

[S]

PROSPECTIVA

INNOVACIÓN

SEGURIDAD

la seguridad
también se
diseña...
con ideas

3[2010]

[01-15] febrero

confidencial quincenal para suscriptores editado por [thint]

- 1 **netINTELIGENCIA POLICIAL**  Tanto la investigación científica como el desarrollo tecnológico nos llevan a una práctica policial interconectada con el territorio, capaz de aprovechar esa interconexión para obtener un mejor conocimiento situacional y comprensión anticipada del entorno de las amenazas...
- 3 **AfPak: DENEGACIÓN DE TERRITORIO**  Aunque al menos hay tres estrategias (antiterrorista, contrainsurgente, estabilización) entre activas y latentes pero en todo caso entrelazadas en Afganistán, la convergente y funcional entre ellas es la que no se menciona...
- 5 **TALENTO OPERATIVO DE INTELIGENCIA**  La Revolución en los Asuntos de Inteligencia ha impulsado el análisis como piedra angular de las agencias pero tiene pendiente la *revolución* del talento operativo....
- 6 **LA ASIMETRÍA ES IDEOLÓGICA**  La asimetría del adversario o el enemigo se menciona frecuentemente como ventaja operacional del terrorismo internacional o la insurgencia, pero la verdadera asimetría procede del pensamiento que ponemos en práctica...
- 7 **ENTRE HEZBOLLAH y AL-QAEDA**  El *yihadismo* puede ser violento o puede constituir un *esfuerzo* constante de ocupación a través de la conquista de los corazones y las mentes...
- 8 **CIENCIA PARA LA SEGURIDAD**  Desde el impresionante presupuesto de investigación de la agencia DARPA hasta los aviones policiales no-tripulados, pasando por la modelización del comportamiento insurgente o la simulación de efectos de los IEDs...
- 10 **SEGURIDAD GLOCAL**  Desde el *partenariado público privado* en la protección de infraestructuras críticas, a la capacidad adaptativa de la empresa criminal en Colombia o a las "coincidencias" entre terrorismo y cambio climático...
- 12 **CIBER**  El ciberespacio nos obliga a re-pensar el concepto de soberanía, pero también a planificar cibermaniobras para anticipar los riesgos, mientras se hackean aviones y se interceptan UAVs y satélites..

NET Inteligencia policial

Desde el primer número de [S] hemos subrayado que la denominada **internet de las cosas** cambiará la seguridad del futuro, no sólo la seguridad de la información o seguridad lógica, sino la seguridad física, nuestra propia concepción de la seguridad.

Aunque la internet de las cosas, esa evolución del ciberespacio en donde los objetos, las máquinas y las personas se intercomunicarán en tiempo real a través de la web, ni siquiera se esté planteando todavía como un escenario de seguridad 3.0. y, por otro lado, esté siendo estudiado principalmente en ámbito de las telecomunicaciones, lo cierto es que en términos de impacto en el ciudadano deberíamos haber comenzado a discutir ya sus implicaciones incluso como modelo social para nuestra seguridad.

Uno de esos elementos que marcará la evolución 3.0. del escenario será la **interconexión del policía** en su ecosistema, en la calle. Esta interconexión le permitirá no sólo ejercer como elemento de represión, de disuasión, de prevención o de investigación sino como nodo informativo en una red.

los ejércitos llevan delantera, en esta concepción de interconexión del hombre sobre el terreno, dentro de sus diversos programas del **soldado del futuro**

En 2005 la ciudad de Nueva York fue de las primeras en aproximarse a esta concepción inaugurando el Real Time Crime Center (**RTCC**), un centro de fusión de datos donde han intervenido compañías como Dimension Data, CISCO o IBM, con acceso a la mayoría de bases de datos de interés policial y con dotación de

el futuro será un policía conectado, con acceso en tiempo real a información de su entorno recogida por sensores, y un contraste, también en tiempo real, de esa información situacional con todas las bases de datos policiales

sistemas de información geográfica. La idea no es sólo conseguir un perfil tremendamente enriquecido de conocimiento situacional para cada escenario policial, sino posicionárselo al policía en la calle en tiempo real y recibir información de ese mismo policía también en tiempo real.

En base a esa concepción 3.0., los centros de fusión han de completarse con dos tipos de flujos de información: el procedente de sensores sobre el terreno y el que ofrezcan fuentes humanas operando sistemas multimedia de obtención activa de información.

En cuanto a sensores sobre el terreno, las cámaras de videovigilancia son sólo un primer paso: el segundo será dotarlas de *tracking* (posibilidad de detectar y seguir un movimiento u objeto sospechoso) y de cognición inteligente (sistemas visuales interpretando qué anomalías están sucediendo). El horizonte que se nos abre es cómo hacer que elementos que actualmente pueblan el paisaje urbano emitan información de

su entorno a partir de sensores (lo que de la mano de la internet de las cosas se conoce como *ambient intelligence*.). Este panorama se está abriendo de momento lejos de planteamientos de seguridad, incluso ajeno a ellos, en la construcción de las denominadas ciudades inteligentes, como [Songdo](#) en Corea del Sur, o [Masdar City](#) en los Emiratos Árabes Unidos, a menudo muy ligadas en su diseño a la utilización eficiente de la energía.

El mismo planteamiento de *sensorizar* el entorno para obtener conocimiento situacional en tiempo real que rige para las ciudades inteligentes es el que cuenta en la vigilancia inteligente de fronteras. Además de los ya conocidos sistema SIVE para la vigilancia de fronteras en España o las arquitecturas israelita, saudita o estadounidense (con México), Argelia

**las tecnologías de
información compartida
en tiempo real serán
clave**

está diseñando una barrera de sensores que sea capaz de informar a un centro de control en la ciudad de *Tamanraset* sobre movimientos en sus fronteras del desierto con Malí, Níger y Mauritania. Es la contemplación de la frontera física como una ventana de entrada a una dimensión social futura interconectada en web.

Respecto de los operadores humanos, de los policías actuando sobre un ecosistema interconectado y funcionando ellos mismos como nodos recolectores-emisores de información, la empresa estadounidense *COPsync* continúa instalando sus sistemas de información compartida en tiempo real por más de una docena de departamentos de policía en aquel país.

COPsync es una plataforma, generalmente integrada en los vehículos patrulla, que permite a los policías consultas integradas en tiempo real a sus bases de datos, al mismo tiempo que provee utilidades para elaborar informes. Aunque su concepción es una ampliación de lo que ya vienen utilizando las policías de tráfico para su trabajo sancionador, extendiendo el concepto a policías trabajando en red y conectados a centros de fusión de datos que reciben información de sensores sobre el terreno en dispositivos portátiles individuales (como *smartphones*), vislumbramos fácilmente a un policía con capacidad para producir y procesar **netinteligencia**, inteligencia en red.

Este tipo de netinteligencia policial no sólo implicará un enriquecimiento sostenido en el conocimiento situacional del policía-en-el-ecosistema, sino que incrementará las capacidades de las unidades de inteligencia criminal de los servicios de policía, beneficiarias así mismo de las tecnologías de información compartida. El programa LEAP (*Law Enforcement Analysis Portal*) de la mancomunidad de condados del Norte de Texas, en los EE.UU., está configurado como una plataforma de análisis compartido de la realidad criminal entre cuerpos de policía distintos. El LEAP proporciona consulta integral a múltiples bases de datos, herramientas de análisis operacional y utilidades para resolver conflictos en investigaciones. La tecnología de base no es innovadora, pues ya está presente en muchas agencias de policía y seguridad, pero sí lo es el enfoque, al combinar la información procedente en tiempo real de los agentes sobre el terreno con el trabajo colaborativo de fuerzas de policía distintas en una especie de esfuerzo regional conjunto de inteligencia policial.

Estas aproximaciones de información compartida e inteligencia policial en red definirán no sólo nuevas realidades tecnológicas, que son las más obvias, sino nuevos modos de operativa policial y, lo que es más relevante en términos sistémicos, nuevas realidades legales.

AfPak: denegación de territorio

Las estrategias de la Comunidad Internacional, principalmente de la OTAN y de los EE.UU., para operar en Afganistán parecen enrocadas en un problema conceptual, que las lleva a ser cada vez más cortoplacistas: es difícil encontrar en otro lugar una variación tan continua de planteamientos estratégicos que, por definición, deberían tener un horizonte temporal más amplio.

El foco estratégico sobre Afganistán no está claro o parece no estarlo. Este efecto de apariencias, es decir, de lo que *parece que es* o del desconocimiento de lo que en *realidad es*, está muy influenciado desde luego por un efecto que podríamos denominar la **democratización del análisis** o la posibilidad de que la opinión pública tenga acceso web a multitud de análisis de expertos sobre cualquier conflicto, en este caso Afganistán. Ese fenómeno, positivo en su mayoría de dimensiones, también genera cierta confusión o ruido de fondo en el momento de interpretar con precisión lo que está ocurriendo, sobre todo si pretendemos que esa interpretación tenga algo de *sostenibilidad*.

En torno a Afganistán se han ventilado tres focos estratégicos, unas veces como planteamientos directrices -es decir, con capacidad para orientar la acción de los actores- y otras interrelacionados e inter-dependientes -o sea, con capacidad de ser ejecutados todos a la vez-. El primero sería que la acción de la Comunidad Internacional (CI) en Afganistán está destinada a democratizarlo. A estas alturas y en la era Obama, esa directriz estratégica parece estar abandonada. El segundo de los enfoques estratégicos sería que las operaciones de la CI están dirigidas a desmantelar a Al-Qaeda. El tercero es que la acción internacional busca estabilizar Afganistán dotándola de las condiciones para que construya un gobierno propio y se haga cargo de su propia seguridad.

Para la primera (democracia) y la tercera (estabilización) de las estrategias es bueno avanzar en la segunda (Al-Qaeda), y en eso estarían relacionadas. Sin embargo por mucho que se hayan comunicado y analizado, ninguna de la estrategias resiste el peso de los hechos. Es decir, ninguna de ellas es cierta.

Uno de los efectos laterales de la interconectada sociedad del conocimiento es que quienes gestionan la información cuiden mucho de que el conocimiento, la penetración al sentido real de lo que sucede, tenga cada vez más valor. Expresado de otra manera, la incertidumbre sobre las estrategias en Afganistán puede que sólo exista en la opinión pública o para la opinión pública.

A la mayoría de las opiniones públicas se les ha trasladado que las fuerzas militares desplegadas en Afganistán están cumpliendo a) una misión antiterrorista; b) una misión de estabilización; c) una misión de paz. Estas misiones coinciden más o menos con las estrategias publicitadas y debatidas en multitud de análisis públicos y/o filtrados a lo público. Todas ellas conllevan un axioma implícito, a saber, que en algún momento las tropas de la CI saldrán de Afganistán... pero, ¿y si no es así?.

La estrategia ejecutándose en Afganistán es la que podríamos denominar **denegación de territorio**. Al igual que la *denial strategy* popular en operaciones navales, la estrategia de denegación para Afganistán estaría dirigida a impedir el asentamiento de un gobierno *yihadista* en un territorio desde el que pudiera lanzar operaciones globales.

La denegación de territorio tanto a los *Taliban* como a *Al-Qaeda* en Afganistán es esencial en la contención del terrorismo *yihadista global* principalmente por tres factores: 1) la posibilidad de que, desde el territorio, accedan a fuentes de financiación como el narcotráfico; 2) la posibilidad de acceder a armamento nuclear vía

desestabilización de Pakistán, en un permanente equilibrio inestable por ser epicentro ideológico del *yihadismo*; 3) la posibilidad de corromper ideológicamente la región, primero y menos probable con alianzas aparentemente antinatura con el *chiismo*, pero segundo y más viable extendiendo el islamismo por Asia Central y por China (el gobierno *Taliban* de los noventa apoyaba la constitución de un emirato en el *Turkeistán* chino, la región musulmana de etnia *Uyghur* que es foco de conflicto permanente).

El bloqueo a las fuentes de financiación que proporciona el narcotráfico no se está consiguiendo de momento, pues los *Taliban* controlan buena parte de la producción del que es primer territorio global en origen de opio para la heroína, Afganistán. Aunque durante el gobierno *Taliban* pre-invasión de la segunda parte de los noventa se había dictado una prohibición de cultivo de opio en el territorio, buena parte de los ahora señores de la guerra oportunistamente ligados ahora a los *Taliban* son responsables de su control. En la doctrina del *yihadismo* global está permitido hacer uso de este tipo de recursos siempre que sea para vencer al enemigo. De hecho, las denominadas “negociaciones” con los *Taliban moderados* que

aunque es un mensaje que la comunicación estratégica del conflicto no ha trasladado (aún) a la opinión pública, es difícil vislumbrar actualmente el escenario de una salida de las tropas internacionales de Afganistán... y quien salga, dejará de estar en el juego global

recientemente propuso el presidente afgano *Karzai* y que recogió la conferencia sobre Afganistán en Londres de enero-febrero, pueden tener más relación con la implantación de una vía instrumental para descontar del escenario amenazante a una serie de señores de la guerra gestores del negocio del opio, sobre quienes tendría una buena influencia Pakistán (para dejarles seguir traficando, incluso ofrecerles una porción del eventual negocio energético, pero sin apoyar a la *yihad*), que con la idea real de negociar con los *Taliban* como concepto. Es ciertamente dudoso, sin embargo, que esta alternativa suponga estabilizar Afganistán, a futuro, “sobre las espaldas” de estos comerciantes del opio, que ya malgastaron su oportunidad en los noventa.

A diferencia de otros países en donde las ideologías salafistas de sustentación del *yihadismo* pueden tener implantación estructural pero no han sido invadidos, la denegación de territorio es necesaria en Afganistán porque allí convergen la ausencia de Estado (que ocurriría también en Somalia o Sudán) con la posición geoestratégica a focos de impacto global. Que en Somalia o Yemen se instalen núcleos de Al-Qaeda, incluso permanentemente, no tiene el efecto potencial que podría tener un gobierno *Taliban* apoyando las operaciones de Al-Qaeda por todo el mundo y presionando a Pakistán en medio, además, de una importante ruta de suministro energético en el futuro que no dependa de Rusia, que conecte con las ricas de regiones de Turkeistán y Turkmenistán (ahora en el centro de todos los planos de gasoductos de la región, tanto de los apoyados por los EE.UU. como por los rusos), y que tenga salida al Mar de Arabia.

La variable de Afganistán como **Estado fallido** no tiene un pronóstico precisamente de cambio ante una eventual salida de las tropas internacionales. Por tanto, si aceptamos este condicionante y lo ajustamos al prisma de una estrategia de denegación de territorio debido a los vectores que hemos detallado, la previsión no sólo es que las tropas de la OTAN tardarán mucho tiempo en salir de Afganistán, sino que es difícil en el punto en el que estamos atisbar un futuro realista en donde hayan sido capaz de haber salido.

talento operativo de inteligencia

Bruce Hoffman, reconocido experto antiterrorista estadounidense y actualmente profesor de la Universidad de *Georgetown*, [ha escrito](#) en el *Washington Post* que los recientes atentados de *Al-Qaeda* contra personas o intereses de los EE.UU. (suicida nigeriano en vuelo a Detroit; ataque al recinto operativo de la CIA en Afganistán) no se han llegado a producir principalmente y en esencia por un fallo de la Inteligencia en *conectar los puntos*, sino que son la consecuencia directa de una falta del enfoque estratégico adecuado. En concreto, un fallo en reconocer el carácter dinámico y evolutivo del adversario, intentando responderle con arquitecturas de seguridad remozadas tras el 11-S pero todavía presas de patrones antiguos de comportamiento en sus orientaciones ante las nuevas amenazas.

Tratamos de responder con un patrón institucional burocratizado a una amenaza que, aunque provista de una ideología rígida y excluyente, [paradójicamente](#) no tiene límites en cuanto a la adecuación de su comportamiento de ataque a las debilidades de su objetivo. En nuestro caso, la cultura corporativa de las agencias pesa más que nuestra necesidad de cambio.

Charles Faddis, ex-responsable de la unidad contraterrorista de la CIA concentrada en

armas de destrucción masiva, [declaró recientemente](#) a la CNN que, aún cuando se han llevado a cabo modificaciones en las estructuras de inteligencia, en realidad tanto la cultura como los procesos de la CIA continúan siendo los que siempre han sido: burocráticos y demasiado centrados en la estructura de gestión de *Langley*. Cada vez será más difícil que las agencias de inteligencia logren atraer recursos humanos capaces de arriesgarse a operar en áreas de conflicto fuera del calor de las estructuras burocráticas en casa.

Quizá tratando de contrarrestar este último efecto de pérdida o disminución del talento, aunque también buscando un efecto lateral de penetración, la CIA dispone de un programa de *luna de miel* en función del cual algunos de sus operativos pueden prestar sus servicios durante un determinado tiempo en corporaciones privadas. Aunque se desconoce el éxito de estos programas, con claridad no sirven para atraer talento operativo a las agencias. Por más que durante años se haya tratado de concentrar capacidades en recursos humanos de alta calidad para el análisis de inteligencia, en el ámbito de las operaciones sobre el terreno se han descuidado las capacidades humanas, cada vez con menos experiencia, mayor aversión al riesgo y menos respaldadas por culturas corporativas de *inteligencia managerial centered*.

Desde 2009 funciona en el *Movimiento de Resistencia Islámica Harakat al-Muqáwama- Hamas* un Departamento de Inteligencia Exterior nominalmente destinado a cooperar con países árabes e islámicos, según *Jane's*

publicidad



INTELIGENCIA COMPETITIVA | INTELIGENCIA DE SEGURIDAD

[S]

3[2010] febrero

La asimetría es ideológica

El atentado del psiquiatra militar estadounidense en *Fort Hood*, el atentado fallido del vuelo que unía *Amsterdam* con *Detroit* y el ataque contra las instalaciones operativas de la CIA en *Afganistán* invitan a reflexionar sobre el papel de la inteligencia en estos escenarios y hasta qué punto la asimetría de fuerzas juega en desfavor del despliegue de la inteligencia estadounidense y cuáles son los elementos que anulan las supuestas ventajas de las capacidades estadounidenses frente a una organización aparentemente más débil.

La asimetría de la amenaza va más allá del uso de la fuerza. Los *yihadistas* son prácticamente impermeables, no se sienten presionados por el tiempo, y se entregan por completo con la causa. Actúan en la clandestinidad y no se manifiestan hasta que cometen un atentado. Son imperceptibles y se hacen más fuertes en sociedades en las que se respetan las libertades. En un Estado policial el nigeriano *Abdulmutullab* no habría conseguido subir a un avión. No habría hecho falta conectar los puntos en un análisis de inteligencia. Ante la duda se habría presumido su culpabilidad. Pero en las democracias se emplean innumerables medidas de seguridad para evitar los errores y excesos de la presunción de culpabilidad. Son estos avances en los derechos de las personas los que hacen vulnerable a países como Estados Unidos. Ésta es probablemente la asimetría más difícil de contrarrestar: respetar las libertades y la presunción de inocencia al mismo tiempo que se persigue a una amenaza invisible que se esconde en la sociedad que pretende atacar.

El fallo de inteligencia del IIS impulsó un cambio de organización en los servicios de inteligencia e incorporó plataformas de integración de las distintas agencias y trabajos colaborativos. Pero de los recientes errores, y en especial del atentado fallido de la pasada navidad, ¿Qué conclusiones se pueden sacar? ¿Qué significa que no se conectaron los puntos? ¿Fue realmente un fallo de análisis?

Se podría afirmar que se trató de un fallo humano por la falta de imaginación para detectar la innovación que el nigeriano empleó para introducir explosivos en el avión. Pero a priori resulta difícil creer que un analista no haya sido capaz de interpretar un informe que avisa de la preparación de un atentado por parte de un nigeriano vinculado con *Al-Qaeda* en *Yemen*. Tampoco resulta comprensible que los sistemas de información no hayan conectado el nombre del pasajero con la listas de personas vinculadas con el terrorismo, con los informes de la preparación del atentado y el aviso de la familia del nigeriano sobre su radicalización, si la interconexión de los sistemas, los trabajos colaborativos y la información compartida están precisamente para detectar estas relaciones y coordinar a las distintas agencias. La razón parece indicar que se trató efectivamente de un fallo humano, pero de **omisión**. Resulta difícil de entender que se haya tratado de un fallo de los sistemas de inteligencia tal cual fueron concebidos después del IIS.

Las conclusiones que se pueden sacar del atentado fallido del 25D y del resto de 'fallos' mencionados es que los servicios de inteligencia están también en situación de asimetría respecto a las organizaciones terroristas. Probablemente su mayor enemigo sean los tiempos con los que se rigen las decisiones políticas y la necesidad de dar soporte a un ejército desplegado en un entorno de combate asimétrico, no sólo en el sentido de la fuerza, sino también en el sentido de las características de las acciones y métodos de los *yihadistas*. Esta serie de fallos no traerá cambios significativos en la configuración de los servicios de inteligencia. Muy probablemente introducirá cambios 'silenciosos' en la visión temporal y espacial de su misión en la seguridad internacional y en la concepción que se tiene de un enemigo que es altamente resistente frente a un entorno militar hostil.

Entre *Hezbollah* y *Al-Qaeda*

EE.UU. acaba de reforzar su presencia militar frente a las costas de Irán. A esta situación de dimensión militar habría que agregar una notoria expansión de los brazos de *Hezbollah* en escenarios claves de la región, y en especial su reciente vinculación, tanto de *Hezbollah* como de Irán, en las actividades del grupo *Al-Houthi* que opera en el norte de Yemen y que se enfrenta al mismo tiempo contra el gobierno yemení y el régimen Saudí.

El caso de Irán es muy distinto al resto de escenarios de la *yihad*. Irán no es un Estado fallido. Es cierto que existen facciones y grupos de poder contrapuestos, pero están estratégicamente equilibrados por su Líder Supremo el *Ayatolá Alí Jamenei*. Por lo tanto, ¿qué efectos tendrá la contención militar sobre Irán? Para que una contención tenga efectos se debe cumplir que los actores que participan del enfrentamiento sean racionales y comprendan las ventajas y desventajas de un juego de tipo suma cero (las ganancias o pérdidas de un jugador están en exacto equilibrio con las del otro -donde uno gana, el otro pierde). Pero estos modelos no explican un comportamiento de racionalidad alternativa, que se salga del patrón habitual, u otro nutrido principalmente por claves emocionales.

Por otro lado la contención militar, tal como está planteada por Estados Unidos frente a las costas de Irán, no tienen efecto sobre la estrategia de expansión ideológica y regional iraní a través de organizaciones como *Hezbollah*. Las tipologías de expansión ideológico-sociales como la de *Hezbollah* han demostrado ser bastante resistentes ante los despliegues de ejércitos convencionales.

La contención debería dirigirse también a contrarrestar la expansión ideológica de *Hezbollah*. Esta es la principal amenaza a la estabilidad regional. Si Irán incorporase la misma estrategia de expansión ideológica que utiliza *Al-Qaeda* para infiltrarse en los distintos escenarios en los que opera, tendría la capacidad suficiente como para

influir en la futura estabilidad de la región. Se abriría un nuevo frente *yihadista*. Y desafortunadamente, como ya es sabido, esta expansión no se contiene sólo con el despliegue de ejércitos.

de momento no tenemos dos grupos *yihadistas* con aspiraciones globales... ¿podríamos?

¿Podría *Hezbollah*, auspiciada por Irán, representar una amenaza para Occidente similar a *Al-Qaeda*? La ideología de ambas organizaciones es distinta como también lo son sus objetivos. *Al-Qaeda* busca Estados fallidos, mientras que *Hezbollah* pretende el control del Estado no su destrucción. Por otro lado, la ideología de *Al-Qaeda* es global, mientras que la de *Hezbollah* es local y engloba a la porción chiíta del Islam. Pero no obstante, ambas organizaciones son contrarias al status quo que defiende la Comunidad internacional, por lo que no se debería descartar esta posibilidad. Hay antecedentes de actuaciones de *Hezbollah* en Occidente. Las posibilidades de infiltración son, como mínimo, similares a las de las redes de *Al-Qaeda*. *Hezbollah* podría expandir sus actuaciones a escenarios de la *yihad* en los que los musulmanes chiítas estén en conflicto con el *status quo*, y/o actuar contra intereses de Occidente que participen de estos conflictos.

La contención o despliegue militar estadounidense podría exacerbar el rechazo de los más radicales de ideología chiíta y alimentar el ideario de *Hezbollah*. Esta es la fórmula de expansión que ha sabido explotar *Al-Qaeda*. Puede que con esta medida se esté contribuyendo, sin quererlo, a que se abra un nuevo frente *yihadista* adicional y complementario al de *Al-Qaeda*, y que ideologías y objetivos opuestos encuentren un punto en común que facilite una unión transitoria frente a un enemigo común. *Al-Qaeda* intentará aprovechar esta situación, dependerá de la voluntad de *Hezbollah* e Irán de aprovechar esta 'oportunidad'.

ciencia para la seguridad

La Agencia de Investigación para Proyectos Avanzados en Defensa (DARPA) de los EE.UU. [ha publicado](#) su estimación de presupuesto para el año fiscal 2011. Aparte de alcanzar los 3.000 millones de dólares, el presupuesto establece las guías de por dónde va la investigación avanzada en seguridad y defensa, tanto en proyectos básicos como aplicados.... porque aunque el grueso de la inversión se la llevan proyectos de investigación aplicada y de desarrollo tecnológico avanzado, la DARPA también dedica 328 millones de dólares a investigación en ciencias básicas, es decir, aquella de la que no se va a ver ningún retorno inicial claro pero que se considera necesaria (básica) para el desarrollo posterior. Dentro de esta investigación básica, por ejemplo, hay un capítulo dedicado a explorar la intersección entre biología, tecnologías de la información y sistemas micro-físicos.

Como programas concretos, la DARPA dedicará fondos a PREVENT, dedicado a entender los mecanismos de los traumas cerebrales producidos por la onda expansiva de explosiones que no dejan herida. También a encontrar nanoestructuras en sistemas biológicos que sean de aplicación en defensa, avanzando en la modelización matemática de estructuras para el desarrollo de contramedidas, por ejemplo, contra ataques químico-biológicos; o el desarrollo de un modelo funcional para representar en un algoritmo el patrón de reconocimiento visual de objetos de los mamíferos, que tendría aplicación en robots con cognición visual inteligente.

Igualmente en el ámbito de la modelización, continuarán impulsando el programa *Mathematics of the Brain* (MoB), dedicado específicamente a recrear y traducir en algoritmos procesos de razonamiento o aprendizaje humanos que puedan ser traducidos a aplicaciones de seguridad. Este programa se complementa con el de *máquinas inteligentes* o con la *tecnología de lectura y razonamiento*, destinados a desarrollar sistemas informáticos capaces de procesar, entender y representar flujos masivos de datos.

El programa ITMANET busca desarrollar una teoría de información para redes móviles inalámbricas en ausencia de cualquier tipo de infraestructura cableada en tierra. Por su parte, la Materia Programable busca el desarrollo de materia sintética que obedezca a órdenes externas... o un programa para la manipulación genética que conduzca a la resistencia de soldado en el campo de batalla o a la reparación de huesos y tejidos. Otros programas, como el TX, buscan el desarrollo de vehículos terrestres que puedan despegar y aterrizar volando; o la construcción de baterías de alta densidad; o armas ligeras láser.

En 2011 inicia un programa sobre *Leyes Fundamentales y Límites de la Ciberseguridad*. Por otro lado, la DARPA no se olvida de la capacitación avanzada de recursos humanos, con el programa de *Entrenamiento para la Adaptabilidad* o el *Training Superiority*, enfocado a la interiorización de competencia técnica y que contiene desarrollos de web semántica y lenguaje natural para el aprendizaje.

aunque muchos de los proyectos parezcan ciencia ficción, tienen en común centrarse en lo nano, en simular estructuras biológicas, en impulsar la hiperconectividad web del humano sobre el terreno y en dotarlo de sistemas inteligentes que sean capaces de procesar grandes flujos de información, interpretarlos y representarlos en tiempo real

aviones policiales no tripulados

Un consorcio de agencias de seguridad británicas [denominado *South Coast Partnership*] encabezado por la *Policía de Kent* está desarrollando un proyecto, junto a la empresa *BAE Systems*, para la utilización de sistemas aéreos no tripulados (UAS) en funciones policiales, tales como la vigilancia de bandas de motoristas, manifestaciones de diverso tipo, delitos en áreas agrícolas, patrullaje de costas y fronteras u operaciones contra el crimen organizado.

Las autoridades aéreas británicas están exigiendo la dotación en los UAS de tecnología *sense and avoid* que sea capaz de detectar y evitar otros aparatos en el espacio aéreo, de manera que así se reduzca el riesgo de colisión de estos aparatos una vez en operaciones.

simuladores de explosiones

La proliferación de riesgos derivados de IED (explosivos improvisados) lleva al desarrollo de vehículos simuladores, como el *IED Battle Drill*, un sistema en *Fort Bragg* (EE.UU.) que utiliza un coche sobre plataformas hidráulicas cuyo comportamiento controla un programa desarrollado por el *Instituto de Tecnologías Creativas* de la Universidad de California. Los simuladores permiten el desarrollo de comportamiento ante tácticas y técnicas utilizadas por grupos hostiles que aplican IED.

modelizando insurgencia

La revista *Nature* ha publicado un artículo [[Common Ecology Quantifies Human Insurgency](#)] que desarrolla un modelo explicativo para la insurgencia humana.

El modelo está basado en el estudio de bajas en conflictos desde 1816 a 1980 y en ataques terroristas hasta el 2005, tratando de reproducir qué tienen todos los escenarios en común y cuáles son sus variaciones, formalizándolo todo en términos cuantitativos. La investigación considera a cada población insurgente como grupos dotados de una organización propia que se mueven en un medio ecológico (de intereses en competencia) en donde toman decisiones.

Los hallazgos cuantitativos respaldan las hipótesis sociológicas de que los conflictos insurgentes representan *guerras de cuarta generación*, con dinámicas distintas respecto a las tradicionales. El modelo tiene en cuenta el retorno de valor informativo por cobertura mediática, y no específicamente táctico, que obtienen las acciones insurgentes en teatros como Iraq o Afganistán bombardeando un sólo vehículo militar de la OTAN o los EE.UU.

En el marco del proyecto *Open Government*, el Departamento de Seguridad Interior de los EE.UU. ha [lanzado una web](#), que estará operativa hasta el 19 de marzo de 2010, en donde se llama a la ciudadanía a expresar ideas sobre cómo mejorar toda una serie de dimensiones de la seguridad, desde la transparencia, pasando por la colaboración o la innovación. Todo sobre seguridad desde el ciudadano y para el ciudadano.



partenariado público-privado

La Fundación ASIS en los EE.UU. junto al sistema de alarma para la policía de Illinois (*Illinois Law Enforcement Alarm System*), que agrupa a 890 cuerpos de policía, desarrolla un programa mediante el cual ha contratado a un especialista en protección de infraestructuras críticas para trabajar en el centro regional antiterrorista, el *Illinois Statewide Terrorism and Intelligence Center*, encargado de analizar información relacionada con el riesgo a las infraestructuras y **diseminarla** a los operadores privados de infraestructuras críticas que tengan que conocerla. El centro regional antiterrorista es un centro de fusión localizado en *Springfield* que incorpora a personal de la policía de Illinois, de su Guardia Nacional, del FBI, la DEA y el Departamento de *Homeland Security*, y es el primero en incorporar de manera permanente a un **analista de la industria** a sus trabajos.

El Departamento de Energía en los EE.UU. está constituyendo un grupo **público-privado** para analizar sistemas de protección del sistema de energía eléctrica contra ciberataques y que tendrá una dotación de fondos de 172 millones de dólares por parte del Congreso. El grupo tendrá como misión establecer políticas y protocolos para asegurar el despliegue efectivo de software y tecnologías de control para proteger la infraestructura eléctrica del país. El grupo se establece en el marco del *Consejo Asesor para el Partenariado en Infraestructuras Críticas* constituido por el Departamento de *Homeland Security* en EE.UU.

academia ciudadana de policía

La policía del Condado de *Sioux Falls* (Dakota del Sur, EE.UU.) organiza un curso para ciudadanos en la denominada *Citizens Police Academy* en donde, en un mes y medio, ciudadanos seleccionados aprenderán como la policía desarrolla sus procedimientos de vigilancia o investigación, protocolos de ciencia forense, operaciones caninas y un abanico en donde los habitantes de la ciudad entenderán más de cerca la labor de su policía.

terrorismo y cambio climático

A final de enero, la cadena de televisión *Al-Jazeera* emitió [una alocución](#) en donde una voz atribuida a *Bin Laden* condenaba a EE.UU. y a otras economías industriales por su influencia en el cambio climático, criticando al ex-presidente George W. Bush por no firmar el protocolo de Kyoto. Aunque, como suele suceder, la autoría no ha sido confirmada, todavía es pronto para evaluar el significado que tendrá la inclusión de este tópico en la narrativa de victimización de Al-Qaeda.

Tres meses antes, la CIA [había anunciado](#) la creación de un **Centro sobre Cambio Climático y Seguridad Nacional**, compuesto por especialistas senior de sus direcciones de Inteligencia y de Ciencia y Tecnología, respectivamente. Entre otras, el Centro tendrá la función de desclasificar documentos e imágenes que puedan ser útiles en investigaciones científicas, impulsando al mismo tiempo investigaciones sobre el efecto del clima en la seguridad.

Colombia como ensayo

Aparte las continuas informaciones globales sobre convergencia entre prácticas del crimen organizado y de financiación del terrorismo, algunas localizaciones como Colombia sirven para entender la capacidad de adaptación de las amenazas criminales.

Las -en otro tiempo enemistadas por el control del territorio- bandas colombianas de las FARC y el ELN han renovado a final de año la alianza a la que habían suscrito en noviembre de 2009 en una localización en la selva venezolana limítrofe con Colombia.

Fuentes del ejército colombiano mantienen que, debido al tradicional enfrentamiento que ambos grupos mantienen por el control de la producción y distribución de cocaína, principalmente en los departamentos de Arauca (frontera con Venezuela) y Nariño (limítrofe con Ecuador), la anunciada alianza no tendría más que contenido propagandístico. Esta primera evaluación cobra sentido a la luz de la propia **narrativa** utilizada por las FARC y el ELN para *comunicar* su alianza, aludiendo a su necesidad

por la utilización de Colombia como base de operaciones por EE.UU. y a conceptos populistas como la lucha anticapitalista. Es decir, la pretensión es re-editar un discurso guerrillero *unido* con el que envolver sus operaciones de narcotráfico.

Por otro lado y también con la motivación de posicionarse en la gestión del narcotráfico, una tercera generación de los denominados grupos paramilitares se ha instituido en Colombia, conglomerado que se conocen entre los organismos de seguridad como BACRIM (*bandas criminales emergentes*). Los informes que maneja la seguridad colombiana sitúan una veintena de grupos fruto de la descomposición de las *Autodefensas Unidas de Colombia* (que ya era una amalgama de grupos) a partir de 2005 que estarían operando principalmente en ciudades como Bogotá, Medellín y Barranquilla, pero no son ajenas a otros departamentos como Meta, Urabá o Nariño. Un [reciente informe](#) de *Human Right Watch* pone el acento en una desmovilización deficiente de las AUC para explicar el resurgir de la violencia *paramilitar*.

DESCUENTO DE CRISIS del 50% en [S] suscripción Institucional.

[S] ha decidido sumarse a los esfuerzos que instituciones y corporaciones llevan a cabo para la contención del gasto en esta coyuntura de dificultades económicas, reduciendo en un 50% el montante de las **suscripciones anuales institucionales o corporativas** (que son las que hacen a [S] sostenible) que se efectúen durante este mes de febrero de 2010 y para el período de publicación de 24 números, colaborando así activamente y en la parte que nos toca en la recuperación de la situación para 2011. Así mismo se mantiene el 25% de descuento en las suscripciones personales realizadas durante febrero.

A partir del número 5 (15 marzo 2010) [S] será distribuido exclusivamente a suscriptores. El formulario para [S] suscriptores ya está disponible en http://www.s-guridad.com/iS_formulario_suscripcion_feb2010.doc

La soberanía del *cibespacio*

La denominada *Operación Aurora* que penetró los sistemas de información de Google y de 33 empresas que representan intereses estadounidenses ha puesto de manifiesto que es posible dirigir ataques desde un país, como China, hacia otro como Estados Unidos, sin afectar al resto del *cibespacio*.

Por otro lado, las reacciones políticas de uno y otro responden a la defensa de sus territorios, en este caso de sus respectivos *cibespacios*, en los términos con los que se defiende la soberanía de los Estados. Por un lado, China exige a las empresas de INTERNET que quieran actuar en su *cibespacio* que cumplan con sus normas, en especial las relativas con la censura y el control de las operaciones. Toda empresa que no esté dispuesta a respetar la legislación que regula el *cibespacio* chino será invitada a retirarse de este mercado. Asimismo el gobierno chino impide el rastreo de las direcciones IP vinculadas con los ataques de la Operación Aurora. Estos son sólo algunos ejemplos de que el gobierno de China ejerce la exclusividad y plenitud en el control de lo que sucede en su *cibespacio*.

En el caso de EE.UU., se ha denunciado formalmente ante el gobierno chino los ataques de la Operación Aurora como acciones de ciberespionaje. Aunque en esta ocasión los ataques no se dirigieron directamente contra la administración del Estado esta decisión responde a la facultad de defender la soberanía de su territorio, y con ello a sus empresas nacionales. Ambas medidas, tanto la de EE.UU. como la de China, responden a la defensa de sus respectivos *cibespacios* en ejercicio de su soberanía.

La interconexión de la red cambia la forma de entender las comunicaciones. La barrera física prácticamente desaparece para algunos de los

aspectos de la sociedad de la información. El *cibespacio* hace posible que el concepto de frontera se convierta en un término más amplio que implique no sólo las limitaciones físicas sino también las fronteras virtuales de INTERNET. A través de la red es posible penetrar las fronteras de un Estado, y por lo tanto de su soberanía, sin la necesidad de presencia física.

China y otros países que controlan sus flujos internos de información en la red, como Cuba e Irán, entre otros, extendieron el control soberano del Estado al *cibespacio* como una dimensión adicional a sus respectivos territorios. De la misma forma que se restringen las libertades físicas también se limitan las libertades de la información que fluye en estos entornos.

No obstante, China no sólo controla su espacio sino que además aprovecha las ventajas de la red para explotar las vulnerabilidades virtuales de sus 'adversarios'. La Operación Aurora no es la primera, y previsiblemente no será la última que se dirija contra intereses estadounidenses. Será una práctica que se transformará en algo común en el sistema internacional y que dará lugar muy probablemente a incorporar este espacio en los términos del **Derecho Internacional Público**.

China no se ha limitado a cuestionar y/o defender la soberanía, sino que ha violado el *cibespacio* de una empresa de los EE.UU. ¿Qué habría sucedido si se hubiera detectado espionaje y una violación del territorio físico de

Cibermaniobras

Adoptando la nomenclatura introducida por las teorías de *Nassim Nicholas Taleb* sobre la ocurrencia de sucesos de difícil predicción, un *Cisne Negro* sería una anomalía que provocaría alto impacto al presentarse en un sistema y que sería explicable sólo retrospectivamente, es decir, impronosticable e inevitable. En esa línea argumental, el 11-S habría sido un ejemplo de Cisne Negro para la comunidad de inteligencia, como lo fue también *Pearl Harbor*. En ambos casos había indicios que **retrospectivamente** han sido esgrimidos como claros indicadores de que un evento de estas características tendría lugar, pero las limitaciones en la capacidad de análisis e imaginación de los seres humanos que tuvieron acceso a estos indicios no permitieron que los eventos fueran distinguidos en **prospectiva**.

Por definición estos eventos son inevitables. Por sus características, esta clase de incidentes suceden en contadas ocasiones y sus efectos producen cambios significativos sobre el sistema en el que tienen lugar. Debido a la limitación general de la mente humana en pronosticar escenarios imaginados por individuos cuya diversidad y componente de racionalidad alternativa y particular no son posibles de representar en modelos de análisis, esta clase de incidentes siempre formarán parte de la inseguridad.

Los **Cisnes Grises** por su parte serían eventos de características similares a los negros (anomalía, alto impacto, explicable retrospectivamente) pero que han sido planteados a priori como resultado de ejercicios en los que se emplean métodos de análisis, pensamiento alternativo y/o cualquier otra técnica que incentive la imaginación de los analistas. Es decir, los Cisnes Grises son anticipables usando la imaginación. La construcción de estos escenarios futuros posibles y el establecimiento de protocolos de actuación reducen el impacto de esta clase de incidentes.

El ciberespacio es un entorno en el que aún no ha tenido lugar un evento que pueda considerarse como un Cisne Negro. Esto significa que tarde o temprano se producirá un incidente de alto impacto en la red, que desencadenará asimismo una anomalía en el funcionamiento de los sistemas de información tal cual fueron concebidos, y será explicado retrospectivamente. El incidente provocará a posteriori cambios sustanciales en la configuración de la red y en el papel que desempeñan los principales actores de los sistemas de información.

Los análisis respecto de la dinámica del ciberespacio discrepan sobre la magnitud de las ciberamenazas en la red. Están quienes consideran que se exageran los efectos que a menudo se pronostican como posibles a partir de incidentes que se podrían dar, y que debido a la configuración de los sistemas de información resultaría muy difícil organizar y ejecutar un evento *negro* de características catastróficas. Por otro lado están quienes estiman que la interconexión de los sistemas y las capacidades desarrolladas por algunos actores estatales y no-estatales serían suficientes como para colapsar el funcionamiento de redes críticas. Los análisis que prevén una catástrofe son útiles si aportan escenarios futuros posibles. En cambio, los análisis que subestiman los efectos de un incidente en el ciberespacio son los que confirman la necesidad de realizar estudios para detectar Cisnes Grises. Esta clase de incidentes *grises* 'poco probables' son los que se escapan a la mente de los analistas. La línea de pensamiento o análisis que subestima los efectos de un incidente de baja probabilidad en la red es la señal que indica que un Cisne Negro tendrá lugar irremediablemente.

El ciberespacio es una construcción humana en la que se integran componentes de hardware, software y la interacción de los individuos con

éstos. Problemas de diseño, fabricación, implementación y utilización de los componentes de la red son todos elementos que hacen de los sistemas de información un entorno vulnerable a acciones malintencionadas, errores u omisiones. Probablemente la principal vulnerabilidad de estas construcciones sea el componente humano y no el componente físico y lógico de la red.

ninguna de las *cibermaniobras* se ha especializado en analizar el comportamiento humano de las operaciones hostiles y bastante poco en imaginar escenarios de baja probabilidad y alto impacto

El Cisne Negro no será resultado de un ataque contra algunos de estos elementos por separado, sino más bien la combinación de todos estos entornos, en el que la participación de los individuos será esencial para que los efectos sean de las características de un Cisne Negro; será la imaginación de unos individuos la que soslaye las capacidades de análisis de los expertos en el ciberespacio; será la racionalidad alternativa o idiosincrásica de algún comportamiento humano la que haga posible que se explote una vulnerabilidad, o una serie de vulnerabilidades interconectadas y que produzcan así mismo un efecto cascada. La participación voluntaria o involuntaria de una serie de hechos e individuos configurarían el primer Cisne Negro del ciberespacio.

Por lo tanto no habría que subestimar las capacidades e intenciones de actores estatales y no estatales que estén apuntando al ciberespacio como una nueva dimensión para explotar la inseguridad. Tampoco habría que alarmar a la sociedad sobre un futuro posible catastrófico. Probablemente la resiliencia sea la mejor estrategia para preparar a la sociedad ante un futuro de estas características. Pero en el ámbito de la seguridad e inteligencia, sí habría que continuar trabajando en la elaboración de

ejercicios que tengan como objetivo la detección de Cisnes Grises prestando especial atención a la participación de individuos o grupos de individuos en la red.

Por ejemplo, el caso de Fort Hood no fue un problema relacionado con la seguridad de las armas que emplean los militares en la base. Sino el uso que un individuo con unas motivaciones particulares hizo con su armamento. Los analistas no se plantean atacar el problema incorporando medidas de seguridad a las armas, sino detectando anomalías en el comportamiento humano que podría derivar en un mal uso de su armamento. Es la combinación de elementos técnicos, mecánicos y humanos individuales lo que hace más compleja la detección de esta clase de incidentes.

El ciberespacio no es un entorno exclusivo de hardware y software sino una forma más de conexión de las personas. La red es una representación de estas relaciones. El componente 'ciber' es simplemente un medio adicional de comunicación e interacción y por lo tanto una dimensión adicional de la inseguridad. Los ejercicios para detectar Cisnes Grises deben concentrarse tanto en la parte técnica para detectar vulnerabilidades que podrían ser explotadas, pero esencialmente en la parte social de la red, es decir, el componente más vulnerable de los sistemas de información.

Los ejercicios [cyberstorm](#) llevados a cabo por el Homeland Security Department de los EE.UU. en 2006, 2008 y 2010, el [CAPP](#) del FSISAC o los incardinados en el Pentágono son *cibermaniobras* destinadas a simular ataques a las infraestructuras críticas a través de sus sistemas de información, de manera que puedan detectarse y corregirse vulnerabilidades anticipadamente. Ése es el propósito también, con un enfoque más investigativo o forense, del proyecto [Grey Goose](#). La Unión Europea, después de que ENISA publicara su [guía de mejores prácticas](#) para los ejercicios nacionales, está por organizar las [primeras maniobras europeas](#) para la resiliencia de las infraestructuras críticas.

hackeo del vuelo

La autoridad estadounidense de aviación [*Federal Aviation Administration - FAA*] ha publicado una nota advirtiéndole de que la nueva versión del mayor avión comercial de la compañía Boeing, el 747-8, puede ser *hackeado* desde el exterior a través de sus sistemas informáticos. La [nota](#) de la FAA advierte de que la arquitectura del sistema permite la explotación de vulnerabilidades por acciones hostiles.

Por otro lado, el *Wall Street Journal* ya [informó](#) en su momento de que insurgentes en teatros de operaciones de Iraq y Afganistán podrían estar utilizando software comercial para recibir la señal de video que los aviones no tripulados (UAV) de las tropas internacionales están enviando a sus centros de mando y control. La interceptación de la señal no conllevaría el control de los aparatos, sino que aprovecharía la falta de encriptación del envío de información desde el aparato a tierra para *piratearlo*, de manera que las pantallas de los insurgentes *verían* lo mismo que las pantallas del ejército.

En la misma línea de *interceptaciones aéreas*, un experto de la compañía de ciberseguridad española **S2Isec** ha demostrado [nuevamente](#) en la conferencia *Back Hat* de seguridad en la información, celebrada a principios de febrero en Arlington (EE.UU.) como acceder, igualmente con software comercial, a señales de conexión a internet por satélite. El esquema sirve a *hackers* para lograr un gran ancho de banda de manera gratuita e ilícita, pero también para utilizar la señal del satélite para navegación anónima por la web, acceder a redes privadas o suplantar webs con fines fraudulentos.

e-Olimpiadas 2012

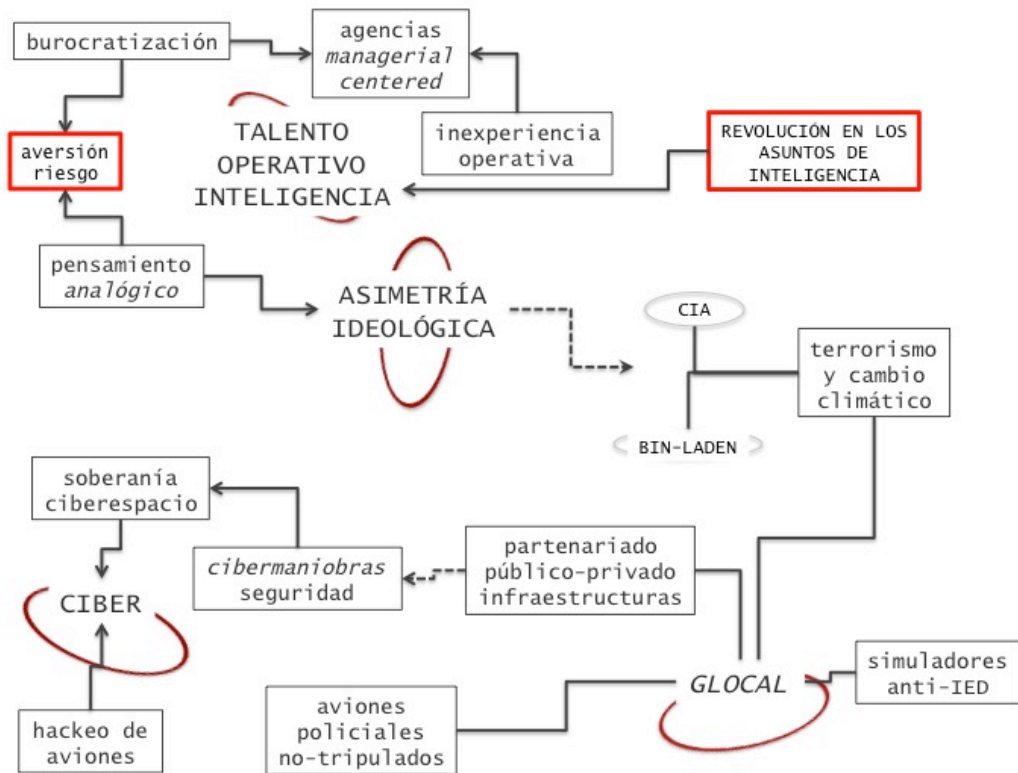
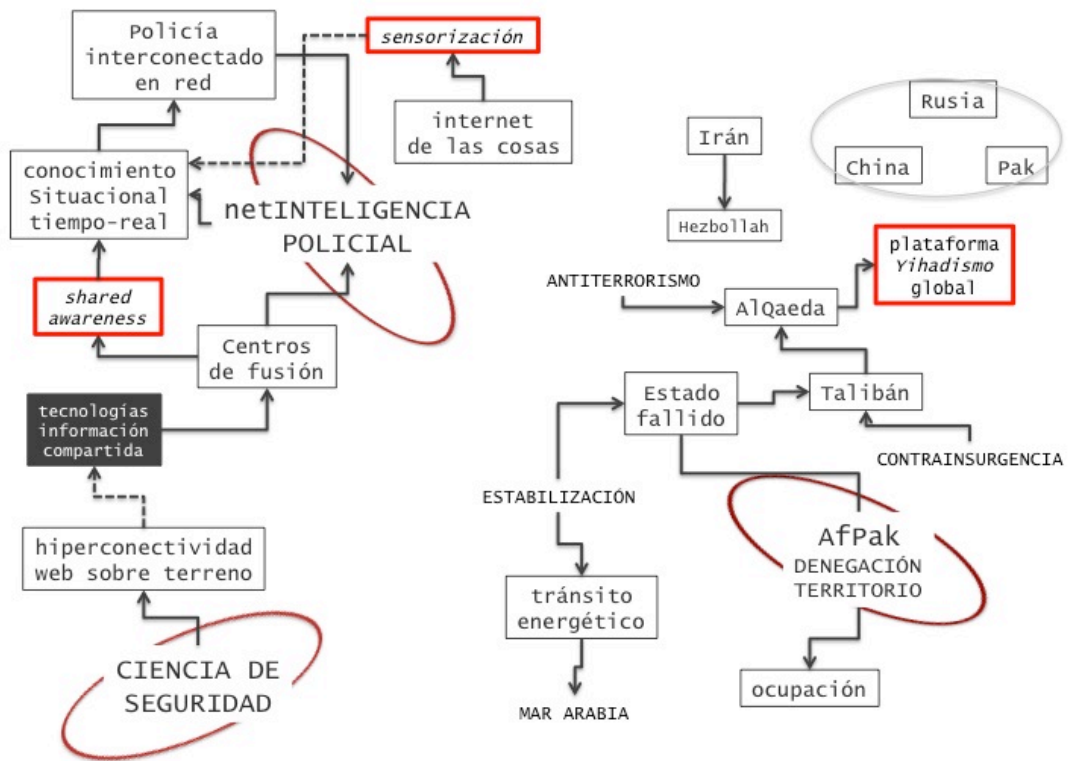
La policía de Londres (*Scotland Yard*) está organizando dos Equipos Olímpicos contra el Delito Cibernético (*Olympics e-Crime Teams*) pensados para reforzar el ciberespacio de las próximas olimpiadas que tendrán lugar en Londres 2012. Estos equipos tendrán como misión rastrear el ciberespacio en busca de operaciones del crimen organizado relacionadas con los juegos.

Uno de los equipos estará enfocado sobre intentos de hackeo de sistemas y esquemas de fraude; el otro sobre venta fraudulenta de entradas y sitios webs relacionados con el aparato comercial de los juegos.

Aunque el objetivo de esta operación es la detección de crimen convencional en la red, consolida la necesidad de desarrollar capacidades específicas para detectar actividades ilícitas en el ciberespacio a través de la organización de ejercicios que emplean la misma dinámica explotada por las amenazas en la red.

Estos equipos se adaptan al entorno y operan utilizando las mismas ventajas que brinda el ciberespacio, es decir la organización de tipo red, que es la misma que utiliza el cibercrimen organizado. Consiste en contrarrestar una amenaza con capacidades *simetrizadas*.

innograma





COPIA EL CONTENIDO CON LIBERTAD PARA TUS INFORMES
SI NO TIENEN NI TIENES ANÍMO DE LUCRO.

[S] es una publicación quincenal sobre innovación en seguridad editada por Thint Intelligence. Todos los derechos comerciales y de distribución reservados

[S] se elabora por analistas expertos en inteligencia y seguridad a partir de información de fuentes abiertas y recursos humanos sobre el terreno

[dirección postal]
Apartado de Correos 57219
28223 Pozuelo de Alarcón
(España)

[teléfono para suscriptores]
(34)618847366

[email para suscriptores]
suscriptor@s-guridad.com

[contacto general]
info@s-guridad.com

[patrocinios]
patrocinio@s-guridad.com

[website]
www.s-guridad.com

 **thint**