Cooperación internacional en temas de *ciberseguridad*

Por Emilio Sánchez de Rojas Díaz

Capítulo quinto

Introducción

> *EE. UU. también debe hacerle frente a la amenaza real y creciente de los ciberataques. Sabemos que los piratas informáticos roban las identidades de personas y se infiltran en correos electrónicos privados. Sabemos que empresas extranjeras sustraen nuestros secretos corporativos y que nuestros enemigos buscan la capacidad de sabotear nuestra red de energía eléctrica, nuestras instituciones financieras y nuestros sistemas de control del tráfico aéreo. (Obama)*

«No podemos mirar hacia atrás en años venideros y preguntarnos por qué no hicimos nada ante las serias amenazas a nuestra seguridad y nuestra economía. Es por eso que hoy, más temprano, firmé un nuevo decreto ejecutivo que fortalecerá nuestras defensas cibernéticas aumentando el intercambio de información y desarrollando normas que protejan nuestra seguridad nacional, nuestros empleos y nuestra privacidad. Ahora bien, el Congreso también debe actuar aprobando las leyes que otorguen a nuestro Gobierno una mayor capacidad para proteger nuestras redes y disuadir los ataques» (1).

Australia (2009), Austria (2012), Canadá (2010), República Checa (2011), Estonia (2008), la Unión Europea (2013), Finlandia (2013), Francia (2011), Alemania, (2011), India (2011), Japón (2010), Lituania (2011), Luxembur-

go (2011), Nueva Zelanda (2011), Noruega, Polonia (2008 y 2011), Rumanía (2011), la Federación Rusa (2000, 2011), Eslovaquia (2008), Sudáfrica (2012), Suiza (2012), Países Bajos (2012), Uganda (2011), Reino Unido (2011), EE. UU. (2011)..., todos ellos forman parte del número creciente de países que están promulgando sus estrategias nacionales de seguridad. España lo acaba de hacer (31 de mayo de 2013). Muchas de ellas recogen en mayor o menor medida la necesidad de cooperación internacional; por ejemplo, la Estrategia Nacional de *Ciberseguridad* de los Países Bajos (2012) recoge entre sus «principios básicos» la «cooperación internacional activa»:

> *El carácter transfronterizo de las amenazas hace que sea esencial promover la cooperación internacional. Debemos aspirar a un campo de juego de nivel internacional. Muchas medidas solo pueden ser eficaces si se toman o son coordinadas a nivel internacional. Los Países Bajos apoyan y contribuyen activamente a los esfuerzos con la Agenda Digital de la UE para Europa y la Estrategia de Seguridad Interior; el desarrollo de la política de ciberdefensa de la OTAN como parte de su nueva visión estratégica; el Foro de Gobernanza de Internet, y otras asociaciones. Países Bajos defiende la amplia ratificación y aplicación del Convenio del Consejo de Europa sobre la ciberdelincuencia.*

Comienza la amenaza transfronteriza

Podría decirse que el primer *ciberataque* ocurrió en la Unión Soviética cuando en 1982 explotó un oleoducto transiberiano[1]. La explosión, registrada por satélites de EE. UU, fue calificada como «la explosión no nuclear e incendio más monumental jamás vistos desde el espacio» (2). Al parecer, la explosión fue causada por un *malware* informático implantado por la Agencia Central de Inteligencia en el *software* canadiense, previendo que el *software* sería obtenido ilegalmente por agentes soviéticos. La explosión ocurrió en la remota Siberia y no dio lugar a víctimas. El KGB, que pensaban que habían robado a los EE. UU. la tecnología de *software* más reciente, estaba avergonzado. Los hechos fueron ocultados y la URSS nunca acusó públicamente a EE. UU. de provocar el incidente (3).

Los ataques informáticos «blandos» contra los sistemas de EE. UU., como Internet, han crecido de manera exponencial en los últimos 25 años. Muchos de ellos intentaban obtener información confidencial o eran ataques de denegación de servicio, relativamente simples pero potencialmente devastadores. Entre los más dañinos se incluyen Moonlight Maze (1998-2001), que puso a prueba los sistemas informáticos gubernamentales y académicos de los EE. UU.; Code Red (2001), que introdujo un gusano

[1] Este hecho fue recogido por *The New York Times* en 2004 en el artículo «*The Farewell Dossier*» (Safire, 2004).

destinado a realizar un ataque de denegación de servicio contra los ordenadores de la Casa Blanca, y Mountain View (2001), una serie de intrusiones en los sistemas informáticos municipales de EE. UU. para recoger información sobre los servicios públicos, oficinas de gobierno y sistemas de emergencia. Aunque se especuló acerca de los orígenes, ninguno de estos incidentes pudo ser atribuido de forma incontestable a un actor estatal (3).

Hace unas semanas, el secretario de Estado de EE. UU. John Kerry criticaba los procedimientos de las elecciones presidenciales iraníes, de las que dijo no mostraban «ningún respeto por la voluntad popular». Describió las medidas del Gobierno iraní para frenar o cortar el acceso a Internet antes de la votación como «indicador de problemas» que privan a los iraníes de su capacidad de compartir información e intercambiar ideas.

Mientras Kerry estaba reprendiendo al régimen de Teherán, un agente de la CIA, Edward Snowden, estaba filtrando documentos al diario *The Guardian* que revelaban cómo la Agencia de Seguridad Nacional de EE. UU. (NSA) había estado espiando a la comunidad mundial de Internet desde 2007. Al participar en un programa secreto denominado PRISM, empresas estadounidenses como Google, Yahoo, Skype, Apple y Facebook, entre otras, dieron acceso directo a la NSA a sus sistemas, lo que permite la vigilancia de las comunicaciones en vivo y la información almacenada como historiales de búsqueda (4).

Dominios conectados globalmente

Los dominios conectados globalmente como el ciberespacio están siendo desafiados de forma creciente por actores tanto estatales como no estatales. Los actores no estatales como grupos terroristas, traficantes o la delincuencia internacional organizada están interesados en explotar estos dominios, mientras que ciertos países desarrollan actividades encaminadas a reducir la libertad de movimiento internacional.

La *ciberamenaza* se extiende y acrecienta por una falta de normativas internacionales, la dificultad a la hora de atribuir ataques, barreras de acceso débiles y una facilidad relativa para desarrollar capacidades de ataque potentes. Nuestra capacidad de operar en el ciberespacio dependerá de la colaboración entre agencias estatales, no gubernamentales, industria y actores internacionales en el desarrollo de nuevas capacidades, organizaciones y normas, de manera que seamos capaces de proporcionar un amplio abanico de posibilidades para asegurar nuestro propio acceso y uso del dominio del ciberespacio así como permitir la persecución de los actores maliciosos. Es necesario mejorar las capacidades de detección, disuasión, bloqueo de acceso y defensa en varias capas (5).

«Hay factores legales y tecnológicos que incrementan las posibilidades de que las *ciberamenazas* se materialicen», como recoge la Estrategia Española de Seguridad (2011):

> *Entre los primeros, la ausencia de una legislación común o de seguridad global que permita una lucha más efectiva contra ellas. Tecnológicamente, Internet fue creado para ser útil y sencillo, no para ser seguro. La creciente interconexión de la Red, incluyendo necesariamente las infraestructuras, suministros y servicios críticos, incrementa los niveles de riesgos sobre estos. El anonimato y la dificultad para rastrear los «ciberataques» son factores añadidos que entorpecen su neutralización (...). Los «ciberataques» más comunes tienen fines comerciales, pero también estamos expuestos a agresiones por parte de grupos criminales, terroristas u otros, incluso de estados.*

«La evolución del ciberespacio es demasiado rápida para hacer predicciones, pero es poco probable que las cuestiones de *ciberseguridad* disminuyan con el creciente consumo de las tecnologías de la información y las comunicaciones (TIC) en todo el mundo»; esto es lo que afirma la OCDE en su informe sobre *Futuros shocks globales* (2011):

> *A menos que el ritmo de los avances en la ciencia forense cibernética alcance la creciente facilidad de despliegue y la sofisticación de los ciberataques deliberados, seguirá siendo extremadamente difícil para las víctimas conocer la identidad de un atacante –lo que se conoce como problema de la atribución–. Esto quiere decir que una doctrina de defensa basada en la disuasión es menos probable que tenga éxito, y que ciertas partes malignas que actualmente carecen de la capacidad para poner en marcha un ataque a gran escala con éxito en el futuro puedan hacerlo.*

Otro informe también publicado por la OCDE, *Reducción del riesgo sistémico en ciberseguridad,* afirma que la cooperación internacional es una de las claves para reducir los riesgos de *ciberseguridad*. Los ataques contra los sistemas conectados a la Internet pública pueden originarse en cualquier parte de esa red. Los fallos en las infraestructuras de información esenciales en una nación pueden transmitirse en cascada en los sistemas dependientes en cualquier parte, pero aunque muchos organismos internacionales han emitido declaraciones de principios de apoyo mutuo y protección, no existe un mecanismo sustantivo o gobernanza internacional para resolver crisis relacionadas con ataques informáticos distintas de la estructura FIRST/CERT dominada por ingenieros (6).

Las principales mejoras que se podrían hacer serían aumentar el número de estados que forman parte del Convenio sobre la Delincuencia Cibernética, y así fortalecer los mecanismos de cooperación

internacional y desarrollo de capacidades. Sería particularmente útil que países con un gran número de usuarios de Internet, como Rusia y China, ratifiquen la convención sobre *cibercrimen*. Pero esto puede requerir flexibilidad por parte de los estados que forman parte actualmente para responder a las preocupaciones sobre soberanía de Rusia y otros (6).

Recientemente, hemos tenido un ejemplo de ataque con transmisión en cascada. Internet es un conjunto de redes independientes conectadas entre sí. CloudFlare dirige una red, Google dirige una red y los proveedores de ancho de banda como Level3, AT&T, y Cogent operan redes. Estas redes se interconectan posteriormente a través de lo que se conoce como relaciones de interconexión. Desde allí, nos conectamos con los puntos de intercambio de Internet (IXP o IX), una infraestructura física a través de la cual los proveedores de servicios de Internet intercambian tráfico entre sus redes (sistemas autónomos).

La mayoría de las ciudades importantes tienen un IX, que son diferentes en cada parte del mundo. En Europa funcionan algunos de los más robustos, y CloudFlare se conecta a varios de ellos. Un altercado entre un grupo *antispam,* Spamhaus, y una empresa holandesa que hospeda sitios *web*, CyberBunker, comenzó cuando Spamhaus situó a la compañía holandesa una lista negra de *spammers*.

El ataque fue escalando en intensidad y nivel, pasando a atacar a CloudFlare, la proveedora de nivel 3 de Spamhaus, y posteriormente a los proveedores de ancho de banda de CloudFlare, proveedores de ancho de banda nivel 2, que a su vez compran ancho de banda de los proveedores nivel 1 (aproximadamente una docena en el mundo). Además de atacar a líneas directamente dependientes de CloudFlare, los atacantes también lo hicieron sobre las infraestructuras IX de London Internet Exchange (LINX), Amsterdam Internet Exchange (AMS-IX), Frankfurt Internet Exchange (DE-CIX) y Hong Kong Internet Exchange (HKIX), alcanzando sus mayores efectos sobre LINX (ver gráfico).

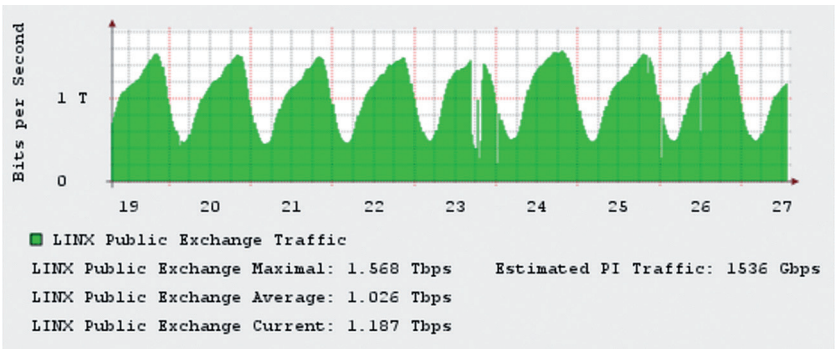


Figura 5.1. Impacto en el tráfico general (7).



Figura 5.2. Zona de concentración de ataques (7).

Para Matthew Prince, de CloudFlare, estos grandes ataques de nivel 3 son difíciles de detener. En pocas palabras: «Si tienes un *router* con un puerto de 10 Gbps y alguien te envía 11 Gbps de tráfico, no importa que dispongas de *software* inteligente para detener el ataque, porque tu enlace a la red está completamente saturado» (7).

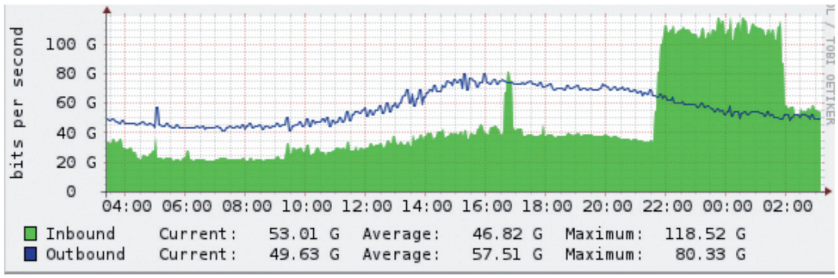


Figura 5.3. Impacto sobre el tráfico 2 (7).

Estos ataques han expuesto algunas vulnerabilidades en la arquitectura de algunos IX. Pero no dejará de impresionarnos cómo una riña entre empresas puede desencadenar el *ciberincidente* conocido de mayor intensidad, especialmente cuando este se ha atribuido a *hackers*.

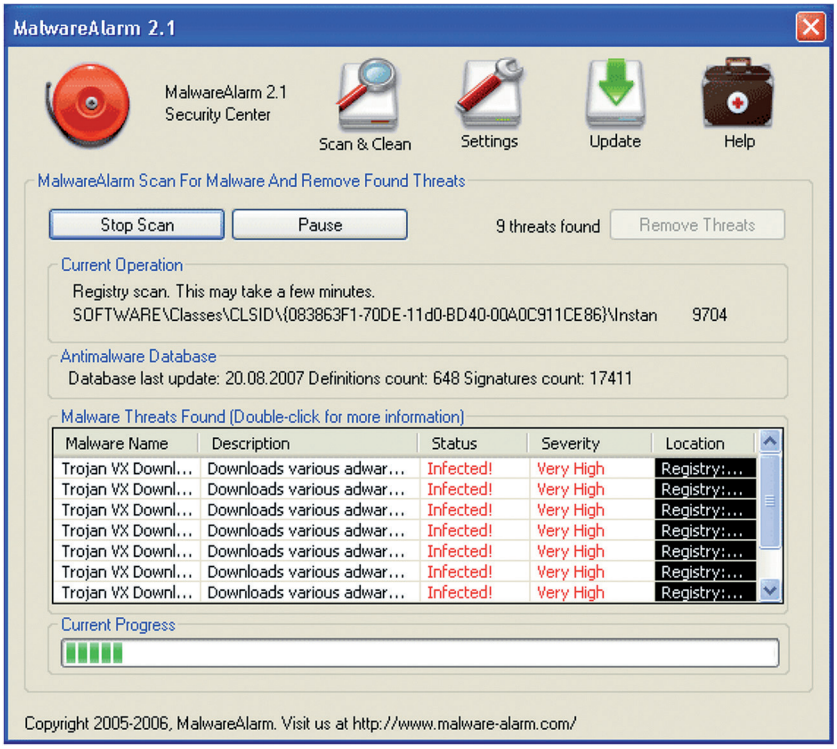


Figura 5.4. Pantalla que muestra los ataques (7).

Spamhaus

Fue un tipo de ataque *smurf* –«pitufos» en inglés– conocido como amplificación DNS. En los ataques *smurf*, enviando una pequeña cantidad de tráfico se consigue que llegue a la víctima mucho más tráfico. ¿Cómo protegerse de este ataque? Difícilmente, ya que el fallo está en equipos ajenos (y en el diseño inicial de Internet y el DNS, basados en gran parte en la buena fe) repartidos por todo el mundo que permiten ser usados como equipos *zombis* para un ataque. Además, los equipos *zombis* que se están usando no son una modesta *botnet* construida con equipos domésticos infectados y con una conexión ADSL: son miles de servidores con conexiones de alta capacidad (8).

El tratamiento de la «ciberdefensa» en las políticas de defensa

Uno de los elementos clave de la *ciberseguridad* es la defensa. El tratamiento de la *ciberdefensa* en las políticas de defensa puede variar de acuerdo con el «color político» de los Gobiernos. La dimensión *cíber* en las políticas de defensa puede depender de múltiples factores, como nos recuerda Daniel Ventre (9):

– El contexto internacional:

  • Los ataques contra Estonia se traducen en una fuerte conciencia de los desafíos para los estados que ha ido acompañada de la creación de instituciones dedicadas a la ciberdefensa (CCDCOE Tallinn).
  • La pertenencia a organizaciones internacionales (como la OTAN) impone directrices y medidas a los estados miembros.

– El contexto nacional e internacional:

  • Japón, país de alta tecnología, hiperconectado, cuya sociedad es probablemente una de las más «dependientes» del ciberespacio, tuvo que esperar hasta 2010 para desarrollar las políticas de *ciberdefensa*[2]. Es uno de los elementos que contribuyen a la reformulación de la política de defensa de Japón y supone una ruptura en cuestiones clave como un nuevo concepto de defensa dinámica para adaptar las fuerzas japonesas en el entorno geopolítico (aumento de las capacidades militares de China, la amenaza de Corea del Norte...).

– Los factores internos:

  • La crisis financiera en los países puede ser una razón para cuestionar los presupuestos destinados a la defensa. Bajo la presión de la opinión pública, se pueden reducir los presupuestos de defensa. Las *ciberamenazas* se pueden considerar como no prioritarias frente a otras contingencias inmediatas.
  • La imagen de la institución militar en la opinión pública puede influir también; una imagen positiva permitiría una mayor receptividad a la hora de obtener financiación.

Los principales actores nacionales

Aunque de hecho tengamos casi tantas aproximaciones como países a la *ciberseguridad*, podríamos definir tres cosmovisiones básicas; la *ciberliberal* defensiva, representada por la UE y compartida por casi todos los países europeos; la *ciberliberal* ofensiva, representada por los EE. UU., y la *cibernacionalista*-aislacionista, representada por China y Rusia. A ellas hay que añadir las que, como Irán o Corea del Norte, sin disponer de la sofisticación de las grandes potencias disponen de unas capacidades ofensivas que están dispuestas a emplear directa o indirectamente.

Rusia y China hicieron un gran esfuerzo para «capturar» el control de Internet en una reunión de la Unión Internacional de Telecomunicacio-

[2] Después de un cambio de Gobierno, cuando el Partido Democrático de Japón llegó al poder en 2009.

nes en diciembre de 2012 y con el objetivo de restringir el acceso a la información. Recibieron un sorprendente grado de apoyo. Muchos países están desencantados con el modelo ortodoxo de múltiples partes de la gobernanza de Internet, al que encuentran incapaz de satisfacer sus necesidades gubernamentales y de desarrollo, y se mueven en silencio hacia un modelo «no occidental» de la gobernanza de Internet. Los regímenes autoritarios se han percatado de esta insatisfacción y la intentan aprovechar para sus propios fines políticos. No ha habido casi ningún nuevo pensamiento en Occidente sobre la manera de ir más allá de la antigua ortodoxia de Internet; todo está diseñado para un momento en que el mundo todavía giraba en torno al Océano Atlántico (10).

El Gobierno de la India, junto con las organizaciones privadas, está poniendo en marcha varias iniciativas para combatir los *ciberataques*. Sin embargo, el mayor desafío que enfrenta actualmente el país es la falta de profesionales de la *ciberseguridad*. Según los últimos datos, la India tiene actualmente alrededor de 22.000 profesionales de la *ciberseguridad* certificados, número que es minúsculo en comparación con China, que tiene casi 25 millones de expertos en cibernética o comandos. Los expertos señalan que el país necesitaría 500.000 expertos de *ciberseguridad* en 2015 para proteger su infraestructura de TI. Como resultado, ellos creen que el país debe prepararse para crear un fuerte grupo de expertos de seguridad informática para fortalecer su espacio de *ciberseguridad* (11).

El Gobierno indio ha aprobado la propuesta de Política Nacional de Ciberseguridad, que está dirigida a la creación de un «entorno informático seguro y la confianza en las transacciones electrónicas adecuadas» (12). Entre las prioridades, figuran: «Acciones de mitigación proactivas, preventivas y reactivas para alcanzar y neutralizar las fuentes de problemas y el apoyo a la creación de un ecosistema global de seguridad, incluidos los acuerdos de colaboración público-privada; el intercambio de información; acuerdos bilaterales y multilaterales con los CERT en el extranjero, los organismos de seguridad y de los proveedores de seguridad...».

En el Reino Unido, no todos los *building blocks* para mover la arquitectura informática del Gobierno a una nube segura están todavía en su lugar. Durante la elaboración de la Estrategia Nacional de Seguridad, un desafío clave fue hacer que departamentos y empresas entendieran que la *ciberseguridad* debe ser entendida como vital para la prosperidad económica del Reino Unido y por ello requiere necesariamente la inversión de una amplia gama de actores. La orientación actual del Gobierno se basa en la seguridad perimétrica.

La seguridad perimetral tiene un defecto importante. Un informe del Centro para la Protección de la Infraestructura Nacional (CPNI) prevé que las mejoras en las medidas de seguridad perimetral solo serán graduales y

se verán emparejadas –si no superadas– por la evolución de los medios de ataque. Este es el riesgo común para la UE y gran parte de sus países, una estrategia de defensa perimetral –similar a la que se empleaba militarmente en el Medievo– pero que no solo es enormemente cara, sino que será –más pronto que tarde– penetrada por ataques en alguno de sus puntos vulnerables.

Posición respecto a la cooperación internacional

Alemania

Werner Hoyer, secretario de Estado del Ministerio Federal de Relaciones Exteriores de Alemania, en una conferencia internacional de alto nivel sobre *Desafíos en ciberseguridad, riesgos, estrategias y fomento de la confianza* que se celebró en Berlín en diciembre 2011, hizo hincapié en la importancia de garantizar la accesibilidad, la transparencia y la integridad de Internet a través de la cooperación internacional. Subrayó que el ciberespacio ha sido desde el principio una red global y abierta (13).

La atención se debería centrar –en opinión de Hoyer– en las áreas donde el consenso para cooperación internacional es más fuerte y pueda dar lugar a normas de conducta políticamente vinculantes. Transparencia y medidas de fomento de la confianza (como las de control de armas convencionales) pueden proporcionar una plataforma para el desarrollo de medidas específicas para el ciberespacio como un «código de conducta cibernética». Alemania está a favor de la creación de una obligación de los países para garantizar la seguridad en el ámbito cibernético, y que esta deba estar anclada en el derecho internacional humanitario (DIH).

Cornelia Rogall-Grothe, secretaria de Estado del Ministerio Federal del Interior de Alemania, opina que los estados tienen un interés vital en asegurar su capacidad de recuperación, la seguridad y la estabilidad por razones económicas, y de seguridad pública, por lo que tiene que proteger el ciberespacio en su propio territorio, pero además deben cooperar a nivel internacional para eliminar las vulnerabilidades en el ciberespacio. El primer paso sería acordar los principios y normas existentes e internacionalmente reconocidos que también podrían aplicarse al ámbito cibernético. Una vez acordados los principios generales, como la utilización con fines pacíficos y la obligación de asegurar la infraestructura crítica, se podría aplicar la cooperación entre estados en la atribución de *ciberataques*. Sin embargo, opina Rogall-Grothe, los estados deben ser responsables de la prevención de *ciberataques* procedentes de su territorio, de lo contrario deben esperar una respuesta razonable, como por ejemplo las sanciones (13). Este último aspecto es significativo puesto que introduce el concepto –disuasorio– de «respuesta razonable».

EE. UU.

Los Estados Unidos dan importancia a la construcción de un consenso internacional sobre normas de conducta en el ciberespacio. De acuerdo con la Estrategia Internacional para el Ciberespacio, elaborada por los Estados Unidos, los acuerdos y normas comunes deberían centrarse en los mundos físicos y cibernéticos por igual. Estos deben incluir las libertades fundamentales en línea y fuera de línea, los derechos de propiedad, la privacidad pública, la protección contra el delito cibernético, el derecho a la legítima defensa, la estabilidad técnica, el acceso fiable y la resistencia nacional (13). Aquí, los EE. UU. van más allá de Alemania e introducen el concepto de «legítima defensa», lo que le supondría el derecho a responder a un ataque digital con cualquier medio.

El Grupo de los Ocho (G8), la OSCE y la Organización para la Cooperación y el Desarrollo Económico (OCDE) son –en opinión de EE. UU.– los foros apropiados para articular estas normas. Según la visión de EE. UU., las medidas de fomento de la confianza de carácter militar deben basarse en los principios de proporcionalidad y distinción, mientras que otras medidas de fomento de la confianza deben tratar de prevenir la escalada. Se destacó la necesidad de un diálogo más global, que se inició en la conferencia de Londres en noviembre de 2011. Es destacable la falta de referencias a la ONU como foro por parte de los EE. UU. La posición de los EE. UU. será desarrollada posteriormente en profundidad.

Rusia

Al igual que otros grandes países, Rusia ha desarrollado capacidades para la guerra de información (IW) y las operaciones de información (IO). Dentro de la Administración rusa, varias organizaciones son responsables del empleo de las capacidades de guerra de información, incluyendo las operaciones de la red de ordenadores, guerra electrónica, operaciones psicológicas y campañas de desinformación (*maskirovka*). El Servicio Federal de Seguridad (FSB) es, probablemente, la autoridad responsable de la seguridad de la información de la Federación de Rusia.

El enfoque de Rusia sobre IW e IO difiere en cierta medida del de los países occidentales, así como desde el punto de vista chino. Desde el punto de vista ruso, la información en sí misma es un activo valioso que se tiene que proteger tanto en tiempos de paz como de guerra. En la doctrina de seguridad de la información de 2000, la protección de la información tiene un valor estratégico y es visto como un factor clave no solo para la estabilidad del Estado, sino también para el régimen y para los actores influyentes e importantes. En la doctrina militar publicada en la primavera de 2010, Rusia toma nota de la importancia de la guerra de la información durante la fase inicial de un conflicto para debilitar el mando

y control de la capacidad del oponente y en la forma de una campaña de información durante la batalla real para crear una visión positiva dentro de la comunidad internacional (14).

Rusia ha sido denunciada públicamente varias veces por no actuar con suficiente fuerza contra las actividades maliciosas en el ciberespacio originarias de ese país. Las acusaciones incluyen una amplia gama de comportamientos, como la criminalidad en Internet, *ciberespionaje* y *hacking* políticamente motivado (llamado *hacktivismo*). Los críticos señalan que los cuerpos de seguridad rusos han sido reacios a hacer frente a los infractores de la ley. Dos casos en particular han llegado a debate en los últimos años con respecto a las operaciones cibernéticas que podrían haber emanado de Rusia: los ataques cibernéticos contra Estonia en 2007 y contra Georgia en el año siguiente. Estos incidentes han supuesto una llamada de atención para poner de relieve los riesgos, amenazas y vulnerabilidades ante una guerra de información (14).

Rusia presentó en 2011 un proyecto de convención de las Naciones Unidas sobre información y seguridad internacionales, con propuestas de que cada Estado sea responsable de su propio espacio de información, incluyendo la seguridad de los datos; que pueda gestionar el ciberespacio en su territorio de acuerdo con las leyes nacionales y haga aplicar las libertades y derechos fundamentales de las personas y ciudadanos, así como que goce de igualdad soberana en el ámbito de la información, y que la seguridad de cada estado sea inseparable de la seguridad de la comunidad global. En junio de 2012, San Petersburgo acogió la tercera reunión internacional de representantes de alto nivel en asuntos de seguridad. Uno de los puntos principales debería haber sido una discusión del proyecto de convención de las Naciones Unidas ya que esta reunión habría sido la última antes de la presentación de la versión final de este documento para su examen por las Naciones Unidas (15).

La esencia del documento, vinculante en el plano internacional, incluye una serie de conceptos como la guerra de información, seguridad de la información, las armas de la información, el terrorismo en el ciberespacio, y otros, que han sido tratados únicamente en trabajos científicos y periodísticos, no en términos de derecho internacional. El proyecto ruso apoya claramente la preservación de la soberanía del Estado sobre su espacio de información, así como las disposiciones relativas a la «acción en el ciberespacio a fin de socavar el sistema político, económico y social de otro Estado, el tratamiento psicológico de la población, la desestabilización de la sociedad» (Fedorenko, 2012). Parece obvio que este último aspecto se refiere al empleo que los EE. UU. hicieron de estas herramientas en Serbia, Ucrania o Kirguistán y que posteriormente fueron imitados en las revueltas árabes de 2011.

En muchos aspectos, el proyecto de convención de la ONU de Rusia «para garantizar la seguridad internacional de la información» es un contrapeso a la Convención de Budapest, que Washington está tratando de imponer como la naturaleza «global» en materia de *ciberseguridad.* A Rusia no le gusta el artículo 32 de la Convención de Budapest, «El acceso transfronterizo», que permite a las agencias de inteligencia de algunos países penetrar en las redes informáticas de otros países para llevar a cabo operaciones allí sin el conocimiento de las autoridades nacionales. Durante mucho tiempo, la parte rusa trató de persuadir a los europeos en eliminar o editar la disposición que viola la soberanía del Estado, pero los países firmantes, con el apoyo de los EE. UU., se negaron rotundamente a realizar cambios en el documento (15). Rusia se niega a firmar el Convenio de Budapest.

Moscú considera que habría que hablar de la totalidad de las acciones relacionadas con posibles actos ilícitos (hostiles) relacionados con la utilización de tecnologías de la información y las comunicaciones (TIC), mientras que Washington insiste en que las negociaciones deben limitarse a las cuestiones de las *ciberamenazas*, lo que excluye las operaciones psicológicas de información, que en los últimos años han proliferado, en particular, a través de las redes sociales. Para los EE. UU., cualquier intento de abordar estos temas como cuestiones de *ciberseguridad* (o seguridad de la información) se considerará como un deseo de presionar a la «sociedad civil» y pone en peligro la «libertad de expresión» y «fortalece tendencias autoritarias» (15).

La interpretación estadounidense del problema está en desacuerdo no solo con Rusia, sino también con el aliado más fiable de Rusia en esta materia, la República Popular de China. Muchos apoyan el enfoque de acercamiento de Rusia, como los países de la CEI, Asia, África y América Latina. Y no todos los estados europeos están de acuerdo con las ideas contenidas en la Convención de Budapest: no es casualidad que solo dos tercios de los países miembros del Consejo de Europa hayan firmado o ratificado la Convención (15).

Francia

La política de seguridad francesa en el ciberespacio señala que las amenazas informáticas en Francia, desde hace muchos años, proceden tanto de actores estatales como no estatales y se ha progresado mucho al ser la seguridad un área prioritaria para el Gobierno francés. Con la aparición de la *ciberdiplomacia*, se ha convertido en global: han comenzado a surgir algunos elementos de consenso para la acción común, las alianzas internacionales y las relaciones bilaterales que están empeñadas en garantizar la seguridad y ayudar a combatir la Delincuencia informática. Destacan para Francia los esfuerzos concertados de la Unión Europea para luchar contra

la delincuencia informática, promover la solidaridad y la *ciberresiliencia* y establecer la política de cooperación con la OTAN (13).

La OSCE se centra en la confianza, en opinión de Francia, mientras que el Grupo de Expertos Gubernamentales de las Naciones Unidas (GEG) 2012 se ha comprometido a la construcción de un consenso internacional. Es necesario un código de conducta para garantizar la libertad de expresión y la fiabilidad de Internet. La Declaración del G8 (Deauville, diciembre de 2011) acordó una serie de principios sobre cómo garantizar la actual fortaleza de Internet como un recurso para la sociedad global: la libertad, la gobernanza de múltiples partes interesadas, el respeto a la privacidad y la propiedad intelectual, la *ciberseguridad* y la protección contra los delitos informáticos.

China

La perspectiva del Gobierno chino sobre seguridad de la información es que a pesar de que la *ciberseguridad* está «de moda», muchos países no están preparados para defenderse contra *ciberataques*. Internet es una red de redes, y podría decirse que a nadie le interesa usar el ciberespacio como un campo de batalla, sino más bien mantenerlo como un espacio pacífico, seguro, equitativo y abierto a la información. Para lograr esto, los conceptos de seguridad común y el «orden favorable» en el ciberespacio y el espacio de la información tienen que desarrollarse en un clima de confianza y entendimiento mutuo (13).

El papel principal de los Gobiernos estatales sería el establecimiento de una cooperación «ganador-ganador» entre la comunidad internacional de estados, por lo que cada uno de ellos podría dotarse de información y de prosperidad cibernética. China no se ve a sí mismo como un «ciberpoder», sino más bien como uno de los mayores usuarios de las TIC que se enfrenta a graves desafíos en el ciberespacio. China –en sus propias palabras– está comprometida con el fortalecimiento de la información y la cibernética desde nuevos ángulos, adoptando un papel activo en la cooperación con el objetivo de alcanzar un consenso internacional así como el desarrollo de normas y reglas internacionales para el dominio cibernético (13).

En septiembre de 2011, se presentó en la Asamblea General de las Naciones Unidas (AGNU) una carta con el esbozo de una propuesta de código internacional de conducta para la seguridad de la información. Dicha carta tenía la intención de proporcionar una base para el proceso de búsqueda de respuestas internacionales a los problemas de seguridad en el ciberespacio y, por tanto, es una invitación para el debate internacional.

La guerra de la información en China, como en otras partes, es un tema amplio, que abarca muchas dimensiones de la actividad. Un debate fun-

damental es si la guerra de información china se aplica sobre todo en tiempos de paz, de guerra o en ambos casos. Para el profesor de West Point Edward Sobiesk, China está actualmente involucrada en una guerra de información en tiempos de paz de largo plazo que «no son combates» per se. Pero este argumento, al parecer, estaría en clara oposición con el énfasis en la acción anticipada y defensa activa que aparece en los textos oficiales chinos sobre defensa (16).

Todas las actividades cibernéticas no son iguales. Dependen del contexto y la cultura de la parte que las realiza. Para algunos, China estaría usando «paquetes de electrones» como estratagemas para llevar a cabo *ciberreconocimientos* o *ciberataques*, una estratagema diseñada para engañar a los procesos de percepción enemigos, su pensamiento, emociones y voluntad. En este caso, los paquetes de electrones podrían ser utilizados como en estratagemas clásicas chinas como «susurro de la hierba para asustar a la serpiente» (tirar miles de *pings* a un sitio determinado hasta que el *IGCC Workshop* informe sobre China, y entonces la *ciberseguridad* se evidenciará al ser estos detectados por los cortafuegos) (16).

China está probablemente influenciada por la táctica conocida como «coctel de guerras», un concepto desarrollado en el libro *Unrestricted warfare* de 1999. Uno de los autores del libro, Qiao Liang (coronel en ese momento), escribió que los nuevos conceptos de armas implican la posibilidad de combinar diferentes elementos para producir tipos de armamento nunca antes imaginados. Por ejemplo, Qiao puede estar refiriéndose a las combinaciones como «precepción cibernética + reconocimiento red + decepción de alta tecnología + desorganización del mercado financiero + disuasión de red» para obtener una nueva arma de efectos globales.

Para *Li Yuxiao*, director del Centro de Investigación de China sobre la Gobernanza de Internet, de la Universidad, Correos y Telecomunicaciones de Pekín, la seguridad del ciberespacio es un problema internacional común que tenemos resolver juntos; pero cada país tiene sus propios problemas de seguridad en Internet, y es injusto que un país mida a los demás de acuerdo a sus propias políticas. Debido a que el tema de la seguridad en el ciberespacio es muy sensible, la discusión no es lo suficientemente completa. Los Gobiernos no pueden llegar a un consenso en algunas cuestiones. A través de la cooperación académica, se podrían definir los principios y las normas básicas y establecer un mecanismo de funcionamiento. La cooperación podría incluir la seguridad informática, la privacidad y protección de datos de negocios (17).

Ubicado en la pintoresca comunidad Xianghongxi en las montañas occidentales del distrito de Haidian de Pekín, el Tercer Departamento del Estado Mayor General (GSD por sus siglas en inglés) del Ejército Popular de Liberación gestiona al parecer una amplia infraestructura de interceptación de comunicaciones orientada a las comunicaciones diplomáticas

extranjeras, actividades militares, entidades económicas o instituciones educativas públicas y particulares de interés. El Tercer Departamento del GSD puede servir como autoridad ejecutiva nacional para la explotación de la red informática (por ejemplo, los *ciberreconocimientos*). Esta hipótesis se basa en tres supuestos:

- La gradual integración técnica y de organización de la inteligencia de señales, seguridad de la información, y *ciberreconocimiento*.
- La competencia básica del Tercer Departamento sobre computación avanzada. La informática y la criptografía son fundamentales para las operaciones de la red de ordenadores (CON).
- El Tercer Departamento sirve como el mayor contratista de lingüistas bien entrenados para la traducción de información. El Tercer Departamento del GSD podrá estar apoyado por empresas comerciales y universidades.

La Estrategia Civil Nacional de Ciberseguridad de China, lanzada en 2003 e inicialmente clasificada pero luego promulgada más ampliamente, es conocida como *Documento 27. Opiniones de fortalecimiento de la información al servicio de garantía de seguridad.* La Constitución consagra el principio de «defensa activa» y establece los cimientos para las políticas para protección de infraestructuras críticas, la criptografía, control dinámico, desarrollo indígena, innovación, el talento, el liderazgo y la financiación. Las iniciativas políticas conjuntas emprendidas por el *Documento 27* han dado lugar a un sistema antagónico de espacios políticos vigorosamente defendidos por las diversas autoridades burocráticas. Cualquier incursión de otras agencias o de recién llegados ha provocado conflictos.

Unión Europea

Desde 2009, y en relación con los esfuerzos de la Unión Europea (UE), ha existido una plataforma de intercambio de información para los estados miembros. Ejercicios de *ciberseguridad* paneuropeos y Equipos de Respuesta a Emergencias Informáticas funcionales (CERT) se establecieron en todos los estados miembros de la UE en 2012 para proteger a Europa de ataques informáticos a gran escala. Se insistió en que la *ciberseguridad* «es una parte integral de la Política Exterior y de Seguridad Común de la Unión Europea (PESC de la UE) ya que tiene una dimensión política», así como la necesidad de defensa. Los próximos pasos del Servicio Europeo de Acción Exterior (SEAE) se centrarán en el desarrollo de normas y estándares para el ciberespacio, la promoción de la Convención de Budapest sobre la Ciberdelincuencia, la creación de capacidades en terceros países, el desarrollo de una estrategia europea para el ciberespacio y la organización de talleres conjuntos con la India, China y la OTAN (13).

Es obvio el cariz de escudo defensivo adoptado por la UE que pretende que otros (OTAN, o sus propios socios) realicen funciones que por su propio carácter global debían ineludiblemente ser realizados por la Unión.

El papel de las organizaciones internacionales

Dado el número de organizaciones internacionales, nos hemos centrado en las que de forma más directa afectan a Europa:

ONU

Antecedentes

A partir del año 2000 se han aprobado una serie de resoluciones de la Asamblea General de la ONU sobre la lucha contra el uso indebido e ilícito de las tecnologías de información. Por ejemplo, en el año 2000, una resolución puso de relieve la necesidad de contar con leyes nacionales modernas y eficaces para enjuiciar adecuadamente los delitos cibernéticos y facilitar la oportuna colaboración de investigación transnacional. En esa resolución, se destacó el valor de una variedad de medidas, que incluían (19):

- Que los estados deben garantizar con sus leyes y prácticas eliminar los «santuarios» para los que usan el ciberespacio con fines delictivos.
- Fomentar la cooperación policial en la investigación y el enjuiciamiento de los casos internacionales de utilización con fines delictivos.
- Que los estados deben intercambiar la información con respecto a los problemas que enfrentan en la lucha contra el uso indebido e ilícito de tecnologías de la información.
- Que los estados deben informar al público en general sobre la necesidad de prevenir y combatir el uso indebido e ilícito.
- Que, en la medida de lo posible, las tecnologías de la comunicación y la información deben estar diseñadas para ayudar a prevenir y detectar el uso indebido e ilícito, para rastrear criminales y reunir pruebas.
- Que la lucha contra el uso delictivo del ciberespacio requiere el desarrollo de soluciones que tengan en cuenta tanto la protección de las libertades individuales como la preservación de la capacidad de los estados para luchar contra el mal uso criminal.

En 2001, una resolución de la Asamblea General sobre la lucha contra los delitos de alta tecnología señaló específicamente la labor de las organizaciones internacionales y regionales. Esta resolución incluye una

referencia a la labor del Consejo de Europa en la elaboración de la Convención sobre el Delito Cibernético, así como la actividad de esas organizaciones en la promoción del diálogo entre el Gobierno y el sector privado en la seguridad y la confianza en el ciberespacio.

En 2003, los Estados reafirmaron la necesidad de crear una cultura de *ciberseguridad* y reconocieron su responsabilidad para llevar, a todos los elementos de la sociedad, a conocer sus funciones y responsabilidades en materia de *ciberseguridad*. Una resolución puso de relieve nueve elementos complementarios que todos los participantes deben abordar (19):

- Aumentar la conciencia de la necesidad de seguridad.
- Medidas que podrían tomar los estados para mejorar la *ciberseguridad*.
- Responsabilidad de la seguridad de las tecnologías de la información y comunicación.
- Capacidad de respuesta para actuar de manera oportuna para prevenir, detectar y responder a incidentes de seguridad.
- Ética en el reconocimiento de que nuestras acciones u omisiones en el ciberespacio pueden dañar a otros.
- Democracia, en el sentido de que la seguridad debe aplicarse de manera coherente con las sociedades democráticas.
- Una gran variedad de medidas de evaluaciones de riesgos, diseño e implementación de seguridad.
- Gestión de la seguridad.
- Recalificación del significando y de los enfoques actuales de las políticas de seguridad basado en el cambio de las amenazas y las vulnerabilidades de este medio de cambio rápido de las comunicaciones.

En 2004 aparece la cuestión de la protección de infraestructuras críticas en una resolución de la Asamblea General de Naciones Unidas (AGNU) que se centró sobre todo en los comportamientos y las acciones que los estados miembros deben tener en cuenta en sus esfuerzos para crear una cultura de *ciberseguridad* y protección de infraestructuras críticas de información. Estos también pueden considerarse un conjunto de acuerdos comunes a los que los Gobiernos se deben adscribir, proporcionando una base esencial para facilitar la comprensión internacional y la colaboración internacional en materia de gestión de riesgos. Entre otras cosas, esta resolución abordó (19):

- La necesidad de redes de alerta de emergencia para las *cibervulnerabilidades*.

- Sensibilización para facilitar la comprensión de las partes interesadas de la naturaleza y la extensión de las infraestructuras de información esenciales.
- El examen de las infraestructuras e identificar la interdependencia entre ellas.
- Promover las asociaciones, tanto públicas como privadas, para compartir y analizar las vulnerabilidades críticas de infraestructura de información y responder a los daños o ataques.
- Creación y mantenimiento de las redes de comunicación de crisis.
- Asegurar que las políticas de disponibilidad de datos tienen en cuenta la necesidad de proteger las infraestructuras críticas de información.
- Y una serie de compromisos en materia de cooperación internacional para asegurar esas infraestructuras, incluida la facilitación del seguimiento de ataques, formación y ejercicios de conducción. Además, tendrán que disponer de leyes procesales sustantivas y adecuadas y personal capacitado para investigar los ataques y procesar a los atacantes.

Otros acuerdos internacionales comunes afectan a cómo los Estados persiguen los objetivos de *ciberseguridad*. El derecho a la libre circulación de la información, por ejemplo, está bien establecido a nivel internacional y está consagrado en la Declaración de la ONU de los Derechos Humanos y el Pacto Internacional de Derechos Civiles y Políticos. Algunos de estos principios se han reafirmado en numerosos foros internacionales, incluyendo la Asamblea General de la ONU, la Unión Internacional de Telecomunicaciones y la Cumbre Mundial sobre la Sociedad de la Información, entre otros.

La Convención Internacional para la Represión de la Financiación del Terrorismo, de la que son parte 169 Estados, ya criminalizó la obtención o provisión de fondos para apoyar actos terroristas. Algunas resoluciones, como la Resolución 1822 (2008), hacen un llamamiento a la cooperación y al intercambio de información relacionada con fines delictivos terroristas, en particular a través de Internet.

La seguridad de la información en la ONU

La cuestión de la seguridad de la información ha estado en la agenda de la ONU desde que la Federación de Rusia en 1998 introdujo por primera vez un proyecto de resolución en la Primera Comisión de la Asamblea General de la ONU. Esta resolución fue aprobada sin votación (A/RES/53/70) y continuó hasta una proposición más detallada, aunque los contenidos eran conflictivos y probablemente inaplicables.

Estos proyectos de resolución se convirtieron en un ejercicio anual de frustración: la iniciativa rusa fue durante muchos años rechazada por algunos países occidentales, pero todavía tiene el mérito indudable de mantener vivo el argumento de que era necesario un esfuerzo normativo importante.

La resolución 66/24, en su apartado 3, invita a todos los Estados miembros a que, teniendo en cuenta las evaluaciones y recomendaciones que figuran en el informe del Grupo de Expertos Gubernamentales sobre los avances en la esfera de la información y las telecomunicaciones en el contexto de la seguridad internacional, sigan comunicando al secretario general sus opiniones y observaciones sobre:

- La evaluación general de los problemas de la seguridad de la información.
- Las medidas que se adoptan a nivel nacional para fortalecer la seguridad de la información y contribuir a la cooperación internacional en esa esfera.
- El contenido de los conceptos mencionados en el párrafo 2 de la resolución.
- Las medidas que la comunidad internacional podría adoptar para fortalecer la seguridad de la información a escala mundial.

El secretario general, en virtud del párrafo 4 de la resolución 60/45, creó un Grupo de Expertos Gubernamentales sobre los avances en el campo de la información y las telecomunicaciones en el contexto de la seguridad internacional. El grupo remitió, en julio de 2010 (A/65/201), las siguientes recomendaciones a la asamblea general:

> *18. Teniendo en cuenta las amenazas existentes y potenciales, riesgos y vulnerabilidades en materia de seguridad de la información, el Grupo de Expertos Gubernamentales considera oportuno recomendar nuevas medidas para el desarrollo de la confianza y otras medidas para reducir el riesgo de error de percepción resultante de las interrupciones TIC:*
>
> *(i) un mayor diálogo entre los estados para discutir las normas relativas al estado de uso de las TIC, para reducir el riesgo colectivo y proteger la infraestructura crítica nacional e internacional;*
>
> *(ii) medidas de fomento de la confianza, la estabilidad y la reducción del riesgo para hacer frente a las implicaciones del uso de las TIC del Estado, incluidos los intercambios de puntos de vista nacionales sobre el uso de las TIC en los conflictos;*
>
> *(iii) el intercambio de información sobre legislación y estrategias nacionales sobre tecnologías de la información y comunicaciones y tecnologías de seguridad, políticas y mejores prácticas;*

(iv) la identificación de medidas de apoyo a la creación de capacidad en los países menos desarrollados;

(v) búsqueda de posibilidades para la elaboración de terminología y definiciones comunes relacionados con la resolución 64/25.

Debido a la naturaleza global del ciberespacio y la utilización más activa de las tecnologías de la información y las comunicaciones (TIC), este problema es de carácter universal y transnacional y afecta a los países, la sociedad y los individuos. El problema de la seguridad de la información no se resolverá por los esfuerzos de un solo estado o grupo de estados o sobre una base regional. La solución de este problema requiere un esfuerzo conjunto de la comunidad internacional en su conjunto.

1. Debido a su carácter universal, las Naciones Unidas deben desempeñar el papel principal en las actividades intergubernamentales para el funcionamiento y la protección del ciberespacio para que no se abuse o sea explotado por los delincuentes, terroristas y estados con fines agresivos. En particular, deberá:

   a. responder a una necesidad esencial y urgente de una ley de consenso amplio del ciberespacio,
   b. avanzar en la armonización de las leyes nacionales contra el *cibercrimen*, y
   c. establecer procedimientos para la cooperación internacional y la asistencia mutua.

2. Hay que trabajar con este fin. La ONU debería reconocer la labor ya realizada por las partes negociadoras en el Consejo de Europa sobre la Ciberdelincuencia (CoE Convención). El Convenio del Consejo de Europa señala a una mayor fuerza si todas las partes que participaron en el proceso de negociación firmasen el Convenio, si aún no lo han hecho, para acelerar los procesos de ratificación y la transformación. Inmediatamente después de la entrada en vigor del Convenio, los firmantes deben adoptar medidas para designar y notificar a su autoridad para el manejo de la asistencia mutua y para participar en la red 24/7, y tomar otras medidas para promover la cooperación internacional en la derrota de delitos informáticos, como el Convenio del Consejo de Europa prevé.

Hamadoun Touré, director de Comunicaciones de la Agencia de la Tecnología de las Naciones Unidas, la Unión Internacional de Telecomunicaciones (UIT), dijo que el mundo necesita un tratado para evitar convertir los *ciberataques* en una guerra sin cuartel. Touré hizo esta declaración en enero de 2010, en el Foro Económico Mundial en Suiza, donde los expertos afirmaron que las naciones ahora debían tener en cuenta cuándo un *ciberataque* pasaba a ser una declaración de guerra. Touré ha añadido así una voz autorizada de la ONU en la búsqueda de un marco normativo.

Pero por muy atractiva que sea la idea de una convención amplia sobre ciberespacio –comparable a la Convención de las Naciones Unidas sobre el Derecho del Mar de 1982–, los obstáculos a dicho instrumento y su creación fueron reconocidos cada vez más como abrumadores. El ciberespacio puede ser aún más complejo que el mundo oceánico, pues las tecnologías digitales y sus usos están aún evolucionando a un ritmo rápido (20).

A pesar del sorprendente apoyo que recibieron China y Rusia en la reunión de la Unión Internacional de Telecomunicaciones en diciembre de 2012 con el modelo «no occidental» de la gobernanza de Internet (10), la negociación del tratado sería un proceso largo, y los procedimientos nacionales de ratificación no procederían en una escala de tiempo, aunque se esté mínimamente de acuerdo con la urgencia de llenar el vacío legal y exista la percepción creciente y compartida entre los Gobiernos de que la amenaza de *ciberconflictos y ciberdaños* se está haciendo inmanejable y puede acabar fuera de control. Los compromisos vinculantes para evitar ataques o actos de hostilidad y las sanciones correspondientes serían entonces inviables. Importantes problemas de definición serían probablemente irresolubles en el texto del tratado. Así, mientras que un tratado universal o ley sobre el ciberespacio sigue siendo un objetivo preferente, un concepto objetivo, razones prácticas requieren un enfoque alternativo (20).

OTAN

> *La OTAN seguirá siendo alianza multilateral preeminente para nuestra nación y seguirá impulsando nuestras relaciones de defensa con Europa. La Fuerza Conjunta seguirá cooperando para combatir el extremismo violento, centrándose en nuestra misión en Afganistán y apoyar a Pakistán. También vamos a apoyar el nuevo concepto estratégico como el espacio y la seguridad del ciberespacio…*
>
> Estrategia Nacional Militar de los EE. UU. de América de 2011

En abril y mayo de 2007, el traslado de un memorial de la guerra de la era soviética desató una serie de grandes y sostenidos ataques distribuidos de denegación de servicio (DDoS) que inundaron redes o sitios *web* con un tráfico de ataques que las hicieron inaccesibles. Los ataques –muchos de los cuales procedían de Rusia o eran escritos en ruso o coordinados en sitios *web* rusos– deshabilitaron los sitios *web* del presidente de Estonia, el Parlamento y los ministerios junto con los sitios *web* de los partidos políticos, los bancos y agencias de noticias. En fases de intensidad variable, los ataques se prolongaron durante más de tres semanas (21).

No se encontraron evidencias que vincularan directamente estos ataques con el gobierno ruso, pero los mismos fueron al menos ignorados y pro-

bablemente alentados por Moscú. Estos ataques supusieron un punto de inflexión en la política de la OTAN sobre *ciberseguridad*.

El crecimiento explosivo de «la banda» durante la década de 1990 coincide con la primera intervención militar importante de la OTAN. Así como la guerra de Vietnam fue la primera televisada del mundo, Kosovo fue la primera guerra de Internet en amplia escala. Cuando los aviones de la OTAN comenzaron a bombardear Serbia, numerosos grupos de *hackers* proserbios (o antioccidentales) como la Mano Negra –tomando prestado su nombre de la sociedad secreta paneslava que ayudó a comenzar la Primera Guerra Mundial– comenzaron a atacar la infraestructura de Internet de la OTAN. Se desconoce si alguno de los *hackers* trabajó directamente para el Ejército yugoslavo; en cualquier caso, su objetivo declarado era interrumpir las operaciones militares de la OTAN (22).

Los ordenadores de la OTAN, EE. UU. y Reino Unido fueron atacados durante toda la guerra por medio de «ataques de denegación de servicio» e infectados con virus por correo electrónico (fueron detectadas 25 diferentes cepas de virus). El ataque a la sede de la OTAN en Bélgica fue una victoria de relaciones públicas y propaganda para los piratas informáticos (22).

En 2002, la cumbre de Praga decide afrontar la defensa de la organización contra ataques informáticos, estableciendo la NATO Computer Incident Response Capability (NCIRC). Pero es en 2006, en la de Riga, cuando el mensaje se hace más evidente; en la declaración final, apartado 24, se lee: «La adaptación de nuestras fuerzas debe continuar. Hemos aprobado una serie de iniciativas para aumentar la capacidad de nuestras fuerzas para hacer frente a las amenazas y desafíos contemporáneos».

> *Trabajar para desarrollar una NATO Network Enabled Capability para compartir información, datos e inteligencia de forma fiable, segura y sin demora en las operaciones de la Alianza, al tiempo que mejora la protección de nuestros sistemas de información clave contra ciberataques.*

La cumbre de 2008 en Bucarest da un paso más en el párrafo 47 de la declaración:

> *47. La OTAN mantiene su compromiso de fortalecer los sistemas clave de información de la Alianza contra ciberataques. Recientemente hemos adoptado una Política de Defensa Informática, y se están desarrollando las estructuras y autoridades para llevarlo a cabo. Nuestra Política de Ciberdefensa hace hincapié en la necesidad de que la OTAN y las naciones, para proteger los sistemas de información clave de acuerdo con sus respectivas responsabilidades, compartan sus mejores prácticas y pongan a disposición sus capacidades, previa solicitud, para ayudar a las naciones aliadas a contrarrestar un ataque informático.*

En la cumbre de Lisboa, en noviembre de 2010, se acordó en el párrafo 2: «... de conformidad con las disposiciones de aplicación de la presente Declaración, hemos también (...) acordado mejorar nuestras capacidades de *ciberdefensa».* Y en el apartado 40:

> *Con el fin de garantizar el acceso permanente y sin restricciones de la OTAN al ciberespacio y la integridad de sus sistemas críticos, (...) se tendrá en cuenta en la doctrina de la OTAN la dimensión cibernética de los conflictos modernos y mejorará sus capacidades para detectar, evaluar, prevenir, defender y recuperar en caso de un ciberataque contra los sistemas de importancia crítica para la Alianza. Nos esforzaremos en particular para acelerar el NATO Computer Incident Response Capability, hasta alcanzar la capacidad operativa plena (FOC) en 2012 y la disposición bajo la protección cibercentralizada de todos los organismos de la OTAN.*

Además, indica que:

> *Vamos a utilizar los procesos de planificación de la defensa de la OTAN con el fin de promover el desarrollo de cibercapacidades de defensa, para ayudar a los aliados tras su solicitud y para optimizar el intercambio de información, la colaboración y la interoperabilidad.*

Por último:

> *Para hacer frente a los riesgos de seguridad que emanan desde el ciberespacio, trabajaremos en estrecha colaboración con otros actores, tales como la ONU y la UE, según lo acordado. Hemos encomendado al Consejo que elabore, basándose sobre todo en las estructuras internacionales y sobre la base de nuestra política actual, una revisión en profundidad de la política de la OTAN en ciberdefensa para junio de 2011 y que prepare un plan de acción para su implementación.*

Un primer borrador del concepto de *ciberdefensa* de la OTAN fue elaborado por los ministros de Defensa en marzo de 2011, lo que constituyó la base conceptual de la versión revisada de la Política sobre Defensa Cibernética de la OTAN. La citada política fue desarrollada y aprobada por los ministros de Defensa el 8 de junio. El documento va acompañado de un plan de acción, lo que representa un documento detallado con las tareas y actividades específicas para las estructuras propias de la OTAN y las fuerzas aliadas de defensa. Los principales elementos del nuevo enfoque son (21):

- Asunción de que la *ciberdefensa* es necesaria para realizar las tareas básicas de la OTAN de defensa colectiva y la gestión de crisis.
- La prevención, la resistencia y la defensa de los activos críticos para la *ciberseguridad* de la OTAN y sus aliados constituyentes.
- La aplicación de capacidades de *ciberdefensa* sólidas y la protección centralizada de redes propias de la OTAN.

- Definición de los requisitos mínimos para la *ciberdefensa* de las redes nacionales críticas para las tareas centrales de la OTAN.
- Asistencia a los aliados para alcanzar un nivel mínimo de *ciberdefensa* que reduzca la vulnerabilidad de la infraestructura crítica nacional.
- Compromiso con los socios, otras organizaciones internacionales, el sector privado y el académico.

Para poner en práctica estas nuevas políticas y capacidades, el principal órgano de gobierno de la OTAN para *ciberdefensa*, el Consejo de Dirección para Ciberdefensa (CDMB), ha firmado memorandos de entendimiento con la autoridad correspondiente de cada país miembro.

La declaración de la cumbre de 2012 en Chicago reafirma –en su artículo 49– los compromisos de *ciberdefensa* de la Cumbre de Lisboa, y, después de Lisboa, el año pasado (2011) se adoptó un concepto, una política y un plan de acción en *ciberdefensa* que ya se están aplicando.

Para hacer frente a las amenazas a la *ciberseguridad* y mejorar nuestra seguridad común,

> *...nos comprometemos a colaborar con los países socios pertinentes sobre una base de caso por caso y con las organizaciones internacionales, en particular la Unión Europea, según lo acordado, el Consejo de Europa, las Naciones Unidas y la OSCE, con el fin de aumentar la cooperación concreta.*

El futuro cibernético de la OTAN pasa por la *ciberdisuasión* de la Alianza. A pesar de que la *ciberdisuasión* es un tema muy discutido, es previsible que la OTAN siga el liderazgo del Departamento de Defensa de los EE. UU. y se centre en la disuasión por denegación. La defensa antes de un ataque, y las respuestas tras él, deben ser lo suficientemente eficaces para que los potenciales adversarios sepan que no pueden alcanzar los efectos deseados. Una fuerte defensa y las medidas de respuesta de la actual política de *ciberdefensa* de la OTAN pueden, en caso de aplicarse, ser un fuerte elemento de disuasión al denegar el beneficio de atacar en el primer lugar, para disuadir a los potenciales adversarios. La Alianza también puede lograr la disuasión castigando de varias maneras (21):

1. Cualquier nación que decida realizar un ataque importante incluso contra un aliado pequeño, como Estonia, ahora sabe que los líderes políticos de la OTAN tienen una forma bien definida para poder escalar la situación, como invocar el artículo 4 o el artículo 5 para una defensa colectiva.
2. Tanto la Casa Blanca como el Pentágono han sido sumamente claros en que los compromisos de la Alianza se extienden a los ataques informáticos importantes.

3. Aunque la OTAN no tiene una capacidad *ciberofensiva*, varias naciones aliadas disponen de las mismas, que podrían utilizarse en respuesta a un ataque importante.

Ni la disuasión ni el castigo garantizan que no habrá ataques futuros, pero las herramientas de las que disponen actualmente los Gobiernos aliados son muy diferentes de las que disponía Estonia cuando fue atacada en 2007. Al menos en la OTAN. Es interesante recordar las organizaciones con las que la OTAN se compromete a colaborar: Unión Europea, el Consejo de Europa, las Naciones Unidas y la OSCE, por este orden; igualmente, es importante recordar que es la OTAN la única organización internacional en la que confía plenamente EE. UU., la principal superpotencia en el ciberespacio.

Consejo de Europa

El Consejo de Europa (CoE) ha estudiado la *ciberseguridad* sobre todo desde el ángulo de la *ciberdelincuencia*. En 2001, el Consejo de Europa presentó la Convención sobre la Ciberdelincuencia –instrumento destinado a apoyar una política penal común encaminada a la protección de la sociedad contra la *ciberdelincuencia*–.

El Departamento de Justicia de EE. UU. ha sido un jugador clave en el desarrollo del acuerdo final.

Según Froomkin (2004), es creencia general que fue impulsada por EE.UU –que la habría redactado– a través del Consejo para obtener acceso a las comunicaciones extranjeras y sobre todo para dar la impresión al Congreso de que *Carnivore* –un *software* para monitorizar correo electrónico y de comunicaciones electrónicas empleado por el FBI– debe ser visto como ordinario, y algo exigido por sus aliados.

Estas afirmaciones son en alguna medida confirmadas por el Informe para el Congreso de Kristin Archick (23):

> *Tanto la Administración Clinton como la de Bush trabajaron en estrecha colaboración con el Consejo de Europa sobre la Convención. Funcionarios estadounidenses creen que «elimina o minimiza los numerosos obstáculos procesales y jurisdiccionales que pueden retrasar o poner en peligro las investigaciones internacionales y el enjuiciamiento de los delitos informáticos» (...). Políticos de EE. UU. afirman que la Convención no exigirá legislación para su aplicación, EE. UU. cumplirá con el Convenio, basado en la existente ley federal de los EE. UU. Los analistas legales dicen que los negociadores estadounidenses habían logrado separar las disposiciones más comprometidas, como por ejemplo el artículo de la incitación al odio, garantizando así que el Convenio se ajusta a las actuales leyes estadounidenses.*

La Convención contra la *Ciberdelincuencia* es referida a menudo como clave para la solución de los asuntos de *ciberseguridad.* Sus artículos 2-13 abordan el sustancial derecho penal que obliga a los estados a que tipifiquen los delitos informáticos. La Convención enumera los delitos contra la confidencialidad, integridad y disponibilidad de ordenadores, datos y sistemas, la falsificación y el fraude informático y delitos relacionados con el contenido así como la propiedad intelectual y la violación de la intimidad. Los artículos 14-22 abordan la ley procesal, incluyendo la evidencia electrónica, los poderes y los procedimientos apropiados para las investigaciones. Comprende, entre otros, el sistema de búsqueda y captura, la recogida de datos del tráfico en tiempo real, la interceptación de los contenidos de los datos y la preservación y rápida divulgación de los datos informáticos almacenados relacionados con el tráfico. Los artículos 23-35 están dedicados a la cooperación internacional (24).

Lo cierto es que la aplicación de la Convención no es uniforme y a menudo no se corresponde con las amenazas emergentes contra la seguridad nacional. Por otro lado, como afirman Schjølberg y Ghernaouti-Hélie (25), «la Convención se basa en las conductas delictivas de finales de 1990 y que no cubren técnicas como el *phishing*, *botnets*, *spam*, o *ciberterrorismo* y la terminología de la Convención es la terminología de los 90, no necesariamente adecuada para la década de 2010».

OSCE

La mayor organización de seguridad del mundo ha estado activa en la *ciberseguridad*, principalmente desde la perspectiva del *ciberterrorismo.* La Unidad de Acción contra el Terrorismo coordinó y facilitó desde 2002 los programas pertinentes de la OSCE para la lucha contra el terrorismo. En 2010, en un taller de la OSCE sobre un enfoque global para mejorar la *ciberseguridad,* los delegados coincidieron en que la función de la OSCE en la *ciberseguridad* mundial necesita ser redefinida:

> *Preocupados por la complejidad de las actividades maliciosas en línea, la OSCE ha decidido intensificar la acción mediante la mejora de la cooperación internacional en la lucha contra el uso de Internet con fines terroristas, para considerar la adopción de todas las medidas apropiadas para proteger las infraestructuras críticas y redes de información vitales contra la amenaza de ciberataques, al considerar ser parte e implementar sus obligaciones en virtud de los instrumentos internacionales y regionales existentes, y para explorar la posibilidad de una participación más activa de las instituciones de la sociedad civil y el sector privado en la prevención y lucha contra el uso de Internet con fines terroristas (26).*

Así es recogido en el informe del secretario general de la OSCE:

> *Desde 2009, la OSCE ha promovido un enfoque más amplio de la ciberseguridad. Este enfoque se basa en el entendimiento de que el uso generalizado de Internet por los terroristas, traficantes y delincuentes hace cada vez más difícil el desarrollo de respuestas eficaces a las amenazas transnacionales sin promover un ciberespacio más seguro. Un enfoque integral de la ciberseguridad debe: (a) fortalecer la seguridad nacional; (b) hacer frente a los ciberdelitos; (c) inhibir la utilización de Internet por terroristas; (d) responder a una amplia variedad de riesgos y amenazas, incluyendo peligros político-militares; (e) permitir a las autoridades competentes la protección de una amplia gama de objetivos que van desde el usuario particular de Internet a las infraestructuras críticas, y (f) salvaguardar Internet como un espacio de libre expresión y de reunión*[3].

El citado informe recoge que:

> *Muchos estados participantes han expresado su apoyo a un enfoque más amplio de la ciberseguridad, tal como se refleja en la FSC. DEC/10/08, en la que los estados participantes decidieron organizar un taller OSCE sobre un enfoque integral de la OSCE para mejorar la ciberseguridad (17 a 18 marzo, 2009, Viena) con la participación de las organizaciones internacionales pertinentes.*

La decisión del Foro de Cooperación en Materia de Seguridad incluye el objetivo del taller:

- Aumento de la conciencia de los estados participantes de la OSCE sobre las medidas concretas que se pueden tomar para fortalecer la *ciberseguridad*.
- Intercambio de información sobre las prácticas nacionales en materia de ciberseguridad entre los estados participantes de la OSCE y las organizaciones y actores internacionales pertinentes.
- Exposición de medidas defensivas potenciales, lecciones aprendidas y mejores prácticas pertinentes.
- Focalización en el posible papel de la OSCE en un enfoque integral para mejorar la *ciberseguridad*, y la identificación de medidas concretas para posibles acciones de seguimiento por todos los organismos pertinentes de la OSCE.

El taller de la OSCE de marzo de 2009 no solo proporcionó una mayor conciencia de las posibles medidas para fortalecer integralmente la *ciberseguridad*; también dio lugar a recomendaciones y sugerencias sobre el futuro papel de la OSCE en este ámbito temático (FSC.DEL/92/09) que siguen siendo objeto de examen por los países participantes.

[3] Report by the OSCE Secretary General on the Implementation of MC.DEC/2/09.

Un cable de la embajada de los EE.UU ante la OSCE indica que:

> *…una de las actividades recomendadas de seguimiento al taller de marzo observó que un «primer paso» esencial para el desarrollo de la ciberresiliencia era un autoestudio que identifique las políticas, las prácticas, las carencias y las capacidades dentro de las infraestructuras nacionales de información. Esta recomendación fue hecha por un experto panelista de EE. UU. y recibió un amplio apoyo. Como resultado, los expertos en ciberseguridad interagencias de Washington han desarrollado un autoestudio y evaluación para los estados participantes de la OSCE. Este documento se basa en una encuesta preparada para –pero nunca utilizado por– la Unión Internacional de Telecomunicaciones (UIT) de Naciones Unidas (27).*
>
> *Cada país debe determinar sus necesidades de ciberseguridad y tomar medidas para proteger sus infraestructuras críticas de información. Este autoestudio está destinado a ayudar a esta introspección para los miembros de la OSCE.*

Entre las preguntas, se tratarían temas como el desarrollo de una Estrategia Nacional de Ciberseguridad, la implementación de la citada estrategia nacional, colaboración Gobierno-industria o la promoción de una cultura nacional de seguridad informática. En una segunda parte, se incluirían descripciones y explicaciones sobre las preguntas de la primera parte, pero también recomendaciones para el desarrollo y la implementación de un programa de *ciberseguridad* nacional para la capa de política y de gestión, y se ocuparía de las políticas, el marco institucional y las relaciones de la *ciberseguridad*. Esta herramienta supondría un modelo marco con el que una nación podría comparar sus propios esfuerzos.

El ámbito geográfico de los 56 estados miembros de la OSCE cuenta con niveles extremadamente altos de penetración de Internet y, aún más importante, muy altos niveles de dependencia del Gobierno en infraestructura cibernética y de los sistemas SCADA (es decir, la energía, el agua y otras infraestructuras críticas que están vinculados a las tecnologías de la información y la comunicación que estamos debatiendo hoy), lo que significa –en opinión de EE. UU.– que la OSCE podría tener un interés particularmente fuerte en la discusión de medidas para aumentar la estabilidad a lo largo de estas líneas. Este foro ofrece un concepto integral de la seguridad y un espacio para el debate maduro en el que plantear estas cuestiones, creemos.

Finalmente, los EE. UU. presentaron un documento de reflexión e invitaron a la panelista Dra. Deborah Schneider a que interviniera ante una sesión conjunta del Consejo Permanente (CP) y del Foro de Cooperación en Materia de Seguridad (FCS). El documento de reflexión presentado en marzo de 2010 muestra el pensamiento de EE. UU. en cuestiones tales como:

– ¿Cómo podemos extender el entendimiento común entre los estados al ámbito cibernético para ayudar a garantizar la paz y la estabilidad internacionales?

– ¿Qué principios existentes del derecho internacional se aplican en el ciberespacio?

– ¿Cómo podemos aumentar la previsibilidad del comportamiento del Estado en el ciberespacio?

En relación con el segundo punto, indico que las delegaciones en el Grupo de Expertos Gubernamentales han estudiado la idea de mejorar la previsibilidad y la regularización de las nociones de comportamiento del Estado. Ese grupo, incluyendo los EE. UU., ha llegado a la conclusión de que los principios del *ius ad bellum* y *el ius in bello* aplican en el ciberespacio. El ciberespacio no está exento de ninguna manera; creemos que los principios básicos se aplican y proporcionan una base sólida para las discusiones sobre las expectativas acerca de la conducta de los estados en el ciberespacio. En concreto, EE.UU opina (Schneider, 2010):

– Con respecto al ius ad bellum, que algunos incidentes cibernéticos pueden elevarse al nivel de un uso de la fuerza.

– Con respecto a la ius in bello, que el derecho de los conflictos armados se aplica generalmente en el ciberespacio.

No obstante, EE. UU. continúa el estudio de los atributos únicos de la información y las comunicaciones, lo que presenta desafíos en la manera de aplicar estos principios. Creemos que esta es una vía útil y fructífera de exploración para el diálogo en el marco de la OSCE.

Este comienzo prometedor en la Organización para la Seguridad y la Cooperación en Europa (OSCE) para lograr un acuerdo sobre las medidas de fomento de la confianza cibernética fracasó cuando Rusia –como era de esperar– se apartó de los anteriores acuerdos. Esto puede haber sido una reacción a la aprobación del Congreso de EE. UU. de una resolución sobre derechos humanos en Rusia, pero también hay una división entre los países sobre cómo abordar el tema de Internet y la *ciberseguridad* basada en las actitudes hacia la democracia, los derechos humanos y el desarrollo económico. Es probable que haya pocos avances en la cooperación internacional en materia de *ciberseguridad* si la oposición rusa permanece firme, lo que puede obligar a EE. UU. a adoptar un nuevo enfoque que se dirija primero hacia un acuerdo con naciones «afines» (10).

Caso de análisis: la Unión Europea

La UE añadió a finales de los 90 el *cibercrimen* a los temas de interés. En abril de 1998, la Comisión presentó al Consejo los resultados de un

estudio sobre los delitos informáticos (estudio de la denominada *Comcrime*). En octubre de 1999, la Cumbre del Consejo Europeo de Tampere llegó a la conclusión de que el examen de delincuencia de alta tecnología debía ser incluido en los esfuerzos para acordar definiciones comunes y sanciones (24).

La decisión marco del Consejo de 2005 relativa a los ataques contra la información *Systems158* es un hito de la actividad de la UE en la lucha contra la *ciberdelincuencia*. Trata de mejorar la cooperación entre el poder judicial y otras autoridades competentes. El documento subraya la importancia de la aproximación de los sistemas de derecho penal y el aumento de la cooperación entre las autoridades judiciales en relación con el acceso ilegal a sistemas de información, la injerencia ilegal en el sistema y la interferencia ilegal en los datos(28). En 2010, se presentó una propuesta de directiva relativa a los ataques contra los sistemas de información, que derogaría la Decisión Marco 2005/222/JAI del Consejo. Por el momento, cuenta con la oposición del Reino Unido.

En opinión de la UE, para que el ciberespacio se mantenga abierto y libre, las mismas normas, principios y valores que defiende la Unión Europea fuera de línea también deberían aplicarse en línea. Los derechos fundamentales, la democracia y el Estado de derecho deben ser protegidos en el ciberespacio. Nuestra libertad y prosperidad dependen cada vez más de una Internet robusta e innovadora, que seguirá floreciendo si la innovación del sector privado y la sociedad civil impulsan su crecimiento.

En febrero de 2013 la Unión Europea (UE) ha aprobado el documento *Estrategia de ciberseguridad de la Unión Europea: un ciberespacio abierto, seguro y protegido.* Como puede apreciarse, deja bien sentada su prioridad: ciberespacio *abierto y libre;* pero cualquiera que esté familiarizado con las negociaciones en el marco de la UE sabe que la sustancia viene después del *but…:*

> *Pero la libertad en línea requiere también protección y seguridad. El ciberespacio debe ser protegido de los incidentes, las actividades maliciosas y mal uso; y los Gobiernos tienen un papel importante para garantizar un ciberespacio libre y seguro.*

Y reserva las tareas más importantes para los Gobiernos:

> *Los Gobiernos tienen varias tareas: para salvaguardar el acceso y apertura, de respeto y protección de los derechos fundamentales en línea y para mantener la fiabilidad y la interoperabilidad de Internet. Sin embargo, el sector privado posee y opera una parte significativa del ciberespacio, por lo que cualquier iniciativa que pretenda tener éxito en este área tiene que reconocer su papel de liderazgo (29).*

Es importante la lectura de este documento porque nuestro país comparte con sus socios de la UE una misma *cosmovisión*, que algunos califican

de posmodernista y que nos diferencia de otras potencias globales, incluso de los EE. UU.

Como nos recordaba Robert Kagan (30), es hora de dejar de pensar en que europeos y americanos comparten una misma visión del mundo:

> *En todos los asuntos importantes relacionados con el poder –la eficacia del poder, la moralidad del poder, la atracción del poder– las perspectivas europeas y americanas divergen. Europa se está moviendo más allá del poder a un mundo autocontenido de las leyes y las normas y la negociación transaccional y la cooperación. Está entrando en un paraíso posthistórico de paz y prosperidad relativa, la realización de la «paz perpetua» de Emmanuel Kant.*

Mientras tanto, los EE. UU. permanecen sumidos en la historia, ejerciendo su poder en un anárquico mundo *hobbesiano*:

> *Donde las leyes y regulaciones internacionales no son fiables y donde la auténtica seguridad y defensa y la promoción de un orden liberal aún depende de la posesión y empleo del poder militar.*

Es por ello que, en las principales cuestiones internacionales de hoy en día, los estadounidenses vienen de Marte y los europeos de Venus: están de acuerdo en poco y se entienden entre ellos cada vez menos, afirma Kagan.

Hay que reconocer que el prestigioso escritor publicó estos párrafos en 2003, y que la aproximación del actual presidente Barak Obama es «cosméticamente» diferente a la de su antecesor George W. Bush y, aun con diferentes cosmovisiones, actualmente es más lo que compartimos que lo que nos separa. Pero, como nos recuerda Noam Chomsky en una entrevista con Eric Bailey:

> *Las políticas de Obama han sido aproximadamente las mismas de Bush, aunque ha habido algunas pequeñas diferencias, pero eso no es una gran sorpresa. Los demócratas apoyaron las políticas de Bush. Hubo algunas objeciones, en su mayoría por razones partidistas, pero en su mayor parte, apoyaron sus políticas y no es sorprendente que no hayan dejado de hacerlo. En algunos aspectos, Obama ha ido más allá que Bush…*

En cuanto a los asesinatos, a pesar de que la campaña fue iniciada por Bush, Obama ha aumentado considerablemente la citada campaña global de asesinatos y se han incluido en la lista a ciudadanos estadounidenses. ¿Se aplica el *proceso legal establecido*? Eric Holder, fiscal general del Departamento de Justicia con Obama, explicó que «sí se había aplicado el proceso legal establecido ya que se discutió previamente en el Ejecutivo». El Gobierno norteamericano ha dejado muy claro que los asesinatos cuentan con la aprobación de Obama (31). En definitiva, EE. UU. y la UE son como Marte y Venus.

La UE se reserva el papel de salvaguarda de los derechos y libertades, mientras deja para los estados miembros los temas de seguridad:

> *La UE debe salvaguardar un entorno en línea que ofrece la mayor libertad posible y la seguridad para el beneficio de todos. Si bien reconoce que es predominantemente la tarea de los estados miembros para hacer frente a los desafíos de seguridad en el ciberespacio, esta estrategia propone acciones específicas que pueden mejorar el rendimiento global de la UE (29 pág. 4).*

Esto nos debería dejar perplejos, dado que si el espacio es parte de los *global commons*, parece que la UE debería llevar la voz cantante y no solo en los asuntos de derechos y libertades, sino también en estos asuntos de seguridad global. La UE propone en esta estrategia una visión articulada en cinco prioridades estratégicas:

- Lograr *ciberresiliencia*.
- Reducir drásticamente la *ciberdelincuencia*.
- El desarrollo de la política de *ciberseguridad* y las capacidades relacionadas con la Política Común de Seguridad y Defensa (PCSD).
- Desarrollar los recursos industriales y tecnológicos para la *ciberseguridad*.
- Establecer una política internacional coherente para la Unión Europea en el ciberespacio y promover valores esenciales de la UE.

Es destacable la *ambigüedad constructiva* del tercer apartado –es el más largo, pero no dice nada– y la omisión expresa de la palabra «intereses» en el último apartado: la UE promueve valores, pero deja la defensa de los intereses a los países. Una aproximación muy lejana de la visión posthistórica; Europa sigue siendo básicamente *westfaliana* por dejación.

Las actividades de la alta representante en relación con el apartado 3 se centrarán, entre otras labores «insustanciales», en promover el diálogo y la coordinación entre los actores civiles y militares de la UE y asegurar el diálogo con los socios internacionales, incluida la OTAN, otras organizaciones internacionales y los centros multinacionales de excelencia, para garantizar las capacidades efectivas de defensa, identificar áreas para la cooperación y evitar la duplicación de esfuerzos. Es decir, promover, coordinar y dialogar (en resumen, nada de utilidad).

Sin embargo, es en el punto 5 donde la UE puede ser más proactiva y eficaz: «Preservar el ciberespacio abierto, libre y seguro es un desafío global que la UE debe abordar junto con los interlocutores pertinentes y organizaciones internacionales, el sector privado y la sociedad civil». La Comisión, la alta representante y los estados miembros deberían articular una política internacional coherente de la UE en el ciberespacio, que se dirigirá a una mayor participación y fortalecimiento de las relaciones con los principales socios internacionales y las organizaciones, así como con la sociedad civil y el sector privado (29 pág. 15).

Las consultas de la UE con los socios internacionales sobre cuestiones cibernéticas deben ser diseñadas, coordinadas e implementadas para obtener valor añadido a los actuales diálogos bilaterales entre los estados miembros de la UE y terceros países:

> *La UE pondrá un énfasis renovado en el diálogo con terceros países, con especial atención a socios afines que comparten los valores de la UE. Se promoverá lograr un alto nivel de protección de datos, incluyendo la transferencia de datos personales a terceros países. Para hacer frente a los desafíos mundiales en el ciberespacio, la UE promoverá una cooperación más estrecha con organizaciones que trabajan en este campo, tales como el Consejo de Europa, la OCDE, la ONU, la OSCE, la OTAN, la Unión Africana, la ASEAN y la OEA.*

Particulariza la cooperación con los EE. UU. –socio afín que comparten los valores de la UE– a nivel bilateral, que se seguirá desarrollando, especialmente en el contexto del Grupo de Trabajo UE-EE. UU. sobre *ciberseguridad* y *ciberdelincuencia* (29).

Considera que «la responsabilidad de un ciberespacio más seguro depende de todos los actores de la sociedad mundial de la información desde los ciudadanos a los Gobiernos».

De acuerdo con el texto, uno de los elementos más importantes de la política internacional de la UE en este campo será la promoción de la libertad y los derechos fundamentales el ciberespacio, y recuerda que las obligaciones legales consagradas en el Pacto Internacional de Derechos Civiles y Políticos, el Convenio Europeo de Derechos Humanos y la Carta Europea de Derechos Fundamentales deben ser respetados también en línea.

La Unión Europea no exige la creación de nuevos instrumentos legales internacionales para asuntos cibernéticos, y considera que:

- Para hacer frente a los delitos informáticos, la Convención de Budapest es un instrumento abierto a la aprobación de terceros países.
- Si los conflictos armados se extienden al ciberespacio, el derecho internacional humanitario y el derecho internacional de los derechos humanos, según proceda, se aplicarán al caso que nos ocupe.

La Comisión y la alta representante, en cooperación con los estados miembros, deberán, entre otras tareas, apoyar el desarrollo de normas de conducta y medidas de fomento de la confianza en la *ciberseguridad*, facilitar el diálogo sobre la manera de aplicar el derecho internacional existente en el ciberespacio y la promoción de la Convención de Budapest para hacer frente a los *ciberdelitos*.

Esto nos da paso al estudio de las relaciones bilaterales, particularmente desde la perspectiva de EE. UU., la cooperación internacional en *ciberdefensa* a través de la OTAN y el desarrollo de normas de conducta y

medidas de fomento de la confianza en la seguridad informática, particularmente en la OSCE, organización con capacidad demostrada en este ámbito, y la ONU.

Caso de análisis: los EE. UU.

Los orígenes de la política de *ciberseguridad* de EE. UU. se basan en los esfuerzos de protección de infraestructuras críticas que comenzaron durante la Administración Clinton. La Orden Ejecutiva 13010, Protección de las Infraestructuras Críticas, de 1996, creó la Comisión Presidencial sobre Protección de Infraestructuras Críticas y destacó la amenaza a la seguridad económica y nacional que los *ciberataques* suponían para la nación. Las recomendaciones de la comisión dieron lugar a la Decisión Directiva Presidencial 63, de mayo 1998 (32).

La Estrategia Nacional para Asegurar el Ciberespacio del presidente George W. Bush fue publicada en 2003, pero fue criticada por representar más una lista de recomendaciones que un documento de estrategia global que recoja los fines, las formas y los medios. Además, la Administración Bush publicó en 2006 el Plan Nacional de Protección de Infraestructuras, que designa 17 (ahora 18) sectores clave de infraestructuras que requieren planes de protección individual. También publicó la *Iniciativa nacional integral de ciberseguridad* en 2008, pero su enfoque en el dominio de Internet del Gobierno era demasiado limitado.

La Administración Obama inició sus esfuerzos en *ciberseguridad* con *Los 60 días de examen de las políticas sobre el ciberespacio.* Publicado en mayo de 2009, presenta una revisión sólida de dónde estaba el Gobierno en relación con la *ciberseguridad,* pero ofrecía poco de su visión de la forma de llegar a su destino. La principal recomendación fue que el presidente debería nombrar a un solo coordinador central de los esfuerzos nacionales y del Gobierno para las políticas de *ciberseguridad* (32).

Para Daniel Ventre (33), la política exterior de EE. UU. desde 1948 es «uno de los principales campos de batalla de los dos grandes partidos». El paso de una Administración demócrata a una republicana se traduce en nuevas formulaciones de las cuestiones estratégicas; así, la llegada de la administración republicana (Gobierno de G. W. Bush) está marcada por un cambio semántico en materia de defensa de misiles (pasando de la defensa nacional de misiles de la noción de defensa de misiles), indicativo de un cambio estratégico y de postura («de un Gobierno demócrata poco convencido [...] una Administración republicana decidida»)[4].

[4] GRAND, Camille. «La défense anti-missile: un nouveau paradigme stratégique? », *Revue Politique Etrangère,* 2001, vol. 66, n.° 4, pp. 811-826. http://www.persee.fr/articleAsPDF/polit_0032- 342x_2001_num_66_4_5125/article_polit_0032-342x_2001_num_66_4_5125.pdf.

Los programas de los partidos Republicano y Demócrata (Plataforma Republicana y Plataforma Nacional Demócrata) dedican un espacio relativamente pequeño al problema (33).

La Plataforma Republicana:

- El Partido Republicano es abiertamente hostil a una mayor regulación.
- Los ataques informáticos han seguido creciendo y el fenómeno crecerá. La estrategia de Obama se basa en las prácticas defensivas, aceptando el riesgo de un Pearl Harbor cibernético.
- La política de *ciberseguridad* Republicana se centraría en la desarrollo de capacidades ofensivas.
- Identifican amenazas: China, Rusia, el terrorismo, el ciberespacio…
- El gobierno debe mejorar la seguridad de sus propios sistemas.
- Los republicanos critican la reducción de los gastos de defensa durante el gobierno de Obama (señal de debilidad).
- Proponen el fomento de la cooperación público-privada. El Gobierno debe compartir la información que obtiene sobre la amenaza cibernética con el sector privado, y viceversa, sin poner en peligro la seguridad nacional.
- El Partido Republicano está a favor de la desregulación.

La Plataforma Demócrata:

- La amenaza cibernética está calificada como uno de las más grandes amenazas emergentes contra la seguridad nacional.
- Herramientas que EE. UU. solía emplear son ahora utilizadas por los delincuentes y terroristas, y por otros países para tratar de interrumpir o destruir infraestructuras vitales críticas para la economía, el comercio, la seguridad o el Ejército.
- Las soluciones que propone son el desarrollo de redes seguras y resilientes, la creación del primer *cibermando* dedicado a la *ciberseguridad*, la disuasión, la prevención, la detección y la defensa del país contra las intrusiones digitales.
- Lo anterior requiere inversiones en I+D, el desarrollo de una cultura de ciberseguridad y el fortalecimiento de la colaboración con los actores privados e internacionales.
- La regulación dirigida al fortalecimiento de la capacidad de *ciberseguridad* y basada en el respeto de los derechos de los ciudadanos.
- Neutralidad de la red, abierta a un Internet libre, que favorezca la innovación, la creación, el consumo y la libertad de expresión, libre de toda forma de censura y de violaciones de los derechos privados.

– La Administración Obama da más poder al Department of Homeland Security (DHS) en su misión de protección de los organismos civiles.

Similitudes y diferencias

– Ambos convergen en el reconocimiento de una importante amenaza de naturaleza cibernética contra la seguridad nacional, la necesidad de la cooperación público-privada y el intercambio de información.
– Las diferencias surgen sobre el papel del Gobierno federal en el establecimiento de normas de seguridad. Los republicanos son más reacios a imponer nuevas regulaciones sobre el sector privado (prefieren que la cooperación público-privada sea voluntaria) mientras que los demócratas son más sensibles con los derechos de privacidad del ciudadano.
– También se aprecian diferencias en la posición a adoptar: más defensiva para los demócratas y ofensiva para los republicanos.

De acuerdo con la conocida experta Melisa Hatada (con la que me reuní en Washington en 2012), responsable de la revisión de la política cibernética del presidente Obama y que también tuvo un puesto de gran responsabilidad en la seguridad informática en la Administración Bush, con el Sr. Romane la política de seguridad informática se enfocaría a la gestión: un análisis coste-beneficio por objetivos. Enfoque que no caracteriza la aproximación de Obama.

Debido a su dependencia del ciberespacio, los EE. UU. conscientemente deberían idear una estrategia para influir en el desarrollo del derecho consuetudinario internacional sobre cibernética en lugar de simplemente observar su desarrollo. La mejor manera de hacerlo es a través de una práctica estatal, reconoció. Debido al secreto en el que se envuelven muchas actividades del ciberespacio, en realidad se influye poco en el desarrollo de las normas. Un examen prudente de las acciones de EE. UU. –y la divulgación pública de algunas– ayudaría a establecer una línea de base para el comportamiento aceptable.

Después de que EE. UU. determine las acciones que cree que está autorizado a tomar en el ciberespacio, debe compartir abiertamente al menos ejemplos de las acciones que ha tomado. Además, sin duda debe mirar a la posibilidad de divulgar las acciones emprendidas en su contra. Al proponer algunas de sus propias acciones como aceptables y reconocer las tomadas en su contra como aceptables o inaceptables, EE. UU. podría liderar un diálogo sobre las normas cibernéticas, conduciendo a conclusiones que serían beneficiosas para su seguridad nacional (3).

Estas afirmaciones del coronel Gary Brown y la comandante Kira Poellet, de la Fuerza Aérea norteamericana, introducen el tema central: qué estrategia sigue y sobre todo qué estrategia debería seguir EE. UU. Por

lo que hemos visto hasta el momento, los EE. UU. practican una política activa en multitud de foros (Consejo de Europa, OSCE, ONU...) internacionales tratando de adaptar las normativas a sus propias necesidades o intereses. Examinemos sus estrategias.

La Estrategia de Ciberseguridad de los EE. UU., tiene dos líneas de acción principales:

- Mejorar su capacidad de adaptación a los incidentes cibernéticos.
- Reducir la amenaza cibernética.

El presidente Obama ha declarado que la «amenaza cibernética es uno de los más graves desafíos de la seguridad económica y nacional al que nos enfrentamos como nación» y que «la prosperidad económica de EE. UU. en el siglo XXI dependerá de la *ciberseguridad*». El presidente ordenó una revisión en profundidad de los esfuerzos del Gobierno para defender su infraestructura de información y comunicaciones que se tradujo en un informe titulado *Examen de las políticas del ciberespacio*. Para poner en práctica los resultados de este examen, el presidente ha nombrado un coordinador de *Ciberseguridad* de EE. UU. y creó la Oficina de *Ciberseguridad* en el Estado Mayor de la Seguridad Nacional.

El vicepresidente Biden (34) identificó en su discurso en la Conferencia sobre el CIberespacio de Londres dónde se encuentra EE. UU. en relación con los retos del futuro del ciberespacio:

> *En primer lugar, ¿qué actitud tomar para asegurarse de que la propia Internet siga siendo segura, abierta a la innovación y al mundo a través de la interoperabilidad, lo suficientemente segura como para ganarse la confianza de nuestro pueblo, y lo suficientemente fiable para apoyar su trabajo? Y, en segundo lugar, ¿cómo podemos lograr la seguridad de las naciones, las empresas y las personas en línea sin comprometer la apertura, que es el mayor atributo de Internet?*
>
> *Parece que la respuesta a estas preguntas es una prioridad fundamental, no solo para nuestra Administración sino para todos los que se reunieron en la sala, y para articular nuestra posición, hemos presentado la Estrategia Internacional para el Ciberespacio. Sabemos que necesitamos muchos años y el compromiso paciente y persistente con personas de todo el mundo para construir un consenso en el ciberespacio, pero no hay atajos, porque lo que los ciudadanos hacen en línea no debe, como algunos han sugerido, ser decretado únicamente por grupos de Gobiernos que toman decisiones desde arriba y en su favor. Hay algunos que tienen un punto de vista diferente. Buscan un instrumento jurídico internacional que conduzca al control gubernamental exclusivo sobre los recursos de Internet, las instituciones y los contenidos y las barreras nacionales a la libre circulación de información en línea. Pero esto daría lugar a un Internet fragmentado que no conecta*

a la gente, sino que los divide, un ciberespacio estancado, no innovador, y, finalmente, un ciberespacio menos seguro con menos confianza entre las naciones.

EE. UU. está detrás del actual enfoque que aprovecha lo mejor de los Gobiernos, del sector privado y la sociedad civil para gestionar la evolución técnica de Internet en tiempo real. Esta colaboración público-privada ha mantenido Internet en funcionamiento en todo el mundo.

Tenemos una expresión en nuestro país: si no está roto, no lo arregles. Sería un error, a nuestro juicio, romper con el sistema que ha funcionado tan bien durante tanto tiempo. Sin embargo, hay maneras de mejorar lo que estamos haciendo, por ejemplo, lograr una mayor transparencia y rendición de cuentas al Gobierno e instituciones de Internet, mediante la inclusión de más voces procedentes de los países en desarrollo y el apoyo a las iniciativas de éxito como el Foro de Gobernanza de Internet.

Estamos trabajando con otros países para combatir la delincuencia transnacional, incluido el de ayudar a otras naciones a construir sus capacidades de aplicación de la ley. Hemos ratificado y promovemos enérgicamente la Convención sobre «Cibercrimen» de Budapest, que establece los pasos que deben adoptar los países para reducir la delincuencia al tiempo que protege los derechos humanos. Y, como era de esperar, seguimos comprometidos con la lucha contra el terrorismo internacional y en frustrar los ataques terroristas que se han planeado y puesto en marcha en Internet. Podemos y debemos hacer todo esto sin tener que recurrir a una falsa solución que racionaliza la apropiación del gobierno de Internet. No hay duda en nuestra opinión de que cada nación debe proteger a sus ciudadanos contra la delincuencia y los ataques en línea, y fuera de línea. Pero hay que hacerlo de una manera que sea consistente con nuestros valores compartidos.

Y esto me lleva al concepto que es absolutamente fundamental, en nuestra opinión, llevar a cualquier negociación sobre el futuro del ciberespacio: los principios existentes del derecho internacional se aplicarán en línea tal como se hace fuera de línea. Internet representa y presenta nuevos desafíos, pero para resolverlos no es necesario empezar de cero. Los principios de derecho internacional no se suspenden en el ciberespacio. Se aplican allí con la misma fuerza y la misma urgencia (34).

Los EE. UU. trabajarán a nivel internacional para promover una información abierta, interoperable, segura y fiable y la infraestructura de comunicaciones que apoya el comercio internacional y el comercio, fortalece la seguridad internacional y promueve la libertad de expresión y la innovación para alcanzar esa meta; vamos a construir y mantener un entorno en el que las normas de conducta de una actuación

responsable guían, sostienen las asociaciones, y apoyan el estado de derecho en el ciberespacio (35).

Entre los objetivos de la estrategia se incluye un objetivo de defensa. Junto con otras naciones, fomentará un comportamiento responsable y se opondrá a aquellos que tratan de interrumpir las redes y sistemas, disuadirá y desalentará a los agentes maliciosos, y se reservará el derecho de defensa de estos recursos nacionales vitales cuando sea necesario y apropiado. Con dos formas de acción:

- *Disuasión. Proteger las redes de alto valor requiere de sólidas capacidades de defensa. EE. UU. continuará fortaleciendo su defensa de la red y su capacidad para resistir y recuperarse de las interrupciones y otros ataques. Contra esos ataques más sofisticados que producen daños, vamos a actuar con planes de respuesta bien desarrollados para aislar y mitigar la interrupción de nuestras máquinas, los efectos limitantes en nuestras redes y sus posibles efectos en cascada más allá de ellos.*
- *Intimidación. Los EE. UU. se asegurarán de que los riesgos asociados con atacar o explotar nuestras redes sean mucho mayores que los beneficios potenciales. Cuando sea necesario, los EE. UU. responderán a actos hostiles en el ciberespacio como lo haríamos con cualquier otra amenaza a nuestro país. Todos los estados poseen un derecho inherente a la legítima defensa, y ciertos actos hostiles realizados a través del ciberespacio podrían obligar a acciones en el marco de los compromisos que tenemos con nuestros socios de tratados militares; nos reservamos el derecho de utilizar todos los medios necesarios –diplomáticos, informativos, militares y económicos– que procedan y sean compatibles con el derecho internacional aplicable, a fin de defender a nuestra nación, nuestros aliados, nuestros socios y nuestros intereses. Al hacer esto, vamos a agotar todas las opciones antes de la fuerza militar siempre que podamos, cuidadosamente sopesar los costos y riesgos de la acción contra los costos de la inacción, y actuaremos de una manera que refleje nuestros valores y se refuerce nuestra legitimidad, en busca de amplio apoyo internacional siempre que sea posible.*

Es más, entre las políticas prioritarias, se incluye la militar:

- *Reconocer y adaptarse a la creciente necesidad de redes militares fiables y seguras. Reconocemos que nuestras Fuerzas Armadas dependen cada vez más de las redes que las apoyan, y vamos a trabajar para que nuestras Fuerzas Armadas sigan estando totalmente equipadas para operar incluso en un ambiente donde otros podrían tratar de interrumpir sus sistemas u otras infraestructuras vitales para la defensa nacional. Como todas las naciones, EE. UU. tiene un interés apremiante en la defensa de sus recursos naciona-*

les vitales, así como nuestros principios y valores fundamentales, y estamos comprometidos en la defensa contra aquellos que tratan de impedir nuestra capacidad para hacerlo.

– *Desarrollar y mejorar las alianzas militares existentes para hacer frente a las posibles amenazas en el ciberespacio. Ninguna nación sola puede lograr la «ciberseguridad», y son necesarios mayores niveles de cooperación internacional para hacer frente a esos actores que tratan de perturbar o explotar nuestras redes. Este esfuerzo comienza por reconocer que la naturaleza interconectada de los sistemas en red de nuestros aliados más cercanos, tales como las de la OTAN y sus estados miembros, crea oportunidades y nuevos riesgos en el futuro. Los EE. UU. seguirán trabajando con los militares y sus contrapartes civiles de nuestros aliados y socios para ampliar el conocimiento de la situación y los sistemas compartidos de alerta, aumentar nuestra capacidad de trabajar juntos en tiempos de paz y crisis y desarrollar los medios y el método de la legítima defensa colectiva en el ciberespacio.*

– *Ampliar la cooperación en el ciberespacio con aliados y socios para aumentar la seguridad colectiva. Mediante el desarrollo de un entendimiento común de los procedimientos normalizados de trabajo, nuestras Fuerzas Armadas pueden mejorar la seguridad a través de la coordinación y un mayor intercambio de información, estos compromisos se reducirá percepciones erróneas sobre las actividades militares y la posibilidad de distensión y diálogos comportamiento intercambios de mejores prácticas para mejorar las capacidades asociadas, como la digital, forense, desarrollo de fuerza de trabajo, y la penetración de la red y las pruebas de resistencia serán importantes para este esfuerzo de EE. UU., que trabajará en estrecha colaboración con los estados de ideas afines para aprovechar las capacidades, reducir el riesgo colectivo y promover iniciativas de participación múltiple para impedir las actividades maliciosas en ciberespacio.*

«Las normas internacionales son fundamentales para el establecimiento de una infraestructura digital segura y próspera», afirma el *Cyberspace Policy Review* (2011). «EE. UU. tiene que desarrollar una estrategia diseñada para conformar un entorno internacional y trabajar junto a naciones afines en una serie de cuestiones, entre ellas unas normas aceptables de jurisdicción territorial, la responsabilidad soberana y el uso de la fuerza». Abordar estos temas requiere de los EE. UU. trabajar con todos los países –incluidos los en vías de desarrollo, organismos internacionales, aliados militares y socios de inteligencia–.

Más de una docena de organizaciones internacionales –incluyendo las Naciones Unidas, el G-8, la OTAN, el Consejo de Europa, el foro Coope-

ración Económica Asia-Pacifico, la Organización de los Estados Americanos, la Organización para la Cooperación y el Desarrollo Económicos, la Unión International de Telecomunicaciones (UIT) y la Organización Internacional de Normalización (ISO)– abordan cuestiones relativas a la infraestructura, información y comunicaciones. Los acuerdos, normas o prácticas promulgadas en estas organizaciones tienen efectos globales y no pueden ser ignorados. El gran número, variedad y diferentes enfoques de estas organizaciones pone a prueba la capacidad de muchos Gobiernos, entre ellos el de EE. UU., para participar adecuadamente (36).

Cuando el 12 de marzo, como todos los años por estas fechas, el director de Inteligencia Nacional de los EE. UU., James R. Clapper, presento la evaluación de la amenaza mundial de la comunidad de inteligencia de los EE. UU., dentro de las amenazas globales, la cibernética ocupaba el primer lugar, por delante de terrorismo y delincuencia transnacional organizada, proliferación de ADM, contraespionaje, medidas contraespaciales o recursos naturales: la inseguridad y la competencia, entre los argumentos.

Inicialmente, define qué entienden por *ciberamenazas*:

> *En los EE. UU., definimos ciberamenazas en términos de «ciberataques» y «ciberespionaje» (37): un «ciberataque» es una operación ofensiva no cinética con la intención de crear efectos físicos o manipular, alterar o suprimir datos. Puede ir desde una operación de denegación de servicio que impide temporalmente el acceso a un sitio «web» a un ataque contra una turbina de generación de energía que causó un daño físico y un apagón que duró varios días. El «ciberespionaje» se refiere a intrusiones en las redes de acceso a información sensible diplomática, militar o económica.*

Luego, se centra en los riesgos crecientes de la infraestructura crítica. Descartando por el momento ataques devastadores por parte de *ciberactores* avanzados como Rusia o China (37):

> *Juzgamos que hay una remota posibilidad de un «ciberataque» importante en contra de los sistemas de infraestructura crítica de EE. UU. durante los próximos dos años, que daría lugar a una interrupción de los servicios de largo plazo y a gran escala como un corte de energía regional. El nivel de conocimientos técnicos y sofisticación operativa necesarios para este tipo de ataque, incluyendo la posibilidad de crear un daño físico o superar los factores de mitigación como el manual, estará fuera del alcance de la mayoría de los actores durante este marco de tiempo. Es poco probable que actores avanzados en el ciberespacio –como Rusia y China– lancen un ataque devastador contra los EE. UU. fuera de un conflicto militar o una crisis que ellos crean que amenaza a sus intereses vitales.*

Actores aislados estatales o no estatales pueden realizar ataques menos sofisticados como una forma de represalia o provocación. Estos actores

muy motivados podrían acceder a redes mal protegidas que controlan las funciones básicas, como la generación de energía, durante los próximos dos años, aunque su capacidad de causar un gran impacto y perturbaciones sistémicas probablemente será limitado. Al mismo tiempo, existe el riesgo de que los ataques sofisticados tuvieran resultados significativos debido a inesperadas configuraciones de sistema, o que la mayor vulnerabilidad de un nodo podría extenderse y contaminar otras partes de un sistema en red (37).

La estrategia del Departamento de Defensa para operar en el ciberespacio de julio 2011 contempla cinco iniciativas estratégicas. La iniciativa estratégica n.º 4 propone «construir relaciones sólidas con nuestros socios y aliados internacionales para fortalecer la *ciberseguridad* colectiva».

Con su compromiso internacional, el Departamento de Defensa apoyará la estrategia internacional de EE. UU. para el ciberespacio y el compromiso del presidente con las libertades fundamentales, la privacidad y el libre flujo de información. El Departamento de Defensa colaborará en los esfuerzos para avanzar en el desarrollo y promoción de unas normas internacionales para el ciberespacio y de los principios que promuevan la apertura, interoperabilidad, seguridad y fiabilidad.

Mientras continúa desarrollándose la cooperación internacional en materia de ciberespacio, el Departamento de Defensa promoverá la cooperación en el ciberespacio con sus aliados más cercanos para defender los intereses en el ciberespacio. El Departamento de Defensa trabajará con sus aliados y socios internacionales para desarrollar capacidades comunes de alerta, participar en la creación de capacidades y llevar a cabo actividades conjuntas de capacitación. Esto creará oportunidades para iniciar diálogos para intercambiar las mejores prácticas en áreas como la forense, el desarrollo de las capacidades, participación en ejercicios y alianzas público-privadas. Además, el desarrollo de los acuerdos para el reparto de carga puede jugar a favor al fortalecer las capacidades centrales de cada país, y lo que reforzará áreas donde los socios son menos competentes aumentará su capacidad y fortalecerá la *ciberseguridad* colectiva.

En su declaración ante la Comisión del Senado de Servicios Armados el 12 marzo 2013, el general Keith B. Alexander (38), comandante del Cibermando de EE. UU., indicó:

> *El Cibermando de los EE. UU. opera en un entorno dinámico y controvertido que cambia literalmente sus características cada vez que alguien enciende la alimentación en un dispositivo de red. Los límites geográficos son quizás menos evidentes en el ciberespacio, pero cada servidor, línea de fibra óptica, antena de telefonía móvil, memoria USB, «router» y ordenador portátil es propiedad de alguien y reside en alguna localidad física. De esta manera, el ciberespacio se asemeja al dominio terrestre –todo tiene un poseedor, y puede ser reformado–.*

> *En este ambiente, que es a la vez ordenado y caótico, beneficioso y peligroso, nosotros en USCYBERCOM tenemos que centrarnos en los actores que poseen la capacidad –y, posiblemente, la intención– de perjudicar los intereses de nuestra nación en el ciberespacio o el uso de medios informáticos para causarnos daño de otras formas. Por desgracia, la lista de los actores de interés para nosotros es cada vez mayor y cada vez también mayor en cuanto a la variedad y complejidad de las formas en que pueden afectar a nuestras operaciones y seguridad. Los agentes estatales siguen encabezando la lista de preocupaciones.*
>
> *Estamos seguros de que los líderes extranjeros creen que un ataque devastador sobre la infraestructura crítica y la población de Estados Unidos por medios cibernéticos sería correctamente remontado hasta su origen y provocaría una respuesta rápida y proporcionada. No obstante, es posible que algún futuro régimen o actor cibernético pudieran malinterpretar el impacto y la certeza de nuestra determinación.*

De acuerdo con la estrategia del Departamento de Defensa para operar en el ciberespacio, el Cibermando de los EE. UU. y la NSA están juntos apoyando al departamento en construir:

- una arquitectura defendible;
- conocimiento de la situación global y una imagen operativa común;
- un concepto para el funcionamiento en el ciberespacio;
- las fuerzas cibernéticas capacitadas y listas, y
- capacidad para actuar cuando sea autorizado.

Y es en este punto donde resalta la importancia de la cooperación con socios y aliados:

> *También nos beneficiamos al compartir con los servicios y organismos asociados y aliados clave.*
>
> *Además, las nuevas reglas de enfrentamiento para el ciberespacio actualmente en desarrollo cumplirán con y apoyarán a las directrices de política recientemente emitidas en «ciberoperaciones» estadounidenses.*

El general de Ejército Keith B. Alexander afirmó que el Mando está desarrollando equipos que protegerían los intereses de la nación en el ciberespacio, junto con las tácticas, técnicas y procedimientos y la doctrina que describe cómo los equipos trabajarán en ese ambiente (39).

> *Estos equipos para defender la nación no son equipos defensivos, son equipos ofensivos que el Departamento de Defensa podría utilizar para defender a la nación si fueran atacados en el ciberespacio (...). Trece de los equipos que estamos creando son solo para ese conjunto de misio-*

> *nes. También estamos creando 27 equipos que apoyarían comandos combatientes y a su proceso de planificación de capacidades cibernéticas ofensivas.*

El CYBERCOM también tiene una serie de equipos que van a defender las redes del Departamento de Defensa en el ciberespacio. La intención es poner en pie cerca de un tercio de los equipos antes de septiembre, otra tercera parte en septiembre de 2014, y la tercera final para septiembre de 2015.

> *Estos tres grupos de equipos son el núcleo, la construcción por el que estamos trabajando con los servicios para desarrollar nuestros cuadros cibernéticos.*

Por su parte, el general C. R. Kehler, comandante del Mando Estratégico de EE. UU., indicó que mejorar la capacidad del Departamento de Defensa para operar de manera efectiva en el ciberespacio requería una inversión en cinco grandes áreas: arquitectura defendible (ambiente de información conjunta), fuerzas entrenadas y listas, mando y control efectivo, conocimiento de la situación global y reglas de enfrentamiento para entablar combate para defender a la nación en el ciberespacio. De todas ellas, la inversión más urgente es aumentar el número, la formación y la preparación de las *ciberfuerzas* (40).

La expansión aumentará el CYBERCOM del Departamento de Defensa a más de 4.000 personas, frente a los actuales 900 –de acuerdo con un funcionario estadounidense–. Un reto formidable para el crecimiento del Mando sería encontrar, formar y retener a un número tan grande de personas cualificadas.

En octubre, el señor Panetta advirtió seriamente de que EE. UU. se enfrenta a la posibilidad de un «Pearl Harbor cibernético» y cada vez eran más vulnerables a piratas informáticos extranjeros que podrían desmantelar la red nacional de energía eléctrica, el sistema de transporte, la red financiera o la del Gobierno. Dijo que «una nación agresora» o grupo extremista podría causar una catástrofe nacional, y que él estaba reaccionando a la creciente asertividad y los avances tecnológicos por los adversarios de la nación, identificados por los funcionarios como China, Rusia, Irán y los grupos militantes (41).

Funcionarios de Defensa dijeron que el señor Panetta estaba especialmente preocupado por un ataque informático en agosto pasado contra la petrolera estatal saudí Aramco, que infectó e inutilizó a más de 30.000 ordenadores. En octubre, los funcionarios de inteligencia estadounidenses dijeron que estaban cada vez más convencidos de que los ataques saudíes se habían originado en Irán. Describieron una guerra en las sombras emergente de ataques y contraataques en curso entre EE. UU. e Irán en el ciberespacio. Entre los funcionarios estadounidenses, la sospecha

se ha centrado en los Cybercorps, creado en 2011 por el Ejército de Irán, en parte en respuesta a los ataques informáticos estadounidenses e israelíes sobre la planta de enriquecimiento de uranio iraní en Natanz. No hay pruebas contundentes, sin embargo, los ataques fueron sancionados por el Gobierno iraní (41).

Un resumen de EE. UU. en el ciberespacio para 2013 sería: ninguna ley y un entorno de negociación internacional duro, pero se aprecian progresos por parte del poder ejecutivo en el esclarecimiento de las actividades militares digitales, vinculándolas a la *ciberdefensa,* y en el establecimiento de normas para el desarrollo de una infraestructura crítica más segura. De ser ampliamente adoptadas las nuevas normas, que se centran en las vulnerabilidades más frecuentes, se acelerará esta tendencia. La *ciberseguridad* en EE. UU. ha mejorado a pesar del *impasse* en el Congreso, pero ulteriores progresos requerirán del acuerdo internacional para limitar la actividad maliciosa en el ciberespacio, lo que parece ser una posibilidad remota. Los EE. UU. son más seguros de lo que eran hace cinco años, pero todavía no son seguros (10).

Conclusiones

Parece existir una práctica unanimidad a la hora de indicar la necesidad de negociar acuerdos internacionales que regulen el ciberespacio. Pero parecen existir diferencias insalvables en cuanto a qué deberían incluir esos acuerdos, el carácter de los mismos y las organizaciones de referencia.

Podríamos definir tres cosmovisiones básicas: la *ciberliberal* defensiva representada por la UE, y compartida por casi todos los países europeos; la *ciberliberal* ofensiva representada por los EE. UU., y la *cibernacionalista*-aislacionista representada por China y Rusia. A ellas hay que añadir las que, como Irán o Corea del Norte, sin disponer de la sofisticación de las grandes potencias, disponen de unas capacidades ofensivas a tener en cuenta.

El paso de una Administración demócrata a una republicana en EE. UU. se traduce en un cambio estratégico y de postura «de un Gobierno demócrata poco convencido (...) a una Administración republicana decidida». De acuerdo con Melissa Hathaway, con el Sr. Romney la política de seguridad informática se enfocaría a la gestión: un análisis coste-beneficio por objetivos; enfoque que no caracteriza la aproximación de Obama.

Más de una docena de organizaciones internacionales –incluyendo las Naciones Unidas, el G-8, la OTAN, el Consejo de Europa, OSCE, el foro Cooperación Económica Asia-Pacifico, la Organización de los Estados Americanos, la Organización para la Cooperación y el Desarrollo Económicos, la Unión International de Telecomunicaciones (UIT) y la Organización Internacional de Normalización (ISO)– están involucradas en seguridad ciber-

nética. EE. UU. y Rusia tienen sus propias organizaciones de referencia, Consejo de Europa y OSCE en el caso norteamericano y Naciones Unidas en el ruso. Ambos se bloquean respectivamente en sus propuestas.

Rusia y China recibieron un sorprendente grado de apoyo en su propuesta ante la ONU. Muchos países están desencantados con el modelo ortodoxo y se mueven en silencio en hacia un modelo «no occidental» de la gobernanza de Internet. Los regímenes autoritarios se han aprovechado de esta insatisfacción y la intentan utilizar para sus propios fines políticos.

El establecimiento de normas para el empleo del ciberespacio por parte de los estados no debería requerir una modificación de las leyes internacionales consuetudinarias ni considerar obsoletas las leyes actuales; lo que sería necesario es aclarar cómo esas normas existentes se aplican y que nuevos elementos serían necesarios para que fueran útiles.

En cualquier caso, se tienen que mantener unos valores esenciales como son: respeto a los derechos fundamentales de libertad de expresión y asociación, incluso *online,* respeto a la propiedad intelectual (patentes, *copyright*), y evitar interferencias estatales injustificadas, pero permitiendo la lucha contra los *ciberdelincuentes*, asegurando el Estado de derecho y evitando la creación de santuarios para estos delincuentes.

Todo país tiene derecho a la autodefensa contra actos de agresión en el ciberespacio, autodefensa enfocada en el mantenimiento del funcionamiento de la red global y en la mejora de *ciberseguridad*.

Otros elementos a tener en cuenta a la hora de redactar normas son: interoperabilidad global, estabilidad de la red y libre flujo de información, acceso fiable a todo individuo y presencia de grupos distintos del Gobierno en la gobernanza de Internet, abierta a actores no gubernamentales

En cualquier caso, no debemos perder la esperanza de que las grandes *ciberpotencias* lleguen a un acuerdo que permita fomentar la confianza y aumentar la transparencia reduciendo los crecientes riesgos asociados con los cada vez más numerosos y cada vez más complejos ataques cibernéticos. En unos años podría alcanzarse un acuerdo…

¡O no!

Bibliografía

1. OBAMA, Barak. *Discurso sobre el estado de la Unión de Barack Obama.* Washington: The White House, 2013.
2. STEPHENS, Bret. «The Limits of Stuxnet». *The Wall Street Journal.* [En línea] 18 de enero de 2011 [citado el 2 de enero de 2013]. http://online.wsj.com/article/SB10001424052748703396604576087632882247372.html.

3. BROWN, Gary y POELLET, Keira. «The Customary International Law of Cyberspace», IV, 2012. *Strategic Studies Quarterly,* otoño de 2012, vol. 6, págs. 126-145.
4. HOWEIDY, Amira. «Big Brother or war criminal?» *Al Ahram weekly.* [En línea] 11 de junio de 2013 [citado el 2013 de junio de 15]. http://weekly.ahram.org.eg/News/2947/19/Big-Brother-or-war-criminal-.aspx.
5. *Estrategia Nacional Militar de los Estados Unidos de América.* Washington, EE. UU.: Joint Chief of Staff, 2011.
6. SOMMER, Peter y BROWN, Ian. *Reducing Systemic Cybersecurity Risk.* Informe OCDE, 2011.
7. PRINCE, Matthew. «The DDoS That Almost Broke the Internet». [En línea] 27 de marzo de 2013 [citado el 28 de marzo de 2013]. *Cloud Flare.* http://blog.cloudflare.com/the-ddos-that-almost-broke-the-Internet.
8. PÉREZ, Jesús. «Cómo Cyberbunker atacó a Spamhaus y casi se llevó a medio Internet por delante». *Security by Default.* [En línea] 28 de marzo de 2013 [citado el 12 de mayo de 2013]. http://www.securitybydefault.com/2013/03/como-cyberbunker-ataco-spamhaus-y-casi.html.
9. VENTRE, Daniel. «Japon: stratégies de cyberdéfense, Multi-System and Internet-Security-Cookbook». *MISC,* 2012, n° 64, págs. 65-73.
10. LEWIS, James Andrew. *Critical Questions for 2013: Global Challenges. What's Next in Cybersecurity?* [En línea] 25 de enero de 2013 [citado el: 30 de marzo de 2013]. Center for Strategic and International Studies. http://csis.org/publication/critical-questions-2013-global-challenges.
11. BAGCHI, Sohini. «India needs more warriors in the cyber space». *Cxotoday.com.* [En línea] 3 de mayo de 2013 [citado el 12 de mayo de 2013]. http://www.cxotoday.com/story/india-needs-more-warriors-in-the-cyber-space/.
12. ZORZ, Zeljka. «India has a new National Cyber Security Policy». *Help net security organization.* [En línea] 10 de mayo de 2013 [citado el 12 de mayo de 2013]. http://www.net-security.org/secworld.php?id=14891.
13. PERTERMANN, Kerstin. *Conference report: Challenges in Cybersecurity, Risks, Strategies, and Confidence-Building International Conference.* Hamburgo: Institute for Peace Research and Security Policy at the University of Hamburg, 2011.
14. HEICKERÖ, Roland. *Emerging Cyber Threats and Russian Views on Information Warfare and Information Operations.* Estocolmo: Swedish Defence Research Agency Division of Defence Analysis, 2010.
15. FEDORENKO, Andrei. «The Fight Over the Draft. UN Convention on International Information Security». *Regulatory cyber security: The*

FISMA focus IPD. [En línea] 15 de julio de 2012 [citado el 12 de mayo de 2013]. http://www.thecre.com/fisma/?p=2173.

16. DEAL, Jacqueline N. *IGCC Workshop Report on China and Cybersecurity. Information Warfare Doctrine. Chinese Information War: Historical Analogies and Conceptual Debates.* San Diego: Universidad de California, 2012.
17. YUXIAO, Li. *National Cybersecurity Policy Cyberspace Security and International Cooperation in China.* San Diego: Universidad de California, 2012.
18. STOKES, Mark. *People's Liberation Army Infrastructure for Cyber Reconnaissance.* San Diego: Universidad de California, 2012.
19. SCHNEIDER, Deborah. *United States Mission to the OSCE Cyber Security Keynote Address by Dr. Deborah Schneider, U. S. Department of State as Delivered to the Joint FSC/PC.* Viena: OSCE, 2010.
20. WEGENER, Henning. *Regulating Cyber Behavior: Some Initial Reflections on Codes of Conduct and Confidence Building Measures.* [En línea] 23 de agosto de 2012 [citado el 29 de marzo de 2013]. http://www.federationofscientists.org/PlanetaryEmergencies/Seminars/45th/Wegener publication.docx.
21. HEALEY, Jason y VAN BOCHOVEN, Leendert. *NATO's Cyber Capabilities: Yesterday, Today, and Tomorrow.* Washington: The Atlantic Council of the United States, 2011.
22. GEERS, Kenneth. *Cyberspace and the changing nature of warfare.* [En línea] 27 de agosto de 2008 [citado el: 31 de marzo de 2013]. http://www.scmagazine.com/cyberspace-and-the-changing-nature-of-warfare/article/115929/.
23. ARCHICK, Kristin. *CRS Report for Congress. Cybercrime: The Council of Europe Convention.* Washington: Congressional Research Service, 2004.
24. TIKK, Eneken. *Comprehensive legal approach to cyber security 2011.* Tarfu, Estonia: Faculty of Law, University of Tartu, 2011.
25. SCHJØLBERG, Stein y GHERNAOUTI-HÉLIE, Solange. *A Global Protocol on Cybersecurity and Cybercrime: An Initiative for peace and Security in Cyberspace,* segunda edición. Oslo: AiTOslo, 2011.
26. OSCE_MC.DEC/7/06. *DECISION No. 7/06 Countering the Use of the Internet for Terrorist Purposes.* Bruselas: OSCE, 2006.
27. [En línea] 16 de octubre de 2009 [citado el 31 de marzo de 2013]. EE. UU.: OSCE, 2013. https://dazzlepod.com/cable/09STATE107552/.
28. Council Framework Decision 2005/222/JHA. *Official Journal of the European Union.* [En línea] 16 de marzo de 2005 [citado el 31 de marzo de 2013]. http://eur-lex.europa.eu/LexUriServ/site/en/oj/2005/l_069/l_06920050316en00670071.pdf.

29. UE. *Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace.* Bruselas: European Commission & High Representative of the European Union for Foreign Affairs And Security Policy, 2013.
30. KAGAN, Robert. *Paradise and Power: America and Europe in the New World Order.* Londres: Atlantic Books, 2004.
31. BAILEY, Eric. *«Nothing Can Justify Torture»: An Interview with Noam Chomsky on Obama's Human Rights Record.* [En línea] 12 de diciembre de 2012 [citado el 30 de marzo de 2013]. http://chomsky.info/interviews/20121212.htm.
32. NEWMEYER, Kevin P. *Who should lead U.S. cyber security efforts? PRISM*, 2012, vol. 3, n.º 2, págs. 115-126.
33. VENTRE, Daniel. *La politique de cyberdéfense peut-elle être a-politique?* Paris: Ministère de la défense Délégation aux Affaires Stratégiques, 2013.
34. BIDEN, Joseph R. *VP's Remarks to London Cyberspace Conference.* Londres: The White House, 2011.
35. *International Strategy for Cyberspace.* Washington: The White House, 2011.
36. *Cyberspace Policy Review.* Washington: The White House, 2011. http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf.
37. CLAPPER, James R. *Worldwide Threat Assessment of the US Intelligence Community 2013.* Washington D. C.: Office of the Director of National Intelligence, 12 de marzo de 2013.
38. ALEXANDER, Keith B. *Statement of general Keith B. Alexander Commander United States Cyber Command before the Senate Committee on Armed Services.* Washington: United States Cyber Command, 2013.
39. PELLERIN, Cheryl. American Forces Press Service. Cybercom Builds Teams for Offense, Defense in Cyberspace. [En línea] 12 de marzo de 2013 [citado el 30 de marzo de 2013]. http://www.defense.gov/news/newsarticle.aspx?id=119506.
40. KEHLER, C. R. *Statement of general C. R. Kehler Commander United States Strategic Command before the Senate Committee on Armed Services.* Washington: United States Strategic Command, 12 de marzo de 2013.
41. BUMILLER, Elisabeth. «Pentagon to Beef Up Cybersecurity Force to Counter Attacks», *The New York Times*. [En línea] 29 de marzo de 2013 [citado el 31 de marzo de 2013]. www.nytimes.com/2013/01/28/us/pentagon-to-beef-up-cybersecurity-force-to-counter-attacks.html.
42. OCDE. *Future Global Shocks. Improving Risk Governance.* París: OCDE, 2011.

43. FROOMKIN, Michael. «Cybercrime Treaty Goes Live». *Discourse.net.* [En línea] 19 de marzo de 2004 [citado el 31 de marzo de 2013]. http://www.discourse.net/archives/2004/03/cybercrime_treaty_goes_live.html.
44. SAFIRE, William. «The Farewell Dossier». *The New York Times.* [En línea] 2 de Febrero de 2004 [citado el 2 de enero de 2013]. http://www.nytimes.com/2004/02/02/opinion/the-farewell-dossier.html?ref=williamsaire.
45. *Estrategia Española de Seguridad.* Madrid: Gobierno de España, 2011.