras, que están desplegadas en el océano Índico y que contribuyen a una selección desconcertante de misiones nacionales e internacionales en aguas abiertas.[118]

---

114 Véase *European Neighbourhood Policy*, página web de la CE: http://ec.europa.eu/world/enp/index_en.htm.

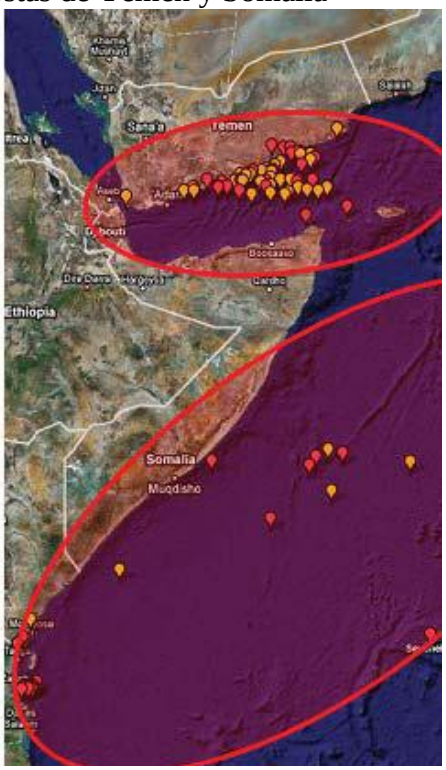
115 FRONTEX es un cuerpo independiente que tiene la tarea de coordinar la "gestión" de las fronteras externas de la UE. También debe encargarse de la inmigración ilegal en el territorio de la UE y desempeña un papel cada vez más importante en la implementación de la estrategia de expulsión de la UE. FRONTEX está supervisada por una junta de dirección compuesta por los "jefes de fronteras" de los Estados miembro. Actualmente la agencia tiene un equipo de 200 personas y su sede está en Varsovia, Polonia. Véase la página web del FRONTEX: http://www.frontex.europa.eu/.

116 Véase la página web de las operaciones conjuntas del, FRONTEX: http://www.frontex.europa.eu/examples_of_accomplished_operati/. Nótese que, si bien el FRONTEX se puso en marcha de forma official en 2006, se llevan a cabo operaciones conjuntas de la agencia desde 2003.

117 CHENS (2005) *A Vision for the Future of EU Maritime Forces by the Chiefs' of European Navies*, disponible en: http://www.chens.eu/products/ENV%202025.pdf. Véase también 'European Interagency Strategy for Maritime Security Operations – A paper Supported by the Chief 's of European Navies', documento sin referencia disponible en: http://www.chens.eu/products/MSO%20Strategy.pdf.

118 Véase: *Operation Atalanta*, Página web del Consejo de la UE: http://www.consilium.europa.eu/uedocs/cmsUpload/081113%20Factsheet%20EU%20NAVFOR%20-%20version%201_EN.pdf.

Figura sobre las operaciones del FRONTEX en África oriental[119]
Figura sobre referencias de actos de piratería en las costas de Yemen y Somalia[120]



La Europa de la seguridad nacional

"El terrorismo marítimo se ha convertido en una enorme amenaza para el mundo que tiene como objetivo navíos militares y civiles. En Europa la amenaza está compuesta por el uso de barcos y rutas marítimas por parte de criminales que a menudo trabajan con terroristas. Con la posibilidad de usar armas de destrucción masiva, los esfuerzos para prevenir tales ataques, que podrían causar multitud de bajas civiles, se ha convertido en una prioridad para Europa, con lo que se hace necesario que la alianza expanda sus fronteras marítimas. Asimismo, con el arresto de diversos marroquíes (*sic*) sospechosos de estar involucrados en los atentados de Madrid del 11M, la gente se pregunta hasta qué punto son seguras las fronteras de Europa".[121]

Los controles fronterizos de la UE también se están extendiendo "hacia dentro", a medida que se desarrollan sistemas de tecnología de la información para detectar a los inmigrantes "ilegales", con el fin de intercambiar información acerca de personas a las que se les debe negar la entrada y para efectuar controles de seguridad a los viajeros. Esto incluyo la introducción de sistemas de identificación biométricos, grabaciones de las entradas, salidas y del tránsito entre países europeos y el desarrollo de sistemas de perfilado de riesgos y de obtención de objetivos automáticos.

---

119 Fuente: gráficos sobre FRONTEX, página web de la BBC: http://news.bbc.co.uk/1/hi/world/europe/5331896.stm.

120 Fuente: página web del Consejo de la UE: http://consilium.europa.eu/cms3_fo/showPage.asp?id=1518&lang=en.

121 'Maritime & Port Security', Revista *Homeland Security Europe*: http://www.homelandsecurityeu.com/coverage_ms.asp. El mismo texto aparece en 'Maritime terrorism: a new challenge for NATO', *Institute for the Analysis of Global Security*, véase: http://www.iags.org/n0124051.htm.

Nanne Onland, presidente de Dartagnan BV, una empresa que vende sistemas de control fronterizo e inmigración y programas de viajeros registrados, afirma que "en última instancia, las autoridades fronterizas del país de destino serán capaces de decirle al viajero antes de subir al avión si será bienvenido en el país al que se dirige. La policía fronteriza del punto de destino se convertirá en la última línea de defensa, en lugar de ser la primera [...] y se encargarán de las excepciones en lugar de comprobar la documentación de los pasajeros para darles permiso para entrar al país en cuestión. De hecho, en teoría se podría prever que la gran mayoría de los viajeros que lleguen a una frontera determinada habrán sido (pre) registrados y, por tanto, serán un "flujo amistoso".[122]

El cada vez más extendido y necesario acopio, análisis e intercambio de datos personales no acaba en las fronteras. Esta nueva generación de "fronteras electrónicas" entra en contacto con las bases de datos sobre la aplicación de la ley y sistemas de la tecnología de la información gubernamentales ya existentes con el fin de proporcionar una lona de seguridad de tecnología punta que acabará por extenderse desde los aeropuertos y puntos fronterizos europeos a "unidades de arresto" de inmigrantes ilegales y policías urbanos equipados con escáneres dactilares portátiles.

Si bien se lamenta el comienzo de la "sociedad de la vigilancia", es importante reconocer que muchos de sus sistemas más polémicos (toma de huellas dactilares, tarjetas de identificación, bases de datos poblacionales, perfilado de "terroristas", vigilancia en viajes, etc) han sido (y aún están siendo) "probadas" en inmigrantes y refugiados o en todo caso legitimadas en las fronteras.[123] La aquiescencia de estos controles y la indiferencia al sufrimiento de los inmigrantes y los refugiados en manos de la "Fortaleza Europa" ha cimentado el camino para el uso de estos sistemas en ámbitos de seguridad doméstica.

122 Onland, N (2007) 'Registered traveller programs - a public and private partnership', *Homeland Security Europe*, disponible en: http://www.homelandsecurityeu.com/currentissue/printarticle.asp?art=271309).

123 Para más información véase Fekete, L. (2009) *A Suitable Enemy: Racism, Migration and Islamophobia in Europe*. Londres: Pluto Press.

12 EUROSUR: el sistema de vigilancia fronteriza europeo

> *Para llevar a cabo los controles necesarios, las fuerzas de la policía nacional de Chipre utilizan un AFIS (sistema de identificación automática de huellas dactilares) suministrado por Motorola y lectores dactilares móviles en centros de asilo y comisarías de policía de todo el país. El sistema proporciona a la policía y a las autoridades en inmigración un enlace electrónico entre el sistema AFIS y la base de datos EURODAC, lo que permite a Chipre capturar las huellas dactilares e imágenes faciales de aquellos individuos que al ser detenidos no contaban con visado o documentos de identificación, o de aquellos que piden asilo. Esta información se transmite a un servidor central en las oficinas de aplicación de la ley de Nicosia. A día de hoy, se resuelven unos 150 delitos al año utilizando la solución de identificación biométrica (BIS) Printak.*
>
> Análisis de la tecnología de la información policial, 2009.[124]

En febrero de 2008, la Comisión Europea emitió un comunicado (de posicionamiento) sobre la creación de un "sistema de vigilancia fronteriza europeo" (EUROSUR) para "ayudar a los Estados miembros a conocer por completo la situación de sus fronteras exteriores y para aumentar la capacidad de reacción de sus autoridades encargadas de la aplicación de la ley".[125]

El principal objetivo de EUROSUR consiste en "reducir el número de inmigrantes ilegales que logran entrar en la UE sin ser detectados, aumentar la seguridad interior de la UE contribuyendo a la prevención de los delitos interfronterizos y mejorar la capacidad de búsqueda y rescate". Con la tecnología de vigilancia como epicentro de otros tipos de políticas marítimas de la UE, desde la aplicación de regulaciones en la industria pesquera y la prevención de las emisiones contaminantes al mar hasta el seguimiento de todo tipo de barcos, la seguridad naval y el desarrollo de sistemas para evitar colisiones, la UE también menciona la necesidad de conseguir la "interoperabilidad" entre sus sistemas marítimos, de seguridad y de defensa. Según la Comisión Europea, el sistema EUROSUR se desarrollará en tres fases: (i) interrelacionar y hacer más eficientes los actuales sistemas de vigilancia nacionales, (ii) herramientas comunes y aplicaciones de la vigilancia fronteriza al nivel de la UE y (iii) crear "un entorno común para realizar seguimientos y compartir información en el dominio marítimo de la UE".

Las dimensiones internas del EUROSUR se establecieron en otro comunicado que incluía planes para la facilitación del movimiento entre fronteras de los viajeros que la Comisión Europea denomina *bona fide* (es decir, no sospechosos), así como la creación de un sistema de entrada y salida de la UE, un sistema electrónico de autorización de viaje (ESTA) para facilitar la entrada de viajeros sospechosos y "una herramienta eficiente para identificar a los individuos que pretenden permanecer en un país durante

---

124 'Fingers on the pulse', Gary Mason, *Police Information Technology Review*, junio y julio de 2009

125 *Commission Communication on the creation of a European border surveillance system (EUROSUR)*, COM (2008) 68, 13 de febrero de 2008, disponible en: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2008:0069:FIN:EN:PDF.

más tiempo del permitido".[126] Esta herramienta es bastante similar a la descrita en el apartado anterior y se creará fusionando el Schengen Information System de segunda generación (SIS II)[127] con los sistemas de información de visados de la UE (VIS), de manera que el nuevo sistema de entrada y salida que registrará todo movimiento hacia dentro y hacia fuera de la UE contendrá las huellas dactilares y datos personales de los individuos que entren utilizando visados.[128] En esos casos, se enviará una "alerta" al SIS, sobre los visados que hayan caducado. El sistema de coincidencia biométrico está siendo construido por Sagem Défense Sécurité y Accenture, lo que permitirá que las huellas dactilares de los viajeros se puedan comparar con las de los sistemas SIS, VIS y EURODAC (la base de datos de la UE sobre ciudadanos que solicitan asilo).

A pesar de la evidente relación entre la visión de la UE de un sistema de vigilancia fronteriza interoperable y el ESRP, en el comunicado del EUROSUR no se mencionan las actividades que está financiando en este ámbito. Tampoco se menciona el ESRIF, cuyo tercer grupo de trabajo se encarga específicamente de la "gestión de fronteras integrada" y de la "vigilancia marítima".

El grupo 3 está encabezado por FRONTEX; su relator es el gigante de la defensa italiano Finmeccanica, que en 2007 anunció una "iniciativa conjunta" con Thales en materia de "control marítimo" para promover los sistemas multiusuarios y una serie de "estándares para fomentar el desarrollo de sinergias entre varios sectores marítimos y civiles". EL grupo 3 está dividido en cuatro subgrupos de "fronteras reguladas" y "fronteras aéreas terrestres y marítimas no reguladas". Cuenta con 80 miembros, 20 de los cuales pertenecen al "sector de la demanda" (gobiernos y agencias estatales) y 60 al "lado de la oferta" (industria).[129]

EUROSUR y el ESRP

El EUROSUR está respaldado por una plétora de proyectos de investigación en seguridad. El consorcio STABORSEC (estándares para la mejora de la seguridad fronteriza, de la PASR), encabezado por Sagem Défense Sécurité, recomendó no menos de 20 tipos de tecnologías biométricas, de detección y de vigilancia para la

126 *Commission Communication on the next steps in border management in the European Union*, COM (2008) 68, 13 de febrero de 2008, disponible en: http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2008:0069:FIN:EN:PDF.

127 El desarrollo del SIS II ha estado caracterizado por los contratiempos, incluyendo alegaciones de mala gestión del proceso inicial en contra de la Comisión y, más recientemente, la falta de progreso en el desarrollo de sistemas compatibles con el SIS II en los Estados miembros.

128 Durante una semana entre el 31 de agosto y el 6 de septiembre de 2009, los Estados miembros de la UE se mostraron partidarios de registrar a cualquiera que cruzara una frontera externa de la UE; los datos se utilizarán para apoyar una "propuesta legislativa sobre la creación de un sistema de registro electrónico de entrada y salida en 2010. Esta práctica se aplicó a ciudadanos de la UE y de países del tercer mundo, lo que indica que el sistema de entrada y salida que planea la UE será mucho más amplio que el de Estados Unidos, que no registra los movimientos de los ciudadanos estadounidenses. Entre los Estados miembros de la UE existen 1.626 puntos designados de entrada por tierra, mar y aire, si bien se permitieron para limitar esta práctica a "los puntos fronterizos más importantes y ocupados". Véase *Outcome of proceedings: Strategic Committee for Immigration, Frontiers and Asylum/Mixed Committee (EU-Iceland/Liechtenstein/Norway/ Switzerland)', on : 19-20 May 2009. Subject: Data collection exercise on entries and exits at the external borders for a short period of time*. Documento del Consejo de la UE 10410/09, 8 de junio de 2009.

129 Sólo entre 15 y 20 de los 80 miembros del tercer grupo de trabajo son participantes "activos". Estos participantes se unieron en un taller organizado en 2009 por la CE con el fin de "preparar el programa de demostración de I+D" para el "sistema de control fronterizo integrado en toda Europa". Entre los ponentes se encontraban la dirección general de las empresas, la dirección general de justicia libertad y seguridad, la Agencia de Defensa Europea, Finmeccanica, Thales, Telespazio, Telvent, Indra, Sagem y la EOS. Véase 'Workshop to prepare the R&D Demonstration Programme: European-wide integrated border control system', 12 de marzo de 2009, página web de la CE: http://ec.europa.eu/enterprise/security/events/border_control_workshop.htm.

estandarización al nivel de la UE.[130] EL proyecto OPERAMAR está encabezado por Thales Underwater Systems junto con Selex (una compañía de Finmeccanica) y ha necesitado el desarrollo de requisitos técnicos, un mapa de investigación estratégico, áreas de prioridad para la investigación en seguridad y unos "requisitos comunes y procedimientos operacionales, así como nuevos estándares de interoperabilidad al nivel de la UE, que deberían adoptarse a nivel nacional y local". El OPREMAR, una continuación del proyecto SOCBAH[131], está siendo probado en tres ámbitos: "mar Mediterráneo, mar Negro y océano Atlántico (Islas Canarias)". El proyecto WIMA2 sobre vigilancia aérea en amplias zonas marítimas (FP7), encabezado por Thales Airborne Systems, esgrime que "no se puede controlar lo que no se patrulla". El EFFISEC, por su parte, es un proyecto de 16 millones de euros sobre puntos de control de seguridad integrada eficientes en fronteras terrestres y seguridad portuaria que promete la "integración de un conjunto de tecnologías existentes y complementarias (biométrica, documentos electrónicos, reconocimiento de señales, análisis de imágenes, seguimiento detección de sustancias, etc);[132] además, representa un "enorme despliegue a medio plazo (2014-2020) en puntos de control marítimos y terrestres".

Vigilancia por satélite para el control fronterizo

El proyecto MARitime Security Service (MARISS, de la PASR) extendió el concepto de vigilancia fronteriza al espacio mediante el desarrollo de "vigilancia por satélite y monitorización para aumentar el conocimiento del control operacional de fronteras marítimas y el dominio marítimo".[133] El MARISS, que recibe el apoyo de la Agencia Espacial Europea, proporcionó herramientas de supervisión "para la detección de navíos que no cooperen y las actividades sospechosas en aguas abiertas" a agencias gubernamentales nacionales y europeas entre las que se incluían cuerpos como "policías, guardas fronterizos, guardacostas, servicios de inteligencia, y ejércitos navales nacionales, así como agencias europeas e internacionales apropiadas". El consorcio MARISS estaba encabezado por Telespazio (una operación conjunta de Finmeccanica y Thales) e incluía Thales Alenia Space, EADS, Astrium, Qinetiq, SELEX-SI y Starlab.

Mientras tanto, el proyecto LIMES sobre "Seguimiento Integrado Marítimo y Terrestre para la Seguridad Europea" (financiado bajo el programa FP6), también encabezado por Telespazio, amplió el alcance del MARISS para incluir fronteras terrestres y vigilancia de infraestructuras críticas utilizando "satélites de muy alta resolución... para permitir el análisis espacial 4D crítico de datos de referencia actualizados con la intención de evaluar riesgos, mejorar la seguridad e incrementar la preparación".[134]

---

130 Véase la página web del proyecto STABORSEC: http://staborsec.jrc.it/.

131 El proyecto Socbah estaba encabezado por Galileo Avionica (una compañía de Finmeccanica) junto con Thales Underwater Systems y Thales Research & Technology. Finmeccanica (Alenia Aeronautica) y Thales también participaron en el proyecto BSUAV sobre el uso de vehículos aéreos no tripulados para la vigilania fronteriza en un consorcio con Dassault Aviation (PASR; para más información acerca de los vehículos aéreos no tripulados véase la sección 19).

132 El EEFISEC está encabezado por Sagem y cuenta con Thales, dos compañías de Finmeccanica, Smiths y TNO. Permitirá realizar controles de seguridad sistemáticos a "viandantes, coches y autobuses" y "mantendrá el flujo en las fronteras al disminuir el número de viajeros, equipaje y vehículos que deben someterse a controles más exhaustivos".

133 Los servicios del MARISS se pusieron a prueba "antes de entrar en funcionamiento en las siguientes zonas: costa sur de España, canal del Atlántico norte, sur del mar Báltico, canal de Sicilia, mar Egeo, costa norte de África, Islas Canarias, costa continental de Portugal (y zona de pesca de Gorringe). Azores y costa de Libia".

134 Las zonas de pruebas del LIMES fueron: fronteras del este de la UE, España y Reino Unido para la vigilancia de infraestructuras, lo que supone una gran oportunidad para la planificación de acontecimientos y las zonas de seguimiento". Véase el folleto del proyecto LIMES, disponible en: http://www.fp6-limes.eu/uploads/docs/Brochure_Limes.pdf.

Sistemas de control fronterizo autónomos

La obsesión por los sistemas de control de tecnología punta queda de manifiesto en el proyecto TALOS, de 20 millones de euros (FP7), que desarrollará y realizará pruebas de mercado de un "sistema móvil, modular, redimensionable, autónomo y adaptable para proteger las fronteras europeas" utilizando vehículos aéreos no tripulados supervisados por un centro de mando y control (los proyectos SECTRONIC, AMASS y UNCOSS, todos del FP7, también están basados en el desarrollo de sistemas de control fronterizo autónomos).[135] Según el contracto del proyecto TALOS "las plataformas básicas serán las estaciones de vigilancia y las patrullas de primera reacción, que informarán al centro de mando y control y a los intrusos de su situación, "y tomarán las medidas necesarias para detener las acciones ilegales de manera casi autónoma con la supervisión de guardas fronterizos". Entre los miembros del consorcio TALOS (FP7) se encuentran PIAP Security Engineering (el coordinador del proyecto, de Polonia), cuyo robot de combate acaba de recibir la medalla de plata en la edición de 2008 del concurso de innovación EUREKA de Bruselas,[136] y el gigante de la defensa Israel Aircraft Industries, cuyas "soluciones operacionales aseguran que se puede detectar, localizar y fijar como objetivo a terroristas, contrabandistas, inmigrantes ilegales y otras amenazas para el bienestar público, de manera rápida y precisa, las 24 horas del día incluso en condiciones climatológicas adversas y de baja visibilidad".[137] Se sabe que la oferta original que se hizo a la Comisión Europea prometía equipar a los robots de los controles fronterizos con menos armas de "energía dirigida" letales (para más información consúltese la página 69 [numeración original]), pero finalmente se eliminó esta propuesta debido a implicaciones éticas.

Como ha señalado Steve Wright respecto al uso de robots de combate, "una cosa es ahorrarle al Presidente el hecho de tener que escribir otra carta expresando sus condolencias a la familia de un soldado fallecido en combate, pero ¿quién va a llevar a un robot ante un tribunal por violar los derechos humanos?"[138]

Los diseñadores del sistema integrado de vigilancia fronteriza europea aspiran a cumplir los estándares establecidos por el SIVE (Sistema Integrado de Vigilancia Exterior) que cubre el Estrecho de Gibraltar, el punto más cercano entre Europa y África, y que abarca 115 km a lo largo de la costa española.[139] El SIVE es capaz de detectar y realizar seguimientos de objetivos de un tamaño mínimo de un metro cuadrado, alcance en el que entra cualquier embarcación que cruce el estrecho, incluyendo las pequeñas "zodiacs" en las que la gente se amontona con la esperanza de llegar a suelo europeo.

---

135 El proyecto SECTRONIC se centra en la "observación y la protección de infraestructuras críticas marítimas; transporte de bienes y pasajeros, suministro de energía e infraestructuras portuarias". Establecerá "centros de control" equipados con "todos los materiales de observación accesibles (en agua, tierra, aire y espacio)…capaces de proteger las infraestructuras de forma no letal en caso de que su seguridad se viera comprometida (énfasis añadido). Entre los participantes en el proyecto SECTRONIC se encontraba el Centro de investigación submarina de la OTAN. Véase su página web: http://www.sectronic.eu/. El proyecto AMAS pretende desarrollar "boyas autónomas y no tripuladas de vigilancia con sensores activos y pasivos" y "sistemas de visión térmica" en zonas costeras para detectar e identificar las amenazas locales a la seguridad. Otro organismo especializado en robótica de defensa, ECA (Francia), encabeza el proyecto UNCOSS que se centra en un sistema "subacuático de vigilancia".

136 Véase la página web del PIAP: http://www.antiterrorism.eu/news026.php.

137 Véase la página web de Israel Aircraft Industries: http://www.iai.co.il/Default.aspx?FolderID=16130&lang=EN.

138 Wright, S. (2006) 'Report. Sub-lethal vision: varieties of military surveillance technology', *Surveillance & Society*, 4(1/2) (página 146), disponible en: http://www.surveillance-and-society.org/Articles4(1)/sublethal.pdf.

139 Véase la página web del *Sistema Integrado de Vigilancia Exterior*, Guardia Civil: http://www.guardiacivil.org/prensa/actividades/sive03/index.jsp.

En la costa africana, la ciudad autónoma española de Ceuta está sellada por 9,7 km de vallas metálicas de tres metros de altura equipadas con alambre de púas.[140]

En una queja a la UE, el presidente de la sección de sistemas de seguridad de Indra describe el SIVE como "un sistema de vigilancia fronteriza marítima pionero" y lo presenta como una víctima de su propio éxito.[141] La "amenaza", según Indra, ha evolucionado; los puntos de salida de los inmigrantes se han extendido por la costa de Marruecos hasta Algeria y al sur y al oeste hacia Mauritania y Senegal; la relativamente escasa vigilancia que hay en las islas Canarias y Baleares las ha convertido en algunos de los nuevos destinos. Las autoridades españolas ya han empezado a usar vigilancia por satélite, utilizando imágenes proporcionadas por el satélite Ikonosos junto con vehículos aéreos no tripulados y equipos de sensores móviles. Todos estos métodos han sido previamente probados para que estén "completamente integrados" en el SIVE. La UE también ha financiado un sistema de comunicaciones "interoperable" (el programa "Seahorse"), que pone en contacto a las autoridades españolas y portuguesas con sus homólogas de Mauritania, Senegal y Cabo Verde con el fin de extenderse a más países tanto europeos como africanos.[142]

Indra y Skysoft son parte del consorcio GLOBE, financiado bajo el ESRP/FP7 y encabezado por Telvent, que pretende dirigir el proyecto de control fronterizo de la UE. Sus planes son muy ambiciosos y se centran en "luchar contra la inmigración ilegal desde todas sus fuentes" mediante "iniciativas preventivas, de control y de integración respecto a los inmigrantes". Además, "representa el nuevo concepto de frontera extendida, que incluye el país de origen, el área de tránsito, los movimientos regulados y no regulados entre fronteras y el propio país de destino".[143]

Otra serie de iniciativas de vigilancia marítima, entre las que se incluyen las acciones del grupo de trabajo de políticas marítimas,[144] el centro de investigación conjunta de la UE,[145] la Agencia de Defensa Europea[146] y FRONTEX[147] están llevándose a cabo fuera del marco del ESRP.[148]

---

140 Tras una serie de intentos desesperados de pasar la valla en septiembre de 2005, España y Marruecos mandaron tropas a Ceuta y Melilla y al menos se disparó a cuatro personas que acabaron muriendo. Un año más tarde Amnistía Internacional informó acerca del "clima de impunidad" de las "continuas muertes de los inmigrantes y los ciudadanos que buscan asilo e intentan cruzar la frontera", así como de "el uso excesivo de la fuerza por parte de los responsables de aplicar la ley y de expulsiones colectivas y de violaciones del principio de repatriación. Véase 'Spain and Morocco: Failure to protect the rights of migrants - one year on', *Amnesty International Spain*, AI Index: EUR 41/009/2006, octubre de 2006.

141 'SIVE: a pioneer System for Border Surveillance. What is beyond?', presentación de Perez Pujazón (Indra) en el taller de la CE, disponible en: http://ec.europa.eu/enterprise/security/doc/border_control_workshop/n_jm_perez_pujazon.pdf.

142 El Seahorse se estableció como un programa de cooperación entre España, Portugal y varios países africanos y se financió bajo el programa AENEAS sobre gestión de la inmigración de la UE

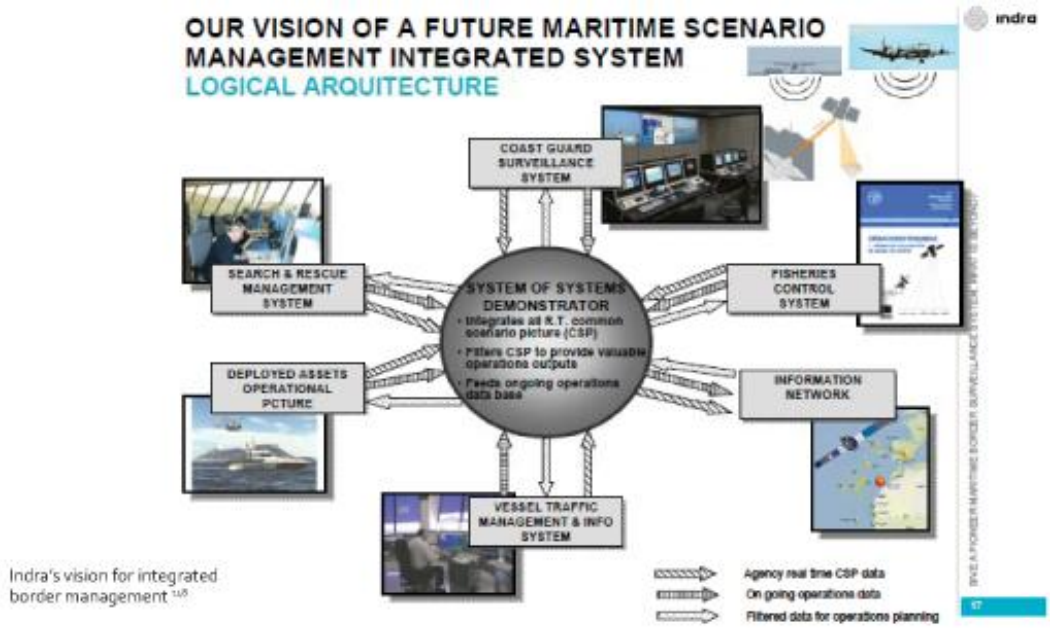
143 Véase la nota de prensa de TELVENT publicada el 22 de abril de 2008: http://www.reuters.com/article/pressRelease/idUS121430+22-Apr-2008+PNW20080422. El propósito del proyecto GLOBE consiste en desarrollar "un sistema de gestión de fronteras integrado en toda su amplitud, que se mueva a lo largo de las cuatro capas principales del control fronterizo (país de origen, zonas de tránsito, fronteras reguladas y no reguladas y territorio interno)". Telvent también encabeza el proyecto INTEGRA sobre "gestión de la inmigración", financiado por el Ministerio de Ciencia e Innovación de España y que trata sobre el desarrollo de un "sistema integrado de gestión de movimientos migratorios desde el país de origen al país de llegada y de cierre de fronteras a inmigrantes ilegales y al tráfico ilegal sin alterar la actividad del ámbito de la legalidad y la regulación". Véase la nota de prensa de TELVENT publicada el 12 de septiembre de 2008: http://biz.yahoo.com/pz/080912/150240.html.

144 El grupo de trabajo de políticas marítimas se estableció para asegurar un acercamiento consensuado a la vigilancia marítima y a las acciones de los políticos en el ámbito de las competencias de la UE.

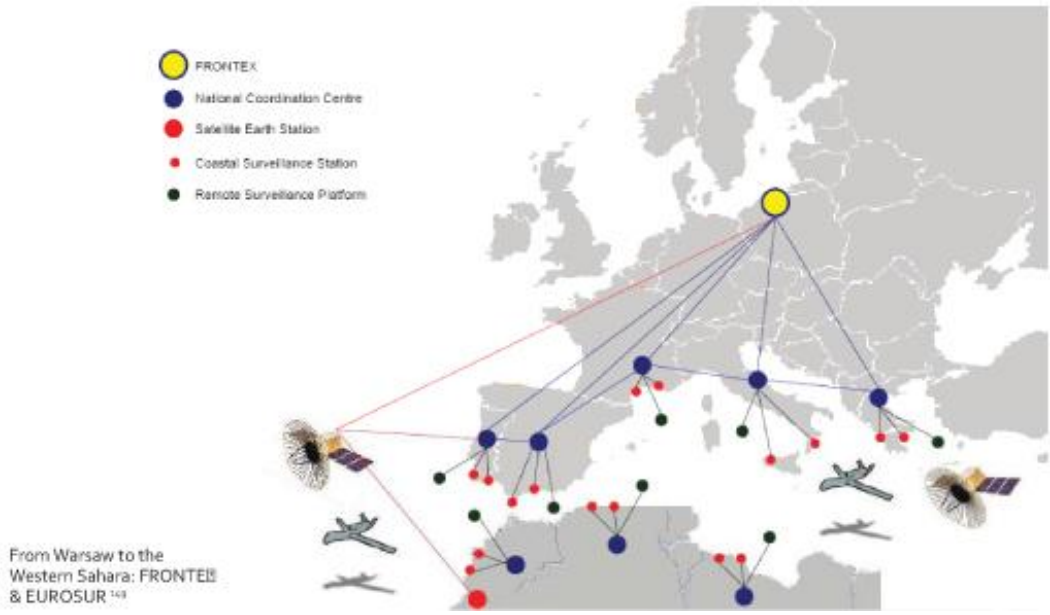
145 La Acción MASURE del grupo de investigación conjunta proporciona: recursos de I+D adicionales en la detección de embarcaciones y en el uso de satélites para la vigilancia marítima; prácticas y políticas de distribución de datos; nuevas herramientas para la vigilancia marítima; seguimiento de la contaminación marítima. Véase 'Maritime surveillance at JRC: MASURE action'. Presentación de Guido Ferraro, Harm Greidanus, junio de 2007, disponible en: https://maritimeaff airs.jrc.ec.europa.eu/c/document_library/get_fi le?p_l_id=9003&folderId=9015&name=DLFE-419.ppt.

146 La Agencia de Defensa Europea ha contratado a Saab Systems en un consorcio con la FOI (la agencia de investigación en defensa sueca) para elaborar un estudio sobre redes de vigilancia marítima. El consorcio también examinará los obstáculos políticos y legales para la

Esquema de la visión de Indra sobre la gestión integrada de fronteras[149]
Figura: "Desde Varsovia al Sáhara Occidental"[150]



Indra's vision for integrated border management [148]



From Warsaw to the Western Sahara: FRONTEX & EUROSUR [149]

implementación del sistema en cuestión. También se han establecido grupos de trabajo sobre establecimiento de redes de vigilancia marítima, futuros sistemas aéreos no tripulados, vigilancia de objetos marítimos pequeños y medidas de respuesta marítimas dentro de la Agencia de Defensa Europea.

147 Como parte de la infraestructura del EUROSUR se está estableciendo una red de comunicaciones entre los centros de coordinación de vigilancia marítima nacionales y el FRONTEX: la Agencia de gestión fronteriza de la UE.

148 Véase también el proyecto CONTRAFFIC sobre tecnología desarrollada por JRC y la Agencia antifraude europea (OLAF) para reunir y analizar de forma automática los datos sobre movimientos marítimos mundiales con el fin de permitir la identificación de posibles conductas sospechosas; el proyecto ROTIS II (FP6) sobre el sistema de inspección de buques dirigidos de forma remota y el proyecto FREESUBNET, una red de entrenamiento que pretende "proporcionar un entrenamiento excelente a investigadores jóvenes y a los experimentados en el campo emergente de los vehículos submarinos de intervención autónoma y cooperativa (AUV) que se están convirtiendo en la principal forma de llevar a cabo misiones marítimas sin una estricta supervisión humana".

149 Fuente: 'SIVE: a pioneer System for Border Surveillance. What is beyond?', Presentación de Perez Pujazón (Indra) en el taller de la CE, disponible en: http://ec.europa.eu/enterprise/security/doc/border_control_workshop/n_jm_perez_pujazon.pdf.

150 Fuente: 'GLOBE: Phase 1 of the Demonstration Project for the Integrated Border Management System', presentación de Víctor Luaces (Telvent) en el taller de la CE, disponible en: http://ec.europa.eu/enterprise/security/doc/border_control_workshop/i_victor_luaces.pdf.

13 ¿I+D para un apartheid mundial?

Según unas declaraciones del 1 de julio de la compañía EADS Defense & Security, Arabia Saudita la ha escogido como principal contratista para un programa completo de vigilancia fronteriza nacional tras un concurso internacional que ha durado varios años.

En palabras de la compañía, según el contrato, durante los próximos cinco años EADS instalará equipo de vigilancia a lo largo de unos 9.000 km de las fronteras del país, incluyendo montañas, desiertos y costas, para proporcionar conocimientos operacionales.

La industria estima que el contrato se encuentra entre 1.500 millones y 1.600 millones de euros.

Según la compañía, "la solución asegurará que el cubrimiento de la frontera sea visible y controlado a nivel del sector, a la vez que proporcionará conocimientos de la situación a nivel regional y nacional".
Defence News, 1 de julio de 2009[151]

Boeing ha firmado un contrato con el gobierno de Estados Unidos para desarrollar tecnologías de seguridad con el fin de realizar seguimientos en las fronteras de este país con México y Canadá. [...]

Los expertos en industria estiman que el contrato de tres años con el Departamento de Seguridad Nacional de Estados Unidos aporta unos 2.100 millones de dólares a Boeing [...]

El proyecto Boeing también implica crear asociaciones con empresas como Unisys.

Incluirá sensores de rastreo y equipo de comunicaciones que permita al personal que patrulla las fronteras vigilarlas con más detalle.

El sistema funcionará junto a cámaras que han sido desarrolladas por una compañía israelí y que permitan reconocer personas a 14 km de distancia
BBC, 21 de septiembre de 2006[152]

151 'Proyecto de vigilancia fronteriza Saudita adjudicado a EADS', *Defence News*, 1 de julio de 2009: http://www.defensenews.com/story.php?i=4166445&c=EUR.

152 'Contrato sobre las fronteras de Estados Unidos adjudicado a Boeing', *BBC*, 21 de septiembre de 2006: http://news.bbc.co.uk/1/hi/business/5368266.stm. Véase también: US Government Accountability Office (2008) *Secure Border Initiative: DHS Needs to Address Significant Risks in Delivering Key Technology Investment*, disponible en: http://www.gao.gov/products/GAO-08-1148T.

De acuerdo con las previsiones más pesimistas, una de cada siete personas del mundo podría verse obligada a abandonar su hogar durante los próximos 50 años a medida que los efectos del cambio climático empeoren la ya grave crisis de la inmigración.[153] Tal y como están las cosas, los refugiados a causa del cambio climático necesitarían visados que no podrían obtener. Como Zygmunt Bauman dijo, el hecho de que en esta era de la globalización y de la migración de masas se anime a viajar cuando esta actividad genera beneficios pero se condene a los que viajan para sobrevivir es una paradoja muy inquietante.[154] Al margen de si somos capaces o no de reducir la emisión de gases de efecto invernadero y sin tener en cuenta hasta qué punto cambiará el clima en el siglo XXI, los "controles fronterizos mejorados" representan a día de hoy el denominador común más bajo de la integración europea y de la inseguridad mundial; lo único que todos los gobiernos y estados consideran necesario es luchar no solo contra la inmigración no autorizada, sino también contra las amenazas de todo tipo. Dado que los controles fronterizos se están militarizando progresivamente, ¿qué aspecto tendrán las fronteras del mundo dentro de diez, veinte o cincuenta años?

La caída del muro de Berlín en 1990 amenazó brevemente con acabar con las barreras de separación y las fronteras físicas, pero en el siglo 21 Brunei, China, Israel, Kazajstán, Iraq, India, Irán, Rusia, Arabia Saudita, Turkmenistán, los EAU y Uzbekistán han construido o empezado la construcción de nuevas fronteras o barreras militarizadas.[155] También lo han hecho la UE y Estados Unidos. Joseph Nevins y otros críticos enérgicos de los controles fronterizos contemporáneos han adoptado el término "apartheid mundial" para captar el peculiar papel de los controles de inmigración en la manutención de las disparidades entre clases y razas por todo el mundo.[156] Si los países más ricos y poderosos erigen este tipo de barreras para mantener al margen o controlar a los más pobres y menos poderosos del planeta no se puede describir este sistema con otro término. Los ciudadanos de la UE pueden tener libertad de movimiento, pero ¿a qué precio?

Frances Webber ha comentado que "el número de muertes en el mar debería haberse reducido notablemente como resultado de la vigilancia intensiva del tráfico marítimo que realizan las patrullas fronterizas de la UE, las fuerzas armadas de Europa y el Mediterráneo meridional. Pero los números de ahogados, o catalogados como desaparecidos siguen aumentando a pesar (y en algunos casos a causa) de la vigilancia y la intercepción".[157] Con compañías como Boeing y EADS firmando contratos tan lucrativos en países como Estados Unidos o Arabia Saudita, la idea de que la UE necesita subvencionar el crecimiento en este ámbito parece, cuanto menos, exagerado. El gasto en I+D parece estar dirigido a coincidir con los objetivos políticos de la UE. Desde 1993, la organización antirracista UNITED ha mantenido una lista de muertes documentadas a manos de la "Fortaleza Europa".[158] La última actualización era de 13.250 muertes, si bien a día de hoy el número es necesariamente mayor. Si las subvenciones a la I+D deben tener un papel en este ámbito, se debería empezar por

153 'Climate change to force mass migration', *Guardian*, 14 de mayo de 2007: http://www.guardian.co.uk/environment/2007/may/14/climatechange.climatechangeenvironment.

154 Bauman, Z. (2002) Society Under Siege. Cambridge: Polity Press (página 84).

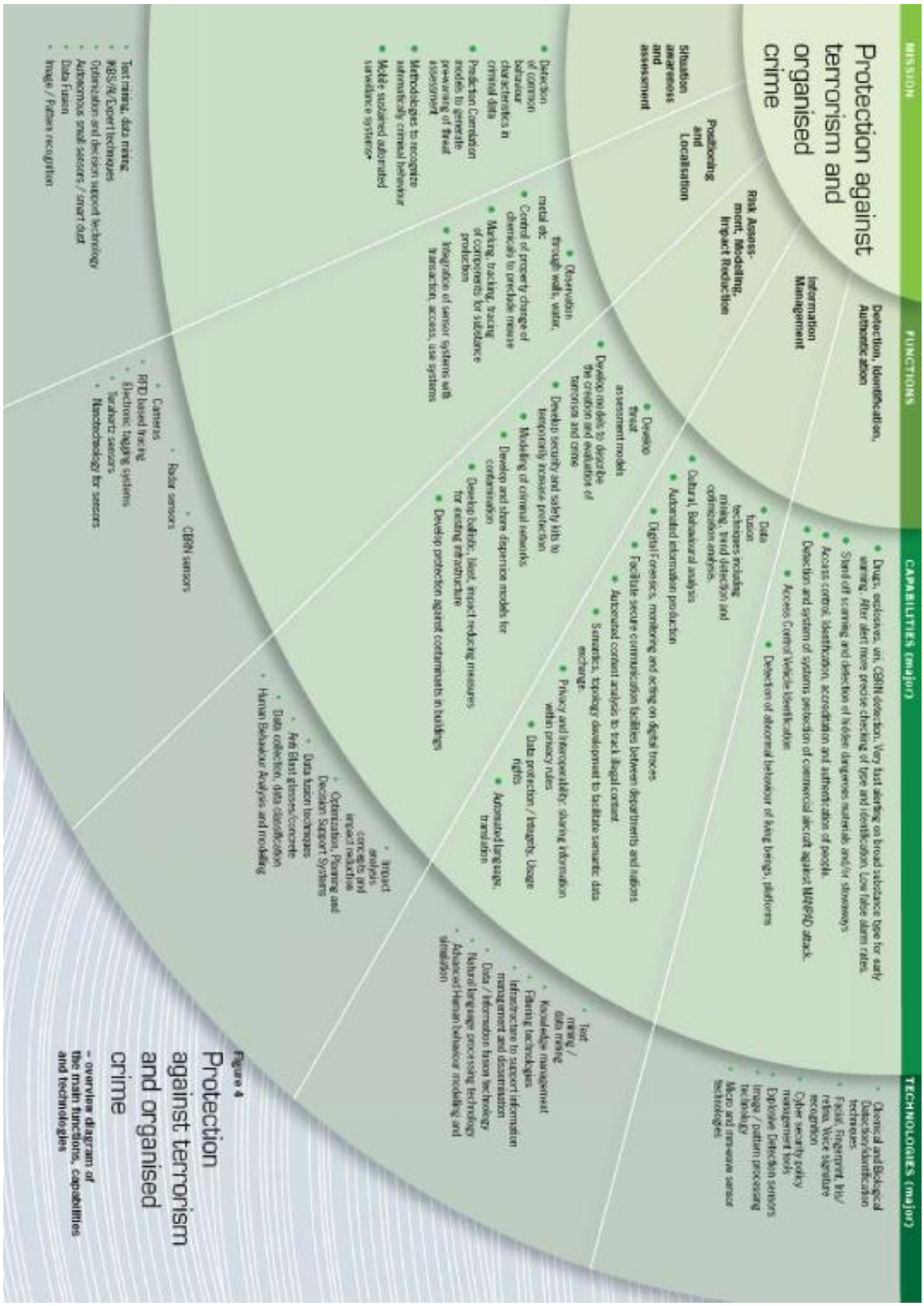
155 Véase la lista de barreras de separación disponible en Wikipedia: http://en.wikipedia.org/wiki/Separation_barrier.

156 Nevins, J (2006) *Boundary Enforcement and National Security in an Age of Global Apartheid*, discurso pronunciado en la recaudación de fondos apra la Coalición de Derechos Humanos, Tucson, Arizona, 7 de julio de 2006, disponible en: http://deletetheborder.org/files/Global%20Apartheid_set%20up.pdf.

157 Webber, F (2006) *Border Wars and Asylum Crimes*. Londres: Statewatch (página 6), disponible en: http://www.statewatch.org/analyses/border-wars-and-asylum-crimes.pdf.

158 Véase *Death by Policy: The Fatal Realities of "Fortress Europe"*: http://www.unitedagainstracism.org/pages/campfatalrealities.htm.

aumentar la seguridad en el mar aunque, como dicen desde UNITED, si 13.250 muertes no remueven la conciencia de Europa, ¿qué lo hará?



PARTE V: LUCHA CONTRA EL CRIMEN Y EL TERRORISMO; VIGILANCIA DE ESPECTRO TOTAL

> *La clave del éxito en los conflictos modernos es la superioridad en cuanto a información. El bando que cuenta con mayor cantidad de información puede maniobrar con rapidez y de forma decisiva para obtener mayores ventajas tácticas y operacionales que su enemigo. Esta superioridad también puede influir de forma precisa y efectiva en las fuerzas enemigas y reducir su capacidad de combate a cero...*
> Michael Fiszer (veterano del servicio de inteligencia militar aéreo del ejército polaco)[159]

14 Las Patriot Acts de la UE

En los años posteriores al 11-S, la UE ha ido mucho más allá que Estados Unidos en lo que a legislación se refiere, para facilitar la vigilancia de sus ciudadanos. Mientras que el Acta Patriótica ha adquirido notoriedad, de forma discreta la UE ha adoptado medidas legislativas relacionadas con la toma de huellas dactilares preceptiva para todos los pasaportes, visados y permisos de residencia de la UE y la retención (con fines de aplicación de la ley) de todos los datos de telecomunicaciones (nuestros teléfonos, correos electrónicos y datos de "tráfico" cibernético), todos los datos de los pasajeros de avión (pasajeros que entran o salen de Europa o que se desplazan por su interior) y todas las transacciones financieras.

Con este tipo de legislación en la UE, los dirigentes están empezando a acceder a una cantidad de información acerca de sus ciudadanos que antes sería impensable, generalmente en ausencia de controles judiciales o democráticos. Por ejemplo, en el Reino Unido, el régimen de retención de datos ha acabado con la obligación de los policías de reclamar una autorización judicial para acceder a registros de telecomunicaciones (ahora basta con el permiso de un agente de rango superior). De acuerdo con las cifras más recientes, la policía británica (junto con una serie de cuerpos públicos del Reino Unido) hizo uso de estos nuevos poderes nada más y nada menos que en 519.620 ocasiones durante el año 2007.[160] A medida que se extiende la retención de datos desde la telefonía móvil y fija a los proveedores de internet, la vigilancia estatal de las telecomunicaciones aumentará aún más. Para los estados, los poderes que ejercen sobre las multinacionales que les proporcionan servicios más allá de sus propias fronteras significan que pueden llevar a cabo la vigilancia de comunicaciones "extranjeras" con tanta facilidad como la vigilancia doméstica.

Parece ser que hay pocas previsiones de que surjan nuevas tendencias hacia unos poderes de vigilancia más regulados en Europa. Se propone un nuevo plan de cinco años sobre política de justicia y asuntos internos de la EU, y esto no es más que el principio de un "tsunami digital" que "revolucionará la aplicación de la ley", lo que

159 'AGS: NATO's Battlefield Eye In The Sky', *Defence Industry Daily*, 20 de octubre de 2006: http://www.defenseindustrydaily.com/ags-natos-battlefield-eye-in-thesky-02727/.

160 Véase 'Telephone tapping (and mail-opening figures) 1937-2007', *Statewatch*: http://www.statewatch.org/uk-tel-tap-reports.htm.

proporcionará una gran cantidad de información nueva a las "autoridades públicas de la seguridad" (véase sección 25).

Los servicios de seguridad también han desarrollado sistemas de escuchas virtualmente indetectables, tecnologías de seguimiento y "programas espía" que pueden instalarse clandestinamente en el ordenador personal de un sospechoso. En noviembre de 2008 el parlamento alemán aprobó una ley que otorgaba a la policía el poder de llevar a cabo "búsquedas remotas" de ordenadores personales. En el mismo mes, la UE adoptó una nueva estrategia en materia de "crimen cibernético" y propuso "una serie de medidas operacionales como patrullas cibernéticas, equipos de investigación conjunta y búsquedas remotas".[161]

La UE también sigue desarrollando una serie de bases de datos y sistemas de información de aplicación de la ley, entre los que se incluye el Schengen Information System, el Europol Information System (la base datos de inteligencia criminal de la policía europea), el Eurodac (una base de datos que contiene las huellas dactilares de todas las personas que solicitan asilo y de los inmigrantes en situación irregular en la UE), el Visa Information System y sistemas de comparación automatizada de datos que conectarán las bases de datos de ADN y huellas dactilares de los Estados miembros.

Con una vigilancia policial doméstica que a menudo está exenta de cumplir las normas y los estándares que se aplican a otros controladores de datos del sector público, las celebradas leyes de protección de datos de la UE ya han quedado atrás. Los derechos individuales sobre la privacidad y la interferencia indebida de la Declaración Universal, que ya ha celebrado su 60 aniversario, están siendo totalmente menospreciados.[162]

En noviembre de 2008 la UE adoptó una esperada decisión marco sobre protección de datos en materia judicial y policial.[163] Sin embargo, la nueva ley solo cubre la transferencia internacional de datos personales. Para desgracia de los que abogan por la privatización, no regula la protección de datos en el sector policial a nivel nacional, donde las normas son inconsistentes, a menudo débiles y no se hace lo suficiente por aplicarlas. La decisión marco, que se supone que debe proteger los bien establecidos derechos fundamentales, ha sido criticada por las organizaciones privadas, el Parlamento Europeo así como otros parlamentos nacionales y el EDPS (supervisor europeo de la protección de datos) por fracasar en la tarea de mantener las garantías más básicas de la primera Convención de Protección de Datos, que tuvo lugar en 1981.[164]

---

161 *Fight against Cyber Crime: Cyber Patrols and Internet Investigation Teams to Reinforce the EU Strategy*, nota de prensa de la CE publicada el 11 de septiembre de 2007, disponible en:
http://europa.eu/rapid/pressReleasesAction.do?reference=IP/08/1827&format=HTML&aged=0&language=EN&guiLanguage=en
Véase también: 'Watching the computers', Tony Bunyan, Guardian, 9 de junio de 2009:
http://www.guardian.co.uk/commentisfree/libertycentral/2009/jun/09/remote-accesssurveillance-rootkit.

162 Véase 'Europe's Big Brothers', Ben Hayes & See T. Hammarberg, *Guardian*, 6 de diciembre de 2008, disponible en:
http://www.guardian.co.uk/commentisfree/2008/dec/06/humanrights-surveillance/print.

163 *Decisión marco de la UE 2008/977/JHA del 27de noviembre de 2008sobre la protección de datos personales procesadores en el ámbito de la cooperación policial y judicial en materia criminal* (OJ 2008 L 350/60).

164 Véase 'Comentarios de las autoridades de protección de datos de la UE a la presidencia del Consejo sobre decisión marco sobre los datos personales en ámbitos policiales y judiciales' (7 de noviembre de 2007), *Statewatch observatory on data protection in the EU*:
http://www.statewatch.org/eu-dp.htm.

15 Conocimiento de la situación

> *Europa se enfrenta a una gran diversidad de amenazas apoyadas por estructuras de mando y mecanismos de financiación casi empresariales. Muchas agencias de seguridad coinciden en que la información es la clave para derrotar al enemigo. Este nuevo entorno ha creado no solo una mayor necesidad de información, sino también la necesidad de compartir más y controlar de manera eficaz el acceso a la información. Este es el reto más importante al que se enfrenta la seguridad europea hoy en día.*
>
> El consorcio STRAW (un proyecto de investigación en seguridad financiado por la UE)[165]

Los sistemas de vigilancia ya no se limitan a mirar. Se está combinando el uso de circuitos cerrados de televisión de alta definición con software de reconocimiento facial (y capaz de identificar andares); las cámaras de las motocicletas pueden leer matrículas y seguir a determinados coches; se está desarrollando una nueva generación de herramientas de vigilancia por satélite; hay programas informáticos capaces de monitorizar y analizar miles de millones de llamadas y mensajes de correo electrónico simultáneamente, en tiempo real; se supone que las nuevas herramientas de software pueden identificar "comportamientos sospechosos" o "intenciones hostiles".[166] La legislación de la UE ha establecido obligaciones en el ámbito de las telecomunicaciones, de las finanzas y de los desplazamientos aéreos con la intención de conservar registros de los usuarios durante largos períodos de tiempo con fines policiales. Combinando estos datos con otros (como las bases de datos sobre el estilo de vida de los consumidores) se puede crear un perfil muy detallado de la vida e intereses de un individuo; sus afiliaciones culturales, religiosas y políticas; su estado financiero y su salud.

La preocupación acerca de la vigilancia entre los ciudadanos europeos ha hecho que el término "conocimiento de la situación" se popularice entre los políticos. El grupo de trabajo 7 del ESRIF, que se dedica al "conocimiento de la situación incluyendo el ámbito espacial" tiene el deber de evaluar la tecnología de vigilancia "relevante en la seguridad urbana, la vigilancia nacional y los escenarios de aplicación de la paz". El "conocimiento situacional" se describe en el informe de la ESRAB como "la captura, fusión, correlación e interpretación de formas dispares de datos históricos y de tiempo real así como su presentación de forma clara, para facilitar la toma de decisiones y las actuaciones efectivas en entornos complejos". Las bases de datos interoperables se describieron como "esenciales para permitir realizar referencias cruzadas de la información derivada de la vigilancia en lugar de utilizar diversas fuentes heterogéneas para controlar el acceso ilícito de personas y bienes.[167]

El grupo de trabajo 7 del ESRIF examinará "los sensores actuales y los necesarios, basados en la tierra, el aire y el espacio"; identificará "nuevas normas y tecnologías para

---

165 Véase la página web del proyecto STRAW: http://www.straw-project.eu/.

166 *Protecting the right to privacy in the fight against terrorism*. Informe de Thomas Hammarberg, Comisario de derechos humanos del Consejo Europeo (CommDH/IssuePaper(2008)3/04). Estrasburgo: Consejo Europeo, disponible en: https://wcd.coe.int/ViewDoc.jsp?id=1380905&Site=CommDH&BackColorInternet=FEC65B&BackColorIntranet=FEC65B&BackColorLogged=FFC679.

167 ESRAB (2006) *Meeting the challenge: the European Security Research Agenda – A report from the European Security Research Advisory Board*. Bruselas: Comisión Europea (página 25), disponible en: http://ec.europa.eu/enterprise/security/doc/esrab_report_en.pdf.

fomentar y poder compartir la información" y propondrá "un marco de cooperación internacional sobre la fusión de fuentes de datos". De esta manera, los legisladores de la UE abdican su responsabilidad de regular los intercambios internacionales y la recolección de datos, lo que estimula al sector privado a desarrollar nuevos marcos y normas a través del ESRIF. El grupo de trabajo 7 está encabezado por EMPORDEF, el grupo de defensa que se encarga de los holdings estatales en la industria de la defensa, con Thales Alenia Space haciendo de relator.

Entre los proyectos financiados bajo la PASR se encontraban el ISCAPS, sobre vigilancia de espacios públicos, el PROBANT y HAMLET, sobre el seguimiento de personas, el TRIPS, sobre la vigilancia de estaciones de tren y el EUROCOP, sobre información geoespacial para la policía. La obsesión por los sistemas de vigilancia ha seguido adelante en el programa FP7 gracias a programas como el SUBITO, sobre la "detección de equipaje abandonado en tiempo real y la rápida identificación del propietario", el LOTUS, sobre la detección de fábricas ilegales de fármacos y bombas, el IDTEC4ALL, sobre tecnología novedosa en detección de intrusos y el ODYSSEY, sobre el desarrollo de una "plataforma de inteligencia balística paneuropea estratégica". La Agencia de Defensa Europea también ha ofrecido varios contratos en el ámbito de la I+D relacionados con la vigilancia.[168]

[168] Véanse los contraltos 4 y 13, 'Lista annual de contratistas – 2007' (2008/S 62-083197**),** página web de la Agencia de Defensa Europea: http://www.eda.europa.eu/procurement.aspx.

16 El comienzo de la era biométrica

> *Diga adiós a los PIN y a las tarjetas de identidad. Salude a las huellas dactilares digitales y a los escáneres de iris (y a las nuevas oportunidades para el negocio de la seguridad).*
> Business Week, mayo de 2009[169]

Compra de identidades

Tras aceptar la toma de huellas dactilares masiva de los ciudadanos europeos, la biométrica representa un área de la tecnología de la seguridad encabezada por Europa. Cuando la UE adoptó la legislación sobre las huellas dactilares de los poseedores de pasaportes en 2005, su centro de investigación conjunta sugirió que "en cuanto la gente se acostumbre al uso de la biométrica en las fronteras se empezará a usar también en aplicaciones comerciales. La introducción de la biométrica a gran escala en Europa es una gran oportunidad: en primer lugar, sirve para crear un mercado de demanda basado en la aceptación del usuario; en segundo lugar, el fomento de un mercado de suministros competitivo".[170] Tal y como ha comentado un observador de Estados Unidos: "Antes del 11-S las expectativas en cuanto al avance de la biométrica eran que se acabara aplicando también al sector comercial. Pero con el énfasis que se puso en la seguridad después de los atentados terroristas, ahora se centran en grandes iniciativas gubernamentales".[171]

Todos los países de la UE deben instituir pasaportes electrónicos con registro de huellas dactilares para el verano de 2010. Deben utilizar tecnología interoperable y, con el Tratado de Prüm, están obligados a proporcionar el acceso a sus bases de datos biométricas nacionales en un futuro para que pueden ser controladas por otros Estados miembros.[172] Actualmente se está estableciendo un sistema de identificación automática de huellas dactilares (AFIS). Estados Unidos, Reino Unido, Australia, Canadá y Nueva Zelanda han establecido un grupo de trabajo, el International Information Consortium, para desarrollar su propio sistema automático de intercambio de huellas dactilares.[173]

El Foro Europeo de Biométrica, un grupo "cuya visión general consiste en hacer de la UE el líder mundial en biométrica mediante la creación de barreras en la adopción y la fragmentación del mercado",[174] ha sido designado como relator del grupo de trabajo 8 del ESRIF, que se dedica a la "identificación de individuos y activos". Este foro

---

169 'The Dawning of the Biometric Age', *Business Week*, 29 de mayo de 2009: http://www.businessweek.com/innovate/content/may2009/id20090520_625039_page_2.htm.

170 Véase 'El informe de la UE sobre biométrica evita los asuntos importantes', *Statewatch news online*, marzo de 2005: http://www.statewatch.org/news/2005/mar/17eubiometric-report.htm.

171 Lawrence Hornak, codirector de la Investigación sobre tecnología de identificación de la fundación científica nacional de Estados Unidos, citado en 'The Dawning of the Biometric Age', *Business Week*, 29 de mayo de 2009: http://www.businessweek.com/innovate/content/may2009/id20090520_625039_page_2.htm.

172 Alemania, España, Francia, Luxemburgo, Países Bajos, Austria y Bélgica firmaron el Tratado de Prüm el 27 de mayo de 2005. Texto íntegro disponible en: http://www.statewatch.org/news/2005/aug/Prum-Convention.pdf. La legislación europea para la implementación del tratado y para ampliar su alcance se adoptó en junio de 2008 (véanse las decisiones 2008/615/JHA y 2008/616/JHA).

173 Véase 'El FBI quiere tener acceso directo a los datos de identidad británicos', Guardian, 15 de enero de 2008: http://www.guardian.co.uk/uk/2008/jan/15/world.ukcrime. Hace tiempo que Estados Unidos, Reino Unido, Canadá y Nueva Zelanda trabajan juntos en la vigilancia a través del ECHELON un sistema mundial de escuchas secretas.

174 Véase la página web del Foro Europeo de Biométrica: http://www.eubiometricforum.com/.

también participa en al menos cinco proyectos de investigación financiados por la UE y dirige el consorcio BIOTESTING EUROPE (de la PASR), apoyando a la legislación de la UE sobre las huellas dactilares en los pasaportes, visados y permisos de residencia.[175]

El desarrollo de la legislación de la UE en este ámbito también fue apoyado por varios proyectos de investigación del FP6, entro los que se incluían los proyectos MTIT y DIGITAL PASSPORT.[176] La UE también financió el 3DFACE, un proyecto de 10 millones de euros encabezado por Sagem, que pretende fusionar "tecnología de reconocimiento facial en 3D, incluyendo la fusión con tecnologías de reconocimiento facial en 2D, con su aplicación en entornos con grandes despliegues de seguridad".[177]

La investigación sobre biométrica de la UE no se limita solo a sistemas de identificación; el financiamiento ha apoyado la investigación a largo plazo en biométrica aplicada durante más de una década, incluyendo diversos proyectos de I+D dirigidos a la aplicación comercial y al desarrollo de la tecnología biométrica.

Selección de proyectos relacionados con la biométrica financiados por la Comisión Europea:

- **BIOTESTING EUROPE** (PASR): guía para la unificación de sistemas biométricos de identificación en la UE.
- **MTIT** (FP6): proyecto de pruebas de interoperabilidad de plantillas detalladas, sobre la interoperabilidad de los sistemas biométricos de toma de huellas dactilares.
- **DIGITAL PASSPORT**: pasaporte digital europeo de nueva generación.
- **BIOSEC** (FP6): identificación de voz, iris y huellas dactilares.
- **3DFACE** (FP6): reconocimiento facial.
- **TURBINE** (FP7): identidades biométricas revocables de confianza.
- **BIO-RESIDENCE** (FP6): el uso de la biométrica en sistemas de entrada y acceso.
- **BIOSECURE** (FP6): aplicaciones delicadas como el comercio y las actividades bancarias por Internet.
- **HUMABIO** (FP6): tecnología requerida para leer y analizar datos biométricos.
- **FIDIS** (FP6): consecuencias de la biométrica en la "sociedad de la información europea".
- **BITE** (FP6): ética de las tecnologías de identificación biométrica.
- **VEIN BIOMETRIC** (FP7): aplicaciones en el campo de la seguridad utilizando imágenes de las venas tomadas mediante infrarrojos.

---

175 BIOTESTING EUROPE servirá de guía sobre "las pruebas que es necesario llevar a cabo", "los componentes que deben utilizarse (sensores, algoritmos, subsistemas, etc.)", "las personas que llevarán a cabo las pruebas", "los costes y los inversores y responsables de su financiación". Véase la página web de BIOTESTING EUROPE: www.biotestingeurope.eu. El Foro Europeo de Biométrica también participó en los proyectos STACCATO (PASR) y CRESCENDO (ESRP, FP7).

176 El proyecto MTIT sobre pruebas de interoperabilidad de plantillas detalladas contaba con Sagem, Motorola y Fraunhofer y prometió "mejorar la interoperabilidad de los sistemas biométricos de toma de huellas dactilares basados en las plantillas detalladas en un plazo de tiempo que coincidiera con la legislación de la UE". El proyecto DIGITAL PASSPORT, sobre "pasaportes digitales europeos de nueva generación con datos biométricos para un tránsito fronterizo más seguro y conveniente (sic)" se diseñó siguiendo el Schengen Information System y las especificaciones de la ICAO.

177 La legislación de la UE exigirá fotografías y huellas digitales en todos los pasaportes europeos. La Organización Internacional de Aviación Civil (ICAO, un cuerpo de las Naciones Unidas) también exige fotografías digitales de acuerdo con especificaciones técnicas unificadas. El proyecto 3DFACE incluía una "prueba a gran escala en algunos de los principales aeropuertos europeos con el fin de poner a prueba el funcionamiento del sistema y de analizar los resultados sociales y operacionales".

- **FINGER_CARD**: sistemas de correspondencia y autentificación biométricos en tarjetas.
- **MOBIO** (FP7): sistemas de autentificación bimodal en el marco de los dispositivos móviles.
- **ACTIBIO** (FP7): autentificación no bloqueante utilizando biométrica ligera y relacionada con la actividad en cuestión.
- **BEE** (FP7): entorno de los negocios de la biométrica relacionados con el comercio electrónico.
- **WABY** (FP7): sistema de identificación biométrica basado en el reconocimiento facial.
- **VIPBOB**: códigos pin virtuales basados en la biométrica.
- **BANCA** (FP7): control de acceso biométrico para aplicaciones de redes y comercio electrónico.
- **SABRINA** (FP7): autentificación segura mediante integración racional biométrica en aplicaciones de redes.
- **HIDE** (FP7): seguridad nacional, identificación biométrica y ética de la detección de personas.
- **RISE** (FP7): mejora del conocimiento paneuropeo e internacional acerca de las implicaciones éticas de la biométrica y la seguridad.
- **BIOTEST** (1996): servicios de pruebas biométricas.

Implicaciones éticas democracia y derechos humanos

Los proyectos de investigación financiados por la UE hasta la fecha asumen que la biométrica está aceptada públicamente y han visto como su oposición pública y potencial se ha visto reducida a "implicaciones éticas". También asume que la recolección y el uso de datos biométricos solo están relacionados con la privacidad y la protección de datos y que, de alguna manera, se pueden solucionar mediante el uso de tecnología compatible con la privacidad. Esto deja muy poco espacio (o ninguno) a aquellos que están en desacuerdo y ven la toma de huellas dactilares como un asunto de gran importancia en materia de libertades civiles y derechos humanos y que pueden hacer que determinadas tecnologías se conviertan en inaceptables o incluso ilegales. Por ejemplo, el proyecto BITE sobre la ética de las tecnologías de identificación biométrica, promueve "la investigación y el debate público sobre las implicaciones bioéticas de las tecnologías emergentes relacionadas con la identificación biométrica",[178] mientras que el proyecto TURBINE pretende "aumentar la privacidad multidisciplinar mediante la tecnología, combinando la innovación en el campo de la criptografía y la biométrica para toma de huellas dactilares". Pretende proporcionar un sistema biométrico integrado efectivo mientras soluciona las principales cuestiones relacionadas con la "preocupación por la privacidad asociada al uso de la biométrica en el control de sistemas de identificación".[179] El HIDE,[180] proyecto sobre seguridad nacional, identificación biométrica y ética de la detección de personas, es la última "plataforma destinada a los asuntos de ética y privacidad de la biométrica y las tecnologías de la detección de

[178] Véase la página web del proyecto BITE: http://www.biteproject.org/.

[179] Véase la página web del proyecto TURBINE: http://www.turbine-project.eu. Véase también la página web del proyecto FIDIS 'Network of Excellence' (2004-7) sobre "el futuro de la identidad en la sociedad de la información", que buscaba proporcionar "tecnologías fiables y seguras": http://www.hideproject.org/.

[180] Véase la página web del proyecto HIDE: http://www.hideproject.org/.

personas que se encarga de problemas transnacionales (europeos) e internacionales". El objetivo del HIDE consiste en "convertirse en el principal catalizador de soluciones políticas innovadoras a los problemas éticos emergentes en el ámbito de las tecnologías de vigilancia… especialmente cuando la colaboración entre agencias, comunidades, negocios y ONG nacionales e internacionales resulta crucial".[181]

Mientras que los "arquitectos" del ESRP ven la introducción de sistemas de identificación biométricos y otras aplicaciones comerciales como un imperativo económico que *podría* conllevar implicaciones éticas, el Tribunal Europeo de los Derechos Humanos ha adoptado una interpretación más crítica. En diciembre de 2008, en el caso *S. & Marper v. UK*, el Tribunal llegó a la conclusión de que la política de la policía de Reino Unido de tomar muestras de ADN y huellas dactilares de todo individuo que era arrestado para posteriormente almacenarlas de manera indefinida en las bases de datos nacionales de la policía (aunque la persona arrestada fuera puesta en libertad sin cargos), violaba la Convención Europea de Derechos Humanos.

El caso se llevó a juicio después de que salieran a la luz los casos de un niño de 11 años que fue acusado de robo y posteriormente puesto en libertad y de un adulto cuyos cargos de acoso sexual fueron retirados. El Tribunal concluyó que: "la naturaleza exhaustiva e indiscriminada de los poderes de retención de huellas dactilares, muestras celulares y perfiles de AND de sospechosos pero no condenados […] no consiguen establecer un balance justo entre el público competente y los intereses privados, ya que el estado ha sobrepasado los límites aceptables en este aspecto". De la misma manera, el Tribunal afirmó que "la retención de las muestras mencionadas constituye una interferencia desproporcionada en el derecho de los ciudadanos al respeto por la vida privada y no puede considerarse necesaria en una sociedad democrática".[182]

La sentencia tuvo consecuencias evidentes en los sistemas de identificación a gran escala que estaba desarrollando la UE; por ejemplo, en el plan para permitir el acceso de agencias de aplicación de la ley al sistema de información de visados de la UE (VIS), que contendría las huellas dactilares de todo individuo que solicitara permiso para entrar a alguno de los Estados miembros (unos 20 millones de personas al año). El VIS contará con registros biométricos de niños de a partir de seis años y de decenas de millones de personas que no han cometido ningún delito. Así pues, esta no parece una idea en absoluto proporcionada en el contexto de la sentencia de S. Y Marper.

Sin embargo, desde hace un tiempo muchos Estados miembros de la UE vienen mostrando distintas interpretaciones de lo que es "proporcionado en una sociedad democrática". Como respuesta a la resolución del Tribunal Europeo, Reino Unido propone acabar con la retención indefinida de las muestras de ADN y las huellas dactilares de personas arrestadas que quedan en libertad sin cargos; en lugar de esta medida, propone retenerlas durante un período de seis años (12 años en los casos relacionados con terrorismo y delitos sexuales graves). Para muchos de los lectores de la

181 El proyecto HIDE está coordinado por el Centro para la Ciencia, la Sociedad y la Ciudadanía (Italia); entre sus participantes se incluyen el Grupo Biométrico Internacional (una empresa estadounidense que se autodescribe como "la principal empresa de servicios de tecnología y consultas de la industria biométrica"), Sagem y Fraunhofer junto con varias universidades europeas y asesores privados. El Centro para la Ciencia, la Sociedad y la Ciudadanía también coordina el proyecto RISE (mejora del conocimiento paneuropeo e internacional acerca de las implicaciones éticas de la biométrica y la seguridad). Entre los participantes en el proyecto RISE se encuentran el EBF y la Global Security Intelligence (Estados Unidos); véase la página web del RISE: http://www.riseproject.eu/ (todavía no estaba disponible en el momento de redactar este informe).

182 Véase el juicio del caso S. & Marper v. UK (30562/04 and 30566/04), disponible en: http://www.statewatch.org/news/2008/dec/echrmarper-judgment.pdf.

sentencia del Tribunal, esta medida sigue excediendo de cierta manera "cualquier margen aceptable de apreciación" en la interferencia del estado en el derecho individual a la privacidad en una sociedad democrática.[183]

183 Véase 'Keeping the Right People on the DNA Database: Science and Public protection", mayo de 2009, disponible en: http://www.guardian.co.uk/politics/2009/may/07/dna-database-reforms-human-rights/print.

17 Comunidades sospechosas: sistemas de perfilado y de obtención de objetivos

> *Tanto la seguridad como la vigilancia nacional se están empleando en gran medida no solo para realizar seguimientos (actividades que van desde catalogar a sospechosos de terrorismo a emplazamientos de infraestructuras críticas, comunidades cercadas, hospitales y escuelas y comportamiento de los consumidores) sino también como principal instrumento de clasificación social que discrimina en función de perfiles informáticos o imágenes.*
> Neve Gordon, Tercer informe del proyecto New Transparency[184]

Un componente básico de la "sociedad de la vigilancia" emergente es el cada vez más extendido proceso de "clasificación social", un proceso continuo basado en "códigos, generalmente procesados por ordenadores, que realizan transacciones, interacciones, visitas, llamadas y otras actividades". Estos códigos son "las puertas visibles que permiten o impiden la participación en una gran multitud de eventos".[185]

En el contexto de la seguridad, esto significa que es necesario identificar y hacer distinciones entre personas que suponen una amenaza, "riesgos" que podían suponer una amenaza y "ciudadanos de confianza" que tienen libertad para dedicarse a lo que quieran. Sin embargo, a menudo estos códigos (también conocidos como "perfiles" en el contexto de la aplicación de la ley) pueden basarse en suposiciones discriminatorias relacionadas con la raza, la clase social, la religión... lo que institucionaliza la discriminación en perjuicio de las minorías étnicas y otras "comunidades sospechosas".

Entre los proyectos financiados por la UE en este ámbito se encuentran: el ya mencionado proyecto HUMABIO, que utilizará "indicadores biodinámicos y análisis de comportamiento" para el seguimiento y la autentificación de personas; el proyecto SAMURAI, sobre la detección de "comportamientos sospechosos y anormales utilizando una red de cámaras y sensores para mejorar el conocimiento de la situación"; el proyecto INDECT, que promete la "detección automática de amenazas y el reconocimiento de comportamientos anormales o actos violentos"; y por último, el proyecto ADABTS, sobre la detección automática de comportamientos anormales y amenazas en espacios con multitudes de gente". El proyecto ADABTS, encabezado por la FOI (la agencia de investigación militar sueca) y que cuenta con el apoyo de BAE Systems, la Home Office de Reino Unido (equivalente al Ministerio del Interior de España) y la TNU (la agencia de investigación militar holandesa), demostrará la "predicción de la evolución del comportamiento, de manera que las actitudes que puedan llegar a suponer una amenaza se puedan detectar a medida que se desarrollan, con lo que se permita la vigilancia pro-activa".

La UE también ha financiado una serie de proyectos relacionados con software de obtención de datos, obtención de datos tanto en mercados financieros como en la

184 Gordon, N. (2009) 'The Political Economy of Israel's Homeland Security', *The New Transparency Project,Working Paper III, IRSP IV*, disponible en: http://www.surveillanceproject.org/files/The%20Political%20Economy%20of%20Israel%E2%80%99s%20Homeland%20Security.pdf.

185 Lyon, D. (ed., 2003) *Surveillance as social sorting*, Routledge: Londres & Nueva York (página 13).

investigación biomédica y por último, investigación medioambiental para la obtención de datos y se ha esforzado en promover el uso de la tecnología tanto del sector público como del privado. Por ejemplo, el proyecto ADMIRE, sobre obtención de datos avanzada e investigación de integración para Europa ("facilitar la obtención de datos"), pretende proporcionar "tecnología de uso fácil para obtener información y conocimientos... a partir de diversos recursos heterogéneos y distribuidos.

Cómo crear amenazas y alienar a la población

En noviembre de 2002 la UE adoptó una recomendación secreta sobre el "desarrollo de perfiles de terroristas".[186] El texto, que no se publicó, afirma que "la mayoría pero no todos los países de la UE estaban trabajando en perfiles en el área del terrorismo" y anima a los Estados miembros a "transmitir información a la Europol, que desarrollará los perfiles de los terroristas y los pondrá a la disposición de las autoridades pertinentes en cada caso".

Las características que se tenían en cuenta para clasificar la propensión a cometer actos de terrorismo eran la nacionalidad, los medios de transporte utilizados, la edad, el sexo, las características físicas distintivas (como las cicatrices), la educación, el "uso de técnicas para prevenir ser descubierto o interrogado", los lugares de estancia, el lugar de nacimiento, las características psico-sociológicas, la situación familiar, el conocimiento en tecnología avanzada y la "asistencia a cursos de entrenamiento paramilitares, de vuelo y otras especialidades". El programa de la UE sobre "radicalización y reclutamiento", que de forma implícita fomenta el uso del perfilado en las operaciones de contraterrorismo y la obtención de objetivos tanto de mezquitas "moderadas" como de las "radicales", así como de escuelas, centros comunitarios, páginas web y sus visitantes, también cuenta con un presupuesto de investigación.[187]

No ha trascendido información acerca de la implementación de las recomendaciones de la UE en este ámbito pero ésta ha financiado el proyecto HITS-ISAC, coordinado por Saab, para desarrollar un marco técnico para "intercambio interfronterizo de distintas fuentes de información" con el fin de "prevenir, predecir y proteger contra posibles actividades terroristas y el crimen organizado".[188] Alessandro Zanasi, un policía italiano jubilado que pertenecía al cuerpo de especialistas en intercepción telefónica, era miembro de la ESRAB y el SHERIFF y cofundó Temis, una compañía especializada en "inteligencia textual", participa en tres proyectos de la Comisión Europea y en "algunos otros confidenciales".[189]

Los sistemas de perfilado y de vigilancia "por-activa" han dado completamente la vuelta al derecho a la presunción de inocencia: todos somos "sospechosos" y podemos ser

---

186 *Draft Council Recommendation on the development of terrorist profiles*; document del Consejo de la UE 11858/3/02, 18 de noviembre de 2002, disponible en: http://www.eclan.eu/Utils/ViewFile.aspx?MediaID=168&FD=4E.

187 *Commission programme for the prevention of and response to violent radicalisation*, página web de la CE: http://ec.europa.eu/justice_home/funding/2004_2007/radicalisation/funding_radicalisation_en.htm.

188 Página web del proyecto: http://www.hits-isac.eu/

189 Temis ofrece "análisis de información automatizados de informes, correos electrónicos, noticias, etc."; véase 'New Tools for New Intelligence: Text Mining and European Commission Funding', presentación de Alessandro Zanasi en la conferencia: *La Inteligencia Competitiva*, Madrid, 29 de noviembre de 2007, disponible en: http://www.madrimasd.org/Inteligencia-Competitiva/documentos/Alessandro_Zanasi-TEMIS_Italia.pdf.

interrogados a partir de presunciones o carencias de información de los encargados de este tipo de vigilancia. Por supuesto, algunas personas son más sospechosas que otras; el perfilado empieza con este principio. En respuesta a la recomendación de la UE sobre "perfilado de terroristas", la red de expertos en derechos fundamentales de la UE, ya disuelta, comentó que el perfilado solo estaba justificado "si se demostraban de manera estadísticamente significativa las relaciones entre estas características y el riesgo de terrorismo, demostración que hasta la fecha no se ha realizado".[190] El Parlamento Europeo "ha expresado en varias ocasiones su preocupación respecto al perfilado, concretamente en lo referente a la raza, etnicidad y religión, en los contextos de la protección de datos, la seguridad del transporte, la inmigración y el control fronterizo y el trato a las minorías. Sin embargo, no se ha llevado a cabo ningún análisis adecuado de los aspectos legales y de otra índole que podrían hacer que se llegara a un acuerdo sobre lo que es aceptable y lo que no lo es".[191]

El comisario de Derechos Humanos del Consejo Europeo ha sugerido que, si bien las tecnologías que permiten el "perfilado" y la "obtención de datos" pueden parecer soluciones interesantes para la seguridad, lo más probable es que acaben actuando en contra de muchas personas inocentes a escalas inaceptables en una sociedad democrática.[192] Es importante enfatizar que se trata de algo inevitable; no se puede arreglar con un diseño mejor. Como ha explicado Douwe Korff, un profesor especializado en tecnologías de vigilancia, "desde un punto de vista matemático, los intentos de identificar objetivos o incidentes muy poco frecuentes entre una enorme cantidad de datos darán como resultado un número inaceptablemente alto de falsos positivos (identificar individuos inocentes como sospechosos) o un número inaceptablemente bajo de falsos negativos (no identificar verdaderos criminales o terroristas)." Se podría decir que si se está buscando una aguja en un pajar, no sirve de nada echar más paja al montón.[193]

Tal y como el experto en privacidad Bruce Schneier comenta: "la efectividad de cualquier sistema de perfilado está directamente relacionada con sus probabilidades de ser subvertido. El perfilado es algo que todos hacemos porque funciona", sugiere Schneier, "pero cuando uno se enfrenta a un adversario inteligente... se está invitando al adversario a subvertir deliberadamente el sistema de perfilado en cuestión".[194]

También hay muchas pruebas que indican que, no solo en Irlanda del Norte, establecer como objetivo una "comunidad sospechosa" y lo que el profesor Paddy Hillyard denomina "sociología de los encuentros en la calle", pueden ser totalmente contraproducentes porque se reducen los esfuerzos en contraterrorismo y se fomenta la "radicalización".[195] En palabras del Comité para la administración de justicia de Irlanda

---

190 *The Balance Between Freedom and Security in the Response by the European Union and its Member States to the Terrorist Threats*, informe de la red de expertos de la UE sobre los Derechos Fundamentales, 2003, Bruselas: Comisión Europea, disponible en: http://ec.europa.eu/justice_home/cfr_cdf/doc/obs_thematique_en.pdf.

191 *Working Document on problem of profiling, notably on the basis of ethnicity and race, in counterterrorism, law enforcement, immigration, customs and border control*, Comité del Parlamento Europeo sobre libertades civiles, justicia y asuntos (*relatora*: Sarah Ludford), 30 de septiembre de 2009 (PE413.954v02-00), disponible en: http://www.statewatch.org/news/2008/oct/ep-draft -report-on-profiling-ludford-oct-08.pdf.

192 *Protecting the right to privacy in the fight against terrorism*. Informe de Thomas Hammarberg, Comisario de Derechos Humanos del Consejo Europeo (CommDH/IssuePaper(2008)3/04). Estrasburgo: Consejo Europeo (página 4), disponible en: https://wcd.coe.int/ViewDoc.jsp?id=1380905&Site=CommDH&BackColorInternet=FEC65B&BackColorIntranet=FEC65B&BackColorLogged=FFC679.

193 Citado en 'Surveillance Society', Ben Hayes, *Red Pepper*, enero de 2008: http://www.redpepper.org.uk/Surveillance-Society.

194 'Behavioral Profiling', *Schneier on Security*, agosto de 2006: http://www.schneier.com/blog/archives/2006/08/behavioral_prof.html.

195 Hillyard, P. (1993) *Suspect Community: People's Experience of the Prevention of Terrorism Acts in Britain*. Londres: Pluto.

del Norte: "la gente no va a informar acerca de incidentes o información crucial a la policía si su último contacto (con la policía o los servicios de seguridad) no ha sido agradable, ha sido humillante y abusivo, o ha oído cómo han tratado a un vecino o un familiar".[196]

La campaña de Amnistía Internacional para acabar con el perfilado racial

"El perfilado racial se da cuando los responsables de la aplicación de la ley o de la seguridad privada basan sus sospechas criminales de investigaciones no específicas en la raza. Tanto este tipo de discriminación como la basada en la religión, la nacionalidad, o cualquier otra identidad particular van en contra de los derechos humanos y las libertades fundamentales a los que toda persona tiene derecho".[197]

Injusticia étnica en la lucha contra el terror

"Desde los atentados del 11-S en Nueva York, el 32% de los musulmanes británicos informaron de que habían sido discriminados en los aeropuertos y las detenciones y registros de los ciudadanos británico-asiáticos se multiplicaron por cinco tras los intentos de atentado en Londres y Glasgow junio de 2007. En las mezquitas alemanas la policía armada con ametralladoras sometió a controles de identidad a niños de 11 años. También en Alemania, se puso en funcionamiento un proceso de obtención de datos que investigó a 8,3 millones de personas sin que se identificara a ningún terrorista. Los musulmanes, los gitanos rumanos y los grupos que migran por Europa han informado de que se sienten sospechosos y de que tienen que demostrar constantemente su inocencia o sus derechos de estancia en el país en cuestión. Desde las detenciones en la calle hasta los registros en aeropuertos pasando por la aplicación de sistemas de obtención de datos, el perfilado étnico afecta a varios miles de personas y estigmatiza a comunidades enteras. Además de ser una actividad muy extendida pero poco controlada, se trata de un tipo de discriminación ilegal en muchas circunstancias (Rebekah Delsol, *Open Society Justice Initiative*, 2008).[198]

196 *War on Terror: Lessons from Northern Ireland – Executive summary*, Comité de administración de justicia,enero de 2008, disponible en: http://www.caj.org.uk/Front%20page%20pdfs/Terror%20summary_12pp%20pages.pdf.

197 *Racial profiling*, página web de Amnistía Internacional: http://www.amnestyusa.org/us-human-rights/racial-profiling/page.do?id=1106650.

198 Delsol, R. (2008) *Ethnic Profiling, ID Cards and European Experience*, presentación de la Iniciativa por la justicia en una sociedd abierta en la mesa redonda: *Identity Cards and Suspect Communities Roundtable Seminar*, organizada por la Comisión de Derechos Humanos de Irlanda del Norte, disponible en: http://www.statewatch.org/news/2008/oct/nireland-nihrc-id-cards-profiling.pdf

18 La carrera espacial europea: Galileo y Kopernikus

> *¿Podemos seguir hablando de un uso pacífico del espacio teniendo en cuenta que las bombas y las granadas están dirigidas por satélites de navegación?*
> Frank Slijper, *From Venus to Mars: The European Union's steps towards the militarisation of space*.[199]

La UE está desarrollando dos sistemas de vigilancia basados en satélites. El primero, además de ser el mejor, que se conoce como sistema Galileo y se concibió a mediados de la década de los 90, está considerado el primer sistema GPS civil del mundo (que proporciona a la UE independencia estratégica de Estados Unidos). El Galileo se convirtió en la primera "colaboración público privada" (PPP) de la UE, con gigantes del sector de la defensa como Thales, EADS y Finmeccanica entre los seleccionados para cofinanciar la fase de despliegue. Un alto cargo de EADS explicó los fundamentos de la corporación: "los GPS empezaron como sistemas militares pero ha emergido un mercado enorme a su alrededor y la industria estadounidense ha sabido recoger los beneficios que genera. Actualmente todo tipo de industrias dependen de los sistemas de GPS (petróleo, gas, distribución de la electricidad, telecomunicaciones...)[200]

Para el 2007, el consorcio PPP Galileo se había desmoronado y las empresas culparon públicamente a la "rígida forma de gobernar" de la UE. Incluso el director general de la Agencia Espacial Europea pidió "visión europea... que no empieza por la forma de gobernar".[201] Actualmente los costes están a cargo de la UE en solitario, y el contrato de 3.400 millones de euros destinado a la fase de despliegue del Galileo se ha sacado a concurso.

Como se explicó en el informe de 2008 del TNI sobre política espacial europea, el sector industrial europeo actual se concentra básicamente en tres grandes compañías: EADS Astrium, Thales Alenia Space (una unión de Thales, 67% y Finmeccanica, 33%, que incorpora a Telespazio) y OHB Technology de Bremen y que ha experimentado un enorme crecimiento en la última década. Otras compañías importantes, con divisiones espaciales que cuentan con menos de mil empleados, son Dassault (Francia), Oerlikon Space (Austria), Saab Space (Suecia), Sonoca (Bélgica), Terma (Dinamarca) y VEGA Aerospace (Reino Unido).[202]

Finalmente la UE puso en marcha la fase de despliegue de 3.400 millones de euros en 2009, con EADS Astrium y OHB como proveedores de componentes para naves espaciales y la compañía de cohetes Arianespace como responsable para lanzar las primeras plataformas operativas del sistema Galileo.[203] Si bien la UE sostiene que el Galileo es otro imperativo económico para Europa, no todo el mundo está convencido de ello. Un diplomado anónimo de un Estado miembro de la UE, citado en

---

199 *Slijper* F (2009) *From Venus to Mars*: *The European Union's steps towards the militarisation of space*. Amsterdam: Transnational Institute, disponible en: http://www.tni.org/detail_pub.phtml?&know_id=276.

200 'Empieza la puja por poner en órbita el sistema de navegación Galileo de la UE', *Independent*, 2 de Julio de 2008: http://www.independent.co.uk/news/business/news/biddingstarts-to-put-eus-galileo-navigation-system-into-space-858415.html.

201 'Empieza la puja por poner en órbita el sistema de navegación Galileo de la UE' (ver nota anterior).

202 *Slijper* F (2009) *From Venus to Mars*: *The European Union's steps towards the militarisation of space*. Amsterdam: Transnational Institute, disponible en:http://www.tni.org/detail_pub.phtml?&know_id=276.

203 Los contratos impulsan el Galileo, BBC, 16 de junio de 2009: http://news.bbc.co.uk/1/hi/sci/tech/8102047.stm

Euractiv.com afirma que "todo el mundo sabe que el Galileo no tendrá oportunidades de negocio. Solo necesitamos un sistema europeo propio porque en un momento muy crítico a nivel militar no podemos confiar en la disponibilidad de GPS (extranjeros)".[204] Este "imperativo estratégico" también proporcionaría a la UE la independencia militar de la OTAN y de Estados Unidos que varios Estados miembros querrían.

La UE, que ha empezado a dar pasos graduales pero firmes hacia la militarización, ha dejado de estar comprometida exclusivamente con el uso pacífico del espacio. En 2008 el Parlamento Europeo (PE) abandonó su larga oposición al uso del Galileo con fines de defensa y de operaciones de control de crisis bajo los auspicios de las relaciones internacionales de la UE. El informe del PE, cuya primera versión fue redactada por Karl von Wogau (miembro del Parlamento Europeo y del grupo de personalidades), también contiene previsiones que favorecen el desarrollo de sistemas de defensa que utilizan misiles guiados por satélite por parte de la OTAN.[205] La Agencia de Seguridad Europea también tiene intereses en el MilSatCom y ha contratado a London Satellite Exchange Ltd. para llevar a cabo un estudio que "apoyará la definición de (sus) futuros objetivos relacionados con MilSatCom".[206]

En las aplicaciones de seguimiento por satélite, la aplicación de la ley podría tener diversos usos. En Alemania ya se utilizan los satélites junto con otros tipos de tecnología para seguir a algunos camiones dependiendo de su tamaño y sus emisiones. En el Reino Unido, esgrimiendo los atascos más que la contaminación del automóvil, el gobierno pretendió realizar seguimientos por satélite de todos los coches para el año 2005. Esta propuesta fue ridiculizada por los medios de comunicación y se topó con una recogida de firmas que alcanzó 1,8 millones de peticiones en su contra.[207] Sin embargo, nadie puso el grito en el cielo cuando en 1999 se decidió que los criminales que hubieran cometido delitos sexuales en el mismo país fueran sometidos a seguimientos por satélite.[208] En diciembre de 2008 la Comisión Europea publicó un plan de acción sobre el despliegue de sistemas de transporte inteligentes (STI) en Europa y la directiva propuesta para establecer un marco para los STI en la UE.[209]

Kopernikus/GMES

El segundo sistema de vigilancia por satélite de la UE se conoce como GMES. En principio eran las siglas en inglés correspondientes a Seguimiento Mundial para la Seguridad del Entorno, pero se cambió a Seguimiento Mundial del Entorno y la

---

[204] Dosier del Galileo, *Euractiv.com*, actualizado el 23 de abril de 2008: http://www.euractiv.com/en/science/galileo/article-117496.

[205] Parlamento Europeo (2008) *Informe sobre espacio y seguridad*, Comité de asuntos exteriores, EP doc. A6-0250/2008, 10 de junio de 2008.

[206] Véase el contrato 16, 'Lista anual de contratistas – 2007' (2008/S 62-083197**),** Página web de la *Agencia de Defensa Europea*: http://www.eda.europa.eu/procurement.aspx.

[207] El Primer Ministro niega el "impuesto invisible" de carreteras, *BBC*, 21 de febrero de 2007: http://news.bbc.co.uk/1/hi/uk_politics/6381153.stm. Véase también: 'El Gran Hermano nos vigila: vuelve el seguimiento a los conductores', *Guardian*, 31 de marzo de 2009: http://www.guardian.co.uk/uk/2009/mar/31/surveillance-transport-communication-box/print.

[208] 'Number of criminals ripping off electronic tags has soared', Daily Mail, 07 April 2008: http://www.dailymail.co.uk/news/article-557781/Number-criminalsripping-electronic-tags-soared.html.

[209] Comunicado de la Comisión Europea, Plan de acción para el despliegue de sistemas de transporte inteligentes en Europa, COM (2008) 886 final, 16 de diciembre de 2008; propuesta para una Directiva del Parlamento y del Consejo Europeo que establezca un marco para el despliegue de sistemas de transporte inteligentes en el ámbito del transporte por carretera y para interfaces con otros métodos de transporte, COM (2008) 887 final, 16 de diciembre 2008: http://europa.eu/legislation_summaries/transport/intelligent_transport_navigation_by_satellite/tr0010_en.htm.

Seguridad. En 2008 el sistema se volvió a lanzar íntegramente rebautizado como Kopernikus. El GMES/Kopernikus es un "sistema de sistemas" para la "observación de la Tierra" basado en el uso común de observación por satélite nacionales. Actualmente se encuentra en modo "pre-operacional" y está desarrollando cinco servicios centrales:

- Servicios del entorno marino
- Servicios del entorno atmosférico
- Servicios del entorno terrestre
- Apoyo en catástrofes y ayuda humanitaria
- Apoyo a actividades relacionadas con la seguridad

Según la Comisión Europea, Kopernikus "mejorará notablemente la calidad de vida de nuestra generación y de la próxima". Lo hará proporcionando "información vital para los políticos y grandes empresarios que dependen de la información estratégica sobre el medio ambiente, por ejemplo, el cambio climático y la adaptación o asuntos relacionados con la seguridad". Como ya sucedía con el Galileo, la Comisión sostiene que el Kopernikus es un imperativo económico y sugiere que cualquier cosa que dificulte su desarrollo "hará que se pierda una gran oportunidad para Europa, tanto en términos de gasto de dinero como de influencia mundial en el área estratégica en cuestión".[210]

El Kopernikus utilizará sistemas de vigilancia por satélite junto con sensores terrestres y acuáticos y vehículos aéreos no tripulados. El alcance de la capacidad de vigilancia del Kopernikus hace que varíe la resolución de km a cm (dependiendo de la frecuencia con la que se tienen que actualizar los datos) y será capaz de monitorizar tanto a personas como al entorno, lo que ofrece "un claro potencial para aplicaciones comerciales en diversos sectores gracias a la posibilidad de proporcionar datos de observación de la Tierra de manera gratuita a cualquiera que pueda darles uso", incluyendo a los supervisores de la calidad del aire y el agua, los planificadores urbanísticos, los jefes de tráfico, los agrimensores y las agencias de aplicación de la ley y de seguridad. En 2007 la UE adoptó la Directiva Inspire, que estableció una infraestructura para la información espacial en la Comunidad Europea.[211]

Vigilancia por satélite e I+D de la UE

Según Iraklis Oikonomou, de la University of Sussex, "los beneficiarios inmediatos del Kopernikus son las dos mayores empresas europeas de la industria espacial: EADS y Thales Alenia Space", que han firmado contratos de cientos de millones de euros para el desarrollo los satélites Sentinel 1, 2 y 3.[212] Mientras que la Agencia Espacial Europea se sitúa a la cabeza, el programa de I+D está siendo supervisado por la dirección general de empresas e industria de la Comisión Europea (que también dirige el ESRP).

---

[210] Fuente: página web del Kopernikus, Comisión Europea: http://ec.europa.eu/gmes/overview.htm.

[211] *Directiva 2007/2/CE del Parlamento Europeo y del Consejo de 14 de marzo de 2007 por la que se establece una infraestructura de información espacial en la Comunidad Europea (Inspire)*.

[212] Oikonomou, I. (2009), 'Kopernikus/GMES and the militarisation of EU space policy', informe presentado en la conferencia: *Militarism: Political Economy, Security, Theory* en la Universidad de Sussex, el 14 y el 15 de mayo de 2009.

La UE ha concedido al menos 116 contratos en el marco del GMES/Kopernikus.[213] La gran mayoría de los proyectos del GMES financiados hasta la fecha se centran en la seguridad del entorno y utilizan sistemas de observación de la Tierra para monitorizarlo todo, desde el cambio climático hasta la degradación del suelo, pasando por la deforestación y los recursos hídricos,[214] pero el Kopernikus tiene componentes de seguridad y defensa más desarrollados.

Dos proyectos, el ASTRO+ y el GEOCREW, demostraron el uso de los sistemas de satélites europeos para dar apoyo a las operaciones de seguridad, defensa y control de crisis interiores y exteriores de la UE. La Agencia de Defensa Europea ha lanzado su propio programa sobre "sistemas multinacionales de imágenes basados en el espacio para la vigilancia, el reconocimiento y la observación" (MUSIS) con el fin de definir "un requisito de la UE en materia de obtención de imágenes desde el espacio, en colaboración con la Secretaría General del Consejo (incluyendo el personal militar de la UE)".[215]

Protección de datos

En su búsqueda por la vigilancia de todo el planeta, empieza a parecer que la UE no dejará ningún rincón por explorar. Pero, ¿qué hay de la seguridad y de la privacidad de los datos que generen el GMES/Kopernikus y el Galileo? Según un periodista que asistió al lanzamiento del Kopernikus en el Foro del GMES, que se celebró en Lille el 16 y el 17 de septiembre de 2008, "no se dieron respuestas. Parece ser otro ejemplo de tecnología que sobrepasa los códigos legales y civiles necesarios para regular su uso".[216] Si bien ha habido serios debates sobre las implicaciones en materia de privacidad de las futuras posibilidades de la vigilancia por satélite en Estados Unidos,[217] en la UE ha habidos pocos o ninguno. Si se observan las actividades financiadas por la UE en este

213 Esto incluye el BOSS4GMES, que "proporcionará las bases técnicas, financieras y contractuales para permitir la transición de la fase conceptual del GMES a un programa operativo efectivo"; el foro GIGAS, que pretende integrar la estructura del GMES/INSPIRE con la del GEOSS, el "Sistema de sistemas para la observación mundial de la Tierra", desarrollado por el "Grupo de observación de la Tierra", compuesto por 76 países; el proyecto HUMBOLDT sobre la "unificación de la información del espacio en Europa; el proyecto OASIS sobre un "sistema avanzado abierto para la gestión de crisis"; el proyecto ORCHESTRA sobre "arquitectura abierta e infraestructura de datos del espacio para el control de riesgos"; el proyecto OSIRIS sobre "arquitectura abierta para redes inteligentes e interoperables en el control de riesgos basado en sensores in-situ"; por último, el proyecto WIN sobre una estructura de la información interoperable para el medio ambiente y el control de riesgos. Existe un interesante resumen sobre los proyectos Kopernikus/GMES en: http://kokos.vsb.cz/wiki/images/6/60/Horakova.pdf.

214 Hasta la fecha, la mayoría de los proyectos del GMES tienen un propósito medioambiental o humanitario, como realizar seguimientos de las repercusiones del cambio climático o ayudar en misiones humanitarias. Entre estos proyectos se encuentran el LIMES, el RESPOND y el PREVIEW, sobre el uso de satélites con el fin de proporcionar servicios de información para la protección civil, "reducir el impacto de las catástrofes" y ayudar en labores de reconstrucción; el proyecto RISK-EOS sobre "servicios de geoinformación para ayudar en el control de inundaciones, incendios y otros riesgos"; el proyecto GEOLAND sobre seguimiento medioambiental; el proyecto FOREST sobre el cartografiado de mapas de zonas y usos del suelo; el servicio de información LAND del GSE; el servicio de información paneuropeo sobre movimientos del suelo TERRAFIRMA; el proyecto GMFS sobre el seguimiento mundial de la seguridad alimentaria; el proyecto POLAR VIEW sobre la detección remota y por satélite en el Ártico y el Antártico; el proyecto PROMOTE sobre "servicios del GMES relacionados con la capa de ozono, la exposición de rayos ultravioleta al suelo, la contaminación del aire y el cambio climático"; el proyecto MERSEA sobre el desarrollo de componentes del GMES basados en el océano; el servicio de información costera y marina MASCOAST; el proyecto MARISS sobre la vigilancia del tráfico marítimo con fines de seguridad y aplicación de la ley; el proyecto TANGO sobre "redes avanzadas de telecomunicaciones para operaciones del GMES";el proyecto del GMES sobre el "sistema de seguimiento mundial y regional utilizando satélites y datos in-situ"; y por último, los proyectos ASTRO+ y GEOCREW sobre el apoyo de la seguridad interna y externa de la UE y las operaciones para la gestión de crisis y el seguimiento de crisis desde el espacio.

215 *EDA and Commission to work closely together on research*, nota de prensa de la Agencia de Defensa Europea, 18 de mayo de 2009: http://www.eda.europa.eu/newsitem.aspx?id=471.

216 Kopernikus – ¿Para qué le sirve al ciudadano de a pie?, Hunt P., *Statewatch news online*, 8 de octubre de 2008: http://www.statewatch.org/news/2008/oct/06Kopernikus-phil-hunt.htm.

217 Gorman, S. 'Satellite-Surveillance Program to Begin Despite Privacy Concerns', *Wall Street Journal*, 1 de octubre de 2008, disponible en: http://online.wsj.com/article/SB122282336428992785.html?mod=googlenews_wsj.

ámbito, no se puede identificar ni un solo proyecto que trate la privacidad ni la protección de datos en el contexto del programa de vigilancia por satélite en expansión de la UE. Tampoco se ve una preocupación por la protección de datos o la privacidad en la Directiva INSPIRE de la UE ni en sus regulaciones de implementación.[218]

218 *Regulación de la Comisión 1205/2008/CE del 3de diciembre de 2008 para implementar la Directiva 2007/2/CE del Parlamento Europeo y el Consejo.*

19 Ojos en el cielo: vehículos aéreos no tripulados

> *El uso de vehículos aéreos no tripulados (UAV) en Europa ha emergido de forma más lenta que en Estados Unidos e Israel. Sin embargo, la experiencia en el uso de sistemas de UAV en operaciones en Iraq y Afganistán han mejorado mucho la perspectiva europea sobre su utilidad y el mercado militar está creciendo a gran velocidad...*
>
> *En cuanto se eliminen las restricciones relacionadas con su aparición, las posibilidades en el mercado comercial serán mucho más grandes que las del mercado militar. [...] En la gran cantidad de ámbitos en los que sería razonable sustituir las naves pilotadas por UAV, el mercado de las aplicaciones no militares es mucho mayor que el sector de la defensa e incluye: aplicaciones policiales, paramilitares y de seguridad; planificación agraria; satélites de órbita terrestre baja; entregas logísticas; transporte comercial de pasajeros; fotografía aérea.*
>
> Frost & Sullivan, estudio sobre UAV para la Comisión Europea[219]

Los vehículos aéreos no tripulados (UAV) han adquirido muy mala fama en Oriente Medio, Pakistán y Afganistán, donde las fuerzas de ocupación los utilizan con frecuencia para la vigilancia y para exterminar objetivos (existen dos tipos de UAV: armados y no armados).. Si bien la aplicación militar ha sido pionera en el desarrollo y el despliegue de los UAV, los fabricantes se entusiasman con su aplicación en el ámbito de la seguridad nacional y en el mercado civil. El intercambio de UAV está dominado por empresas estadounidenses e israelíes, pero los mayores contratistas europeos del sector de la defensa están listos para explotar este mercado emergente.[220]

La UE ha apoyado la investigación en el desarrollo comercial de los UAV. Hasta la fecha se han financiado al menos una docena de proyectos bajo varios programas marco de investigación de la UE. Entre estos se encuentran los proyectos mencionados anteriormente sobre el uso de UAV para la vigilancia fronteriza (BSUAV y WIMA2S); el CAPECON es un estudio de 5 millones de euros sobre la "utilización de UAV seguros y de bajo coste en el ámbito comercial civil", encabezado por la empresa propiedad del estado israelí Aircraft Industries Ltd.; el IFATS es un proyecto de 5,5 millones de euros sobre "sistemas innovadores de transporte aéreo en el futuro" que cuenta con el apoyo de Aircraft Industries Ltd., EADS y Thales; el INOUI es un proyecto de 4,3 millones de euros que sirve de "guía" para la "integración innovadora y operacional de UAV" y cuenta con el apoyo de Boeing Europe; por último, el proyecto µDRONES se centra en el desarrollo de UAV para la vigilancia de entornos urbanos y cuenta con el apoyo de Thales.

---

219 Frost & Sullivan (2007) *Study analysing the current activities in the field of UAVs*, Comisión Europea,disponible en: http://ec.europa.eu/enterprise/security/doc/uav_study_element_1.pdf.

220 Frost & Sullivan (2007) *Study analysing the current activities in the field of UAVs*, Comisión Europea,disponible en: http://ec.europa.eu/enterprise/security/doc/uav_study_element_1.pdf.

Uno de los principales obstáculos para la introducción de los UAV es que actualmente tienen prohibido sobrevolar el espacio aéreo europeo a causa del peligro bien fundado, de posibles colisiones con aviones tradicionales. La comunidad del control del tráfico aéreo se mantiene escéptica y solicita que los UAV sigan las normas unificadas que tienen que cumplir los aviones tripulados, lo que en palabras de algunos, los haría demasiado caros como para implementarlos.[221] La Comisión Europea ha hecho caso omiso y se limita a ver la situación como una oportunidad que llevará a un cambio inevitable en la legislación.

En junio de 2009 la Agencia de Defensa Europea firmó contratos para un sistema de prevención de colisiones en vuelo (MIDCAS) con la finalidad de "detectar y esquivar" los UAV, lo que se considera elemental para permitir el uso de éstos en el espacio aéreo civil. El consorcio EDA MIDCAS, apoyado por Suecia, Francia, Alemania, España e Italia, incluye a Thales y a Sagem, que son las empresas responsables de la función de "detectar". Sagem también está a cargo de los aspectos de unificación, estableciendo un vínculo con las autoridades reguladores (Eurocontrol, EASA, FAA, SGAC, etc.) y con la comunidad aérea (fabricantes de aviones, asociaciones de pilotos, etc.), "para desarrollar un estándar europeo para la función de detectar y esquivar".[222] El EDA y la Comisión Europea ya han empezado a unir sus esfuerzos en el ámbito de la I+D para crear software de radios para los UAV.[223]

Los ministerios de Interior y de Defensa de Reino Unido han desarrollado grandes planes de despliegue de UAV. El Ministerio de Interior británico pretende desarrollar una flota nacional de vehículos no tripulados para dar apoyo en operaciones policiales y de respuesta de emergencia, "probablemente mediante contratos en lugar de plena adquisición",[224] y al menos cuatro divisiones de los servicios policiales y de emergencia (Merseyside, West Midlands, Kent y Essex) han pilotado o tienen pensado utilizar UAV en sus operaciones. El Ministerio de Defensa británico cuenta con un programa de I+D sobre aviones espía equipados con "equipo de seguimiento muy sofisticado que permite realizar seguimientos secretos a sospechosos y fotografiarlos sin que lo sepan", que se puede desplegar en tres años.[225] Por su parte, BAE Systems encabeza el proyecto ASTRAEA, un consorcio público privado de 32 millones de libras (unos 36 millones de euros) "para promover y permitir el uso seguro rutinario y no restringido de UAV".[226]

Según un informe de Frost & Sullivan para la Comisión Europea, las fuerzas militares europeas han "expandido progresivamente su inventario de sistemas UAV".[227] Reino Unido, Francia, Alemania, Suecia, Irlanda, Italia, España, los Países bajos, Dinamarca, Polonia y Noruega utilizan mini UAV. Reino Unido, Francia e Italia están considerando la posibilidad de adquirir UAV de gran resistencia y media altura además de haber

---

221 'UAV en Europa: ¿Cuándo empezarán a funcionar y a volar?' Revista A*vionics*, 1 de julio de 2006: http://www.aviationtoday.com/av/categories/military/UAVs-in-Europe-When-Will-They-File-and-Fly_1009.html.

222 Thales y Sagem desempeñan un papel muy importante en el contrato de MIDCAS con la Agencia de Defensa Europea', *ASD-Network*: http://www.asd-network.com/press_detail_B.asp?ID=21012&NID=283303.

223 *La EDA y la Comisión van a trabajar conjuntamente en la investigación*, nota de prensa de la Agencia de Defensa Europea, 18 de mayo de 2009: http://www.eda.europa.eu/newsitem.aspx?id=471.

224 'El Ministerio del Interior de Reino Unido planea proporcionar una flota de UAV a la', *Flight International*, 17 de julio de 2007: http://www.flightglobal.com/articles/2007/07/17/215507/uk-homeoffice-plans-national-police-uav-fl eet.html.

225 'UAV para la policía británica', *Independent, 6 de agosto de 2008, disponible en:* http://www.independent.co.uk/news/uk/home-news/unmanned-spyplanes-to-police-britain-886083.html.

226 Véase la página web del ASTRAEA: http://www.projectastraea.co.uk/.

227 Frost & Sullivan (2007) *Study analysing the current activities in the field of UAVs*, Comisión Europea, disponible en: http://ec.europa.eu/enterprise/security/doc/uav_study_element_1.pdf.

estado “examinando el potencial de dotar de armas a los actuales modelos de UAV”. La OTAN también está desarrollando su habilidad para hacerse con la vigilancia avanzada del terreno mediante el uso de flotas de UAV para apoyar a toda una serie de requisitos de misiones como “la reconstrucción de estados, la seguridad nacional y la ayuda humanitaria” (Alemania, Italia, Polonia, Grecia, España, Eslovenia, Rumanía y Turquía han ofrecido bases europeas para el sistema AGS de la OTAN).[228] A partir de estos y otros desarrollos, en el informe de Frost & Sullivan se predice que el número de UAV militares en servicio aumentará rápidamente a corto plazo antes de estabilizarse. El crecimiento del mercado más allá de este punto depende de cómo se reciban los UAV en el sector civil.

228 AGS: El ojo de batalla de la OTAN en el cielo’, *Defence Industry Daily*, 20 de octubre de 2006: http://www.defenseindustrydaily.com/ags-natos-battlefi eld-eye-in-thesky-02727/.

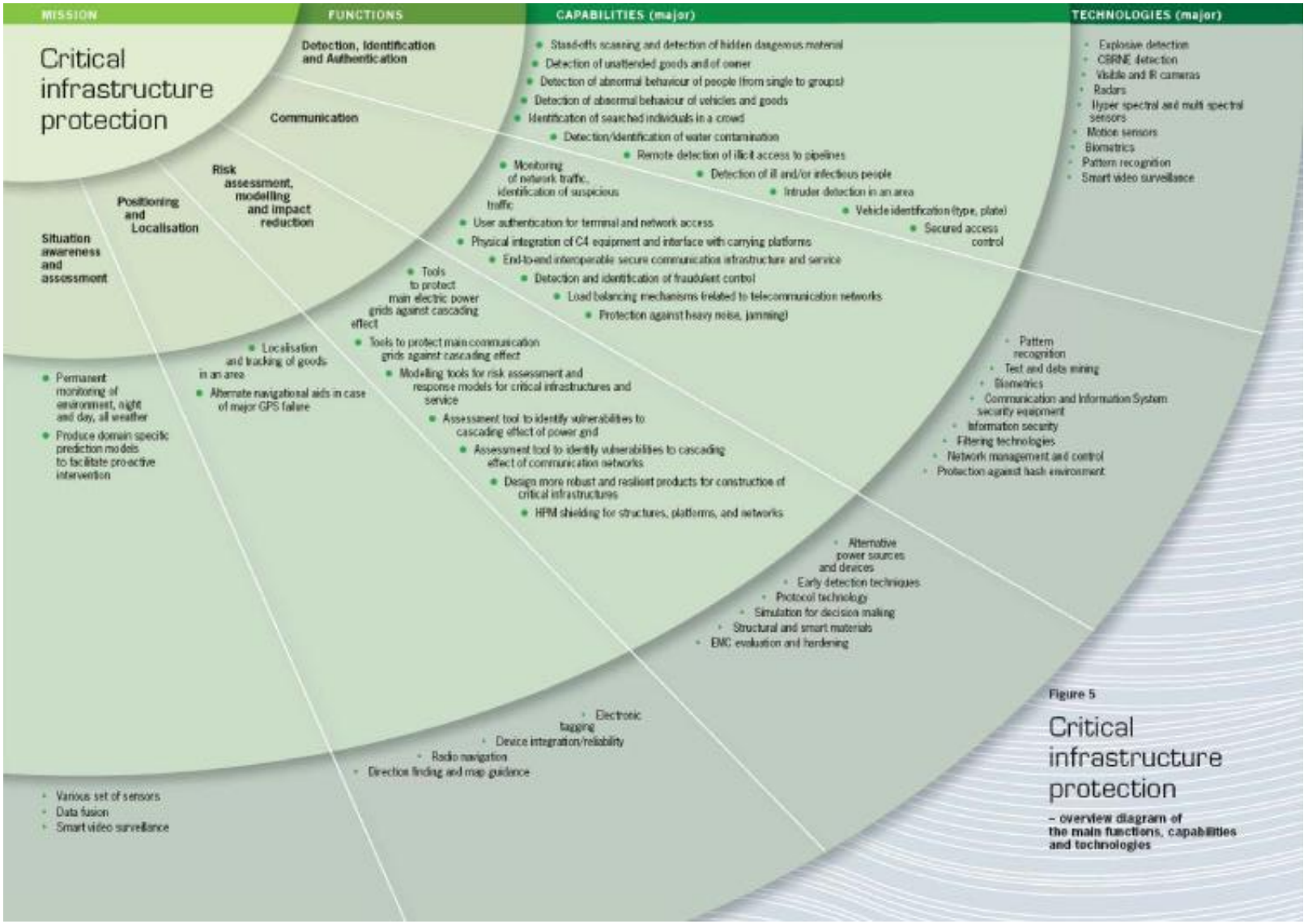


Figure 5

Critical infrastructure protection

– overview diagram of the main functions, capabilities and technologies

PARTE VI: UN MUNDO DE ZONAS VERDES Y ROJAS

> *Europa se ha convertido en un campo de batalla para todos aquellos que buscan agujeros en la red protectora que debería mantener a salvo a los ciudadanos. La mejora de los servicios de inteligencia y su colaboración ha adquirido una gran importancia en la lucha contra el terrorismo, pero los hechos acontecidos demuestran que los servicios de inteligencia por sí solos no son la respuesta cuando las amenazas a las que nos enfrentamos se planean y ejecutan de forma encubierta. Si bien los servicios de inteligencia deben formar parte de la lucha contra el terrorismo, deben apoyarse en tecnologías protectoras...*
>
> Artículo publicado por Niche Events, organizadores de la Transec World Expo 2007[229]

20 Protección de infraestructuras críticas

Los ataques terroristas de Nueva York, Madrid y Londres han hecho que se centre la atención en la protección de "infraestructuras críticas" públicas y privadas así como en el modo en que los gobiernos responden a estas situaciones y a otras emergencias. Por ejemplo, el gasto de 75 millones de euros en el aumento de la seguridad tras los atentados de Madrid, han hecho que la industria de la seguridad nacional se centre en el mercado potencial de la protección de infraestructuras críticas (PIC) y control de crisis.

La UE no ha emitido mandatos muy claros en este ámbito (las políticas domésticas y de defensa son competencias estatales), pero afirma que "a causa de las interdependencias y la naturaleza general de la economía, hoy en día, existe un cierto número de infraestructuras críticas en la Unión Europea cuya hipotética destrucción tendría un gran impacto en toda la Comunidad o en diversos Estados miembros".[230] En palabras de Tom Hardie Forsyth, presidente del grupo de protección de infraestructuras críticas de la OTAN, "sería totalmente utópico pensar que una sola nación fuera capaz proteger sus bienes sin problemas".[231]

El programa de PIC de la OTAN está basado en su experiencia en la protección de infraestructuras críticas en los Balcanes y en Afganistán. La alianza militar también ha contribuido en operaciones de CIP dentro de la UE, incluyendo el enorme despliegue de seguridad que se llevó a cabo durante los JJ.OO. de 2004 en Grecia, la Eurocopa de Portugal del mismo año, y la Copa del mundo de 2006 en Alemania. Sin acuerdos formales, el programa de PIC de la OTAN parece haberse convertido en obligatorio en las "operaciones domésticas para el mantenimiento de la paz". Las bases de la doctrina emergente de PIC son bastante similares a las del modelo explicado anteriormente: establecer centros de mando y control equipados con las últimas tecnologías de

---

229 'EUROPE: Europe fights a rearguard action combating terrorism', disponible en la página web de *Cargo Security International*: http://www.cargosecurityinternational.com/channeldetail.asp?cid=19&caid=8625.

230 Véase *The European Programme for Critical Infrastructure Protection (EPCIP)*, nota de prensa de la Comisión Europea, 12 de diciembre de 2006 (Referencia: MEMO/06/477), disponible en: http://europa.eu/rapid/pressReleasesAction.do?reference=MEMO/06/477&format=HTML&aged=0&language=EN.

231 Citado en la documentación para la conferencia: *Partnership for Peace Seminar: Critical Infrastructure Protection and Civil Emergency Planning*, 17 y 18 de noviembre de 2003, Estocolmo, disponible en: http://www.krisberedskapsmyndigheten.se/upload/6332/critical-infrastructure-protection_november-2003.pdf.

localización y conocimiento de la situación; emplear una gran diversidad de tecnologías de detección, identificación y autentificación; utilizar técnicas de evaluación de riesgos y de reducción de impacto; intervenir rápidamente para neutralizar cualquier amenaza para la seguridad.

En 2004 la UE lanzó su programa de protección de infraestructuras críticas (PIC), seguido por un programa de financiación sobre "prevención, preparación y control de las consecuencias del terrorismo y otros riesgos relacionados con la seguridad", que se enmarca en el ESRP/FP7 (2007-2013). En diciembre de 2008 la UE adoptó una directiva sobre identificación y designación de infraestructuras críticas.[232] Según el presidente de la Comisión Europea, Barrot, la directiva "aumentará el nivel de seguridad de todos los ciudadanos de la UE, proporcionará claridad legal a los operadores y aumentará la competitividad".[233] Bajo la directiva, la UE identificará y designará "infraestructuras críticas europeas" (ICE) en los sectores de la energía y el transporte para después desarrollar un "acercamiento común" a su protección. La directiva será revisada tres años después de su entrada en vigor y existe la posibilidad de extenderla al sector de las tecnologías de la información y la comunicación. Para cada ICE se desarrollarán unos planes de seguridad del operador que se encargarán de temas como "la identificación de bienes importantes, el análisis de riesgos basado en escenarios bajo amenazas mayores y la vulnerabilidad de cada emplazamiento, y por último, la identificación, la selección y la priorización de las medidas y los procedimientos de respuesta". El número total de ICE aún se desconoce pero el informe de la ESRAB predijo que "el número de sistemas empleados por estas infraestructuras será de varios miles".[234]

> *"El sistema usará todo tipo de sensores remotos y locales para advertir de incursiones. Habrá un campo de sensores y se podrá controlar a distancia desde un ordenador portátil y decir: 'Vaya, tenemos un intruso'. Está muy vinculado a los sistemas de sensores avanzados."*
> Art Schatz, exmiembro veterano de Metal Storm[235]

En 2009 la UE llegó a un acuerdo para crear un esperado paquete de medidas independientes sobre seguridad química, biológica, radiológica y nuclear para restringir el acceso a materiales potencialmente mortales. El paquete incluye 100 millones de euros de financiación para mejorar la protección de instalaciones relacionadas con el uso de estos materiales. Rebecca Harms, colíder del nuevo grupo ecologista del parlamento, se encontraba entre quienes recibieron con agrado las medidas y afirmó: "la tecnología nuclear supone una clara amenaza terrorista. Las centrales nucleares son como bombas preinstaladas porque no están a salvo de, por ejemplo, ataques aéreos".[236]

---

232 Directiva 2008/114/CE *sobre la identificación y designación de infraestructuras críticas europeas y la evaluación de la necesidad de mejorar su protección.*

233 Véase "El poder de la UE complica su seguridad", European Voice, 29 de enero de 2009: http://www.europeanvoice.com/folder/energyquarterlypipelinesandsecurityofsupply/100.aspx?artid=63804.

234 ESRAB (2006) *Meeting the challenge: the European Security Research Agenda – A report from the European Security Research Advisory Board*. Bruselas: Comisión Europea, disponible en: http://ec.europa.eu/enterprise/security/doc/esrab_report_en.pdf.

235 Wright, S. (2006) 'Informe. Sub-lethal vision: varieties of military surveillance technology', *Surveillance & Society*, 4(1/2): 136-153, disponible en: http://www.surveillance-and-society.org/Articles4(1)/sublethal.pdf (página 144).

236 'La UE dedica 100 millones de euros a la seguridad nuclear y radiológica', *euobserver.com*, 24 de junio de 2009: http://euobserver.com/885/28368.

Si bien la directiva sobre PIC aún no ha entrado en vigor, la UE ya está intentando implantar políticas que la favorezcan en las siguientes áreas: energía, tecnologías de la información y la comunicación, agua, alimentos, sanidad, sistema financiero, orden público, administración civil, transporte, industrias químicas y nucleares y por último, el sector espacial. En 2004 se estableció una agencia de seguridad de redes e información (ENISA) de la UE[237] y en 2005 la Comisión Europea creó una red de advertencias sobre infraestructuras críticas (CIWIN), reuniendo a expertos en PIC de los Estados miembros para proporcionar asesoramiento acerca de los programas para facilitar el intercambio de información de amenazas y vulnerabilidades comunes y para adoptar estrategias y medidas de respuesta apropiadas.[238] La UE ha debatido la posibilidad de establecer una red de advertencia sobre terroristas por todo su territorio (como la que ya existe en Estados Unidos o Reino Unido).

La intervención de la UE en la PIC no ha estado libre de polémica. En las semanas posteriores al intento de atentado contra los aviones transatlánticos utilizando explosivos líquidos, la Comisión Europea adoptó una regulación sobre el seguimiento del equipaje de mano de los pasajeros y sobre el hecho de llevar líquidos, que llevó a la "norma de los 100 ml" y a la confiscación de cientos de toneladas de agua embotellada y artículos de tocador en toda Europa. Desafortunadamente la Comisión Europea decidió no consultar el contenido de la regulación (que supuestamente debía proporcionar el MI5 como respuesta a la investigación policial transatlántica) con los Estados miembros ni publicar el anexo actual de la regulación, que contiene nuevas normas. Después de que algunos miembros del Parlamento Europeo y organizaciones de la sociedad civil lo reclamaran por vía legal, la Comisión Europea cedió y publicó el anexo (que ya habían filtrado Statewatch y otras organizaciones).[239] Esta especie de elaboración secreta de normas está legitimada en situaciones de "control de crisis".

Protección de infraestructuras críticas e investigación en seguridad

El grupo de trabajo 2 del SHERIFF, que se dedica a la "seguridad de infraestructuras críticas", tiene el deber de mejorar la protección de infraestructuras e instalaciones como "suministro de energía (incluyendo el suministro de agua y gas)", "seguridad alimentaria", sanidad, "infraestructuras financieras", transporte e industria química y espacial. El líder de este grupo de trabajo es Transports Security Solutions (Irlanda); el relator es el gigante de la defensa EADS.

A pesar de que la UE ha financiado la investigación civil en este ámbito (protección del suministro de agua, sistemas de información gubernamentales y consecuencias de los problemas medioambientales en la seguridad),[240] la mayoría de reflexiones que han dado lugar a las técnicas de PIC que está tratando el ESRP proceden de la práctica y la tecnología militar.

---

237 http://www.enisa.europa.eu/.

238 *Communication on a European Programme for Critical Infrastructure Protection*, Comisión Europea, COM (2006) 786 final, 12 de diciembre de 2006, disponible en: http://eur-lex.europa.eu/LexUriServ/site/en/com/2006/com2006_0786en01.pdf.

239 25 de octubre de 2007, *European Parliament v Commission of the European Communities* (Caso C-474/07).

240 Véase también el proyecto VIKING (FP7) sobre "análisis , diseño y operación de sistemas de control industriales seguros y fiables para infraestructuras críticas"; GST (FP6) sobre el uso de la "telemática" en la seguridad de los automóviles; el proyecto UAN sobre una "red acústica submarina para proteger infraestructuras críticas como plataformas y centrales energéticas marinas" (FP7).

EADS encabeza el consorcio PALMA, sobre sistemas portátiles de defensa aérea para la protección de aviones comerciales de ataques con cohetes. Actualmente el consorcio, en el que se encontraba Thales, está esperando a que se decida si se acepta su petición para formar parte del ESRP y contar con una mayor financiación. En 2008, BAE Systems firmó un contrato de 29 millones de dólares con el Departamento de Seguridad Nacional para probar su sistema de defensa de misiles por infrarrojos en aviones comerciales, bajo el programa MANPAD. Existen muy pocos indicios (si es que los hay) de que las compañías aéreas estén interesadas en la tecnología del MANPAD, o de que los terroristas armados con lanzacohetes portátiles lleguen a significar un verdadero peligro para los pasajeros de aviones europeos.

Seguridad del transporte

El programa PIC de la UE se centra en la seguridad de la energía y el transporte, pero es el último aspecto el que se ha situado en el punto de mira del programa de I+D de la UE hasta la fecha. Bajo la PASR, la UE financió proyectos de investigación relacionados con la protección de los sistemas de transporte aéreos (PATIN) y las infraestructuras del transporte (TRIPS, encabezado por Ansaldo STS, una compañía de Finmeccanica y contando con Thales, BAE Systems, Diehl, Sagem y PIAP). Bajo el programa FP6, la UE financió el programa COUNTERACT, que incluía una serie de "estudios diana" para equipar a los operadores de transporte públicos con nuevas herramientas para combatir las actividades terroristas. El consorcio destaca que "gracias a las semejanzas entre los problemas de las grandes ciudades europeas, estas soluciones de seguridad tienen un mercado potencial muy importante que comprende todo el territorio de la UE". La fase II del proyecto se centrará en la "definición y los fundamentos del transporte en masa" (es decir, recomendaciones para crear un programa de seguridad de transporte en la UE).

Soluciones de seguridad integrada para infraestructuras críticas

El IMSK es un proyecto del ESRP de 23 millones de euros encabezado por Saab en un consorcio que cuenta con TNO, Telespazio, Fraunhofer, Selex, Thales y Diehl y que ha recibido fondos del ESRP para producir un "kit de seguridad móvil integrado" que combinará tecnologías de vigilancia de áreas, puntos de control, detección de elementos químicos, biológicos, radiológicos y nucleares y apoyo para la protección VIP en un sistema móvil de rápido despliegue en eventos y emplazamientos (hoteles, eventos deportivos, festivales, etc.) que necesiten un aumento temporal de la seguridad.

El objetivo del IMSK consiste en "aumentar la seguridad de los ciudadanos en acontecimientos que reúnan a grandes números de personas, como acontecimientos deportivos (desde partidos de fútbol a JJ.OO) o cumbres políticas (G8).

La mayoría de europeos recibirá con los brazos abiertos los esfuerzos por proteger las infraestructuras críticas de ataques terroristas en los sistemas de transporte públicos. Sin embargo, algunos parecen haber establecido un vínculo entre la PIC mediante tecnología punta y el verdadero despliegue policial "sobre el terreno". Las

infraestructuras críticas pueden ser públicas o privadas e incluso estar protegidas por empresas privadas, pero es evidente que en cualquier caso su protección tiene efectos sobre el espacio público. Desde las cámaras de vigilancia a los puntos de control de seguridad, la protección de infraestructuras críticas afecta cada vez más a la manera de controlar los espacios públicos que las rodean y de acceder a ellos.

[Figura sobre la seguridad integrada en la ciudad, Siemens][241]

Los habitantes de Hackney, Londres (principal emplazamiento de los JJ.OO de 2012), están preocupados por el hecho de que el legado de los juegos no solo consistirá en la remodelación de lugares abandonados, sino también en una red de seguridad de tecnología punta que se utilizará para el control policial de la zona.[242] El presupuesto de seguridad para los juegos ya se ha ampliado de 600 a 838 millones de libras (cerca de un millón de euros) y se han criticado intensamente los procedimientos que deben seguir los trabajadores y residentes de la zona olímpica a favor de su seguridad.[243] A pesar de estas preocupaciones, parece ser que en Europa hay muy pocas personas analizando con rigor la PIC en la UE.

241 Fuente: Presentación sobre "asuntos prioritarios para las conclusiones de futuras investigaciones sobre un entendimiento común de la seguridad" de Alex Birsul (Siemens), en el taller sobre "Seguridad de los transportes en masa", disponible en: http://www.bmbf.de/pub/WS_MT_Birsul.pdf.

242 Véanse las entradas sobre seguridad en: http://www.gamesmonitor.org.uk/topic/security.

243 Los ministros planean conceder a la policía poderes dignos del "Gran Hermano", Telegraph, 4 de febrero de 2007: http://www.telegraph.co.uk/news/uknews/1541513/Ministers-plan-Big-Brother-policepowers.html.

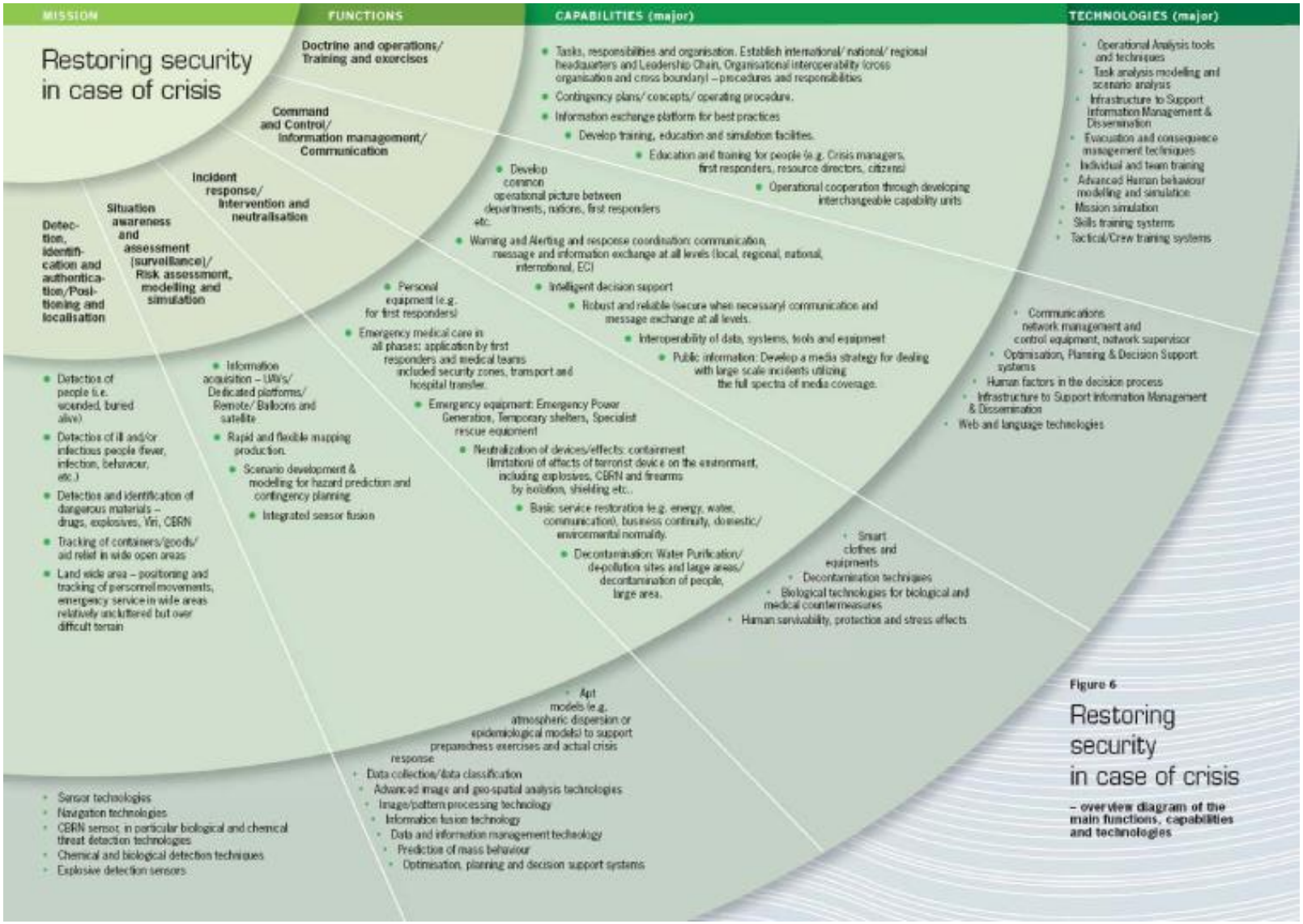


Figure 6

Restoring security in case of crisis

– overview diagram of the main functions, capabilities and technologies

21 Control policial en la zona roja: políticas de control de crisis

> *Al principio pensaba que el fenómeno de la zona verde era exclusivo de la guerra de Iraq. Ahora, tras haber pasado años en otras zonas devastadas, me he dado cuenta de que la zona verde aparece siempre allá donde va el complejo del desastre del capitalismo, con las mismas particiones entre incluidos y excluidos y entre protegidos y condenados.*
> Naomi Klein[244]

> *¿Podría un acontecimiento con un solo Estado miembro precisar una respuesta de la UE? ¿Qué umbral habría que aplicar?*
> Presidencia del Consejo de la UE, octubre de 2005[245]

Mientras que la política de PIC de la UE trata sobre "zonas verdes" (lugares que necesitan mucha seguridad y que deben protegerse de amenazas externas), la política de control de crisis de la UE se centra en el control policial de la "zona roja" (un lugar metafórico no definido por sus límites espaciales, sino por el estado de emergencia que prevalece en él). Por ejemplo, en los ámbitos del cambio climático y de las situaciones de seguridad internacional, Europa es la zona verde y África la roja. De nuevo vuelven a cobrar importancia los acercamientos militares a las crisis de seguridad, que han evolucionado como parte de la capacidad de control de crisis externas de la UE y el desarrollo de nuevos enfoques para solucionar situaciones de "crisis" en Europa.

La capacidad militar de la UE lleva desarrollándose una década y, según la Estrategia de Seguridad Europea de 2003, está basada en una "nueva cultura estratégica que fomenta la intervención temprana, rápida y, cuando sea necesario, contundente" en los "estados fallidos". Con el apoyo de las fuerzas turcas, el 1 de enero de 2007 la UE alcanzó su "objetivo principal" de tener 60.000 soldados disponibles para operaciones de reacción rápida, si bien solo seis meses más tarde Turquía abandonó el marco de defensa de la UE.[246]

Esto echó por tierra las intenciones de la UE de mantener rotaciones de 15 "grupos de batalla" de al menos 1.500 soldados, de los cuales dos grupos estarían listos para el despliegue en todo momento. Los grupos de batalla aún no han entrado en acción, exceptuando una maniobra de entrenamiento de la UE que consistía en enviar a un grupo al país ficticio de Vontinalys para supervisar "las primeras elecciones democráticas" y contrarrestar la amenaza de "la mafia local y los piratas".[247]

---

244 Klein, N. (2007) *The Shock Doctrine*. Londres: Penguin (página 414).

245 *EU Critical Infrastructure Protection (CIP)*, Documento del Consejo de la UE 13882/05, 28 de octubre de 2005: http://register.consilium.eu.int/pdf/en/05/st13/st13882.en05.pdf.

246 Turquía, que no es un estado miembro de la UE, participó de forma activa en operaciones militares de la UE entre 2003 y 2007. La negativa a institucionalizar el papel de Ankara en la toma de decisiones del EDSP mientras que se les permitía participar en la Agencia de Defensa Europea, además de sus antiguas disputas con Grecia por Chipre, precipitaron el abandono de Turquía, véase 'Turkey Turns Cold to European Defense: Implications for Western Security', Washington Institute, 2 de junio de 2008: http://www.washingtoninstitute.org/print.php?template=C05&CID=2894.

247 'In defence of Europe', Euroblog de Mark Mardell, *BBC*, 5 de junio de 2008: http://www.bbc.co.uk/blogs/thereporters/markmardell/2008/06/in_defence_of_europe.html.

A pesar de que los grupos de batalla han permanecido a la espera, desde 2003 la UE ha desplegado personal no militar (policial y civil) para el control de crisis y para el mantenimiento de la paz en más de 20 operaciones en África, los Balcanes, Oriente Medio y el Sureste asiático.[248] La UE también ha puesto en marcha dos misiones de control fronterizo en las fronteras de Moldavia con Ucrania y de Georgia con el sur del Cáucaso. Los mayores despliegues de tropas de la UE son en misiones de apoyo a la ONU en Chad (3.700 miembros), Bosnia-Herzegovina (2.900; reducidos a partir de los 7.000 iniciales) y la República Democrática del Congo (2.300). La mayor operación de control de crisis es la misión de Kosovo, a la que se han enviado 1.900 policías, jueces, fiscales y oficiales de aduana para reforzar el "cumplimiento de la ley" en el territorio recientemente independizado. En el despliegue de Kosovo (que en principio era una misión de la OTAN) se demostró que la UE está preparada para actuar sin un mandato del Consejo de Seguridad, a pesar de sus continuas promesas de actuar solo bajo el auspicio de las Naciones Unidas.

La Agencia de Defensa Europea también parece estar preparándose para poner en marcha un programa de procedimientos de control de crisis.[249] A pesar del aparentemente rápido desarrollo de la capacidad militar de la UE, todavía está muy lejos de lograr su capacidad operacional deseada de 60.000 soldados disponibles, más teniendo en cuenta los compromisos de varios Estados miembros en Afganistán.

El continuo de seguridad interna-externa

En el año 2000, la UE llamó a los estados a "cooperar voluntariamente para proporcionar 5.000 policías para misiones internacionales en los ámbitos de prevención de conflictos y de operaciones de control de crisis". En octubre de 2003, en una reunión informal de los ministros de defensa de la UE se propuso la creación de una "Fuerza de Gendarmería Europea" (FGE).[250] Francia, Italia, Países Bajos, Portugal y España firmaron una declaración de intenciones en otra reunión informal de ministros de defensa en septiembre de 2004. Los cinco estados pusieron en marcha la Fuerza de Gendarmería Europea el 19 de enero de 2005. La sede se encuentra en Vicenza, Italia, que también es donde se encuentra Camp Ederle, una base estadounidense. LA FGE está compuesta por 800 oficiales procedentes de la Gendarmeria National de Francia, la Arma dei Carabinieri de Italia, la Koninklijke Marechaussée de Holanda, la Guarda Nacional Republicana de Portugal y la Guardia Civil de España. Además, la FGE está lista para desplegarse en 30 días y cuenta con 2.300 "reservas".[251]

Según un informe del Instituto de Estudios Estratégicos e Internacionales español, la FGE puede "llevar a cabo una gran variedad de actividades relacionadas con sus deberes policiales, entre los que se encuentran: seguridad y orden público; supervisión y asesoramiento a cuerpos policiales locales; vigilancia pública, legislación de tráfico, control fronterizo e inteligencia general; investigación criminal, incluyendo la detección

248 Véase la lista de operaciones de la UE, políticas de defensa y seguridad europeas, página web del Consejo de la UE: http://www.consilium.europa.eu/showPage.aspx?id=268&lang=EN.

249 Véase la página web de la EDA: http://www.eda.europa.eu/ccm.aspx.

250 'Cinco países establecen una fuerza policial paramilitar europea'. *Statewatch news online*, septiembre de 2004: http://www.statewatch.org/news/2004/sep/06paramilitary.htm.

251 Véase la página web de la Fuerza de Gendarmería Europea: http://www.eurogendfor.org/.

de delitos, el seguimiento de los delincuentes y su presentación ante las autoridades pertinentes; protección de bienes y personas y mantenimiento del orden público en caso de disturbios; entrenamiento de policías de acuerdo con estándares nacionales; entrenamiento de instructores, principalmente mediante programas de cooperación".[252] Rumanía se unió a la FGE en diciembre de 2008 y Turquía se unió como "observador" en 2009.

En julio de 2005, una semana después de los atentados del Londres, el Consejo de la UE instigó al desarrollo de "acuerdos para compartir información, asegurar la coordinación y permitir la toma de decisiones colectiva en casos de emergencia, en concreto en casos de ataques terroristas en más de un Estado miembro". El "programa de La Haya" de la UE, sobre cooperación en justicia y asuntos internos, también llamó a establecer "un acuerdo integrado de la UE para el control de crisis".

Bajo los "Acuerdos para la coordinación de crisis y emergencias" redactados por los encargados de coordinar las acciones de contraterrorismo y adoptados sin debate previo por los Estados miembros y el Grupo de dirección de crisis, el Alto Representante de la Unión para Asuntos Exteriores y Política de Seguridad (Javier Solana), la Comisión Europea y los Estados miembros afectados se encargarán de coordinar la respuesta de la UE a las emergencias.[253] Tendrán a su disposición la "Célula civil-militar" del personal militar de la UE (EDSP), una "estructura dedicada a la coordinación de crisis" (ARGUS) que está siendo desarrollada en la Comisión y una serie de agencias de la UE entre las que se encuentran el Centro de Información y Seguimiento, el SITCEN (la agencia de inteligencia europea), el Coordinador de contraterrorismo de la UE (CFSP), la EUROPOL y otras agencias de la UE, entre las que probablemente se encontrará la FGE. Para facilitar la toma de decisiones rápida y cohesiva en tiempos de crisis, el Grupo de dirección de crisis "preparará las decisiones de emergencia para el COREPER", el cuerpo de toma de decisiones de la UE en Bruselas.

Estos "Acuerdos para la coordinación de crisis y emergencias", que el COREPER adoptó sin llevar a cabo consultas previas en el Parlamento Europeo (ni en los parlamentos nacionales), proporcionan la capacidad de tomar decisiones a los Estados miembros y a los oficiales de la UE en Bruselas en caso de crisis. La conveniencia de estos acuerdos se encuentra en la ostentación de "poderes de emergencia", pero en ausencia de un examen significativo de estas previsiones, reina la confusión. ¿Cuáles son los poderes y los deberes de la UE? ¿Dónde acaban las responsabilidades de los Estados miembros y empiezan las de la UE? ¿Qué papel desempeñarán el personal militar y las agencias de la UE en caso de crisis o emergencia? Estas preguntas deberían responderse antes de que se implementaran los acuerdos y no después.

¿Qué se aprendió del Katrina?

Tras el huracán Katrina, las preocupaciones se centraron en la manera de actuar del ejército estadounidense y de las agencias de aplicación de la ley y de respuesta de

252 'La nueva Fuerza de Gendarmería Europea', análisis de Enrique Esquivel Lalinde, 9 de mayo de 2005, *Real Instituto Elcano*: http://www.realinstitutoelcano.org/analisis/735.asp.

253 'EU emergency and crisis co-ordination arrangements', documento sin fecha ni referencia disponible: http://consilium.europa.eu/uedocs/cmsUpload/WEB15106.pdf.

emergencia, así como en las distintas formas de actuar que se llevaron a cabo en función de la raza y la clase social.[254] La respuesta del gobierno al huracán, que se pudo seguir con detalle por televisión, consternó a los espectadores de todo el mundo. Se envió al ejército a zonas "seguras" y pobres mientras la gente moría en sus casas o pasaba hambre y frío en un pabellón deportivo; el gobierno federal y la entonces recién creada Agencia de control de emergencias federal (FEMA) tardaron días en responder.

Como apuntó Naomi Klein: "una ciudad que ya estaba dividida se ha convertido en un campo de batalla entre zonas verdes separadas de zonas rojas furiosas". ¿Se trató solo de la actuación deficiente de un gobierno incompetente desbordado (los principales informativos aseguraron haber visto mejores despliegues en casos de catástrofes en el tercer mundo), o representó una profunda transformación, un nuevo tipo de control policial para una era de control militarizado de la población segregada por razas y zonas?[255]

En el ESRP, el control de crisis y la protección de infraestructuras críticas ya han tomado un giro militarista. Esto no implica necesariamente que se realicen despliegues muy militarizados en caso de una crisis doméstica, a pesar de que aumenta las posibilidades de que así sea, pero lo que cabe destacar es que pone de manifiesto la importancia de preguntarse cómo responden los estados a los desastres y a las emergencias. El tema más importante es la responsabilidad. Como se dijo desde el departamento de responsabilidad federal del gobierno estadounidense en mayo de 2006: "a pesar de un enorme despliegue de recursos y apoyo tanto de agencias militares como civiles, muchos consideran inadecuada la respuesta federal. A medida que los gobiernos locales, estatales y el federal respondieron tras el Katrina, quedó patente la confusión sobre el tipo de responsabilidades del ejército y su capacidad para planificar las actuaciones y responder a una catástrofe natural".[256]

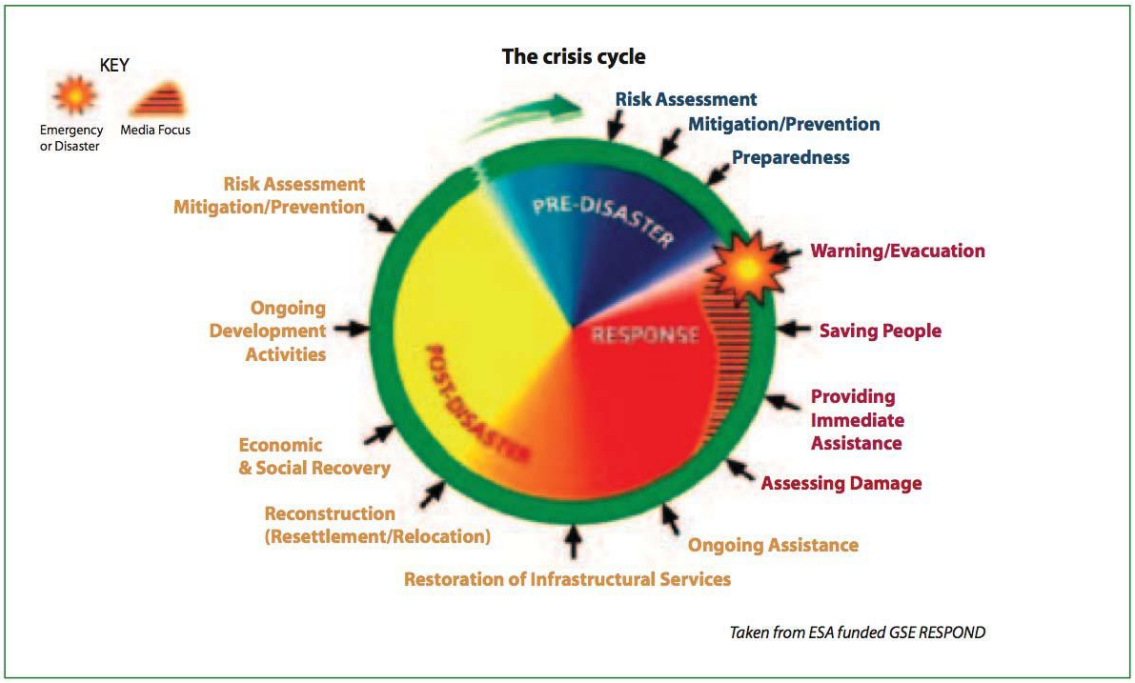
Sería interesante comparar el desarrollo del programa de capacidad de control de crisis en ciernes de la UE con los cambios en la estructura federal del gobierno de Estado Unidos al que muchos culpan por los errores cometidos tras el paso del huracán Katrina, pero, como ya se ha dicho, nadie parece estar examinando de forma crítica estás políticas de la UE.

---

254 Véase Reifer, T., "Blown Away: U.S. Militarism & Hurricane Katrina' in Hillary Potter, ed., *Racing the Storm: Racial Implications and Lessons Learned from Hurricane Katrina* Lexington Books, publicación pendiente.

255 Esta pregunta va más allá del alcance de este informe, pero los lectores de *'Shock Doctrine'* tendrán pocos problemas en relacionar la mala respuesta del estado con la emergencia de un complejo capitalista para grandes desastres. Véase Klein, N. (2007) *The Shock Doctrine*. Londres: Penguin.

256 *Hurricane Katrina: Better Plans and Exercises Needed to Guide the Military's Response to Catastrophic Natural Disasters*, Informe del Tribunal de Cuentas estadounidense a los Comités del Congreso de los Estados Unidos. Oficina del Tribunal de cuentas estadounidense, mayo de 2006 (GAO-06-643), disponible en: http://www.gao.gov/new.items/d06643.pdf.



Control de crisis e investigación en seguridad

El grupo de trabajo 4 del SHERIFF está encabezado por la Oficina del Gobierno Federal Alemán para la Protección Popular y la Ayuda en Catástrofes (BBK), con Frequentis, el autoproclamado "proveedor número uno" de soluciones centrales de control de Europa, designado como relator. Este grupo de trabajo informará sobre la preparación de Europa para responder a catástrofes de todo tipo (no solo naturales) mediante el "control de riesgos y crisis" interno y externo. Entre sus responsabilidades, se incluyen "ejercicios asistidos por ordenador para el control de crisis y emergencias", sistemas integrados de advertencia temprana, sistemas de comunicación de emergencia, cooperación civil y militar y, por último, planificación y entrenamiento de intervención civil-militar.

Como sucede en otras áreas temáticas del ESRP, algunos de los proyectos financiados hasta la fecha son meramente civiles, otros se centran en la tecnología militar y otros son una combinación de los dos anteriores. Bajo la PASR, la UE financió el proyecto MARIUS, sobre el desarrollo de "sistemas de información reactivos autónomos y móviles" para "situaciones de emergencia", encabezado por EADS; el proyecto TIARA, sobre la creación de una red europea para la reacción a incidentes radiológicos; el proyecto BIO3R, que cuenta con Sagem, TNO y FOI y trata sobre las amenazas y respuestas al uso de armas biológicas; el proyecto AEROBACTICS sobre modelos de dispersión microbiana en caso de ataque biológico; y el proyecto CRIMSON, sobre simulaciones virtuales de situaciones de crisis con fines de entrenamiento.[257]

Los últimos proyectos de tecnología de seguridad financiados bajo el ESRP se centran en dos ámbitos. El primero es la comunicación del control de crisis. En este caso, la I+D incluye el proyecto CHORIST (FP6), sobre "desastres medioambientales" y el proyecto BESECU (ESRP/FP7), que se pregunta si "la gente de distintos países actúa de formas

257 Entre los proyectos de gestión de crisis financiados en el marco de los programas marco de investigación de la UE se encuentran el OASIS (FP6), sobre investigación general de gestión de crisis, el SPADE (FP6) sobre respuestas a emergencias de transporte y el SICMA (FP7/ESRP) sobre la estimulación de las actividades de gestión de crisis.

distintas durante una crisis" y si "la cultura y la etnicidad desempeñan un papel determinante en la manera de responder a los desastres". Las conclusiones proporcionarán a la UE "seguridad para predecir como se comportará la gente durante las emergencias, sabiendo que [sus] modelos informáticos se basan en comportamientos de personas reales".[258] El segundo foco de atención del ESRP son los servicios de emergencia civiles, lo que la industria de la seguridad nacional denomina "los primeros en responder".[259]

Mientras que el programa de investigación en seguridad de la UE está por ahora limitado a sistemas de comunicaciones, EADS ha desarrollado un nuevo tipo de sistema de desinfección que ofrece unas "posibilidades notablemente mejoradas de contrarrestar epidemias y armas biológicas". El sistema TransMADDS (sistema de desinfección y descontaminación modular y transportable mediante aerosoles) de EADS ha demostrado "una efectividad hasta ahora sin igual contra los gérmenes patógenos durante dos importantes pruebas" que llevó a cabo el Ministerio de Defensa de Reino Unido. Se dice que "el sistema también se puede desplegar para neutralizar armas nucleares, biológicas y químicas.... así como emergencias civiles, como por ejemplo, desinfectar hospitales afectados por microorganismos resistentes a antibióticos. "Las epidemias representan un gran peligro para todo el mundo", comentó Bernd Wenzler, presidente de Defence Electronics (parte de EADS Defence & Security). "Este sistema de desinfección puede contribuir en gran medida a la prevención de la expansión de enfermedades infecciosas... nuestro nuevo producto es un ejemplo ideal de cómo las tecnologías modernas pueden utilizarse para aumentar nuestra seguridad en la vida diaria".[260] Parece ser que las industrias de defensa y seguridad están decididas a obtener beneficios de todos los posibles ámbitos del bienestar.

---

258 Estos son los siguientes: proyecto EULER (15 millones de euros), encabezado por Thales, cuenta con EADS, Astrium, Selex, Elsag Datamat y Telespazio y proporcionará el material en las futuras misiones de seguridad y gestión de crisis de la UE; proyecto CITRINE, sobre "Inteligencia común y trazabilidad para rescates y operaciones de identificación", también encabezado por Thales y que cuenta con EADS y Finmeccanica y proporcionará "sistemas de información en tiempo real en misiones de rescate"; SERICOM, encabezado por Qinetiq (la agencia de investigación en defensa de Reino Unido, ahora privada), que promete "comunicaciones transparentes para la gestión de crisis"; el proyecto COPE, que pretende mejorar la gestión de crisis civiles mediante nuevas tecnologías enfocadas hacia "la explotación de visiones comunes de la situación"; INFRA, encabezado por Anthena GS3 Security Implementations Ltd.(Israel), que está desarrollando redes de comunicación de banda ancha para infraestructuras críticas y nuevas aplicaciones para los equipos de primera respuesta.

259 Los proyectos del ESRP que se centran en las necesidades de los servicios de emergencias son los siguientes: proyecto CAST, que proporcionará "una valoración comparativa de procesos de entrenamiento centrados en la seguridad para los equipos de primera respuesta en la gestión de catástrofes en la UE"; proyecto FRESP, encabezado por la Real Academia Militar de Bélgica, que está desarrollando una "bombona para máscaras antigás y una capucha protectora" utilizando materiales absorbentes "nanoporosos" para proporcionar protección respiratoria a los equipos de primera respuesta en ataques químicos, biológicos, radiológicos y nucleares; proyecto NMFRDISASTER, que establecerá una red de investigadores civiles, incluyendo la Universidad Al Quds de Palestina, para examinar las "necesidades de los equipos médicos de primera respuesta en catástrofes".

260 'EADS culmina con éxito las pruebas de un nuevo sistema de desinfección para contrarrestar epidemias', ASD-Network, Julio de 2009: http://www.asd-network.com/press_detail_B.asp?ID=21699&NID=283303.

22 Control policial de las protestas: un estudio de caso de dominio de espectro total

> *Los manifestantes pagaron un alto precio por molestar a Jacques Chirac y Tony Blair mientras dormían. La policía holandesa arrestó a 143 de ellos a las afueras del hotel que se sumaron a los 300 arrestados el día anterior en una casa ocupada cercana a una comisaría de policía y a otros 150 arrestados en diversos lugares de Ámsterdam. Todos se mostraron pacíficos (aunque ruidosos), pero se les acusó de "pertenencia a una organización que pretende cometer delitos". Unos 100 fueron deportados inmediatamente sin poder rebatir su arresto en un juicio; otros fueron deportados sin sus pertenencias; impidieron al cónsul danés visitar a sus compatriotas detenidos; algunos fueron devueltos a Dinamarca en un avión militar con un bombardero holandés de escolta; se envió información sobre los detenidos a algunas agencias de inteligencia policiales. Se desconoce el número de detenidos que fueron registrados en bases de datos. Los que no fueron expulsados estuvieron retenidos tres días antes de ser puestos en libertad y algunos denunciaron malos tratos por parte de la policía así como la negación de su derecho a realizar una llamada; ninguno fue condenado pero, por entonces, el evento contra el que estaban protestando ya había concluido. Los líderes de los estados y gobiernos reunidos (tras haber descansado bien) llegaron a un acuerdo sobre el Tratado de Ámsterdam. De esta manera nació el "Área de libertad, seguridad y justicia".*
>
> Stece Peers, Ley de justicia y asuntos internos de la UE (2000)[261]

Durante la primavera de 2009, las cámaras de los teléfonos móviles fueron testigos de los métodos de control policial en Europa y los pusieron de manifiesto. En Londres, varios policías equipados con porras y escudos arremetieron contra los protestantes del el G20. Ian Tomlinson, un quiosquero londinense, murió tras sufrir una hemorragia interna al ser aplastado contra el suelo por varios policías mientras regresaba a casa del trabajo. En Moscú, la policía y un grupo de *skinheads* atacaron a los participantes de una manifestación por los derechos de los homosexuales. En Barcelona, los Mossos d'Esquadra actuaron de la misma forma contra los estudiantes en huelga de la UB y contra aficionados del FC Barcelona que causaron altercados en Las Ramblas. Las alegaciones de brutalidad policial pueden ser más o menos frecuentes dependiendo del país europeo en cuestión, pero ¿existe alguna relación entre este tipo de actuaciones policiales y las medidas que ha adoptado la UE?

El control policial del Eurotop de 1997 en Ámsterdam (descritas anteriormente por el profesor Peers) sirvió de ejemplo para la cooperación de la policía de la UE posteriormente. Bajo las leyes sobre orden público de la UE adoptadas ese mismo año, los Estados miembros están obligados a compartir información sobre todos los grupos que entran a otro Estado miembro para asistir a cualquier evento que precise actuación respecto al orden público, como "acontecimientos deportivos, conciertos de rock,

[261] Peers, S. (2000) *EU Justice and Home Affairs Law*. Londres: Longman (página 225).

manifestaciones y campañas de protesta en las que se bloqueen carreteras". La información debe ser tan detallada como sea posible y debe incluir: (a) el grupo en cuestión: composición general, naturaleza del grupo; (b) rutas que seguirá y puntos en los que se detendrá; (c) medios de transporte que utilizará; (d) cualquier otro tipo de información relevante.[262] Por asombroso que parezca, el mero hecho de asistir a un partido de fútbol o a una manifestación para acabar con la pobreza pueden implicar abrir historiales policiales.

Tras las grandes protestas contra la UE en Goteborg y contra el G8 en Génova en 2001,[263] donde la policía llegó a disparar a los protestantes, la UE estableció sus propias reglas operacionales para protestas y cumbres internacionales. El "manual sobre orden público en acontecimientos internacionales" de la UE (2001) incluía información acerca de los recursos de inteligencia, de cómo detener y entregar a los protestantes "sospechosos" a las fronteras y cómo expulsar a los protestantes de manera "eficiente" si son arrestados.[264]

Como ha expresado Tony Bunyan, director de Statewatch: desde entonces ha emergido un patrón según el cual los ciudadanos de la UE que deseen ejercer su derecho democrático a protestar (y a asistir a protestas en el extranjero) se enfrentan a controles policiales paramilitares, negación de entrada, detención preventiva, control y dispersión de las protestas e incluso ser expulsados del país, en ocasiones con prohibiciones de reentrada bastante duraderas.[265]

También ha existido un intento concertado entre los responsables de las políticas de la Unión Europea de igualar las protestas al terrorismo, ya sea tomando a los protestantes por terroristas o utilizando leyes y poderes sobre terrorismo contra los activistas y los grupos de protesta.[266]

En 2004 la UE redactó un segundo manual sobre prevención de ataques terroristas durante la celebración de los JJ.OO. y acontecimientos deportivos comparables. El modelo de seguridad adoptado era muy similar al del enfoque de las protestas (planeamiento operacional, evaluación de amenazas, análisis de riesgos, control fronterizo, medidas preventivas, investigaciones criminales y acusaciones). En 2006, los

---

262 *Acción conjunta 97/339/JHA* (OJ 1997 L 147/1).

263 'Una visión italiana del "mantenimiento del orden público"', Statewatch bulletin vol 11, no ¾: http://www.statewatch.org/news/2002/jul/08genoa.htm.

264 *Resolución del Consejo del 6 de diciembre de 2001 relacionada con un libro de recomendaciones para la cooperación policial internacional y una serie de medidas para prevenir y controlar la violencia y los altercados en partidos de fútbol con una dimensión internacional, en los que haya al menos un Estado miembro relacionado; disponible en:* http://europa.eu/cgi-bin/eur-lex/udl.pl?REQUEST=Seek-Deliver&COLLECTION=lif&SERVICE=all&LANGUAGE=en&DOCID=302G0124(01).

265 'No somos los únicos que ocultan su disconformidad', *Guardian*, 8 de mayo de 2009: http://www.guardian.co.uk/commentisfree/libertycentral/2009/may/08/civil-liberties-protest. Se supone que el derecho al "libre movimiento" es fundamental para la UE y que debería estar garantizado por el Tratado de Schengen, pero éste permite a los Estados miembro reintroducir los controles fronterizos "donde lo requieran las políticas públicas o la seguridad nacional", condición que comentó en primer lugar Bélgica cuando selló sus fronteras en enero de 2000 antes de llevar a cabo un programa de regularización de inmigrantes. Tras esto, Francia y España reintrodujeron los controles fronterizos para evitar que se desplazaran manifestantes a una convocatoria contra la UE en la cumbre de Biarritz de 2000. Esta restricción excepcional del libre movimiento y del derecho a la libertad de asociación se convirtió en la norma a medida que los estados fueron imponiendo controles para prevenir que los manifestantes acudieran a manifestaciones en al menos 15 ocasiones en los dos años posteriores.

266 En 2002 la presidencia española de la UE publicó un borrador de recomendaciones sobre el intercambio de información acerca de los manifestantes en el que se afirmaba: "El grupo de trabajo [sobre terrorismo de la UE] ha percibido en varias cumbres de la UE y otros eventos, un aumento en la violencia y los daños criminales orquestados por grupos radicales extremistas que aterrorizan a la sociedad. Estos actos son el fruto de una red extendida que se esconde detrás de varios frentes sociales, es decir, organizaciones que se aprovechan de su condición legal para ayudar a conseguir los objetivos de grupos terroristas." Documento del Consejo de la UE 5712/02, 29 de enero de 2001). Véase: '¿Intercambio de información sobre terroristas, o sobre manifestantes?' *Statewatch news online*, abril de 2003: http://www.statewatch.org/news/2003/apr/16spainterr.htm.

dos manuales de seguridad de la UE se fusionaron para formar un solo libro sobre "la seguridad (tanto desde un punto de vista público como con fines contraterroristas) de todos los acontecimientos internacionales", ya sean "políticos, deportivos, sociales, culturales o de otra índole", combinando la amenaza de las protestas, el terrorismo y los acontecimientos de masas y proponiendo una respuesta integrada y singular.[267]

Control policial público: el G8 en Alemania

Resulta interesante analizar el reciente "planeamiento operacional" para el control policial de protestas a larga escala en Europa, que empieza antes que la propia protesta o manifestación, con la vigilancia de los organizadores, incursiones en sus hogares u oficinas y requisado de ordenadores y teléfonos móviles. Otro objetivo antes y durante las protestas suelen ser las organizaciones de medios independientes y las páginas web críticas. Se fotografía, filma y registra a los protestantes de forma rutinaria, con unidades policiales y unidades paramilitares listas para entrar en acción al menor indicio de "problemas". Tras las protestas, las agencias policiales analizan, conservan y se intercambian estos datos.

En la cumbre del G8 de Heiligendam (Alemania) en junio de 2007, la policía utilizó material de vigilancia militar como satélites e intercepciones de telecomunicaciones. Un mes antes 1.000 policías habían registrado los hogares de 40 activistas. Se llevaron ordenadores personales, agendas y hasta colillas de cigarrillos para obtener "muestras de olor" (este método lo desarrolló la policía secreta de Alemania Oriental, la Stasi, para identificar a los disidentes con perros). Estas irrupciones fueron autorizadas por el artículo 129ª del código criminal alemán (la "formación de una organización terrorista") pero más tarde fueron declarados ilegales por los tribunales federales. Justo antes de que empezara la cumbre, la policía alemana confiscó el autobús de un medio de comunicación independiente. Se llevó a cabo el despliegue de 17.800 policías y 2.000 militares para la ocasión (un despliegue que también pareció violar la constitución alemana). De entre las 1.474 investigaciones preliminares que se llevaron a cabo, en la gran mayoría de casos se retiraron los cargos.

Las fuerzas aéreas alemanas contribuyeron a crear un clima de intimidación al sobrevolar con sus aviones de guerra Tornado los campamentos de activistas situados cerca del recinto en el que se celebró la cumbre. Al final, los protestantes, muchos de los cuales habían viajado cientos o miles de km para mostrar su desacuerdo, no pudieron acercarse al lugar donde se celebró el encuentro contra el que protestaban. Alrededor de esta zona levantaron una valla de 12 km con alambre de espino rodeada por una segunda zona de 10 km en la que se prohibió toda reunión de personas.

Orden público e investigación en seguridad de la UE

La UE ha financiado proyectos consecutivos para "coordinar los programas de investigación y las políticas nacionales sobre seguridad en grandes acontecimientos" (el EU-SEC y el EU-SECII) durante los últimos cinco años. Al igual que las políticas de la

267 *Security handbook for the use of police authorities and services at international events*, document del Consejo de la UE 15226/1/06 REV 1, 22 de diciembre de 2006, disponible en: http://www.statewatch.org/news/2007/jan/eu-sec-handbook-int-events.pdf.

UE sobre el control policial de las protestas, estos proyectos están dirigidos a la "armonización" y a la "mejor práctica". El proyecto EU-SEC, financiado bajo el programa FP6, estaba coordinado por el Instituto de investigación interregional sobre crimen y justicia de las Naciones Unidas (UNICRI, que se autodefine como un laboratorio de "gobernanza de seguridad y contraterrorismo) e incluía a la policía y ministros de diez Estados miembro de la UE y a la EUROPOL. Su objetivo era definir unas necesidades de investigación "armonizadas" en la UE para producir "un mapa de investigación estratégica para orientar la agenda de investigación europea y la asignación de fondos".[268]

El EU-SEC fue en gran medida un "proyecto de investigación" operacional. Contribuyó a establecer un "observatorio internacional permanente sobre seguridad en grandes acontecimientos" (IPO) en el UNICRI y un "modelo de planeamiento de seguridad", una herramienta para que las autoridades nacionales puedan planear la seguridad en grandes acontecimientos.[269] El EU-SEC también proporcionó el estudio de caso sobre "asociaciones público-privadas de investigación en seguridad en grandes acontecimientos".[270] El UNICRI, en colaboración con "investigación innovadora de inteligencia y cooperación en la UE para combatir el terrorismo", también publicó un manual para los países del G8 sobre cómo actuar en caso de protestas. Al finalizar el proyecto de tres años, el consorcio del EU-SEC lanzó una petición de propuestas sobre "herramientas electrónicas" para cómo compartir de información entre planificadores de seguridad en la UE y un registro de grandes acontecimientos europeos (EMER).[271] Estas iniciativas "también proporcionarán beneficios para el mercado europeo de la tecnología de seguridad".

El EU-SECII está financiado bajo el ESRP/FP7 y también está coordinado por el UNICRI. El proyecto se amplía geográficamente para incluir a las fuerzas policiales y ministros de interior de 20 Estados miembros, además de la EUROPOL. Los proyectos continuarán con la "armonización de las políticas de investigación nacionales" y establecerán las "necesidades y prioridades entre sus compañeros, que constituyen el lado de la demanda del mercado europeo de la tecnología.[272]

Mientras tanto, al otro lado del Atlántico...

La Dirección conjunta del Pentágono sobre armas no letales ha dado con su propia solución en "métodos no letales de dispersión de multitudes, seguridad en puntos de control, seguridad perimetral, negación de áreas, protección de puertos, protección de infraestructuras y clarificación de intención (identificar combatientes y no combatientes)".[273] El sistema Joint Silent Guardian es un arma no letal de energía

[268] Véase 'Manual EU-SEC (2007), disponible en: http://www.unicri.it/news/0807-1_EU-SEC_II/eusec_080707_manual.pdf.

[269] *Programa IPO*, página web del UNICRI: http://www.unicri-ipo.org/.

[270] 'Asociaciones público-privadas de investigación en seguridad en grandes acontecimientos. Un estudio de caso', disponible en: http://www.unicri.it/news/0807-1_EU-SEC_II/eusec_080707_ppp_cs.pdf.

[271] 'Registro de grandes acontecimientos europeos (EMER) & Grupo de especialistas en equipo (STEP). Propuesta de esquema de bases de datos', disponible en: http://www.unicri.it/news/0807-1_EU-SEC_II/eusec_080707_emer_step.pdf.

[272] *EU SEC II*, página web del UNICRI: http://lab.unicri.it/eusecII.html.

[273] *Preguntas más frecuentes relacionadas con el sistema "Active Denial", página web de la Dirección General de armas no letales del Pentágono:* https://www.jnlwp.com/misc/faq/ADS%20FAQs%20September%202008.pdf.

dirigida desarrollada por Raytheon.[274] Con un alcance de más de 250 metros, el Silent Guardian se ha instalado en vehículos militares con fines de control de multitudes. Según Global Research, este aparato de microondas de gran potencia (HPM) calienta agua en la superficie de la piel de su objetivo hasta que produce dolor. En las pruebas se ha demostrado que las microondas pueden traspasar muros de cemento y ventanas de coches.[275]

Desde Raytheon describen el sistema Silent Guardian como "una aplicación revolucionaria de energía no letal que emplea tecnología de ondas milimétricas para repeler a individuos o multitudes sin ocasionar lesiones" y promueve el arma como un "sistema de protección" que puede "reducir la cantidad de agresiones durante misiones para el cumplimiento de la ley, la seguridad de los puntos de control y el mantenimiento de la paz". El Silent Guardian se controla mediante un "joystick de fácil manejo que realiza seguimientos automáticos" que permiten "apuntar con precisión a individuos concretos". El Instituto nacional de justicia de Estados Unidos también está promoviendo el uso de la llamada tecnología de "sistemas de negación activa" para su uso en instalaciones correccionales como las prisiones.[276]

Otros no se muestran tan entusiasmados con estas nuevas tecnologías. Según un informe publicado en 2008 por la Deutsche Stiftung Friedensforschung (DSF, la Fundación alemana para la investigación sobre la paz), el arma podría causar heridas serias e incluso mortales.[277] Esta tecnología ya se ha probado en cientos de voluntarios. Con el fin de producir dolor e impedir causar quemaduras, el poder y la duración de las microondas emitidas están controladas por un programa informático. La DSF calcula que a la máxima potencia, el arma puede ocasionar quemaduras de segundo y tercer grado con necrosis dérmica (muerte de las células de la piel) tras una exposición de menos de dos segundos. Es más, incluso al utilizarla con la mínima potencia y duración, existe la posibilidad de volver a dispararla de inmediato. Según un informe de accidentes publicado por Wired, al menos un voluntario ha precisado tratamiento en la unidad de quemados de un hospital.[278] Steve Wright ha comentado: "si se llega a permitir que se despliegue este sistema en un formato algorítmico en forma de rayo de dolor que apunta automáticamente, estaremos entrando en una nueva era de violaciones en masa de los derechos humanos."[279]

En el borrador de la ESRAB al que tuvo acceso el autor de este informe se mencionaban las "armas menos letales", pero no se hizo referencia a ellas en la versión final.[280] Sin embargo, muchos de los "actores principales" del lado de la oferta del ESRP también son parte del grupo de trabajo europeo sobre armas no letales, que "apoya el desarrollo

---

274 *Silent Guardian™ Protection System: Less-than-Lethal Directed Energy Protection*, página web de Raytheon: http://www.raytheon.com/capabilities/rtnwcm/groups/rms/documents/content/rtn_rms_ps_silent_guardian_ds.pdf.

275 El cambio en las protestas sociales en América: armas "no letales" de microondas para el "control de multitudes". Justo a tiempo para la debacle del capitalismo: Ejército, Departamento de Justicia para poner a prueba el "rayo del dolor, *Global Research*, 14 de octubre de 2008 http://www.globalresearch.ca/index.php?context=va&aid=10564.

276 *El sistema de negación active disuade a los objetivos sin causarles daños*, Instituto Nacional de Justicia de Estados Unidos, página web del Departamento de Justicia de Estados Unidos: http://www.ojp.usdoj.gov/nij/topics/technology/less-lethal/denial-system.htm

277 Altmann, J. (2008) Millimetre Waves, Lasers, Acoustics for Non-Lethal Weapons? Physics Analyses and Inferences, Deutsche Stiftung Friedensforschung, disponible en: http://www.bundesstiftung-friedensforschung.de/pdf-docs/berichtaltmann2.pdf.

278 Sujeto de prueba del "rayo del dolor" expuesto a "dolor desmedido, *Wired.com*, 14 de octubre de 2008: http://blog.wired.com/defense/2008/10/pain-ray-accide.html.

279 Wright, S. (2006) 'Report. Sub-lethal vision: varieties of military surveillance technology', *Surveillance & Society*, 4(1/2): 136-153, disponible en: http://www.surveillance-and-society.org/Articles4(1)/sublethal.pdf (página 147).

280 "Versión final" no publicada del informe de la ESRAB, v.2.7, septiembre de 2006 (página 52).

y el uso de tecnologías, aparatos y tácticas que buscan preservar la vida a la vez que permitir el uso apropiado y constitucional de la fuerza como respuesta a amenazas, ya sean individuales o multitudinarias".

En 2006, el Comando (militar) Europeo de Estados Unidos exhibió su programa de armas no letales durante una cumbre y una demostración de capacidades en una base alemana.[281] Desde entonces, la Agencia de Defensa de la UE ha establecido un equipo para el proyecto de capacidades no letales y ha ofrecido un contrato a Thales Electron Devises para llevar a cabo un ejercicio de "cartografiado" del "desarrollo de capacidades de energía dirigida y su potencial de crecimiento centrado en el EDA".[282]

Actualmente no hay acuerdos internacionales sobre la restricción del desarrollo y la proliferación de tecnología armamentística basada en microondas, exceptuando un protocolo adicional a la convención sobre ciertas armas convencionales que prohíbe las armas láser diseñadas para cegar intencionalmente. Según un informe de la Universidad de Bradford, las instalaciones militares se resisten a acatar nuevas restricciones en el desarrollo y el uso de "armas no letales". La propia OTAN ha afirmado que "con el fin de asegurar que las fuerzas de la OTAN sigan teniendo la capacidad de cumplir misiones, será importante que las naciones que participen en sus operaciones vigilen el desarrollo de determinados regímenes legales que limitan de manera innecesaria la capacidad de utilizar armas no letales".[283]

281 *U.S. European Command Highlights Non-Lethal Alternatives*, página web del Departamenteo de Defensa de Estados Unidos: véase http://www.defenselink.mil/transformation/articles/2006-06/ta062206b.html. "Hemos llevado a cabo pequeñas demostraciones anteriormente, pero esta es la primera vez que hemos puesto a prueba de forma exhaustiva armas no letales para nuestros aliados europeos y africanos. Es una demostración importante de nuestra interoperabilidad y nuestra cooperación", dijo un portavoz.

282 Véase el contrato 18, 'Lista anual de contratistas – 2007' (2008/S 62-083197), página web de la Agencia de Defensa Europea: http://www.eda.europa.eu/procurement.aspx.

283 Davison, N (2007) *The Contemporary Development of 'Non-Lethal' Weapons*, Bradford University Non-Lethal Weapons Research Project (página 37), disponible en: http://www.bradford.ac.uk/acad/nlw/research_reports/docs/BNLWRPResearchReportNo8_Mar06.pdf.

PARTE VII: GOBERNANZA DE ESPECTRO TOTAL

> *Cuando la gente empezó a preocuparse por los ataques asimétricos y el armamento bélico químico, lo que sucedió fue que la tecnología militar se puso en manos de la policía.*
> Bill Mawer, Director de estrategia y tecnología, Smiths Detection[284]

23 Interoperabilidad

La "interoperabilidad" podría situarse entre una creciente colección de "palabras engañosas" que Deirdre Curtin y otros han identificado en una disertación acerca de la UE.[285] Lo mismo sucede con palabras como "gobernanza" y "legitimidad", que tienen significado para los estudiantes que se centran en la UE y para los oficiales de la UE, pero no dicen gran cosa a los demás. El diccionario de inglés Oxford describe el concepto de interoperabilidad como "(de sistemas informáticos o software) capacidad de intercambiar y utilizar información". La Wikipedia ofrece una interpretación más rica: "propiedad que hace referencia a la habilidad de trabajar juntos (interoperar) de diversos sistemas y organizaciones", añadiendo que "el término se suele utilizar en el ámbito de la ingeniería técnica de sistemas o, de forma más amplia, teniendo en cuenta factores sociales, políticos y de organización que influyen en el rendimiento entre sistemas. En un contexto gubernamental europeo, la interoperabilidad se suele referir a "la capacidad de colaboración de los servicios interfronterizos para los ciudadanos, empresas y administraciones públicas".[286]

La UE aplicó por primera vez el "principio de interoperabilidad" al "sistema de ferrocarril de alta velocidad transeuropeo" en la década de los 90 para armonizar las infraestructuras y facilitar los servicios de tren entre fronteras.[287] Desde entonces se ha convertido en un principio muy utilizado y elemental en la integración europea. También puede verse como un proceso importante de globalización. En el "primer pilar" (mercado internacional y política social), la UE ha dedicado un programa a la "interoperabilidad de servicios gubernamentales electrónicos europeos a las administraciones públicas, empresas y ciudadanos" (IDABC). La IDABC emite recomendaciones, desarrolla soluciones y proporciona servicios que permiten a las administraciones nacionales y europeas comunicarse electrónicamente y financia proyectos sobre requisitos de política europea.

La tendencia a la interoperabilidad en los ámbitos de justicia y política interior en Europa empezó a darse en 2002, con la formación del "grupo de información de sistemas del tercer pilar" para explorar las posibles "sinergias" entre los sistemas de el SIS II, la EUROPOL, el CIS y el EURODAC. El grupo sugirió dos posibles opciones: (a) fusionar los sistemas existentes en un único "sistema de información unido" (que pareció ser tanto ilegal como técnicamente imposible); (b) armonizar los "formatos de

---

[284] Citado en 'el dosier sobre infraestructuras críticas, *euractiv.com*: http://www.euractiv.com/en/security/critical-infrastructure/article-140597.

[285] Cutrin D. (2006) 'European Legal Integration: Paradise Lost?' in Curtin et al (eds) *European Integration and Law* (páginas 1-54). Amsterdam: Intersentia.

[286] Interoperabilidad, *Wikipedia*: http://en.wikipedia.org/wiki/Interoperability.

[287] *Directiva 96/48/CE del Consejo de 23 de julio de 1996 relativa a la interoperabilidad del sistema ferroviario transeuropeo de alta velocidad* (OJ 1996 L 235/6).

datos y sus respectivas reglas de acceso... mientras se permite que los sistemas actuales evolucionen para lograr la interoperabilidad".[288]

El plan de contraterrorismo adoptado por la UE tras el 11-M supuso un llamamiento a la Comisión Europea para "emitir propuestas para aumentar la interoperabilidad" y "explorar la creación de sinergias entre los sistemas de información actuales y los futuros". En el comunicado que publicó la Comisión a continuación se describía la interoperabilidad como la "habilidad de los sistemas de la tecnología de la información (y de los procesos empresariales a los que apoyan) de intercambiar datos y permitir compartir información y conocimiento".[289] También la describió como un "concepto más técnico que político"; un principio que está "desconectado de la cuestión de si el intercambio de datos es posible o indispensable de manera legal o política".

De la misma manera, la Comisión Europea introdujo el "principio de disponibilidad", bajo el cual los datos en posesión de agencias de aplicación de la ley de un Estado miembro deberían, en principio, ponerse a disposición de todos los demás (una especie de "mercado libre" de datos policiales), con lo que se establecería el marco político y legal deseado por la UE. El Tratado de Prüm de 2005, mencionado anteriormente, (que fue diseñado por siete Estados miembros y posteriormente extendido por la UE) buscaba implementar el principio de disponibilidad mediante la creación de nuevos sistemas de comparación de datos automatizados que interrelacionarían las bases de datos de ADN y de huellas dactilares de los Estados miembros.

Este tipo de interoperabilidad tiene mucho que ver con la armonización del acceso a datos, que se ve con mejores ojos que la creación de nuevas y extensas bases de datos. Por supuesto, en la práctica la centralización del acceso lleva a los mismos conceptos: la ruptura de los cortafuegos que existen entre los datos de que dispone el gobierno, la creación de sistemas de vigilancia multifunción y la erosión de las leyes y principios de protección de datos que actualmente funcionan como barreras para el acceso policial y el intercambio de datos. El principio de "causa probable", la idea de que la gente solo debería estar sujeta a medios de aplicación de la ley en caso de ser sospechosos de cometer algún crimen, también queda socavado por los principios de interoperabilidad y disponibilidad.

En junio de 2009 la Comisión Europea propuso la creación de una agencia de la UE responsable de la dirección operacional de sistemas de tecnología de la información a gran escala, esgrimiendo que la situación actual "no permite la plena explotación de las sinergias que existen entre estos sistemas y ocasiona grandes costes, menos eficiencia y solapamientos".[290] Esta "agencia específica también será capaz de conseguir

---

288 *Informe del grupo para el estudio de los sistemas de información del tercer pilar*, Consejo de la UE 8857/03, 6 de mayo de 2003, disponible en: http://www.statewatch.org/news/2008/aug/eu-databases-8857-03.pdf.

289 *Comunicado de la Comisión sobre la mejora en la efectividad,la interoperabilidad y las sinergias entre las bases de datos europeas en el ámbito de la justicia y los asuntos internos*, COM (2005) 597 final, 24 de noviembre de 2005: http://www.eurowarrant.net/documents/cms_eaw_id1623_1_52005DC0597.pdf.

290 *Paquete legislativo que establece una agencia para la gestión operativa de sistemas de tecnología de la información a gran escala en el ámbito de la libertad, la seguridad y la justicia, Comisión Europea*, COM(2009) 292 final, 24 de junio de 2009: http://www.statewatch.org/news/2009/jun/eu-com-it-agency-proposal-292-09.pdf; Propuesta para establecer una agencia para la gestión operativa de sistemas de tecnología de la información a gran escala en el ámbito de la libertad, la seguridad y la justicia, Comisión Europea, COM(2009) 293 final, 24 de junio de 2009: http://www.statewatch.org/news/2009/jun/eu-com-it-agency-prop-regulation-293-09.pdf; Propuesta para otorgar a la agencia mencionada las tareas relacionadas con la gestión operativa del SIS II y el VIS en aplicación del Título VI del Tratado de la UE, Comisión Europea, COM(2009) 294 final, 24 de junio de 2009: http://www.statewatch.org/news/2009/jun/eu-com-it-agency-prop-op-decision-294-09.pdf http://www.statewatch.org/news/2009/jun/eu-com-it-agency-prop-regulation-293-09.pdf.

importantes sinergias y economías de escala" y contará con la ayuda de grupos de asesoramiento compuestos por expertos nacionales y deberá asumir la dirección operacional del SIS II, el VIS y el EURODAC en 2012. Tal y como sugería el registro, "haga lo que haga el sistema para que los ciudadanos de la UE estén más seguros, el resultado beneficiará a distintos elementos. Algunos gobiernos estarán encantados con la posibilidad de realizar seguimientos de personas dentro de la comunidad. Los vendedores relacionados con la tecnología de la información se beneficiarán de los enormes sistemas paneuropeos y sus respectivos presupuestos. Por su parte, los piratas informáticos podrían disponer de toda la información de identificación de Europa reunida en un solo punto".[291]

Desde los datos interoperables a los servicios de seguridad integrados

En el contexto de la seguridad, la "interoperabilidad" también implica una mayor cooperación entre las agencias de policía, inmigración, inteligencia, militares y gubernamentales, así como con las organizaciones de seguridad del sector privado. Ahora la UE ha dado con un nuevo principio, la "convergencia", que consiste en "compartir soberanía" apuntalado por la unificación legal y la disposición de planes de entrenamiento estándar, equipo y tecnología de la información en todas las agencias de aplicación de la ley de Europa. En lugar de la clásica "separación de poderes" y agencias, la interoperabilidad y la convergencia implican un nuevo sistema de redes de aplicación de la ley en el que los órganos ejecutivos desempeñarán un papel crucial y donde dejarán de aplicarse los sistemas tradicionales de pesos y contrapesos.

El grupo de trabajo 1 es el que tiene la tarea más amplia del ESRIF: "Seguridad de los ciudadanos" [sic]. Este concepto incluye tecnologías mejoradas en las siguientes áreas: "terrorismo y crimen organizado, protección de objetivos vulnerables (grandes acontecimientos y multitudes), seguridad urbana, protección civil, seguridad sanitaria pública (pandemias), crimen cibernético, investigaciones por Internet, modelos de intercambio de información público-privados, amenazas económicas (manipulación de divisas o del valor de las acciones) [y] no proliferación de armas cortas y armas ligeras".

El relator, responsable de publicar los hallazgos del grupo de trabajo 1, es Sagem Défense Sécurité, una compañía cuya misión global consiste en proporcionar "una interfertilización entre soluciones que aparentemente pertenecen a dos mundos distintos: multibiométrica (tecnología de huellas dactilares) para hacer más seguro el transporte, optoelectrónica (generalmente con fines militares) aplicada a la seguridad nacional, navegación inercial aplicada a vehículos aéreos no tripulados, etc".[292]

Mientras tanto, el grupo de trabajo 10 del ESRIF, se encarga de la "gobernanza y la coordinación" de "la estrategia de investigación en seguridad y la implementación entre la UE y sus Estados miembros y las instituciones y organizaciones pertinentes, como la Agencia Espacial Europea, y la OTAN". Su relator es el Royal Services Institute de Reino Unido.

---

[291] 'La UE planea crear una red de tecnologías de la información enorme por la "libertad, la seguridad y la justicia, *The Register*, 25 de junio de 2009: http://www.theregister.co.uk/2009/06/25/eu_it_system/.

[292] Véase la página web de SAGEM: http://www.sagem-ds.com/eng/site.php?spage=02000000.

24 Expansión del concepto de seguridad nacional

> *Percibo un cambio en el énfasis y un creciente equilibrio entre lo que vemos como defensa y seguridad nacional.*
>
> *La "seguridad" es una manera más aceptada a nivel político de describir lo que antes se denominaba defensa.*
> Tim Robinson, Vicepresidente de la división de seguridad de Thales y antiguo presidente de la ESRAB.[293]

La trayectoria del ESRP y los principios de "interoperabilidad" y "convergencia" están cada vez más integrados en nuevos planteamientos relacionados con la seguridad a nivel nacional, especialmente entre los Estados miembros más poderosos de la UE. A pesar de las divisiones respecto a la guerra de Iraq y las tensiones sobre la futura relación entre la UE y la OTAN, las similitudes de las estrategias de seguridad y defensa de Francia, Reino Unido y Alemania constituyen la base para el tipo de integración europea que se describe en este informe. A través de la UE, su visión de seguridad global en el siglo 21 se está imponiendo de manera uniforme por toda Europa.

Después del 11-S, el Ministerio de Defensa de Reino Unido revisó su capacidad de responder a los retos que suponía el terrorismo internacional abriendo un "nuevo capítulo" en la *Strategic Defence Review* de 1998. El libro blanco *Defence* de Reino Unido de 2003, que trataba sobre "proporcionar seguridad en un mundo cambiante", se inclinaba por una reestructuración radical de la defensa tradicional para "afrontar los nuevos retos y amenazas del terrorismo internacional, la proliferación de armas de destrucción masiva y los estados débiles y fracasados".[294] La estrategia de seguridad de la UE de 2003 llamó al desarrollo de sus capacidades militares y no militares para conseguir los mismos propósitos.[295] El libro blanco de Reino Unido también reconoció "la valiosa contribución que podría aportar *Defence* a la defensa y la seguridad nacionales".

En 2006 Alemania publicó un libro blanco sobre políticas de seguridad para cumplir los objetivos paralelos de la seguridad nacional ("la soberanía e integridad del territorio alemán") y una política exterior proactiva que "confronta retos globales sobre todas las amenazas que suponen el terrorismo internacional y la proliferación de armas de destrucción masiva".[296] Estos objetivos pertenecen a una política de globalización económica ("mercado mundial libre y abierto como base de la prosperidad"). La publicación alemana concluye afirmando que "la seguridad no se puede garantizar con los esfuerzos de una sola nación o por fuerzas armadas exclusivamente, sino que requiere un acercamiento que lo abarque todo y que solo se puede desarrollar mediante estructuras de redes de seguridad y en el contexto de una filosofía de seguridad global y nacional exhaustiva".

---

293 Fuente: página web de *Euractiv*: http://www.euractiv.com/en/security/critical-infrastructure/article-140597.

294 *Delivering Security in a Changing World: Defence White Paper 2003*, Secretary of State for Defence, diciembre de 2003 (Cm 6041-I), disponible en: http://www.mod.uk/NR/rdonlyres/051AF365-0A97-4550-99C0-4D87D7C95DED/0/cm6041I_whitepaper2003.pdf.

295 *A secure Europe in a better world: European Security Strategy*, documento del Consejo de la UE 15895/03, 8 de diciembre de 2003; disponible en: http://www.iss-eu.org/solana/solanae.pdf.

296 *Libro blanco de 2006 sobre políticas de seguridad alemanas y el future Bundeswehr*, Ministerio Feredal de Defensa, disponible en: http://www.realinstitutoelcano.org/materiales/docs/LibroBlanco2006_english.pdf.

La primera estrategia de seguridad nacional de Reino Unido, publicada en marzo de 2008 y subtitulada "la seguridad en un mundo interdependiente", planteaba el mismo enfoque.[297] Además de los "riesgos y amenazas" del terrorismo, la proliferación nuclear, las armas de destrucción masiva, la inestabilidad global, y los estados en conflicto, "fracasados" y "frágiles", esta estrategia trata "el crimen transnacional, las pandemias y las inundaciones (que no son parte de la idea tradicional de seguridad nacional, pero son retos que pueden afectar a un gran número de personas y que requieren respuestas similares a las de otras amenazas más tradicionales como el terrorismo".

"Dentro del gobierno", Reino Unido promete "un acercamiento más integrado. La distinción entre política interior y exterior no ayuda en un mundo en el que la globalización puede exacerbar los retos de seguridad domésticos, pero también dar nuevas oportunidades para hacerles frente". Reino Unido también promete afrontar "los multiplicadores de riesgo" como el cambio climático, la competición por los recursos energéticos así como la pobreza, las desigualdades y los gobiernos deficientes. El libro blanco de Javier Solana, trata sobre "El cambio climático y la seguridad internacional" y se publicó una semana antes que la estrategia de seguridad nacional de Reino Unido. En él, se utiliza el mismo lenguaje para ejercer presión y conseguir políticas de la UE que se encarguen de "las amenazas a la seguridad internacional creadas por el cambio climático".[298] La publicación de Solana sugiere que "el cambio climático es un multiplicador de riesgos que exacerba las tendencias, tensiones e inestabilidades existentes", como "los estados y las regiones frágiles y propensas a sufrir conflictos", "las disputas fronterizas", "la inmigración inducida por cuestiones ambientales", "los conflictos por los recursos" y " las situaciones de fragilidad y radicalización".

Resulta chocante lo poco que han tardado en dominar la elaboración de políticas occidental estas definiciones de seguridad nacional que abarcan "todos los riesgos" y la escasa oposición que hay frente a la "segurización nacional" de cuestiones de política social sobre sanidad y seguridad. En Alemania en 2008 un grupo de miembros del Parlamento Europeo procedentes de diversos partidos publicó un "libro verde" sobre "riesgos y retos para Alemania", hablando de una "nueva concepción de seguridad pública transnacional que abarca el terrorismo, el crimen organizado, la tecnología de la información, las enfermedades infecciosas y la seguridad de los servicios básicos".[299] El objetivo de esta nueva definición consiste en permitir "procesos complejos y sistemas (de seguridad) a nivel local, nacional y transnacional, que funcionen de la mejor manera posible". Según lo esgrimido en el libreo verde, "cuantos más recursos puedan movilizar la sociedad y el estado, más fuertes serán en tiempos de crisis". De manera similar, en 2009 una Comisión de seguridad nacional de varios *stakeholders* creada por el Instituto de investigación de políticas públicas de Reino Unido concluyó una investigación de dos años con la publicación de un informe titulado "Responsabilidades

297 *The National Security Strategy of the United Kingdom Security in an interdependent world*, Oficina del Gabinete, 2008, disponible en: http://interactive.cabinetoffice.gov.uk/documents/security/national_security_strategy.pdf.

298 *Climate Change and International Security: Paper from the High Representative and the European Commission to the European Council*, documento del Consejo de la UE S113/08, 14 de marzo de 2008, disponible en: http://www.consilium.europa.eu/ueDocs/cms_Data/docs/pressData/en/reports/99387.pdf.

299 *Risks and Challenges for Germany: Scenarios and Key Questions*, Green paper of the Forum on the Future of Public Safety and Security, editado por Gerold Reichenbach (SPD), Ralf Göbel (CDU/CSU), Hartfrid Wolff (FDP) y Silke Stokar von Neuforn (Alliance 90/Greens). Versión en inglés publicada el 8 de octubre de 2008, disponible en: http://www.zukunftsforum-oeffentliche-sicherheit.de/download/27/.

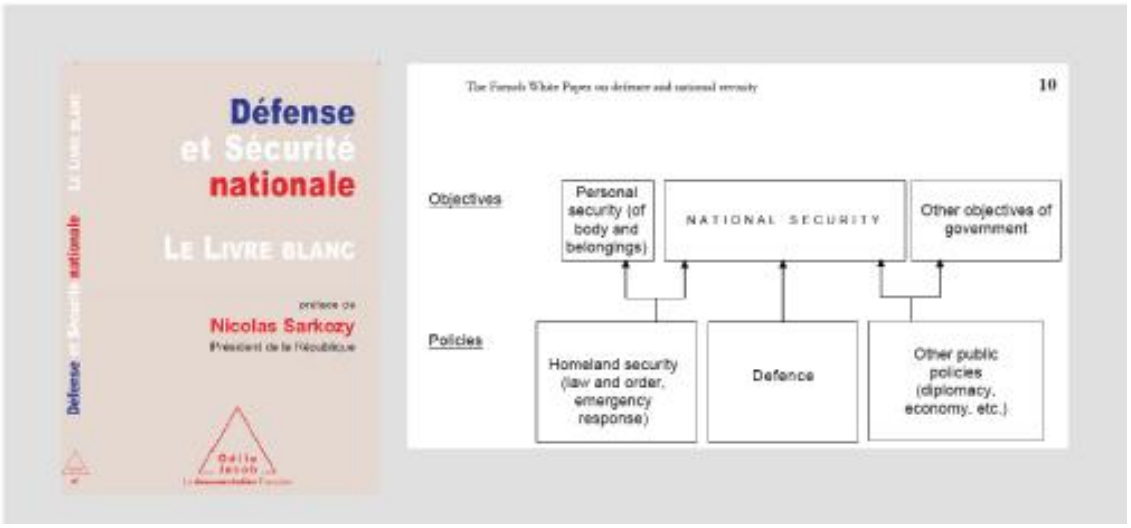
compartidas: estrategia de seguridad nacional para Reino Unido".[300] En él se adopta la misma definición abierta de seguridad "para proteger a la población británica de todo tipo de riesgos de manera que puedan seguir viviendo en libertad y con seguridad bajo un gobierno basado en acuerdos". En el informe del IPPR se destaca que "los riesgos a la seguridad nacional deben definirse de forma amplia en las condiciones actuales, para cubrir las grandes amenazas ocasionadas por el hombre y por los desastres naturales"; además, se afirma que "el trabajo conjunto de sociedades en Reino Unido con el sector privado, grupos de comunidades, gobernantes locales y ciudadanos debe ser una característica de la política de seguridad". En el informe se llega a la conclusión de que Reino Unido necesita "capacidades nacionales flexibles y bien coordinadas, que forjen una gran variedad de instrumentos políticos, tanto militares como no militares en un conjunto coherente".

Superioridad operacional: ¿un proyecto para una nueva seguridad europea?

Mientras que las estrategias de Reino Unido y Alemania se centraban en expandir el concepto de seguridad nacional, el libro blanco francés sobre defensa y seguridad nacional de 2008 se centra en las medidas operacionales necesarias para alcanzar unas capacidades de seguridad nacional coordinadas.[301] En él se utiliza el concepto de "superioridad operacional" para describir su búsqueda y dominar el espectro total con el fin de "aprovechar las tecnologías que aseguran ventaja operacional sobre cualquier adversario", incluyendo "medios de información, comunicación, bienes espaciales; protección de la fuerzas de defensa, especialmente contra amenazas emergentes (químicas, biológicas, radiológicas y nucleares); impactos de precisión de largo alcance; capacidad de operar en entornos urbanos en contacto con la población; superioridad naval, especialmente en aguas litorales; superioridad aérea; y por último movilidad aérea". Estas medidas están pensadas para la seguridad doméstica y para la defensa externa con el fin de combatir todas las amenazas descritas anteriormente. El libro blanco francés aboga por llevar a cabo diversas reformas tanto nacionales como de la UE para alcanzar estos objetivos.

300 *Shared Responsibilities: A national security strategy for the UK*, Comisión del IPPR sobre seguridad nacional en el s. XXI, 30 de junio de 2009, disponible en: http://www.ippr.org.uk/publicationsandreports/publication.asp?id=676.

301 *Libro blanco francés sobre defensa y seguridad nacional*, Presidence de la Republique, junio de 2008, disponible en: http://www.globalsecurity.org/military/library/report/2008/livre-blanc_france_2008.pdf.



White Paper francés sobre la defensa y la seguridad nacional: puntos clave

3. La estrategia de defensa nacional incluye cinco funciones estratégicas que deben ser dominadas: conocimiento y anticipación, prevención, disuasión, protección e intervención. La combinación de estas cinco funciones debe ser flexible y evolucionar a lo largo del tiempo, adaptándose a los cambios en el contexto estratégico...

4. El conocimiento y la anticipación representan una función estratégica nueva y han pasado a ser una prioridad. En un mundo caracterizado por la incertidumbre y la inestabilidad, el conocimiento representa nuestra primera línea de defensa. El conocimiento garantiza nuestra autonomía en la toma de decisiones y permite a Francia preservar su iniciativa estratégica. Es el conocimiento el que debe ser transmitido tan pronto como sea posible a los decisores, comandantes militares y aquellos al mando de la seguridad interna y civil con el objetivo de ir desde predicciones a acciones informadas. La inteligencia de todo tipo, incluyendo los estudios espaciales y prospectivos, toma una gran relevancia.

5.... Reforzar la flexibilidad requiere un cambio en los medios y metodología de vigilancia utilizada sobre el territorio nacional incluyendo tierra, mar, aire y ahora espacio y desarrollar una capacidad de respuesta de las autoridades públicas francesas más rápida y amplia en enfoque. Los sistemas de comunicación e información y los sistemas de advertencia civil permanecen en el centro de los sistemas de gestión y reacción ante crisis. Un aspecto novedoso es que los objetivos operacionales en misiones de protección están ahora asignados conjuntamente a servicios de seguridad interna, servicios de seguridad civil y fuerzas armadas. La coordinación entre departamentos civiles y militares y agencias es uno de los principios fundamentales de esta nueva estrategia...

8. La ambición europea representa una prioridad. Hacer de la Unión Europea un gran actor en la gestión de crisis y la seguridad internacional es uno de los principios centrales de nuestra política de seguridad. Francia quiere que Europa se equipe con la correspondiente capacidad militar y civil... Además, el White Paper pone énfasis en cuatro áreas de prioridad para la protección de los ciudadanos

europeos: el refuerzo de la cooperación en la lucha contra el terrorismo y el crimen organizado; el desarrollo de capacidades civiles en Europa; la coordinación de la defensa contra los ciber-ataques; y la garantía del subministro de energía y materias primas. Finalmente, el White Paper aboga por el esbozo de un White Paper europeo sobre defensa y seguridad.

25 Los próximos años

> *La Agencia de Defensa Europea pretende establecer un **marco de cooperación** europeo para la investigación en seguridad y defensa, junto con la Comisión Europea. Este nuevo marco proporcionará la estructura fundamental para maximizar la complementariedad y las sinergias entre la defensa y las actividades relacionadas con la investigación civil.*
> Nota de prensa de EDA, 18 de mayo de 2009[302]

El mandato del SHERIFF expira a finales de 2009. El grupo publicará su informe final en la SRC 09, la conferencia anual sobre investigación en seguridad de la UE que tendrá lugar en Estocolmo en septiembre de 2009.[303] Sigue sin estar claro qué dirección tomará el desarrollo estratégico del ESRP tras estos, pero se está incorporando a un nuevo programa de trabajo de cinco años sobre política de justicia y asuntos internos de la UE y la Agencia de Defensa Europea se está posicionando como el hogar a largo plazo para la investigación en seguridad europea.

El "programa de Estocolmo"

Cada cinco años la UE adopta un plan quinquenal de justicia y asuntos internos que afecta a todas las áreas de este tipo de políticas: control policial, inmigración y asilo, leyes criminales, bases de datos y protección de los mismos. El "programa de Tampere" (200-2004) fue continuado por el "programa de La Haya" (2005-2009), que incluía el compromiso de introducir los pasaportes y documentos de identidad biométricos y los principios de interoperabilidad y disponibilidad. El nuevo programa se adoptará en Estocolmo en diciembre de 2009. Como Tony Bunyan ha explicado, "el proceso de decidir el contenido de estos planes quinquenales es largo y complicado y rara vez llega a tener relevancia en las noticias de los principales medios de comunicación hasta que se adopta (cuando es demasiado tarde para que el público influencie su contenido o dirección)".[304]

El programa de Tampere fue esbozado y negociado por oficiales de la UE, del Consejo Europeo y de la Comisión Europea, sin realizar consultas en parlamentos nacionales ni en el europeo ni entre la sociedad civil y adoptado en sesiones cerradas del Consejo Europeo (primeros ministros de la UE). En esta ocasión se dispone de más información. En enero de 2008 el Consejo de la UE estableció el "grupo futuro", que redactó un informe acerca de las políticas de asuntos internos de la UE.[305] Sus propuestas, incluyendo el nuevo principio de convergencia, se analizan en un informe especial de

---

302 *La EDA y la Comisión trabajan en conjunto en investigación*, nota de prensa de la Agencia de Defensa Europea, 18 de mayo de 2009: http://www.eda.europa.eu/newsitem.aspx?id=471.

303 Véase la página web de la conferencia SCR09: http://www.src09.se.

304 La sociedad de la vigilancia concierne a toda, Guardian, 28 de mayo de 2009: http://www.guardian.co.uk/commentisfree/libertycentral/2009/may/28/eu-viewsurveillance-society.

305 *Freedom, Security, Privacy: European Home Affairs in an open world*, informe del grupo de asesoramiento informal de alto nivel sobre el futuro de las políticas de asuntos internos europeas, disponible en http://www.statewatch.org/news/2008/jul/eu-futures-jha-report.pdf.

Statewatch: *The Shape of Things to Come* (La forma de los próximos acontecimientos).[306]

La red de libertades civiles europea ha descrito la ideología del programa de Estocolmo como "peligrosamente autoritaria".[307] Para aprovechar lo que denomina "tsunami digital", las propuestas del grupo futuro presagian una obtención masiva de datos personales sobre viajes, detalles bancarios, localizaciones de teléfonos móviles, registros sanitarios, uso de Internet, registros de delitos (incluyendo los pequeños), huellas dactilares y fotografías digitales que se pueden aplicar a diversos escenarios. En el mismo informe, el grupo futuro también sugiere limitar la disponibilidad de tecnologías que aumenten la privacidad esgrimiendo que podrían ser utilizadas por terroristas y criminales. El grupo propone que para el año 2014 la UE necesita crear una "zona de Euro-atlántica de cooperación con Estados Unidos en los ámbitos de la libertad, la seguridad y la justicia". Esto iría más allá que la cooperación actual y significaría que las políticas que afectan a las libertades y a los derechos de todos los europeos no se determinarían solo en Bruselas, sino en reuniones secretas entre la UE y Estados Unidos.

> *La capacidad de determinar la posición de cualquier teléfono móvil (y de saber dónde se encendió y se apagó por última vez) es solo el principio. Durante los próximos años miles de millones de aparatos estarán conectados utilizando tecnologías como la identificación de radiofrecuencias (RFID), la banda ancha inalámbrica (WiFi, WiMAX), satélites y conexión inalámbricas de áreas pequeñas (Bluetooth, wireless, USB, ZigBee). Esto significa que será posible localizar más objetos en tiempo real y analizar su movimiento y su actividad. Pronto empezaremos a verlo en coches, pero es probable que esta tendencia también se extienda a otros muchos objetos de cualquier valor. En un futuro cercano la mayoría de objetos generarán torrentes de datos digitales sobre su localización y su uso, lo que desvelará patrones y comportamientos que los profesionales de la seguridad pública podrán utilizar para prevenir o investigar incidentes.*
> "Grupo futuro" de la UE[308]

El ESRP y el programa de Estocolmo

Está claro que los objetivos de la agenda de investigación en seguridad de la UE estarán integrados de manera firme en el programa de Estocolmo. En el informe del grupo futuro de junio de 2008 se recomendaba "hacer un uso intensificado de los medios disponibles en el contexto de la investigación en seguridad de la UE para los objetivos relacionados con la cooperación policial, la lucha contra el terrorismo, el control fronterizo y las tecnologías de información y comunicación" y se propuso que los Estados miembros de la UE "deben avanzar hacia la obtención de redes convergentes

306 Bunyan, T. (2009) *The Shape of Things to Come*. Londres: Spokesman. Versión en línea disponible en: http://www.statewatch.org/analyses/the-shape-ofthings-to-come.pdf. Véase también Observaciones sobre el Programa de Estocolmo de *Statewatch*: http://www.statewatch.org/stockholm-programme.htm.

307 Comentario sobre el Programa de Estocolmo, Red europea de libertades civiles: http://www.ecln.org/ECLN-statement-on-Stockholm-Programme-April-2009-eng.pdf.

308 Informe del "grupo futuro", (página 6): http://www.statewatch.org/news/2008/jul/eu-futures-jha-report.pdf.

(o, si fuera necesario, soluciones que asegurasen que todas sus redes estuvieran comunicadas) y deben asegurarse de que todos los datos son digitales y pueden fusionarse". Según el grupo, el ESRIF debería proporcionar las "herramientas de colaboración". En su conclusión se menciona que "el reto general para el futuro es el desarrollo de nuevas tecnologías y su relación con la financiación a nivel de la UE, incluyendo los ámbitos de investigación en seguridad y de fondos estructurales".

El grupo futuro también recomendó el lanzamiento de un "fondo común europeo de herramientas de seguridad... que permita a los Estados miembros y a las instituciones (de la UE) hacer disponibles herramientas seguras con potencial demostrado para ser utilizadas en el ámbito de la seguridad para ser evaluadas por las autoridades o por otros Estados miembros". El nuevo programa de trabajo quinquenal de la UE también se percibe como "un momento oportuno para ir más allá de la limitada perspectiva de los enfoques caso por caso y plantearse un objetivo que lo abarque todo en el control de la información relacionada con la aplicación de la ley", basándose en "el uso profesional, empresarial y eficiente de la tecnologías y redes de la información".

El primer borrador del programa de Estocolmo actual se publicó en junio de 2009 y va aún más lejos, proponiendo que "si los países tienen que ir viendo Europa como el escenario en el que se juzgarán sus acciones, será necesario que exista una mayor confianza entre ellos".[309] Aboga por cursos de entrenamiento conjuntos basados en "objetivos ambiciosos", por ejemplo, "entrenar a un tercio de los policías europeos y guardas fronterizos en asuntos europeos durante los próximos cinco años". La necesidad de la "interoperabilidad" cultural encaja con el deseo de conseguir una mayor interoperabilidad a nivel de la UE con el fin de "asegurar que las soluciones técnicas adoptadas a nivel nacional son interoperables con los sistemas europeos existentes o futuros y que se desarrollarán de manera coherente... Esta estructura también permitirá economías de escala a medida que los sistemas implicados entren en funcionamiento y hará posible programar a nivel nacional las inversiones que sirven para cumplir los objetivos de la estrategia de seguridad interna (de la UE)". Dicho de otra forma, si se desarrollan sistemas nacionales uniformes de acuerdo con los requisitos de la UE, será mucho más barato desarrollar los objetivos de la UE descritos.

Más allá del ESRIF: ¿hacia un consejo de seguridad y defensa de la UE?

Sigue sin estar claro cómo funcionará el desarrollo estratégico del ESRP una vez que el mandato del ESRIF haya expirado. La dirección general para las empresas y la industria retendrá la responsabilidad general del programa, pero todavía no hay una base legal clara para la cooperación continuada con el entramado de defensa y seguridad de la UE. Es posible que se forme otro grupo de personalidades informal en el ámbito de la ESRAB y el ESRIF, pero más adelante; si la UE quiere seguir estableciendo sinergias entre sus políticas de I+D, de seguridad y de defensa, debe encontrarse una solución más definitiva. Mientras que el programa FP7 se acaba de poner en funcionamiento (y funcionará hasta 2013), los arquitectos del ESRP están pensando en los fondos para los próximos años y en maneras de financiar la obtención así como la I+D de las tecnologías de la seguridad. En el primer borrador del programa de Estocolmo, la

309 Comunicado de la Comisión en Una zona de libertad, seguridad y justicia para server a los ciudadanos, COM (2009) 262 final, junio de 2009: http://www.statewatch.org/news/2009/jun/eu-com-stockholm-prog.pdf.

Comisión Europea sugirió que "debe tenerse en cuenta la posibilidad de establecer un fondo de seguridad interna".

En mayo de 2009 los ministros de defensa de la UE, encomendaron a la Agencia de Defensa Europea el desarrollo de propuestas concretas para un "marco europeo de cooperación para la investigación en materia de seguridad y defensa". Si bien el control de los marcos de I+D de defensa y seguridad no sufrirán cambios, la intención a largo término parece consistir en situar el desarrollo estratégico del ESRP bajo los auspicios de la Agencia de Defensa Europea. En principio se ha sugerido que un "marco de cooperación" podría asumir la responsabilidad del "conocimiento situacional", desde "la percepción hasta el mando y el control de bienes interconectados". En palabras de Javier Solana, "La coordinación de las inversiones en investigación entra la Agencia y la Comisión harán que los contribuyentes europeos se ahorren dinero, puesto que nuestras acciones estarán concertadas".

En la SRC 09, la conferencia anual sobre investigación en seguridad de la UE, la Comisión Europea llevará la idea un paso más allá, aprovechando la ocasión ara "ampliar y profundizar" el ESRP mediante la creación de un mercado único para la tecnología de defensa y seguridad modelado según las redes transeuropeas de transporte, energía y telecomunicaciones. Estas redes, percibidas como un componente crucial en el mercado interno de la Comisión Europea, están diseñadas para mejorar la "interconexión e interoperabilidad de las infraestructuras nacionales". Además de los fondos de la UE para estas redes, el programa también recibe financiación estructural y de cohesión, así como préstamos del Banco Europeo de Inversiones.[310]

¿Cómo se podrían administrar estos fondos? En el libro blanco francés sobre defensa y seguridad nacional se aboga por la "reorganización de las autoridades públicas" para una nueva era de defensa integrada y funciones de seguridad. Seguiendo este planteamiento, se crearía un "Consejo de defensa y seguridad nacional presidido por el Presidente de la República de Francia". Mirando al futuro, sorprendería poco que este modelo emergiera como la opción favorita para la "convergencia" del entramado de seguridad y defensa de la UE.

PARTE VIII: BALANCE

> *Es necesario ir con cuidado de no caer en un estilo de vida en el que la libertad se vea coaccionada por la presión implacable de un estado de la seguridad.*
>
> *Debemos comprender que debido a la naturaleza del poder estatal, las decisiones que se tomarán en los próximos meses y años sobre el modo y las dimensiones en los que el estado emplea sus poderes (de vigilancia) serán probablemente irreversibles. Se quedarán con nosotros para siempre y servirán de base para las que vendrán en el futuro. Debemos imaginarnos el mundo que estamos creando antes de*

[310] *Trans-European Networks*, página web de la Comisión Europea: http://ec.europa.eu/ten/index_en.html.

construirlo. Podríamos acabar viviendo con algo que no somos capaces de soportar.
Ken Macdonald, Director de acusaciones públicas de Reino Unido, octubre de 2008[311]

26 Conclusiones y recomendaciones

¿Un NeoConÓptico?

Este informe se propuso examinar el desarrollo y la implementación del ESRP y poner en un contexto político y económico más amplio la obsesión actual por la vigilancia y la tecnología de seguridad nacional. Aquí se ha explicado la historia de cómo un pequeño grupo de compañías de la industria militar se ha unido para asegurarse subsidios sustanciales de I+D relacionados con la seguridad nacional de la UE y de la rapidez con la que sus peticiones se han incorporado a la estructura de políticas de seguridad y defensa de la UE. La marginación casi absoluta de los parlamentos, ONG críticas y otros *stakeholders* ha llevado a que, en ocasiones, la búsqueda se haya parecido a la investigación de un golpe empresarial multimillonario.

La idea del "NeoConÓptico" consiste en enfatizar tanto el papel central que desempeña el sector privado en la facilitación de políticas de seguridad basadas en la vigilancia como en la voluntad inherentemente neoconservadora de "defender el territorio propio" de las "amenazas contra el estilo de vida occidental". La convergencia de estas ideologías está acelerando el desarrollo de una "sociedad de la vigilancia" en Europa, lo que aumenta el potencial que tienen los gobiernos de someter a los ciudadanos (y a los no ciudadanos) a detallados exámenes; esto transforma las relaciones entre ellos y va en contra de los principios fundamentales de la democracia.

Si bien según los ideales de la democracia se supone que los gobiernos dependen de la opinión del pueblo, las técnicas basadas en la vigilancia están transformando esta relación; de esta forma nos encontramos con que la gente depende de lo que decida el gobierno, mientras se agranda la diferencia entre la élite política y aquellos que han sido escogidos para servir. En lugar de aumentar la legitimidad política de la UE, estos tipos de políticas solo pueden alimentar el sentimiento de alineación que mucha gente siente respecto a los responsables políticos de Bruselas.

Paradójicamente, mientras que las preocupaciones principales de George Orwell, Michel Foucault y aquellos que comparten sus opiniones sobre un estado que lo ve y lo puede todo, se están afianzando en las políticas de la UE a medida que pasa el tiempo; las nuevas generaciones restan importancia a estas preocupaciones porque las consideran paranoicas o infundadas. Con todo, es difícil concebir de otra manera un mundo caracterizado por la vigilancia obligatoria y el perfilado de riesgos exhaustivo; un mundo en el que el control policial depende de sistemas informáticos, robots de combate y aviones no pilotados; un mundo en el que la población, o ciertos sectores de ella, están sujetos a un dominio de espectro total.

311 'Ken Macdonald: No debemos degradar nuestras libertades en el nombre de su defensa", Independent, 21 de octubre de 2008: http://www.independent.co.uk/opinion/commentators/ken-macdonald-we-must-not-degrade-our-liberties-in-the-name-of-defending-them-967706.html.

Cabe destacar que el ESRP se encuentra en una fase de desarrollo temprana. Ya se han acordado otros seis años y varios miles de millones de euros en cientos de proyectos de investigación en seguridad; la agenda descrita en este informe ofrece una visión resumida de lo que está por llegar. Además, si bien el ESRP centra su atención en la articulación de preocupaciones sobre políticas de seguridad contemporáneas, está muy lejos de ser un factor explicatorio único para la emergencia y la búsqueda de estas políticas, que son más bien un complejo de seguridad industrial más amplio en un gran despliegue de relaciones sociales, políticas y económicas.

Es necesario que hay un cierto debate acerca del tipo de seguridad nacional y vigilancia que la UE y sus Estados miembros están llevando a cabo, así como acerca de las razones por las que lo están haciendo. Sin embargo, la carga ha recaído en la sociedad civil independiente, que debe evaluar la trayectoria, las implicaciones y los riesgos del ESRP.

Seguimiento del dinero

Este informe se basa en una simple lectura de los flujos de capital en el ESRP (tanto económicos como políticos y sociales). Se pone de manifiesto que el programa ha sido diseñado en gran medida por grupos de presión y para grupos de presión; se trata del producto de un conflicto estructural de intereses que emerge a raíz del fracaso en la separación del desarrollo y la implementación del ESRP. En este marco de trabajo, las compañías cuyos nombres aparecen con frecuencia en este informe han desempeñado un papel muy importante, lo cual, junto con una ausencia casi absoluta de control democrático sobre el ESRP, garantiza la realización de concursos estrictos y el análisis completo de los proyectos financiados hasta la fecha. El tipo de investigaciones llevadas a cabo por el organismo responsable de supervisar la contabilidad en Estados Unidos podría proporcionar un modelo válido; el Tribunal de Cuentas de la UE también podría someter el programa a exámenes más rigurosos si fuera necesario.

También existe una necesidad de aclarar los objetivos e intenciones del ESRP. El programa predica los objetivos paralelos de apoyar la emergencia de una industria de seguridad nacional europea y aumentar la seguridad pública. Lo que sucede en la práctica es que las multinacionales están utilizando el ESRP para promover sus agendas con fines lucrativos, mientras que la UE utiliza el programa para cumplir sus objetivos relacionados con las políticas de defensa y seguridad. Como se viene sugiriendo en este informe, el tipo de seguridad descrita anteriormente representa una unión de poderes policiales no comprobados y capitalismo desenfrenado a expensas del sistema democrático.

Por lo que se refiere al ESRP, también es difícil dibujar las necesarias líneas entre la investigación y la obtención, entre el control de tecnología civil y militar, y entre aplicaciones de seguridad nacional y de defensa. Entre toda esta confusión, si el programa continúa, los parámetros del ESRP deben redibujarse radicalmente para ponerlo bajo el control democrático, con el fin de separar la investigación y la obtención así como la seguridad y la defensa, con el fin de proporcionar vías objetivas e imparciales para la investigación y para situar los derechos humanos y la justicia social en el centro en lugar de al margen de cada proyecto.

Esta es una tarea abrumadora que requiere deshacerse de los miedos (reales e imaginarios) que sostienen la demanda de nuevas políticas de seguridad. Como han explicado los autores de *Making Tretas: Biofears and Environmental Anxieties*, "deshacerse del miedo es un proceso complicado porque tenemos que enfrentarnos a los demonios de nuestra historia, política, ideología y economía... En estos tiempos llenos de terror, la búsqueda de soluciones justas y pacíficas depende de la capacidad de ver más allá de nuestros miedos y buscar nuevas elecciones morales y posibilidades políticas".[312]

Europa necesita limitar los poderes policiales y la vigilancia

Las preocupaciones en materia de libertades civiles sobre el impacto de la "guerra contra el terror", la vigilancia no comprobada y la ausencia de controles de responsabilidad en los marcos de la UE relacionados con el control policial y la cooperación para la aplicación de la ley están bien documentados y han caracterizado hasta cierto punto el debate sobre la seguridad durante la última década. Sir Ken McDonald citado anteriormente, está lejos de ser una voz solitaria del *establishment* al expresar sus preocupaciones; Sir Richard Dearlove (antiguo jefe de MI16) y Dame Stella Rimington (antigua jefa del MI5) también se han pronunciado acerca de las invasiones estatales "chocantes e inquietantes" en la privacidad y acerca del hecho de que Reino Unido "se esté convirtiendo en un estado policial", respectivamente.[313] Cabe destacar la importancia que han cobrado estas preocupaciones (al menos en Gran Bretaña) pero el pequeño impacto que han tenido en la agenda política.

Mientras que el régimen de Obama promete "romper con el pasado" en Estados Unidos, las políticas actuales de la UE se caracterizan por una deriva hacia la derecha. Si bien es la derecha la que tradicionalmente ha favorecido la creación de leyes y políticas del orden público más estrictas, el discurso político en el que se enmarca el ESRP parece ir más allá de los partidos políticos. Entre las tendencias más reveladoras de la investigación llegada a cabo durante la realización de este informe se encuentra el uso de la palabra "seguridad", que ahora sirve para justificar la instauración de medidas permanentes que hace unos pocos años parecían "descabelladas". A pesar de las extendidas preocupaciones sobre las libertades civiles, parece ser que estamos entrando en una nueva era caracterizada por un cambio que ha pasado de centrarse en la "lucha contra el terror" a centrarse en la creación de entramados permanentes para la vigilancia y el control social. Incluso en países del norte de Europa y Escandinavia, donde hasta ahora la palabra "seguridad" hacia referencia a un cojín protector proporcionado por el estado, la seguridad nacional está empezando a instar a los estados a combinar y aumentar su poder coactivo para encargarse de manera rápida y punitiva de todos los riesgos.

Este cambio en el énfasis ha puesto la vigilancia en el centro de las políticas sobre defensa y seguridad de la UE. Si queremos que las generaciones futuras disfruten del derecho a la privacidad debemos tener serios debates acerca de las técnicas de

---

312 Hartman, B., Subramaniam, B. & Zerner, C. (2005) *Making Threats: biofears and environmental anxieties.* Nueva York: Rowman & Littlefield (página 250).

313 'La antigua jefa de espionaje Stella Rimington dice que los minsitros han convertido Reino Unido en un estado', *The Times,* 17 de febrero de 2009: http://www.timesonline.co.uk/tol/news/politics/article5750713.ece; 'El Gran Hermano ha ido demasiado lejos ... y lo dice una antigua jefa de espionaje', *Daily Mail*, 2 de junio de 2009.

vigilancia, sus límites y las maneras de controlarlas. Congelar las medidas pendientes de aplicación y revisar la política de seguridad existente tras una década de legislación de vigilancia intrusiva no perjudicará a nuestra seguridad, como se dice. Es esencial dar a Europa la oportunidad de valorar hacia dónde se dirigen la política y la tecnología e idear nuevos marcos robustos para la regulación del poder policial y la protección de los derechos y las libertades individuales en el siglo XXI. Una opción inmediata y obvia para los encargados de elaborar las políticas europeas consiste en la regulación de tecnologías de seguridad polémicas en lugar de proporcionar generosos subsidios a su desarrollo.

La estela de la democracia

El camino hacia la seguridad mediante la tecnología y la voluntad lucrativa que ha emprendido la UE es muy distinto de la búsqueda de seguridad mediante la democracia. Mientras que esta última representa ostensiblemente un "compromiso" entre las instituciones democráticas y la ley, la primera se basa en el determinismo económico y tecnológico, es decir, en valorar si es posible y provechosa. Sólo tras satisfacer estos criterios se tienen en cuenta la democracia y la ley, que suelen verse como posibles barreras para la instauración de cualquier tipo de nuevo poder policial o solución de tecnología punta que se haya convertido en el imperativo actual.

Algunos de los proyectos de I+D de la UE mencionados rayan lo increíble, pero están basados en la oferta y la demanda de tecnología militar novedosa que resulta muy costosa y potencialmente muy peligrosa. La sostenibilidad de este mercado requiere tanto una exageración de las "amenazas" como una reorganización radical de las agencias estatales para formar un nuevo marco de trabajo integrado para la defensa y la seguridad nacionales. Al estar privada de voluntad política y de los medios para llevar a cabo contribuciones importantes en las políticas sociales basadas en la justicia con capacidad para solucionar las desigualdades y la inseguridad, la UE se ha retirado hacia el único ámbito político en el que los Estados miembros pueden mostrarse poderosos y decididos. Actualmente la defensa y la seguridad nacionales se encuentran en el centro del proyecto europeo.

El principio que sostienen el sector público y privado de que ahora la seguridad es un "bien común" es peligroso, no porque la seguridad privada sea necesariamente mala, sino porque el ánimo de lucro y la percepción de la seguridad como tecnología punta por parte del sector privado se contrapone a las tradiciones democráticas y a las aspiraciones de justicia social del "mundo libre". También se han eclipsado otras políticas sociales y económicas más matizadas que estaban diseñadas para resolver las causas principales de complejos fenómenos sociales como la inmigración, el terrorismo y el subdesarrollo.

La nueva asociación público-privada para la seguridad nacional está basada en una simple compensación: beneficios para las empresas y poder para los estados; dicho de otra forma, la habilidad de los estados de mitigar o neutralizar las amenazas de espectro total a la seguridad, de manera local, nacional y a través de las fronteras mediante sistemas de comunicación y vigilancia supervisados por nuevos centros de mando y control. A efectos prácticos, lo que se desarrollará será una red de formaciones estatales permanentes y con gran movilidad a nivel local, regional, nacional e internacional

equipadas con tecnología punta interoperable militar y de seguridad. Algún día estas formaciones gobernarán un mundo administrado en forma de zonas rojas y zonas verdes.

El abrumador énfasis del ESRP en el desarrollo de un conjuntos de sistemas de seguridad interoperables por toda la UE tiene la función de reforzar el creciente entramado estatal europeo, sus instituciones y sus agencias. Cuando la UE habla de "soberanía común" y sus críticos hablan de "ejércitos europeos", el verdadero interés nacional en este tipo de integración europea se pone de manifiesto: la total libertad en las acciones relacionadas con la aplicación de la ley, la seguridad y la vigilancia en un entramado colectivo para la seguridad y la defensa.

Esta nueva forma de estado internacional ya se ha establecido más allá de los confines de las naciones-estado y de los sistemas de control de la responsabilidad, que siguen anclados en el pasado. En lugar de "democratizar" la políticas de seguridad de la UE como respuesta a las extendidas preocupaciones, parece ser que este entramado formará parte del marco de defensa de la UE, lo que hace que sea más difícil de controlar puesto que la "seguridad nacional" le permite cubrirse con un velo de secretismo.

El paradigma de la seguridad nacional se basa en la idea de que las naciones occidentales se enfrentan a una amenaza sin precedentes contra su estilo de vida. Ya sean las pandemias, la violencia política o las protestas, el "problema" se percibe como un grave peligro y la "solución" se expresa en términos que favorecen la transferencia de la capacidad de dar respuestas a políticas sociales de las agencias civiles a las prescripciones militares y de aplicación de la ley desarrolladas por los segurócratas y los tecnócratas. Este proceso se alimenta de gran parte del reciente discurso de la globalización, que afirma que los estados occidentales, lejos de convertirse en más autoritarios y militarizados, deben defender su estilo de vida. Es necesario poner en cuestión estas ideas. Evidentemente, existen verdaderas amenazas para la seguridad, pero parece que se ha perdido por completo el sentido de la proporción. En un mundo con tantos problemas y desigualdades, Europa es una zona relativamente segura.

Dominancia de espectro total

La "dominanción de espectro total" puede ser una manera extrema de describir el marco emergente del control policial (mundial) que se detalla en este informe; sin embargo, parece que se está produciendo un cambio particularmente profundo en el ámbito de la "seguridad, la defensa y la libertad" de la UE. Mientras que los subsidios a las empresas de seguridad y defensa transnacionales se pueden relacionar con una determinada medida política de la UE totalmente contraria a los principios de la democracia (el ESRP), el paradigma de la dominanción de espectro total se basa en pilares más sólidos.

El consenso político respecto a las medidas más duras relacionadas con la inmigración "ilegal", los poderes especiales para combatir el terrorismo, la creación de un marco internacional para combatir el crimen organizado, la adaptación de nuevas tecnologías de seguridad, el derecho del estado a poner bajo vigilancia intensiva y constante a los "sospechosos" y la "segurización" de una serie de nuevas amenazas; los discursos que hacen referencia a la enumeración de estos conceptos están adquiriendo la categoría de "verdad incuestionable" puesto que ejercen un gran poder sobre los gobiernos de las

economías capitalistas avanzadas. Dicho de otra forma, existe el peligro de que la "lógica de la seguridad" se esté convirtiendo en el concepto "de sentido común", que controla tanto el consenso como el consentimiento mientras que desautoriza otras alternativas y produce ingerencia respecto a los daños y desigualdades que causa. Puede que la UE alcance su nivel más bajo de popularidad entre aquellos a los que gobierna, pero su entramado de seguridad y defensa está firmemente basado en el populismo autoritario. De hecho, las políticas de globalización neoliberal y las neoconservadoras de seguridad nacional pueden acabar percibiéndose como las dos caras de la misma moneda "globalista".

También existe una relación entre las nuevas formas de represión de tecnología punta y las prácticas de "rendición extraordinaria", la tortura de sospechosos de terrorismo y el encarcelamiento de hombres y niños en jaulas situadas en islas prisión que han reaparecido recientemente. Estos fenómenos se han presentado como el nuevo "excepcionalismo", como los excesos de los señores de la guerra contra el terror de un régimen neoconservador que pronto quedará confinado en la historia. Como ha explicado Gareth Peirce, un abogado de Reino Unido especializado en derechos humanos, estas demostraciones de fuerza excepcionales taimen tienen otro propósito. "Las primeras imágenes impactantes de seres humanos encapuchados y maniatados siendo transportados por el Atlántico... La humillación a que los captores someten a estos seres humanos (descargados en Guantánamo, donde permanecen agachados en jaulas al aire libre con uniformes naranjas) estaba pensada con antelación".[314] Estas imágenes han hecho que los europeos se acostumbren a medidas más extremas, lo que Jackie Orr denomina la "militarización del espacio interior",[315] que sirven para legitimizar a ojos del público lo que son, a ojos de la comunidad legal, sistemas de justicia paralelos para encargarse de los no ciudadanos, los "buscadores de asilo", los "terroristas" y los disturbios civiles.

Los responsables de estos programas utilizan la respuesta del mundo que observa la situación como barómetro para medir lo que es políticamente aceptable (un experimento grotesco para medir el apetito del público por las medidas "extraordinarias"). Cuando la "indignación" pública alcanza un punto crítico, los programas no se cancelan, sino que se retiran del alcance de la vista del público. Esto es lo que sucedió con las políticas más polémicas de la UE, incluyendo los regímenes de vigilancia obligatoria, las políticas de defensa y la investigación en seguridad. En cuanto se adopta la legislación que lo permite, todas las decisiones clave sobre la implementación se toman en secreto en lo más recóndito del Consejo y la Comisión.

Se ha inventado un nuevo lenguaje para disfrazar los propósitos de las políticas de la UE. En el caso del ESRP, esto significa una serie de "principios" con los que todo el mundo puede estar de acuerdo: la necesidad de aumentar la seguridad, la necesidad de fomentar la competitividad industrial de la UE y de crear trabajos en la UE, la necesidad de hacer algo con la inestabilidad del mundo, etc. Las políticas reales están enterradas bajo millones de páginas de legislación y comunicaciones; más tarde los resultados se ocultan al escrutinio público. La cooperación en el ámbito de la UE se oculta bajo el

[314] Peirce, G (2009) ''Make sure you say that you were treated properly', *London Review of Books*, vol 31 no. 9: http://www.lrb.co.uk/v31/n09/peir01_.html.

[315] Orr, J. (2005) 'Making Civilian-Soldiers: The Militarization of Inner Space' en Hartman, B., Subramaniam, B. & Zerner, C. (eds) *Making Threats: biofears and environmental anxieties.* Nueva York: Rowman & Littlefield (página 250).

lema de que es la única y la mejor manera de actuar para los Estados miembros, por lo que se presta muy poca atención a lo que conlleva en realidad.

Otro mundo está comprometido

Una vez que hayan sido promulgados, los entramados de seguridad descritos en este informe serán muy difíciles de desentrañar. Los encargados de diseñar las políticas perciben esta década de contraterrorismo y legislación permisiva con la vigilancia, no solo como el camino a seguir, sino también como el mero inicio de una revolución en la aplicación de la ley. A pesar de que la capacidad estatal de entrometerse en la vida privada de los ciudadanos y en los espacios públicos ha llegado a límites insospechados, las recurrentes promesas de revolución en cuanto al control de las responsabilidades gubernamentales han fracasado estrepitosamente, especialmente al nivel de la UE.

Mientras que la sociedad civil ha mostrado y en algunos casos denunciado los peores excesos de la "lucha contra el terror" (Guantánamo, la rendición y la tortura, etc.), ha fracasado en la tarea de hacer lo mismo en los enfoques similares que se ponen en práctica en los sistemas de control de inmigración, contraterrorismo y justicia criminal que han dado lugar a un nuevo autoritarismo.

Ahora más que nunca, lo que se necesita es una nueva Europa que sitúe la justicia social y los derechos por encima de todo. Esto requerirá realizar notables reformas en el sistema de gobierno de la UE, medidas constructivas para evitar que Europa se convierta en la sociedad de la vigilancia y del poder militarista de la que han advertido muchos expertos y la revaluación total de un paradigma económico basado solamente en la obtención de beneficios. Esto requiere un esfuerzo constante por parte de la sociedad civil que consiste en informarse los unos a los otros sobre el tipo de UE que tenemos actualmente y en darle la vuelta a la resistencia progresiva para convertirla en medios tangibles que contribuyan al cambio político. Sin estos esfuerzos, la UE seguirá su camino de forma discreta y secreta hasta que sea demasiado tarde para actuar.

Acerca del autor

Ben Hayes ha trabajado para la organización por las libertades civiles Statewatch (basada en Londres) desde 1996 y se ha especializado en los ámbitos de justicia en la UE y legislación nacional, cooperación policial, controles fronterizos, tecnologías de vigilancia y políticas sobre contraterrorismo. Además, Ben trabaja con el Transnational Institute (Amsterdam), el Centro europeo de los derechos humanos y constitucionales (ECCHR, Berlín) y ha sido asesor en diversas organizaciones de derechos humanos, de justicia social y de desarrollo. Asimismo, tiene un doctorado del Magee College (Derry/Londonderry), otorgado por la universidad del Ulster en 2008.

Acerca del TNI

El TNI (fundado en 1974) es una red internacional de activistas y expertos que se dedican a realizar análisis críticos de los problemas mundiales de hoy en día y del futuro. Se busca proporcionar apoyo intelectual a los movimientos que pretenden renovar el mundo de forma democrática, igualitaria y sostenible.

Acerca de Statewatch

Statewatch es un grupo de voluntarios sin ánimo de lucro formado en 1991. Está compuesto por abogados, profesores universitarios, periodistas, investigadores y activistas con una red de contribuidores procedentes de 17 países. Statewatch fomenta el periodismo de investigación y la investigación crítica en Europa, en ámbitos de asuntos internos y justicia, libertades civiles, control de responsabilidades y transparencia. Para más información visite www.statewatch.org.