

[S]

PROSPECTIVA

INNOVACIÓN

SEGURIDAD



QOM

2[2010]

[15-30] enero

confidencial quincenal para suscriptores editado por [thint]

CONTENIDOS

Resiliencia Estratégica

p1

Las aproximaciones a la seguridad nacional comienzan a contemplar que cierto tipo de ataques serán inevitables. Por tanto, hay que prepararse para que los efectos sean mínimos y la recuperación rápida.

Inteligencia y AlQaeda

p2

La inteligencia contrainsurgente no es lo mismo que la inteligencia de operaciones militares. En Afpak confluyen los dos escenarios.

La revolución Flynn

p4

El informe Flynn sobre capacidades de inteligencia en Afganistán es revolucionario no tanto por su contenido, sino por la manera de elaborarse y difundirse.

Disuación Emocional

p7

El programa nuclear iraní no sólo tiene que ver con factores geoestratégicos, sino con la propia identidad iraní... la disuasión comienza a tenerlo en cuenta...

Terrorismo Organizado

p6

El terrorismo *yihadista*, al igual que las FARC colombianas, utilizan prácticas de crimen organizado para financiarse. La seguridad pública se adapta...

Ciencia y Tecnología

p9

El futuro nos adelanta tecnología para patrullado robótico de escenarios y visión inteligente que pueden combinarse para la acción preventiva.

Seguridad Glocal

p10

Coches con wifi // inteligencia forense // somalíes en Panamá // impuestos de seguridad // twitter anti controles de alcoholemia // ADN en piezas de coches robados

Ciberseguridad

p13

La manipulación y control en la red nos aproximan a una creciente dimensión de desinformación /// El Departamento de Defensa EEUU apuesta por la nube

Resiliencia Estratégica

La *resiliencia* es la capacidad de un sujeto y, por extensión, de un organismo o colectivo, para sobreponerse a un contratiempo o período de dificultad. En seguridad está identificada con la capacidad de recuperación ante un ataque y, más ampliamente estirando el concepto, con la reducción de vulnerabilidades ante las amenazas.

Actualmente, elaborar una estrategia de seguridad nacional no es en sí mismo un ejercicio innovador. Tampoco diseñarla en este momento supone para algunos países, como España, ir en exceso retrasados con respecto a otros. El Reino Unido, caracterizado siempre por la posesión de un renombrado pensamiento estratégico en sus instituciones, no sistematizó una estrategia formal hasta 2008. Lo que sí va a ir diferenciando a las estrategias o, por mejor precisar, a los enfoques de seguridad nacional de los países será su aproximación, su conceptualización, sobre qué ejes hacen pivotar sus capacidades o qué concepto o conceptos de fondo utilizan para apalancar el esfuerzo estratégico.

Aunque ya se ha empleado el término, por ejemplo, en enfoques sobre no-proliferación, utilizar la resiliencia como columna conceptual de un desarrollo estratégico integral para seguridad nacional es novedoso. Y lo es no tanto porque supondría que la capacidad básica de un colectivo frente a sus amenazas estaría pivotando alrededor de la creación de fortalezas (o la reducción de vulnerabilidades) para recuperarse ante eventuales ataques, sino precisamente por un hecho aceptado implícitamente en la adopción del concepto: **que los ataques, inevitablemente, se van a producir**. Este punto es revolucionario en términos estratégicos y, desde la perspectiva de las incertidumbres asociadas a las amenazas irregulares, bastante necesario en términos de preparación de la población hacia una nueva realidad de seguridad incierta o cambiante.

En el Reino Unido acaba de realizarse la propuesta. A punto de cumplirse dos años tras elaborarse y publicarse su Estrategia de Seguridad Nacional bajo el gobierno laborista de Gordon Brown, el Partido Conservador de David Cameron ha publicado un *green paper* bajo el título "[A Resilient Nation](#)".

Con independencia del signo político de los ponentes, la visibilización del concepto de resiliencia estratégica es novedosa, pero también lo es su desarrollo en la propuesta, que comienza identificando al Reino Unido directamente como una *global trading nation*, un punto de interconexión global para el comercio mundial. Este principio activador del pensamiento estratégico británico alrededor de su *salud comercial* conecta con los principios de inteligencia económica [España está por desarrollar su propio esquema nacional de inteligencia económica] que vinculan la promoción y protección de los intereses económicos de un país con el bienestar de sus ciudadanos... la asociación entre resiliencia económica o financiera y bienestar ciudadano aparece con claridad a primera vista.

Este pronunciamiento coincide con las informaciones que apuntan a la creación en el Reino Unido de un Consejo de Seguridad Nacional, similar al estadounidense y ya apuntado para España en el número 1 del informe [S]. La virtualidad de los consejos de seguridad nacional es que se convierten en los gestores del concepto diseñado de seguridad nacional para un país y de su aplicación a través de la estrategia, haciendo de *cámara de compensación* de las distintas fuerzas institucionales involucradas (interior y exterior, militar y policía, comercio y control) en la aplicación de la estrategia y, principalmente, interponiendo un cortafuegos político ante los primeros ministros o presidentes de gobierno.

Inteligencia y Al Qaeda

Estados Unidos tiene dos frentes abiertos en la lucha contra el terrorismo. Por un lado están los escenarios en los que el ejército estadounidense se enfrenta con un amplio despliegue de *yihadistas* vinculados con organizaciones locales cuyo principal interés es el control del Estado. Los casos más relevantes son Irak, Afganistán y Pakistán. Las acciones *yihadistas* en estos escenarios se caracterizan por infringir daños y provocar la muerte indiscriminada de civiles locales, fuerzas de seguridad locales y extranjeras. Se trata de acciones sistemáticas y cotidianas destinadas a desestabilizar las instituciones del Estado y a los ejércitos extranjeros que intentan sostenerlas.

Por otro lado, en estos mismos escenarios actúa la organización de Al-Qaeda cuyo apoyo logístico e ideológico está más orientado a atacar las tropas estadounidenses y/o cualquier otro interés Occidental que a las propias instituciones locales. Este tipo de acciones requiere una planificación exhaustiva que implica el estudio de las fuerzas enemigas, la preparación precisa de cada aspecto del atentado, y en la que se explotan al máximo el **simbolismo mediático** para provocar un efecto asimétrico en la sociedad de forma tal que un simple atentado tenga repercusiones en la estabilidad y la seguridad de todo un ejército o del mismo Estados Unidos en su conjunto.

El perfil de la actividad *yihadista* diseñada para crear inestabilidad cotidiana es el que día a día golpea a Irak, Afganistán y Pakistán. De acuerdo con los datos publicados por el *Worldwide Incident Tracking System* (WITS) del *National Counter Terrorism Center* (NCTC), desde enero a septiembre de 2009 se han registrado 665 incidentes en Afganistán y 223 en Pakistán organizados por los Talibán (de un total de 1387 incidentes), 31 incidentes en Pakistán organizados por *Tehrik-i-Taliban Pakistán* (de un total de 1097 incidentes), 91 incidentes en Irak organizado por *Islamic State of Iraq* (de un total de 377 incidentes). La mayoría de los incidentes sin clasificar corresponden a grupos desconocidos que

operan de forma independiente o cuya vinculación con alguno de los grupos principales no es confirmada.

Este gran número masivo de actividad *yihadista* que se concentra en estos escenarios corresponde a la primera clasificación de amenaza *yihadista* a la que se enfrenta el ejército estadounidense. En esta categoría que engloba el 75% de toda la actividad terrorista no está incluida la organización de Al-Qaeda. Si bien es cierto que Al-Qaeda apoya a los Talibán y a la organización *Tehrik-i-Taliban Pakistán*, los atentados son llevados a cabo con recursos de estas organizaciones y la participación de Al-Qaeda es subsidiaria, es decir que su ausencia del territorio no mermaría la actividad *yihadista* en Afganistán, Pakistán e Irak.

En cambio el perfil de la actividad *yihadista* de Al-Qaeda es menos masivo y más selectivo. En el mismo período de enero de 2009 a septiembre de 2009 se han registrado 31 incidentes en Algeria (de un total de 59), 1 en Mali (de un total de 1), 3 en Mauritania (de un total de 4) y 2 en Níger (de un total de 2), organizados por Al-Qaeda en el Magreb Islámico. La tipología de estos incidentes es muy distinta a la actividad masiva de los principales escenarios en los que hay un despliegue militar estadounidense. En Algeria los atentados están dirigidos contra las instituciones locales, pero su actividad está limitada por los esfuerzos de las instituciones locales para contener esta amenaza. En el caso de los países del *Sahel* la actividad es prácticamente nula, comparada con el resto de escenarios, no obstante como la mayoría de sus acciones están dirigidas específicamente contra objetivos Occidentales, aunque también locales, ya sea a través de atentados contra la vida de las personas, o bien organizados en forma de secuestros prolongados, atraen mayor interés mediático y por lo tanto su influencia es asimétricamente mucho más considerable que la que ejercen los Talibán en Afganistán y Pakistán.

Estados Unidos se enfrenta al mismo tiempo a ataques masivos contra sus ejércitos y a ataques selectivos contra objetivos elegidos estratégicamente para ejercer presión mediática y desmoralizar la política de seguridad estadounidense. Se trata de **dos enemigos distintos** y por lo tanto requiere dos estrategias distintas. La lucha contra el terrorismo es la que tiene lugar en escenarios como Irak, Afganistán y Pakistán. El despliegue militar que se ha utilizado hasta el momento para contener esta amenaza se ha mostrado incapaz de contener a un enemigo invisible capaz de aprovechar al máximo las ventajas de la guerra asimétrica. Irak, Afganistán y Pakistán se han transformado en escenarios altamente inestables, resistentes al despliegue de tropas extranjeras, y con una capacidad de desgaste atemporal que hace aún más evidente la asimetría entre ejércitos dirigidos por estrategias con tiempo de caducidad frente a ejércitos de terroristas despreocupados por el tiempo terrenal.

Por otro lado, la lucha contra el terrorismo de Al-Qaeda es más estratégica y depende exclusivamente de los servicios de inteligencia. Son éstos los que están mejor capacitados para contener la amenaza y eventualmente neutralizarla. Aplicar la misma estrategia de

**la necesidad de
simetrizarse ante la
asimetría de la amenaza
ha llevado a los EEUU a
concentrar gran parte de
sus capacidades en
fuerzas especiales.**

**Obama prevé un
incremento de 58 mil a
72 mil efectivos del Joint
Special Operations
Command en Florida**

despliegue militar para contener a una organización tan dispersa física e ideológicamente sería un error estratégico. La mejor forma de contener esta asimetría es concentrar todos los esfuerzos para que los servicios de inteligencia sean, en primer lugar, capaces de anticiparse a los intentos de atentados, y en segundo lugar, capaces de desarticular sistemáticamente a los individuos o grupos de individuos que se adhieran a la ideología de Al-Qaeda y estén dispuestos a actuar en su nombre.

Yemen no debería convertirse en un nuevo escenario de actividad *yihadista* masiva. En el período de enero de 2009 a septiembre de 2009 se han registrado 3 incidentes (de un total de 4) organizados por Al-Qaeda en la Península Arábiga. Se trata de un escenario de tipo selectivo, por lo que la mejor estrategia es la explotación de los servicios de inteligencia y descartar cualquier tipo de despliegue militar. Estados Unidos no debería cometer el error estratégico de concentrar un nuevo foco de desgaste militar y político, y un nuevo escenario en el que *yihadistas* de todo el mundo se concentren para atacar a Occidente. No debería suceder que un simple intento fallido de atentado, con un costo ínfimo para Al-Qaeda, sea capaz de provocar una respuesta que costará muchísimo a la comunidad internacional. La asimetría entre causa y efecto debería alertar para que la respuesta de Estados Unidos sea también selectiva.

Tampoco es comprensible por qué tendría más trascendencia un escenario como el yemení frente a otro como el somalí cuya actividad *yihadista* en el período de enero a septiembre de 2009 registró 157 incidentes organizados por *Al-Shabab* (de un total de 315). No significa que en Somalia debería desplegarse capacidades militares, sino que en ambos casos, y en especial en los que participa Al-Qaeda, se debería contener la necesidad de una respuesta contundente e inmediata por otra a largo plazo y estratégicamente selectiva para desarticular las organizaciones y sus aliados sin provocar escenarios de inestabilidad e inseguridad. Y a pesar de que los servicios de inteligencia estadounidenses se han visto cuestionados por la falta de coordinación de la pasada navidad, son la mejor estrategia para contener una amenaza asimétrica y selectiva como la de Al-Qaeda.

La revolución Flynn

Un innovador informe ha sido publicado en enero de 2010 por el think-tank estadounidense Center for a New American Security. Está firmado por tres militares especialistas en inteligencia y en activo, siendo uno de ellos un general y otro un agente senior de la Agencia de Inteligencia de Defensa. El general es además *Michael T. Flynn*, Jefe de Estado Mayor para inteligencia de la Fuerza ISAF para Afganistán, es decir, el responsable de inteligencia en las operaciones militares de la OTAN en Afganistán.

El informe, titulado [*Fixing Intel: a Blueprint for Making Intelligence relevant in Afghanistan*](#), es innovador ya antes incluso de entrar en su contenido. Las reflexiones de Flynn, Pottinger y Batchelor son revolucionarias porque han sido producidas en abierto, por tres militares en activo (uno de ellos general de división), aplicando análisis profesional y enfocándolo sobre lo que en el imaginario popular y en la mayoría de los profesionales se ha considerado siempre que debe quedar en el ámbito de lo reservado: la inteligencia... y no una inteligencia cualquiera, sino aquella referida a un teatro de operaciones en activo. Sólo recurriendo a pensar que el propio informe es un ingrediente de una operación de información en sí misma es como se entendería que el análisis publicado se ha ajustado al marco mental y procedimental dominante en estas disciplinas. Sino es así, es auténticamente revolucionario en su aparición.

En todo caso, forme parte del esquema intencional que sea, el informe Flynn, que ya en su contenido propugna una masiva utilización de las fuentes abiertas de información para comprender la realidad afgana, supone la utilización de esas mismas fuentes abiertas para difundir un análisis crítico de primer nivel sobre un conflicto activo en curso. Es decir, si bien en los últimos tiempos hemos venido asistiendo a una emergencia significativa de la inteligencia de fuentes abiertas (OSINT) en la recogida de información para su

análisis, el informe Flynn también supone centrar la diana en otro de los procesos ligados al ciclo de inteligencia de fuentes abiertas: la difusión de inteligencia. Y este aspecto aunque pudiera parecer superficial entendemos que es crítico, pues supone modificar el concepto de cliente o consumidor del producto de inteligencia. Con el informe Flynn ya no suponemos a la línea de mando militar o política, o al presidente Obama, como consumidores de la inteligencia elaborada y difundida, sino a toda la sociedad, aunque especialmente, con toda seguridad, a aquellos que pueden ejercer algún tipo de influencia creando opinión. Por más que las operaciones de información y decepción sean un clásico, el informe Flynn tal como se ha escrito y difundido representa también, pues, un **cambio sustancial en la difusión y consumo de inteligencia**, entendiendo que el consumidor es social, global y abierto, y también la influencia que genera (y las decisiones que provoca). Por supuesto, este ensachamiento en el *cliente* de consumo también tendrá efectos en la contrainteligencia desplegada por las amenazas.

El informe Flynn también considera una reordenación del tradicional consumidor de análisis en su arquitectura de inteligencia para Afganistán, pues lejos de establecer una pirámide jerárquica (se obtiene sobre el terreno, se produce por los analistas y se consume por los mandos) propone una actuación en red en donde el producto de inteligencia está distribuido, de forma que se forma una especie de **malla integrada de conocimiento situacional en red**.

Respecto del contenido, la innovación es menor, aunque muy válido en cuanto a destacar lo que le falta a la inteligencia en un teatro de operaciones militares con distintas dimensiones complejamente entrelazadas de desarrollo en Afganistán. La tesis de Flynn, Pottinger y Batchelor es, en síntesis, que más allá de la inteligencia destinada a operaciones militares sobre el terreno, en Afganistán está

fallando el enfoque de inteligencia destinado a fraguar la estrategia de estabilización diseñada para Afganistán. Con independencia de que el presidente Obama se haya expresado en el sentido de que la estrategia para Afganistán no es democratizarlo sino combatir a AlQaeda, el informe Flynn subraya que la manera de lograr el éxito de una operación sostenible de estabilización pasa por obtener y elaborar inteligencia hacia esa estabilización. En realidad lo planteado por Flynn no contradice a Obama, puesto que la estabilización, aunque no sea con vistas a la democratización del país, sí es necesaria para conseguir otro de los objetivos estratégicos de Obama, a saber, que Afganistán se haga cargo de su propia seguridad en un marco de estabilidad regional.

La **inteligencia estratégica de estabilización** no se limitaría a la inteligencia militar o a la tradicional contraterrorista, más enfocadas a las operaciones de combate o a las contrainsurgentes, sino pasaría por la construcción de una estructura de recogida y análisis de inteligencia que confluyera hacia unos centros de información de operaciones (*Stability Operations Information Centers*) de estabilización destinados a obtener un continuo y completo conocimiento situacional de la realidad del territorio, incluidas todas las dinámicas sociales involucradas y más allá de las operaciones militares.

El informe Flynn insiste en que la estructura de inteligencia que propone emplee a órganos de obtención y análisis desplegados en red por el territorio y que actúen como células de conocimiento locales, entendidas como **órganos de comprensión de la realidad**. Es llamativo, y en eso sí proporciona un salto conceptual sobre

las doctrinas dominantes, que el informe Flynn mencione a los analistas -en todo momento de una procedencia multidisciplinar, y no sólo militares o agentes de inteligencia tradicional- como si fueran ellos mismos órganos de obtención, a la manera de una figura híbrida que no sólo obtiene la información sino que es capaz de hacer una interpretación analítica dirigida a un consumidor.

El enfoque Flynn, aunque novedoso en su puesta en escena, es de sentido común en inteligencia. Si el objetivo es estabilizar, no militarmente sino institucional y socialmente el territorio, antes es necesario comprenderlo... y para comprenderlo, es privativo obtener información multidimensional y, sobre todo, culturalmente sintonizada. De este modo podrá producirse, por analistas también multidisciplinares, una interpretación integral y compleja de la realidad que lleve a decisiones más ajustadas. Es más, ese tipo de interpretaciones culturalmente amplias también ayudarán a la inteligencia contrainsurgente a diseñar operaciones más efectivas

Desde hace más de una década, y sobre todo desde la emergencia de las operaciones de mantenimiento de la paz, se viene hablando ya en doctrina de inteligencia de lo que se conoce como **socio-ethnic intelligence**, aquél tipo de esfuerzo de inteligencia destinado a conocer y comprender las claves sociales del área de operaciones [y estas operaciones ya pueden ser militares, policiales o, incluso, económicas] en orden a tomar decisiones sobre cursos de acción eficientes y efectivos. Lo que hace el informe Flynn es recordárnoslo haciendo uso de mecanismos de difusión globales en una audiencia de inteligencia también global.

publicidad



INTELIGENCIA COMPETITIVA | INTELIGENCIA DE SEGURIDAD

[S]

2[2010] enero

Terrorismo Organizado

La piratería en Somalia y la industria del secuestro en el *Sahel* y en los principales escenarios de la *yihad* son algunos indicadores de que las organizaciones terroristas podrían estar buscando en el crimen organizado nuevas ideas para la financiación de sus actividades.

En informes de la Agencia Antidroga de Estados Unidos (DEA), que citaron dos congresistas estadounidenses a principios de este año, para solicitar que se incluyera a Venezuela en la lista de países promotores del terrorismo, se describieron asimismo los contactos que tuvieron las FARC (Fuerzas Armadas Revolucionarias de Colombia) con al-Qaeda para establecer una ruta de tráfico de droga que iría desde Colombia vía Malí hacia España. De acuerdo con los mismos informes, la **simbiosis** entre las actividades del crimen organizado y las posibilidades de las organizaciones terroristas aportarían a las FARC nuevas vías de acceso para la introducción de drogas en Europa, y nuevas fuentes de financiación para al-Qaeda.

Esta derivación hacia el terrorismo organizado no es nueva. Las FARC nacieron originalmente como una organización terrorista, con una ideología contraria al Estado y con la clara intención de controlar al mismo, pero poco a poco, a medida que la ideología se hizo menos realizable, sus actividades fueron derivando hacia el crimen organizado, primero como fuente alternativa de ingresos económicos, y posteriormente como actividad principal.

En el *Sahel*, por ejemplo, la combinación de un escenario en el que las instituciones del Estado son débiles o incapaces de controlar la seguridad de sus territorios, en el que la actividad *yihadista* no produce el efecto desestabilizador deseado, y en el que la comunidad internacional no tiene especial interés geoestratégico, y por lo tanto no interviene activamente, las organizaciones terroristas encontrarían en el crimen organizado

una actividad que podría producir el efecto de desestabilización deseado, trascendencia mediática internacional, atraerían la atención de la comunidad internacional, y además obtendrían beneficios económicos, ya sea para sostener sus operaciones en el tiempo a la espera de una coyuntura geopolíticamente más propicia para sus intereses, o para contribuir con la financiación de la *yihad* global.

Organizaciones como *al-Qaeda en el Magreb Islámico*, y sus facciones en el *Sahel*, están utilizando muy hábilmente esta posibilidad dual del terrorismo organizado. Las actividades delictivas que están realizando, en especial los secuestros, consiguen al mismo tiempo el efecto mediático deseado de un atentado terrorista, y los beneficios económicos de una actividad delictiva muy rentable.

Y aunque estas actividades tienen un punto débil, ya que requiere un tipo de organización jerárquica y un despliegue logístico menos invisible que el de las células terroristas, proliferan en espacios en los que no llega el control del Estado. Las actividades en el *Sahel* demuestran una vez más la capacidad de adaptación de Al-Qaeda a los distintos entornos en los que opera. Probablemente sea éste el 'éxito' de su expansión global y lo que garantice, a largo plazo, su permanencia entre las principales amenazas a la seguridad y estabilidad internacional.

Preet Bharara, el Fiscal de los EEUU en Manhattan (NY) está fusionando dos unidades policiales especializadas bajo su jurisdicción, la *Terrorism and National Security* con la *International Narcotics Trafficking*, para actuar integradamente en investigaciones sobre grupos y células terroristas, especialmente las *yihadistas*

Disuasión Emocional

La primera reacción del gobierno de Irán de acusar a Estados Unidos e Israel de estar involucrados en la muerte, por atentado con bomba, del físico nuclear *Massud Alí Mohamadi* forma parte de la retórica que se espera de un gobierno que se siente amenazado y perseguido por sus enemigos, y cuya estabilidad interna podría recuperarse si el pueblo iraní se manifiesta unido frente a un enemigo común.

Aun se desconocen quienes fueron los autores del incidente y aunque Irán culpe a Estados Unidos e Israel, no se descarta que detrás de este atentado esté el grupo contrario al régimen teocrático iraní *Mujahidin Jalq*. Pero lo más relevante sobre este hecho es que el gobierno de Ahmadinejad intentará fortalecer la cohesión interna, en un contexto de inestabilidad política, sobre la amenaza de dominación extranjera, y en especial sobre la necesidad de un programa nuclear iraní que le otorgue preponderancia respecto a otros Estados.

Actualmente, en un escenario de mínimos, el objetivo de la capacidad nuclear iraní para uso civil es un hecho probado. Sin embargo, desde que en 2002 se descubrieron los planes secretos del programa nuclear no se han encontrado evidencias significativas para rechazar la hipótesis de que dichas capacidades tuvieren un destino militar.

¿Qué hacer entonces con un Irán nuclear? ¿Qué diferencia tiene un Irán nuclear respecto a otras amenazas reales como Corea del Norte? ¿Por qué la amenaza de un Irán nuclear y de la posibilidad de que estas capacidades acaben en manos de *Hezbollah* es distinta de la posibilidad de que los *Taliban* accedan al control de la capacidad nuclear pakistaní?

Con estos interrogantes no se pretende justificar un nuevo actor nuclear en el mundo, y menos aún en un contexto en el que las dos

principales potencias nucleares están en procesos de negociación para reducir sus arsenales. De cumplirse estos pronósticos de un Irán nuclear, o de cualquier otra nueva potencia nuclear, se trataría de una **involución** del sistema internacional, o visto de otra forma, una evolución con 50 años de atraso. Los interrogantes planteados sirven para señalar que un Irán nuclear es un futuro posible.

Si a este escenario se suma que la política exterior e interior iraní está guiada principalmente por un sentimiento de inferioridad respecto al resto de potencias mundiales, en especial de Estados Unidos e Israel, por lo que Irán fue en su momento y pretende ser en el futuro, y a la sensación de humillación y decadencia en la que está sumido tanto Irán como el Islam, la racionalidad deja paso a las emociones en la toma de decisiones, y de ser así, la contención y la disuasión, ambos elemento puramente racionales, dejarían de ser efectivos para un Irán que quiere recuperar protagonismo mundial. La posibilidad de que se utilicen armas de destrucción masiva se convierte en una realidad posible y preocupante. La administración Obama ha captado esta particularidad y desde que asumió la presidencia de Estados Unidos incorporó en su discurso el elemento emocional para establecer un *status quo* de contención y disuasión que anule las capacidades iraníes sin desafiar su poderío, sin entrar en conflicto directo, y sin que el pueblo iraní se sienta de alguna manera humillado o en posición de inferioridad.

Esta política no evitará que Irán continúe desarrollando su programa nuclear para uso militar. Tampoco evitará un posible ataque preventivo contra las instalaciones iraníes. Si esta estrategia tiene éxito en contener y disuadir a Irán para que no haga uso de su armamento nuclear, servirá simplemente como precedente para demostrar que la racionalidad en la toma

de decisiones, en algunos casos, debe incorporar un componente emocional que tenga los mismos efectos de contención y disuasión ante actores estatales (y no estatales) que actúan guiados por emociones como el orgullo, la humillación o el sentimiento de inferioridad.

Pero esta estrategia tiene inconvenientes. El exceso de precauciones a la hora de manifestarse sobre un asunto de política internacional coartaría las libertades de expresión y opinión ante el temor de una respuesta violenta desproporcionada. Asimismo, la amenaza de una respuesta violenta, como así también el uso, o amenaza de uso, de poder como medio de coerción ante un 'agravio' de los sentimientos de un Estado es una **incoherencia** para la razón y una involución también en el sistema internacional. Si bien es conveniente tener en cuenta las emociones de los actores del sistema internacional, las acciones no deben estar guiadas exclusivamente por las emociones

sino por la proporcionalidad de la razón, por el respeto mutuo y por la libertad de expresión. La principal amenaza a la seguridad internacional no es un nuevo Estado con armamento nuclear, sino un Estado que sea capaz de actuar guiado por sus emociones.

La razón debería contener, pero no anular, a las emociones. Como afirmó Aristóteles en el punto medio está la virtud del hombre. La comunidad internacional debe continuar con sus esfuerzos de contener por todos los medios el expansionismo nuclear de Irán, pero aceptando que tarde o temprano Irán conseguirá dicho armamento. Mientras tanto, la mejor estrategia de la comunidad internacional es que hasta que llegue ese momento, en el que se confirme la posesión de armamento nuclear, los intentos de contención y disuasión no hayan exacerbado mucho más las emociones iraníes. La mayor prioridad es evitar que Irán se convierta en una potencia nuclear emocionalmente inestable.



Thaler, David E., et. al. 2010: [Mullahs, Guards and Bonyads - an Exploration of Iranian Leadership Dynamics](#). Rand National Defense Research Institute.

[S]uscripción

El formulario para [S]uscriptores ya está disponible en http://www.s-guridad.com/iS_formulario_suscripcion.doc

El régimen de suscripciones para el informe [S] se ha establecido bajo dos parámetros: 1) garantizar la independencia de las reflexiones y análisis y, por tanto, servir el mayor valor a los profesionales que eligen [S] como medio complementario para sus propios pensamientos e ideas sobre la seguridad; 2) compensar una asequible cuota anual para las suscripciones personales con una incrementada, aunque muy razonable, cuota para las suscripciones institucionales.

A partir del número 5 (15 marzo 2010) [S] será distribuido exclusivamente a suscriptores. Las suscripciones realizadas antes del 1 de marzo de 2010 tendrán un descuento del 25% sobre su precio.

Robots de Vigilancia

El parque científico y tecnológico de Albacete en España acoge a la empresa *MoviRobotics*, diseñadora y constructora de *mSecurit*, un vehículo robot de vigilancia con capacidad para realizar rondas en exteriores de forma semi-autónoma, detectar intrusos y dar la alarma al centro de control.

En el marco de lo que se viene conociendo como vehículos robots inteligentes (UGV) dentro una dimensión de inspección preventiva, *mSecurit* está dotado de un sistema de navegación que le permite evitar obstáculos y operar en condiciones de oscuridad, humo, polvo o niebla.



MoviRobotics ha desarrollado además, junto al Centro de Excelencia de Software Libre de Castilla la Mancha, un paquete software denominado *MolinuxLITE*, basado en código abierto Linux y destinado a aplicación en proyectos de robótica y visión artificial como los UGV. La apuesta innovadora de esta empresa española la sitúa en la senda de los proyectos tecnológicos globales avanzados en seguridad.

Visión del comportamiento

La Universidad Autónoma de Barcelona ha desarrollado un nuevo sistema de visión por ordenador capaz de prever ciertos tiempos de movimientos corporales humanos. El sistema ha sido bautizado como Hermes y el proyecto, financiado por el Sexto Programa Marco de I+D de la Unión Europea, está dirigido por Juan José Villanueva.

El esquema tecnológico está basado en la detección de movimientos a través de cámaras y en la interpretación de su significado a través de algoritmos de manera que, a partir de un conjunto de reglas, es capaz de deducir si el movimiento detectado es anómalo en función del contexto. El sistema dispone de cámaras estáticas y activas de alta resolución con sensores de inclinación horizontal y vertical con zoom que permiten realizar el seguimiento de los objetos que aparecen en una escena.

Este proyecto se inscribe en la tendencia actual de percepción automática inteligente a través de robots y, una vez alcanzados los escalones tecnológicos de interpretación adecuada de movimientos anómalos, tendrá su futuro en dispositivos móviles, como el desarrollado por *MoviRobotics*, combinados con sistemas 3D, como los estadounidenses *Canesta*

Coches 3.0.....

Uno de los escenarios emergentes para la seguridad del futuro es el derivado de la denominada *Internet de las Cosas*, un esquema multipunto-multipunto en donde no sólo las personas estarán conectadas a la web, sino también las cosas, comunicándose bien con las personas (*people-to-machine*, P2M) bien las cosas o máquinas entre sí (M2M). Por simplificar, será ese escenario en donde podamos gobernar nuestros electrodomésticos en casa a través de la web vía *smartphone* mientras estamos en una reunión de trabajo o en una escapada de fin de semana en la playa. Nuestros vehículos, coches, motocicletas o camiones no serán ajenos a esa realidad de la que será la web 3.0.

Durante la primera semana de enero, el *Consumer Electronics Show* de las Vegas (EEUU) ha mostrado por dónde avanzan las tendencias en lo que a introducción de la web en los vehículos se refiere, en principio tomando como trasfondo lo que se denomina *infotainment systems* (dispositivos que mezclan entretenimiento con diversión).

En esta feria especializada se han mostrado consolas incrustadas en el salpicadero de los vehículos desde las cuales

los usuarios. Más allá de los tradicionales sistemas de navegación, las nuevas consolas son unidades de conexión a Internet en cuyo diseño y manufactura ya estarían participando compañías como Intel (microprocesadores) o Google (software y conectividad). Las consolas incorporarían capacidades wi-fi y puertos USB.

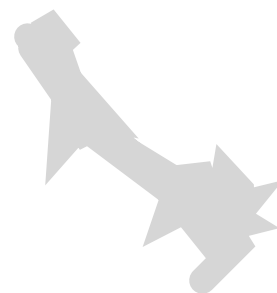
En principio, los dispositivos llevan instalados sistemas de seguridad que previenen la activación de algunas funciones (como el visionado de video) cuando el vehículo

está en movimiento, pero no otras como la consulta de información sobre restaurantes o sobre música.

Esa web 3.0. que nos anticipan, entre otros, estos dispositivos móviles ligados al vehículo necesitará una seguridad 3.0., no tanto por todo lo relativo a la ciberseguridad, sino porque se crea una nueva dimensión en donde el usuario desarrolla conductas en la realidad física que requieren coberturas de seguridad que integran a la denominada seguridad lógica (o de las tecnologías de la información) con la tradicional seguridad física (o de las personas y bienes).

Así las cosas, mientras en un número creciente de países los protocolos de seguridad vial apuestan por restringir las **distracciones** del conductor, las evoluciones del Internet de las Cosas crean nuevas dimensiones de realidad ante las cuales la seguridad como diseño tendrá, también, que evolucionar.

la evolución de la sociedad hacia la interconexión en red (sociedad red) está reclamando la emergencia de una disciplina de diseño de seguridad, que sea capaz de interpretar la realidad compleja y aportar soluciones integradas que trasciendan los tradicionales compartimentos estancos



Inteligencia Forense

En su primer año de operaciones, el británico Servicio Nacional de Inteligencia Balística (*National Ballistics Intelligence Service-NABIS*) ha ligado más de 350 armas con hechos delictivos.

El NABIS fue establecido por el *Home Office* en noviembre de 2008 y está estructurado en tres áreas (Servicios Forenses, Inteligencia y Conocimiento) más una serie de centros regionales en donde las policías locales pueden enviar sus muestras balísticas. El propósito del NABIS es conectar los puntos, conectar los indicios forenses con los hechos delictivos teniendo acceso a un mapa global de lo ocurrido en el Reino Unido en cuanto se refiere a la utilización de armas de fuego.

NABIS responde a la filosofía de establecer centros de fusión de datos para el conocimiento

situacional (no es extraño que una de sus divisiones se denomine así, “conocimiento”) que sirve tanto a propósitos investigativos como de seguridad preventiva.

Además de la interconexión de las bases de datos policiales de huellas dactilares y ADN, en España existe en algún momento la intención de establecer una Agencia Nacional de Policía Científica que, si siquiera este modelo, además de un departamento de análisis forense serviría como centro de conocimiento forense integral de apoyo a las investigaciones, que si además conectara con otros centros de inteligencia criminal policial como la UCIC del Cuerpo Nacional de Policía, el SINVES de la Guardia Civil, el CICO de la Secretaría de Estado de Seguridad o los órganos de las Policías Autonómicas, representaría una arquitectura poderosa de apoyo a la investigación criminal.

Somalíes en Panamá

El 3 de enero de 2010 el Servicio Nacional de Fronteras de Panamá (SENAFRONT) arrestó a un grupo compuesto por nueve nacionales somalíes y un colombiano que trataban de cruzar ilegalmente la frontera por el puerto de Lajas Blancas, en la provincia oriental panameña de Darien limítrofe con Colombia.

La operación policial ha sido enmarcada en el tráfico ilegal de seres humanos. La provincia de Darien es lugar de trasiego habitual de multitráficos (armas, explosivos, dinero, drogas y seres humanos) con tránsito o destino en Panamá. Algo más de medio año antes y también en otro pueblo de la provincia de Darien, Chiman, fue interceptado un bote con once nacionales de Somalia a bordo, quienes manifestaron haber pagado a una red de contrabando de seres

humanos para ser transportados hasta Londres acabando en realidad en Panamá.

Aunque de momento no se han planteado conexiones con otras variantes de crimen organizado y los nacionales somalíes detectados en Panamá responden al patrón de inmigrantes traficados, es cierto que estos sucesos apuntan, de entrada, a la utilización de Panamá como punto de interconexión de rutas globales de tráfico. También que en Nueva York existe una amplia colonia de somalíes y varias operaciones de inteligencia policial han establecido vínculos entre algunos residentes de esas colonias y el grupo yihadista *Al-Shabaab*, que actúa como guerrilla por el control del territorio en Somalia y tiene conexiones con la urdimbre AlQaeda, entre otras, a través de Yemen.

Impuesto de seguridad

En el Reino Unido se están pensando gravar con una tasa impositiva local por parte de los ayuntamientos a los locales nocturnos que, por sus características como epicentros de problemas de seguridad, requieren una concentración adicional de servicios policiales para la prevención de hechos delictivos y alteraciones de la convivencia.

Esta medida pretendería tanto ejercer como elemento disuasorio como introducir una especie de responsabilidad social en los locales, de manera que compensaran al municipio el exceso de gasto en seguridad que sus actividades obligan a hacer a los ciudadanos.

Twitter anti-controles

El Departamento de Seguridad Pública de la Ciudad de México está promoviendo sanciones para las personas que utilicen mensajes a través del sistema de mensajería breve *Twitter* avisando de la disposición de controles de alcoholemia en la ciudad.

La advertencia fue realizada después de localizar una cuenta en *Twitter* que con 3.400 seguidores situaba las localizaciones de los puntos de control.

ADN en coches robados

En la ciudad estadounidense de Dallas han establecido una *task force*, denominada *Forensic Evidence Auto Recovery (FEAR)*, destinada a imprimir otro enfoque a las investigaciones sobre robos de vehículos.

La unidad FEAR no se concentrará en encontrar vehículos individuales, sino en aquellas localizaciones sospechosas de ser puntos de distribución de piezas que se derivan del desmantelamiento de vehículos robados. El esquema de investigación está sustentado en la utilización de pruebas de ADN para vincular piezas con sospechosos.

Desde el punto de vista legal, en el sistema penal estadounidense, este enfoque permitirá a FEAR imputar principalmente casos de crimen organizado vinculando a los sospechosos con distintos tipos de piezas asociadas a su vez a una variedad de vehículos robados.

El esclarecimiento de este tipo de robos en Dallas es del 11%, por debajo de la media nacional en los EEUU que está en el 13%. Según el Instituto Nacional de Justicia de los EEUU, actualmente se identifican más sospechosos utilizando la base de datos nacional del FBI que su base nacional de huellas.

El Emirato Saharaui de Al-Qaeda

La cadena de [TV Al-Jazeera](#) anuncia la formación por Al-Qaeda de un Emirato en Sáhara a partir de una escisión de la denominada *Al-Qaeda en el Magreb Islámico*. ¿Alguna vez *Al-Qaeda en Al-Andalus*?

Ataque a la legitimidad

Páginas webs oficiales del gobierno de Filipinas fueron objeto de ataques que alteraron el contenido y la información *on line*. Las consecuencias de este tipo de ataques no afectaron al normal funcionamiento del gobierno sino que simplemente provocaron molestias a los usuarios y a los miembros del gobierno.

No obstante, estos incidentes están siendo utilizados para cuestionar el escrutinio informático de las **próximas elecciones** que tendrán lugar en mayo de 2010. Si bien el gobierno insiste en defender la integridad de sus sistemas, analistas expertos sugieren que existen vulnerabilidades que permitirían a un atacante alterar los resultados electorales.

Muy probablemente el gobierno filipino utilizará este incidente para reforzar los sistemas de información, detectar y solucionar las vulnerabilidades. En el transcurso de los próximos meses previos a las elecciones se habrán resuelto la mayoría de los puntos débiles del sistema de escrutinio.

Pero la relatividad del ciberespacio hace posible que la sensación de vulnerabilidad del escrutinio electrónico, y la imposibilidad de otorgar absoluta certeza del correcto funcionamiento de los sistemas de información, resten legitimidad a los resultados electorales. Si además las votaciones electrónicas no se pueden reconstruir y/o verificar por medios no electrónicos la incertidumbre sobre la verdadera voluntad de la sociedad traería inestabilidad institucional al próximo gobierno electo.

Se trataría de una nueva dimensión de inseguridad en el ciberespacio que podría ser explotada por quienes no acepten los resultados de una votación electrónica. Una campaña de desinformación de estas características provocarían inestabilidad institucional a Estados que apuesten por estos métodos y que no sean capaces de contrarrestar la **desinformación** y brindar la suficiente sensación de seguridad a los electores como para que confíen en los resultados.

..... Gobernanza del ciberespacio

La seguridad del ciberespacio en el futuro va a depender en gran medida de cómo definan el ciberespacio las entidades estatales en un mundo basado en las fronteras. Las distintas evoluciones de Internet están creando, literalmente, una nueva dimensión que todavía estamos gobernando con **antiguas** reglas. Y, en esa nueva dimensión, gobernabilidad no significa concretamente control, sino creación de condiciones para el progreso en condiciones de seguridad y libertad de los ciudadanos.

En los EEUU existe un coordinador de ciberseguridad en la Casa Blanca; un mando de ciberguerra en el Pentágono (USCYBERCOM) por el que han pugnado el mando aéreo (que tiene el suyo en Lackland) y la Marina y que finalmente

dirigirá la propia Agencia de Seguridad Nacional; una División de Ciberseguridad en el *Homeland Security*; y un FBI con mandato para investigar cibercrimen y ciberterrorismo (y contraespionaje). Todo esto sin contar a la ciberinteligencia de la CIA. Un modelo antiguo para toda una nueva dimensión de la realidad.

Lo más extraordinario del ataque que ha sufrido - entre otras- *Google* recientemente en China ha sido la protesta oficial del Departamento de Estado USA ante el gobierno chino. Atacar a un país sin atacar *territorialmente* ese país es un nuevo modelo de conflicto que relaciona, en una nueva ecuación con incógnitas sin despejar, a la economía, la soberanía, la seguridad, la defensa y la diplomacia.

Realidad relativa

China vuelve a ser protagonista en el ciberespacio. Estados Unidos ha denunciado públicamente que intereses estadounidenses, en especial empresas estratégicas, han sido ciberatacadas desde China. Estos ataques son los mismos que Google y Adobe denunciaron recientemente. Según Google se trataron de ataques bien coordinados contra sus redes de información, contra su buscador en China, y contra algunas cuentas de Gmail pertenecientes a activistas de derechos humanos. Asimismo Google ha denunciado que otras 30 compañías también fueron víctimas de estos ataques, entre las que se encontrarían Yahoo, Symantec, Northrop Grumman (fabricante del B-2), Dow Chemical y Juniper Networks.

Por otra parte, el bufete de abogados *Gipson Hoffman & Pancione*, que inició recientemente una demanda contra el gobierno chino por espionaje industrial, también ha denunciado que fue víctima de un ataque a través de sus cuentas de e-mail.

Al mismo tiempo que Google hacía público las características de los ataques, China denunciaba también ser víctima de ciberataques contra su principal buscador *Baidu*. Según el gobierno chino, estos ataques fueron organizados presuntamente por el *Ejército Cibernético Iraní* y fueron de características similares a los que esta organización dirigió recientemente contra *Twitter* por su participación en las manifestaciones contrarias al régimen iraní.

El ciberespacio es un terreno inmenso y aun inexplorado totalmente por la estrategia, la inteligencia y la seguridad de los Estados y de las empresas. Es un entorno en el que florece la desinformación y la incertidumbre. Es también un espacio con unas **reglas muy distintas** a los tradicionales escenarios en los que se enfrentan las fuerzas de seguridad. La invisibilidad de las amenazas, la dificultad en rastrear la fuente de los ataques, y la posibilidad que tienen los

atacantes y atacados de explotar las técnicas de engaño y negación (*Deception & Denial*) hacen de INTERNET un espacio en el que la realidad, además de ser virtual, también puede ser relativa.

Por ejemplo, un ataque proveniente desde China hacia intereses estadounidenses tiene lógica ya que ambos países se disputan el poderío económico. Que los ataques asimismo se dirijan contra Google, en un entorno censurado y controlado por el gobierno chino, también tiene lógica ya que Google es una fuente de información cuyas libertades podrían menoscabar el control chino sobre el adoctrinamiento de su sociedad. El ataque contra el bufete de abogados, que está llevando la causa contra el gobierno y empresas chinas, también tiene lógica ya que hay intereses en conflicto y cualquier información que el gobierno chino pudiera obtener por esta vía podría significar una ventaja comparativa.

Pero el ataque contra el buscador chino Baidu, supuestamente organizado por el Ejército Cibernético Iraní, no tiene lógica en los términos habituales de una situación de conflicto. China e Irán no son enemigos ni compiten por su primacía. De hecho se suelen complementar mutuamente. China es uno de los países que representan las posiciones más moderadas sobre el programa nuclear iraní. Se podría decir que son países amigos. Por lo tanto el ataque no tiene razón lógica. Sería más lógico que el Ejército Cibernético Iraní atacase a Google o a cualquier otro objetivo en el ciberespacio que represente intereses estadounidenses.

Que no tenga lógica no significa que no haya sucedido o que no pueda suceder en el futuro. No todos los actos se rigen por la lógica. Pero el ciberespacio es un lugar en el que todo es relativo y la certidumbre sobre los detalles de un ataque es una utopía. Ante el conocimiento de un ataque, como por ejemplo el que denuncia

China sobre su buscador *Baidu*, cabría preguntarse si realmente tuvo lugar o, si no se trata de una campaña de desinformación oportunamente orquestada para contrarrestar las acusaciones de intromisión del gobierno chino en el ciberespacio estadounidense.

En este entorno no hay nada absoluto y mucho relativo. Tanto el acusado como el que acusa se puede escurrir en la imposibilidad de detectar con certidumbre el origen del ataque. Uno u otro podría afirmar que no es posible probar con certeza las acusaciones, o bien que el rastreo del origen del ataque que llevan hacia una dirección es también un ataque dirigido para desviar la atención del verdadero origen del ataque, etc. Es todo tan relativo que el paradigma para explicar la ciberseguridad debería incorporar, entre otros asuntos, las particularidades de las campañas de desinformación y el engaño y la negación como elementos fundamentales para entender la seguridad en el ciberespacio.

La era de la información abre camino a la era de la desinformación. Información encriptada, compartimentada, e incluso información falsa, complementarán las medidas de seguridad en los sistemas de información. Todo será relativo, y la incertidumbre prevalecerá sobre la certidumbre. Engañar y desviar la atención del enemigo será uno de los niveles adicionales de las políticas de ciberseguridad destinado a proteger los sistemas de información.

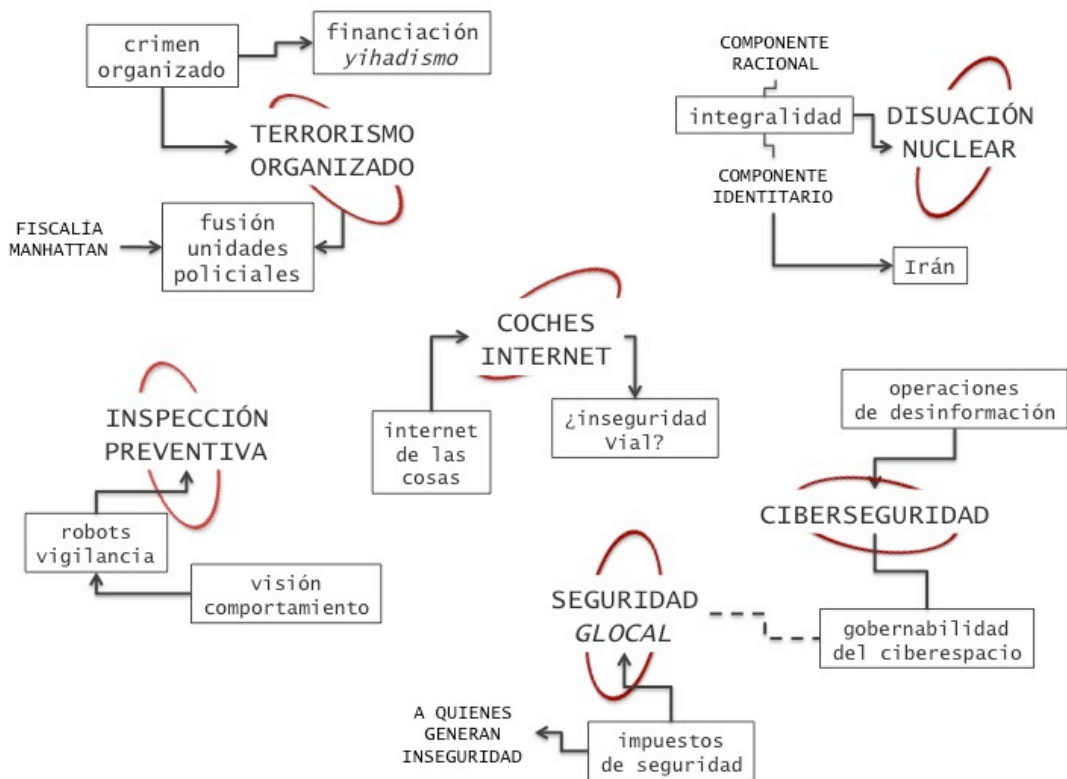
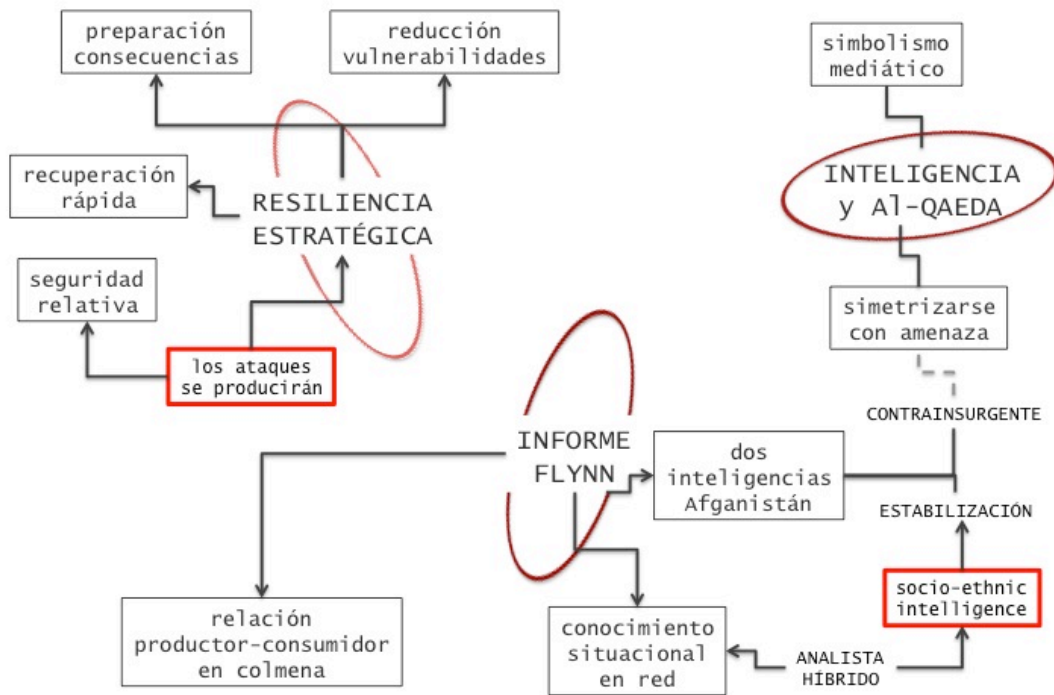
Rapid Access Computing Environment

A final de 2009 la *Agencia para los Servicios de Información de la Defensa (DISA)* de los EEUU divulgaba la nueva versión de arquitectura de computación en la nube que va a emplear en Departamento de Defensa (DoD). La han denominado RACE (esquema computacional de rápido acceso) y, en síntesis, está basado en suministrar software de manera “casi ilimitada”, en palabras del director técnico del programa en la DISA Henry Sienkiewicz, para las necesidades operativas de las unidades de defensa.

RACE está definido para que los usuarios establezcan unos requerimientos de capacidades software y estos puedan ser desarrollados y posicionados en la nube, de manera que se produzca <<que el desarrollo de software se incardine en el ciclo de toma de decisiones>>. RACE suministrará al DoD con plataformas software altamente estandarizadas en un ambiente virtualizado de bajo costo, total disponibilidad y con servicio técnico incluido.

La apuesta del DoD estadounidense por el *cloud computing* traslada el mensaje de que la tendencia a virtualizar el software está superando las prevenciones iniciales de seguridad que ocasiona(ba) este paradigma.

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

