XI Congreso Español de AECPA
GT 6.3 Estudios estratégicos y seguridad internacional.

"Inteligencia y Ciberdefensa; nuevos paradigmas en las Estrategias de Seguridad Nacional."

Autor: Celso Perdomo González (Universidad de Las Palmas de Gran Canaria)
cperdomo@dede.ulpgc.es

Resumen:
La tendencia de los últimos cinco años en el entorno de la ciberseguridad, y la ciberdefensa, ha ido evolucionando en un "ecosistema" cada vez más complejo, dinámico e interrelacionado. Los incidentes de seguridad cibernética trascienden el ámbito político, de comunicación social, desestabilizan el marco económico-financiero, y producen vulnerabilidad de las infraestructuras críticas; así las ciberamenazas comienzan a tener la consideración de político-estratégicas.
Analizando aquellos países y organizaciones que han realizado, se encuentran realizando o actualizando estrategias de ciberseguridad y/o ciberdefensa; se constata que existe ya una tendencia para que la comunidad de inteligencia; agencias de inteligencia y las unidades de inteligencia militar tengan un papel preponderante y significativo en la orientación general de la ciberseguridad.

Palabras clave:
Ciberseguridad, Ciberdefensa, Inteligencia, Estrategias de Seguridad Nacional.

Nota biográfica del autor:
Ingeniero Industrial. Master Universitario en Gestión de la Calidad, ULPGC (2000-2001). Diploma de Estudios Avanzados en Tecnologías de la Información y sus aplicaciones, ULPGC (2000-2002). Master Universitario en Paz, Seguridad y Defensa, IUGM, UNED (2009-2012). Doctorando en la ULPGC. Inspector-Analista de Servicios en el Cabildo Insular de Gran Canaria.

1. Introducción.

En los últimos cinco años ha habido una creciente preocupación en el entorno de la "seguridad internacional" por la ciberseguridad, la ciberdefensa y el control e invulnerabilidad de las infraestructuras críticas con soporte en Internet.

La Comisión Europea, junto con la Alta Representante de la Unión para Asuntos Exteriores y Política de Seguridad, ha publicado recientemente una estrategia de ciberseguridad acompañada de una propuesta de Directiva de la Comisión sobre la seguridad de las redes y de la información (European Commission, 2013). Se prevén una serie de medidas específicas para reforzar la ciberresiliencia de los sistemas informáticos, reduciendo la delincuencia en la red y fortaleciendo la política de ciberseguridad y ciberdefensa internacional de la UE.

La estrategia articula la visión de la UE sobre la ciberseguridad en torno a cinco prioridades:

- la ciberresiliencia;
- la reducción drástica de la delincuencia en la red;
- el desarrollo de una política de ciberdefensa y de las capacidades correspondientes en el ámbito de la Política Común de Seguridad y Defensa (PCSD);
- el desarrollo de los recursos industriales y tecnológicos necesarios en materia de ciberseguridad;
- el establecimiento de una política internacional coherente del ciberespacio en la Unión Europea y la promoción de los valores europeos esenciales

Aun determinando las capacidades tecnológicas necesarias en este ámbito, cada una las naciones está planteando una estrategia diferenciada fundamentada única y exclusivamente en sus capacidades militares o en otras mixtas sobre la base conceptual del término (Libicki, 2009, 4). A modo de ejemplo, Estados Unidos ha planteado en los últimos meses nuevas estrategias, planes y políticas de actuación (Pereda, 2013), para adecuar sus organizaciones de seguridad y defensa ante lo que se ya se denomina "ciberguerra fría" (Caño, 2013).

En nuestro país, al igual que el resto del mundo, el número de ciberincidentes crece exponencialmente, así el director del Centro Nacional de Inteligencia, CNI, General Félix Sanz Roldán, comentaba que en lo que iba de año el Centro había recibido más de 200 ataques, frente a la veintena que se producían en el año 2009 (Villarejo, 2013).

2. ¿Qué es la Ciberseguridad?

El informe de Riesgos Mundiales del *World Economic Forum* (2012) incluye una descripción y un análisis de los datos asociados a 50 riesgos mundiales repartidos en cinco categorías: económica, medioambiental, geopolítica, social y tecnológica. Entre los riesgos tecnológicos, los considerados como de mayor probabilidad e impacto son: ciberataques, fallo de los sistemas críticos e incidentes masivos de fraude o robo de datos.

En este sentido, lo que el informe define como “el lado oscuro de la conectividad” muestra la parte del mapa de riesgos mundiales relacionados con la ciberdelincuencia y la alteración de sistemas. Este tipo de riesgos podrían intensificar las preocupaciones tradicionales en materia de seguridad, como la resolución diplomática de los conflictos y el terrorismo. Además la potencial inoperatividad de cualquiera de las llamadas “infraestructuras críticas” se considera como el centro de gravedad de las amenazas de naturaleza tecnológica, señalando igualmente que, aunque el riesgo de que la probabilidad de que una sola vulnerabilidad pudiera provocar la caída en cascada de otras infraestructuras críticas (o las redes que las sustentan) es relativamente baja, tendría, no obstante, un altísimo impacto. En su parte final la sucesión de hechos podría claramente minar la gobernabilidad global.

Los ciberataques se están convirtiendo en un arma "barata", "silenciosa" y "fácil de enmascarar" para cualquier organización con intereses hostiles, y puede tener efectos desastrosos en aquellos países u organizaciones que los sufren (Libicki, 2009, 33) Podemos comprobar prácticamente en tiempo real por medio de la herramienta de Deutsche Telekom, Sicherheitstacho.eu los ciberincidentes, ciberataques con información sobre su naturaleza, país de origen y servicios objetivo (Network World, n.d.).

Es importante tener en cuenta que la ciberdefensa no debe ser una actividad aislada en sí misma, sino que debería estar incluida, o contemplarse desde las siguientes perspectivas: Estrategias de Seguridad Nacional, Protección de Infraestructuras Críticas, Lucha contra Organizaciones Terroristas y Criminales (OECD, 2011).

Aún así y como veremos en los siguientes epígrafes, la tendencia de los últimos meses, siguiendo el modelo de Estados Unidos de América es redactar documentos específicos en el ámbito de ciberdefensa o ciberseguridad, aun cuando estos países carezcan de Estrategias de Seguridad Nacional.

3. Operaciones de Información; entre la Ciberseguridad y la Ciberdefensa.

La Doctrina Conjunta de Operaciones de Información de Estados Unidos (Joint Publication 3-13, 2013) expone que "para tener éxito, es necesario que las fuerzas armadas estadounidenses obtengan y mantengan la superioridad de información". Las operaciones de información se definen como el empleo integral de la guerra electrónica (EW), las operaciones de las redes de computadoras (CNO), las operaciones psicológicas (PSYOP), el engaño militar *military decepction*, (MILDEC) y las operaciones de seguridad (OPSEC), en conjunto con capacidades específicas de apoyo, para influenciar, interrumpir, corromper o usurpar las decisiones de los adversarios humanos y sus sistemas para proteger a las nuestras.

MILDEC promueve el análisis equivocado, provocando al adversario a llegar a conclusiones falsas, mientras que las operaciones de seguridad (OPSEC) buscan negar información verdadera a un adversario y prevenir que lleguen a conclusiones puntuales; estas últimas se vinculan con la Doctrina de Inteligencia de EEUU (Joint Publication 2-12, 2007).

Así según la doctrina estadounidense, se especifica un nivel físico asociado a equipos, otro de aplicaciones y procedimientos y un último nivel vinculado al uso de la información, su percepción y manipulación. Si adaptamos el modelo propuesto por Daniel Ventre (2012, 302-306), podemos definir los tres niveles del ciberespacio como:

- Una primera capa, la capa física de las infraestructuras y hardware;

- Una segunda capa de software y aplicaciones; y

- Tercera capa, llamada "cognitiva". Esta capa está vinculada al ámbito de la comunicación, de la generación de opinión pública y de las percepciones personales y sociales.

Este modelo de tres capas se puede utilizar para:

- Volver a examinar nuestra percepción y representación de la amenaza: ¿hay tipos especiales de operaciones, tipos de agresores y habilidades específicas que corresponden a cada capa?

- Organizar ciberdefensa. Esto supone tener en cuenta los aspectos técnicos, sino también de las capacidades cognitivas, los aspectos políticos, jurídicos y económicos. Es decir, debe involucrar múltiples habilidades y diferentes sectores (proveedores de servicios de Internet y operadores de telecomunicaciones, proveedores de tecnología, centros de investigación y redes sociales capaces de actuar en el nivel de "manipulación de la información"). Estas consideraciones nos permiten validar el enfoque holístico de

ciberdefensa. Las características y asociación de cada capa con sus actores se presenta en la tabla 1.

Tabla 1: Adaptación de la asociación de cada nivel del ciberespacio con sus características y actores.

Capas o Niveles	**Características**	**Formas de posible ataque a esta capa**	**Hechos / Ejemplos**	**Perspectiva Teórica**
Capa Superior L3	Capa cognitiva	Modificación de la información que aparece en los monitores de ordenador; introducción de mensajes distorsionadores; desestabilización de la capa L2; propaganda; operaciones psicológicas; desconfiguración del sitio web; aumento de la sensación de amenaza, divulgación de secretos…	Anuncios propagandísticos en sitios webs oficiales vulnerados; wikileaks; usos de información distorsionada en la redes sociales para movilizar grupos; hacking cognitivo: entendiendo un ataque a la capa cognitiva o de pensamiento como un ataque para manipular contenidos, así mismo manipular información para manipular a los actores o interlocutores que las reciben.	Netwar (Arquilla, Ronfeldt); *information warfare* (Libicki); operaciones psicológicas; manipulación de información…
Capa Media L2	Capa de aplicaciones: software, aplicaciones de comunicaciones, código fuente, normas de seguridad, protocolos, configuración de sistemas, datos…	Ataques por código dañino, hacking, virus espía, difusión de virus, Ataques botnet. DDoS (*Distributed Denial of Service* – ataque distribuido de denegación de servicio; Ataque DoS (*Denial of Service* – denegación de servicio).	Vulneración de sitios web; activismo; piratería en centros oficiales y gubernamentales; saturación de sitios oficiales; ataques a servidores y proveedores de servicios de Internet; robo de información… Ingeniería social, interceptación y registro de tráfico de red, *sniffing* y *wiretapping.* Vulneración de sistemas SCADA (Vulneración del Control de Infraestructuras Críticas).	*Cyberwar*. La capa L2 constituye el centro del concepto *cyber warfare.* Recientemente es considerada uno de los aspectos de la *information warfare*; desde un punto de vista teórico *cyber warfare* es definida por J. Arquilla and D. Ronfeldt (*Cyberwar is coming!*)
Capa Inferior L1	Capa física, hardware, cables, servidores, hubs, routers, satélites, computadores, elementos de telecomunicaciones…	Corte de comunicaciones de cables submarinos; inutilización de satélites; desvío de satélites de sus trayectorias; utilización de bombas de pulso electromagnético, destrucción de nodos de comunicaciones…	Corte de las comunicaciones por cable submarino, paralizando Internet en Egipto. Corte de conexión entre Rusia y Georgia.	Las acciones en este nivel están a menudo vinculadas al dominio de la guerra electrónica.

Un ataque a las capas más bajas siempre tiene un impacto en las capas superiores, pero lo contrario no es necesariamente cierto:

- Un ataque a las infraestructuras puede dañar el código de funcionamiento y tiene un impacto sobre el nivel cognitivo;

- Un ataque sobre el código por medio de código malicioso (*malware, spyware*…) tiene un impacto en la capa cognitiva, pero no necesariamente en la capa anterior; y

- Un ataque en el código puede interrumpir la función de un PC o un sistema SCADA e incluso destruirlo.

Hay combinaciones de acciones en las diversas capas, de acuerdo con la ecuación: actuar sobre una de ellas, produce un efecto sobre la siguiente, o sobre las anteriores.

Así a modo de ejemplo, actuando en el nivel L3 para producir un efecto de activación en L2 de manera que, difundiendo una lista de *websites* que puedan ser atacadas y seguidamente pasar el testigo a los *hackers* para que actúen en L2 en los sitios webs designados, proveyendo herramientas y procedimientos para los ataques o movilizando comunidades de *hackers*… y así sucesivamente.

Vinculando las actuaciones en cada uno de los niveles con las implicaciones en los otros, estaríamos conceptualmente confrontando los términos *cyberwarfare* (Brenne y Clark, 2010) e *information warfare* (Ventre, 2009 y Office of the Secretary of Defense, 2010) y esta confrontación nos lleva a recuperar las acepciones de la *information age warfare* (Carr, 2010, 165 - 166).

4. Incidentes de Ciberseguridad y Ciberespionaje.

Pasaremos a continuación a referenciar algunos recientes "ciberincidentes" que reflejan la interrelación entre la ciberseguridad y las funciones de inteligencia.

La compañía de seguridad McAfee[1] dio a conocer en agosto de 2011 un informe en el que asegura la existencia de un ataque masivo a 72 organizaciones, Gobiernos y empresas en todo el mundo que se prolongó durante cinco años. *Se trata del mayor robo de riqueza en términos de propiedad intelectual en la historia de la humanidad*, aseguraba Dmitri Alperovitch (2011), vicepresidente del área de investigación de amenazas a la empresa.

[1] McAfee descubrió la extensión de la campaña de violaciones en marzo de 2012, cuando sus investigadores descubrieron registros de los ataques mientras revisaban los contenidos de un servidor de "comando y control" que colocaron en 2009 como parte de una investigación sobre violaciones de seguridad en firmas de defensa.

La lista de víctimas de la campaña incluye los gobiernos de Estados Unidos, Taiwán, India, Corea del Sur, Vietnam y Canadá; la Asociación de Naciones del Sudeste de Asia (ASEAN, por su sigla en inglés); el Comité Olímpico Internacional (COI); la Agencia Mundial Antidopaje, y una serie de firmas, desde contratistas de defensa a empresas de alta tecnología. Según se desprende del informe de la compañía, Estados Unidos fue el país con mayor número de ataques (49).

Por otro lado el último informe de tendencias de la citada compañía sitúa a los ataques de reputación en la red o e-reputación como una de las amenazas que más va a crecer, se trata de ataques a la imagen personal, trayectoria, reputación de mercado de las empresas, otras organizaciones, e incluso sobre la credibilidad de instituciones del Estado. Se fundamentarán de manera clásica, pero sustentados en el auge de las redes sociales y entornos 2.0. En cuanto a las tendencias de los próximos años, debido al aumento de personas con conocimientos para convertirse en *hackers* y fruto de la crisis económica, aumentarán las múltiples conexiones y motivaciones del los *hacktivistas* (Mcafee, 2011). En el mismo sentido Symantec, una de las tres grandes empresas mundiales de seguridad informática, resalta el aumento del ciberespionaje durante el 2012, así como la utilización de las redes sociales para ejercer "ingeniería social" y acceder a datos e información sensible de personas y organizaciones públicas y privadas (Symantec, 2013).

Por último, el 29 de mayo de 2012 todos los centros de Respuesta Rápida a Incidentes de Seguridad (CERT, *Computer Emergency Response Team*) alertaban del descubrimiento de Flame, catalogado como una herramienta de espionaje cibernético altamente sofisticada (Symatec, 2012) detectada contra objetivos de Oriente Próximo y Europa del Este (Budapest University of Technology and Economics, 2013). Flame puede propagarse a otros sistemas a través de la red de área local (LAN) y mediante memorias USB. Tiene la capacidad para grabar audio, y realizar capturas de pantalla, pulsaciones de teclado y tráfico de red. El programa también intercepta y graba conversaciones de Skype. Estos datos, junto con los documentos almacenados en el ordenador, son enviados a uno o varios servidores dispersos alrededor del mundo; cuando termina, el programa se mantiene latente hasta que recibe nuevas instrucciones de esos servidores.

4.1 Ataques dirigidos. Modelo APT (Amenazas Persistentes Avanzadas). Ciberespionaje.

El término APT hace referencia a un ataque que normalmente está patrocinado por el estado. También hace referencia a las técnicas utilizadas por el adversario para mantener una presencia prolongada sobre los sistemas de información de la víctima. La misión del atacante es el robo de información sensible. Dado que el objetivo de estos atacantes es una infiltración a largo plazo, el código dañino que utilizan suele adaptarse a cada víctima.

Además de la ya citada operación "Shady RAT", han salido a la luz 3 campañas APT con origen en China: la Operación Aurora,[2] la red de espionaje de Shadow Network y las intrusiones contra la industria petrolera de EE.UU (2008). Estos ataques se centraron en más de una víctima o empresa, y afectaron a grupos de organizaciones con un perfil similar.

Trend Micro ha publicado un documento titulado "Luckycat Redux" centrado en el análisis de las actividades de la campaña Luckycat**,** descubierta y documentada por primera vez a principios de marzo de 2012 por Symantec. Una campaña de Amenazas Persistentes Avanzadas (APTs) que ha efectuado ataques contra diferentes organizaciones del sector aeroespacial, energético, ingenierías, industria naval e investigación militar, entre otros (Trend Micro, 2012).

A pesar de que China cuenta con el mayor ejército convencional, sus capacidades en C4I (Mando, Control (C2), Comunicaciones, Computación e Inteligencia) no son demasiado eficientes. Las autoridades militares chinas han gastado recursos considerables en actualizar sus redes C4I (Sharma, 2011). Estos esfuerzos vienen como resultado de lo que parece ser una apreciación de la potencial vulnerabilidad de los sistemas construidos con tecnología comercial, así les ha llevado a invertir en la defensa de redes, sobre todo frente a virus. En el ejército chino, se entrena a sus oficiales, entre otros aspectos, en tecnologías de la información. En los dos últimos años China ha preparado a estos expertos no sólo en ataques, sino en la capacidad para detectar vulnerabilidades en sistemas que permitan obtener información sensible fundamentalmente de carácter militar, tecnológica y económica (Lieberthal y Singer 2012). Como conclusión resaltar que en mayo de 2011 un portavoz del Ministerio de

[2] Este ataque lo sufrió Google y otras 30 compañías más, se trató de un ataque altamente sofisticado y coordinado que tenía como objetivo obtener información estratégica de las compañías.

Defensa de China confirmaba a *The Times* en una amplia entrevista la existencia del *"Blue Army"*, una unidad especializada en Ciberguerra (Fox News, 2011).[3]

Recientemente hemos conocido el informe elaborado por la consultora Mandiant (2013). El informe encargado por *The New York Times* para que rastreara y limpiara sus sistemas informáticos, identifica la Unidad 61398 del PLA, con sede en Shanghai, como la responsable. Los marcadores digitales de sus incursiones virtuales han sido rastreadas hasta un edificio de 12 pisos en el barrio financiero de Pudong, en Shanghai.

En mayo pasado en la presentación del Informe Anual al Congreso 2013, sobre la evulación de la capacidad militar de China, la Secretaría de Defensa de Estados Unidos acusaba directamente a China de ciberataques al Pentago y diversas empresas contratistas de sector de la defensa.[4] Si bien por parte de la Oficina Nacional de Contrainteligencia y otras agencias y comisiones del Congreso de EEUU ya apuntaban desde el 2009 a las capacidades de ciberespionaje y ciberataques vinculados a China.[5]

4.2 Ataques contra infraestructuras críticas. El caso de Stuxnet.

Stuxnet, descubierto en 2010, es el primer código dañino conocido que estaba destinado a atacar sistemas industriales de control (SCADA), (Centro Nacional para la Protección de las Infraestructuras Críticas, n.d.) los que controlan las infraestructuras críticas; inicialmente se creía que se trataba de un código espía pero además se ha

[3] China cuenta con un escuadrón de expertos en seguridad IT, cuya única misión es responder de forma letal contra cualquier ciberataque o intento de ciberguerra contra la nación asiática. Su nombre: Ejército Azul, confirmó el actual general del Ejército Popular de Liberación. Según el funcionario el Ejército Azul es parte del comando militar de Guandong, parte del Ejército Popular de Liberación Chino y está dedicado a mejorar la seguridad de las fuerzas militares del país. Ante la noticia, medios chinos han informado que el escuadrón fue creado formalmente desde hace dos años, pero destacaron que las labores desempeñadas por el Ejército Azul se han ejecutado de forma paulatina durante más de una década dentro del PLA.

[4] La primera motivación para estos ciberataques chinos es el espionaje industrial, en el informe se recuerdan los ataques contra el propio Departamento de Defensa, entre otros organismos, en 2012. Hay indicios de ataques encaminados a obtener claves sobre las decisiones políticas estadounidenses. Además se alerta de que esa recopilación de información podría ser utilizada fácilmente para la generación de un patrón o una imagen de las redes de defensa estadounidenses, de elementos de logística y de capacidades militares relacionadas, que podrían ser explotados durante una crisis.
Office of the Secretary of Defense. Annual Report to Congress: Military and Security Developments Involving the People's Republic of China 2013.
http://www.defense.gov/pubs/2013_china_report_final.pdf

[5] "China utiliza una red grande y organizada de empresas, fábricas del sector defensa, instituciones de investigación, filiales y operaciones en redes informáticas para facilitar la recopilación de información sensible y exportar tecnología, así como investigación y ciencia básica que sostiene la modernización del sistema de defensa estadounidense".
Office of the National Counterintelligence Executive. Foreign spies stealing US economic secrets in cyberspace. Report to Congress on Foreign Economic Collection and Indsutrial Espionage, 2009 – 2011.
http://www.ncix.gov/publications/reports/fecie_all/Foreign_Economic_Collection_2011.pdf

demostrado que estaba diseñado para sabotear determinadas instalaciones industriales (Rollins y Theoracy, 2011).

El 1 de junio de 2012, conocimos que Stuxnet había sido creado por el gobierno de Estados Unidos. En 2010, el presidente norteamericano Barack Obama intensificó una campaña secreta de cibertataques contra el programa nuclear de Irán, con la que EE UU, con la ayuda de Israel, llegó a deshabilitar 1.000 centrifugadores de la planta de Natanz, un quinto de los que estaban en activo. El virus empleado escapó de Natanz en 2010, se replicó en la Red aprovechando un fallo en el sistema operativo Windows y fue bautizado por los expertos en seguridad como Stuxnet (Alandete, 2012).

4.3 Ataques Botnet.

Se aprecia un fuerte crecimiento de los usuarios afectados por algún tipo de botnet,[6] en los últimos tres años. Las principales formas de extraer beneficio de las botnet fueron el envío de *spam*, el *phishing*, los ataques de denegación de servicio distribuidos (DDoS), la distribución de código dañino y el fraude.

A nivel mundial se ha elevado la actividad en el mercado negro relacionada con las botnets. La variedad de productos y servicios en este campo es amplia, yendo desde la venta de kits de código dañino para la creación de una botnet propia, hasta el alquiler y venta de botnets existentes (IC3, 2010).

4.4 Difusión de información sensible; de Wikileaks al Incidente Snowden o del *big data* al *big brother*.

La difusión de información sensible, sin las debidas cautelas, puede ser más perjudicial que la manipulación, bloqueo o desinformación masiva. Durante el año 2010 la noticia más destacable publicada relacionada con la divulgación no autorizada de información sensible ha sido el denominado “escándalo Wikileaks”, desencadenado por la publicación de miles de mensajes clasificados del Departamento de Estado de Estados Unidos. El 28 de noviembre de 2010, WikiLeaks filtra a la prensa internacional (The Guardian, The New York Times, Le Monde, El País y al semanario Der Spiegel) una colección de 251.187 cables o comunicaciones entre el Departamento de Estado estadounidense con sus embajadas por todo el mundo (denominados en inglés United

[6] Conjunto de ordenadores infectados con programas (bots) que, de forma automatizada y controlada remotamente por sus propietarios (bot-herders) realizan determinadas tareas con cierto grado de autonomía, y que persiguen fines dañinos.

States diplomatic cables leak, Cablegate o Secret US Embassy Cables). El hecho pone de manifiesto la dificultad de las organizaciones para defenderse frente a amenazas internas, así como la irreversibilidad de la filtración de la información (ENISA. European Network and Information Security Agency, 2010, *"ENISA statement on Wikileaks events"*).

El pasado 5 de junio, el diario británico "The Guardian" revela la existencia de una orden judicial que permite a la NSA, National Security Agency, acceder durante tres meses al registro de todas las llamadas telefónicas efectuadas por los clientes del operador estadounidense Verizon. Al día siguiente los diarios "The Washington Post" y "The Guardian" informan de que la NSA y el FBI han solicitado a nueve gigantes de Internet, entre ellos Microsoft, Yahoo!, Google y Facebook, acceder a sus servidores para vigilar e interceptar comunicaciones de internautas extranjeros fuera de Estados Unidos (Greenwald, 2013). Este programa, hasta entonces secreto, denominado Prism, forma parte de una ley aprobada en 2007, bajo el mandato de George W. Bush, y renovada en diciembre de 2012. En un principio las compañías afectadas negaron que hubieran autorizado a los servicios de espionaje entrar en sus servidores, posteriormente hemos conocido la necesaria colaboración entre las compañías y diferentes agencias de seguridad.

No podemos dejar de mencionar la interrelación existente entre las capacidades de análisis masivo de datos, las herramientas tecnológicas vinculadas al *big data* y la privacidad y derecho a la intimidad del ciudadano. La connivencia de las grandes empresas de tecnologías de la información de Estados Unidos con la Agencia Nacional de Seguridad y la CIA, puestas en conocimiento de la opinión pública por las filtraciones del citado caso Snowden alientan a la identificación del binomio *big data* / *big brother*.

La cronología de la noticia, las siguientes filtraciones y sus implicaciones en las relaciones bilaterales de muchos países con Estados Unidos se han visto afectadas y desconocemos el impacto social y económico que el desarrollo del incidente nos puede deparar.[7]

[7] La recopilación de noticias y enlaces a los periódicos receptores de la filtraciones *The Guardian* y *The Washintong Post* se encuentra disponible en sitio específico de El País http://elpais.com/tag/edward_snowden/a/

5. Estrategias de Ciberseguridad y Ciberdefensa. Ciberejércitos.

Actualmente, aproximadamente 120 países en el mundo están examinando de forma activa y concienzuda las capacidades de ciberdefensa. EEUU, Rusia y China lideran esta carrera seguidos por India, Irán, Corea del Norte, Japón e Israel. Esta clasificación puede cambiar rápidamente debido al mercado negro en Internet de las modernas cibercapacidades (Instituto Español de Estudios Estratégicos, 2011). Tal es así que el último informe conocido sobre ciberdefensa de la prestigiosa consultora Verisign, establece a finales de 2011 una clasificación atendiendo a cuatro niveles de seguridad según sus políticas (Verisign iDefense, 2010). Esta clasificación está encabezada por EEUU, China y Rusia; las cuáles poseen capacidades de ciberguerra. La adaptación de la citada clasificación se muestra como tabla 2.

Tabla 2: Clasificación de países en cuatro niveles según sus políticas de ciberseguridad y/o ciberdefensa.

Nivel	Países incluidos	Elementos Diferenciadores y Atributos	Ámbito y madurez organizativa	Capacidad y actividad
1	EEUU China Rusia	- Determinan la política internacional sobre ciberseguridad. - Líderes en temas de ciberdefensa . - Invierten muchos recursos humanos y económicos. - Son modelo en acciones de ciberseguridad para otras naciones.	- Organizaciones diferenciadas a nivel funcional en capacidades militares y de inteligencia. - Muchos recursos disponibles.	- Integran en sus mecanismos de defensa convencional la ciberdefensa. - Actividad defensiva, ofensiva, sofisticada y continuada contra otros países
2	Francia Reino Unido Israel	- Tienen “unidades de excelencia” con capacidades comparables a las del primer nivel. - Disponen de menos personal e infraestructuras.	- Algunas organizaciones desarrollan capacidades militares y de inteligencia. - Disponen de menos recursos que los países de nivel 1.	- Menor escala pero similar sofisticación en operaciones ofensivas y defensivas. - Menor número de acciones ofensivas.
3	India Corea del Sur Taiwán Alemania Corea del Norte Turquía Canadá Australia	- Dedican bastantes recursos al desarrollo de políticas de ciberseguridad y capacidades de defensa. - Suelen imitar las prácticas de los países de nivel 1 y nivel 2.	- Tienen algunas organizaciones bien definidas. - Necesitan crear nuevas instituciones con responsabilidades en el ciberespacio.	- Actividad defensiva continua y extensa. Acciones ofensiva limitadas y menor escala. - Actividad ofensiva no reconocida
4	Suecia Japón Países Bajos Irán Pakistán Finlandia Noruega	- Recursos limitados para el desarrollo de las políticas de ciberseguridad y las capacidades de defensa. - Disponen de política de ciberdefensa.	- Pocas organizaciones. - Misiones no bien definidas.	- Actividad defensiva incompleta pero sólida. - Actividad ofensiva limitada y no reconocida. - Se centran en proteger los recursos nacionales.

Nota. Adaptación de la clasificación de naciones y ciberdefensa de Verisign. (The Verisign® iDefense®)

A continuación analizaremos de manera general aquellos países que han realizado, se encuentran realizando o actualizando estrategias de ciberseguridad y/o ciberdefensa, para determinar las tendencias y características más relevantes.

Tabla 3: Análisis de la Estrategias Nacionales de Ciberseguridad y/o Ciberdefensa.

Previas a 2010	Publicadas o en fase de proyecto en 2011	Publicadas o en fase de proyecto en 2012
- EEUU (2008 y 2010)[a] - Rusia (2010)[b] - Reino Unido (2009)[c] - Australia (2008) - Canadá (2009) - Estonia (2008) - Singapur (2009)	- República Checa[d] - Alemania[e] - Israel (proyecto)[f] - Letonia (proyecto)[g] - Nueva Zelanda[h] - Dinamarca (borrador)[i] - Francia[j] - India[k] - Japón (proyecto)[l] - Holanda[m] - Polonia (proyecto)[n] - Corea del Sur[ñ] - Reino Unido (actualización)[o] - Colombia[p] - EEUU[q]	- Finlandia[r] - Sudáfrica[s] - Perú[t] - Brasil[u] - Rusia (actualización)[v]

Nota: Fuente elaboración propia.

[a]CSIS. Commission on Cybersecurity for the 44th Presidency, http://csis.org/program/commission-cybersecurity-44th-presidency

[b] Giles, K. (2011), *Information Troops: Russia Cyber Command*, 3rd International Conference on Cyber Conflict, NATO Cooperative Cyber Defense Centre of Excellence, http://www.ccdcoe.org/publications/2011proceedings/InformationTroopsARussianCyberCommand-Giles.pdf

[c]UK Cabinet Office, (June 2009), "Cyber Security Strategy of the United Kingdom", http://www.official-documents.gov.uk/document/cm76/7642/7642.pdf

[d]Ministry of the Interior of the Czech Republic, (August 2011), "Cyber Security Strategy for the Czech Republic for the 2011 – 2015 Period.", http://www.enisa.europa.eu/media/news-items/CZ_Cyber_Security_Strategy_20112015.PDF

[e]German Federal Ministry of the Interior, (2011), "Cyber Security Strategy for Germany", http://www.bmi.bund.de/SharedDocs/Downloads/DE/Themen/OED_Verwaltung/Informationsgesellschaft/cyber_eng.pdf;jsessionid=586A04D370083C12D1DFE3255CAE59BF.2_cid231?__blob=publicationFile

[f]Muhareb, M. (2011). "Israel and Cyber Warfare.", *Doha Institute Book Review*, http://english.dohainstitute.org/Home/Details/5ea4b31b-155d-4a9f-8f4d-a5b428135cd5/c82f6a5e-6ba7-40c0-ba42-819b34167108

[g i n]Klimburg, A., Tirmaa-Klaar, H., (2011) *Cybersecurity and Cyberpower: Concepts, Conditions and Capabilities for Cooperation and Action within the EU*, Ad Hoc Study to the European Parliament, http://www.evi.ee/lib/cyber.pdf

[h]New Zealand Government, (2011) "National Cyber Security Strategy.", http://www.dpmc.govt.nz/sites/all/files/publications/nz-cyber-security-strategy-june-2011_0.pdf

[j]Agence nationale de la sécurité des systèmes d'information, (2011), "Défense et sécurité des systèmes d'information, Stratégie de la France", http://www.ssi.gouv.fr/IMG/pdf/2011-02-15_Defense_et_securite_des_systemes_d_information_strategie_de_la_France.pdf

[k]Ministry of Information and Technology, (2011) "National Cyber Security Strategy of India.", http://www.mit.gov.in/content/cyber-security-strategy

[l]National Security Information Center (2010) **"**Information Security Strategy for Protecting the Nation", http://www.nisc.go.jp/eng/ http://www.nisc.go.jp/eng/pdf/New_Strategy_English.pdf

[m]Ministry of Security and Justice, (2011), "The National Cyber Security Strategy (NCSS)", https://www.ncsc.nl/binaries/en/organisation/about-the-ncsc/background/1/National+Cyber+Security+Strategy.pdf
[n]Valdez, A. (2011), *South Korea Outlines Cyber Security Strategy*, http://www.futuregov.asia/articles/2011/aug/13/south-korea-outlines-cyber-security-strategy/
[o]UK Cabinet Office, (2011), "The UK Cyber Security Strategy", https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60961/uk-cyber-security-strategy-final.pdf
[p]Ministerio de Defensa de Colombia, (2011), "Colombia presenta estrategia de Ciberseguridad y Ciberdefensa", http://www.mindefensa.gov.co/irj/go/km/docs/documents/News/NoticiaGrandeMDN/60a20bd2-8890-2e10-7dab-8a117a5461d8.xml
[q]Actualización de políticas estratégicas principales: Departamento de Defensa, Departamento de Estado y la Casa Blanca. US Department of State, (2011 Mayo), "International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World.", http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf
US Department of Defense, (2011 Julio), "Strategy for Operating in Cyberspace", http://www.defense.gov/news/20110714cyber.pdf
[r]Secretariat of the Security and Defence Comité, (2013) "Finland´s Cyber Security Strategy", http://www.yhteiskunnanturvallisuus.fi/en/materials/doc_download/38-finlandas-cyber-security-strategy
[s]South African Government (2012), "National Cybersecurity Polic Framework For South Africa", http://www.info.gov.za/speech/DynamicAction?pageid=461&sid=25751&tid=59794
[t]E-Gov, (2012), "Declaración de Ciberdefensa del Perú y la informática gubernamental", http://www.egov.pe/declaraci%C3%B3n%20-de%20Ciberdefensa%20del%20Per%C3%BA%20y%20la%20inform%C3%A1tica%20gubernament|sal
[u]Presidência da República. Secretaria de Assuntos Estratégicos, (2012), "Segurança e Defesa Cibernética", http://www.sae.gov.br/site/wp-content/uploads/Seguranca_Cibernetica_web.pdf
[v]Atlantic Organization for Security, (2012), "Russia's Cyber Strategy", http://www.aofs.org/2012/04/15/russia%C2%B4s-cyber-strategy-published/

Aquellas naciones marcadas en gris ya poseían o poseen estrategias de seguridad y/o defensa nacionales, y en todas se hace referencia a la seguridad de infraestructuras críticas, la seguridad económica o financiera y la ciberseguridad.

Estudiando las diferentes estrategias, se constata que existe ya una tendencia para que la Comunidad de Inteligencia; agencias de inteligencia y las unidades de inteligencia militar tengan un papel preponderante y significativo en la orientación general de la ciberseguridad. En el mismo sentido se resalta la necesidad de más esfuerzo en formación en TIC para poder alcanzar las capacidades necesarias, así como una coordinación de estrategias y esfuerzos con el entorno empresarial privado. Otras características que se repiten son:

- La ciberseguridad es considerada un asunto de Seguridad Nacional o de Defensa Nacional.
- Propuesta o existencia de una estructura institucional formal, con reparto de funciones claramente establecidas, y en algunas, determinación de las coordinaciones entre estructuras civiles, militares y policiales.
- Determinación de organismo específico de seguridad vinculado a la protección de infraestructuras criticas.
- Establecimiento de coordinación con otras organizaciones de seguridad y/o defensa para la cooperación en materia de ciberseguridad.

Son ejemplos significativos: EEUU, Reino Unido, gran parte de Europa occidental, India, Singapur, Corea del Sur, Japón, Australia, la OTAN (2008) y la Unión Europea. Además, este enfoque convergente es la base de los documentos "*Cyber Security Strategy Guide*"(International Telecommunications Union [ITU], 2011) y "*Self-Assessment Tool"* (ITU, 2010) ambos publicados por la UIT de la ONU, y dirigidos a aquellos países menos desarrollados en materia de ciberseguridad o que están en proceso de redacción de sus propias estrategias nacionales.

Otras organizaciones y autores consideran que se deben contraponer como diferentes estados de evolución la *cybersecurity* y la *cyberwarfare*; entendiendo que el grado de madurez de sus estructuras civiles y militares en este campo es lo que determina la capacidad para la ciberguerra, en cualquiera de sus acepciones. Aún así existe cierta controversia respecto a que si las capacidades de defensa determinan a corto plazo cibercapacidades de ataque (Maurer, 2012). Por ejemplo, UNIDIR, *United Nations Ideas for Peace and Security*, en su informe *Cybersecurity and Cyberwarfare*, mantiene una clasificación diferenciada entre aquellos países (33 estados) que poseen una Doctrina Militar y Organizaciones para la Ciberseguridad y la Ciberguerra; y de otro, aquellos países (36 estados) que mantienen un Política Civil y Organizaciones para Ciberseguridad (Lewis y Timli, 2011).

Para concluir destaquemos el proyecto de la *Intelligence Advanced Research Projects Activity* (IARPA, agencia gubernamental de investigación avanzada en inteligencia, en cierto modo equivalente a la DARPA de defensa) para identificar actuaciones especulativas en los mercados financieros globales, que pudieran dañar la seguridad económica de EEUU, el proyecto conocido como *Markets Analysis and Testing of Contextual Hypotheses Enhancement System*, MATCHES (Lee, 2011).

En este contexto entre el límite de la seguridad y la defensa, la capacidad para resistir un ataque y la posibilidad de infligirlo ha llevado a definir el término *cyberpower.* Así, la capacidad de un estado para responder a los ciberataques, es lo que se ha denominado Cyber Power; un índice que refleja esta capacidad dependiendo de varios factores: marco legal, contexto económico, entorno y desarrollo social, infraestructuras tecnológicas, capacidad innovadora en tecnologías de la información y comunicaciones y desarrollo industrial (Ciber Hub, n.d. y Nye, 2010).

Estos planteamientos ya se determinaban por ejemplo en la Estrategia de Seguridad Nacional de EEUU, (US Departament of State, 2010), así la Seguridad Nacional pasa

por mantener la supremacía en la economía, la ciencia (y tecnología) la innovación y la educación.

6. Conclusiones.

La velocidad con la que se han producido los cambios tecnológicos, propiciados en gran medida por el desarrollo de las tecnologías de la información y comunicación, determina una nueva manera de entender el mundo. Esto, además nos debe hacer reconocer que la capacidad de anticipación y de respuesta ante los diferentes eventos nos ha superado; baste con analizar la evolución en los últimos seis meses tanto de "ciberincidentes" como de noticias relacionadas publicadas en medios de comunicación.

Por otro lado, podemos afirmar que ciberamenazas y cibercrimen no son categorías equivalentes en la medida que existen ciberdelitos que no constituyen amenazas a la seguridad de los estados y es evidente que la inmensa mayoría de las amenazas a la seguridad nacional no nacen del entorno del cibercrimen.

La ciberguerra es asimétrica y, como tal, el acceso a las capacidades para llevarla a cabo es asequible por organizaciones de toda índole, lo que convierte el ciberterrorismo en una amenaza real y emergente.

En el ámbito geoeconómico nos encontramos en la actualidad con el reto de la existencia de una inteligencia muy diversificada y capacitada, tanto en el ámbito público como privado, que combina de manera sinérgica la capacidad de adquisición de inteligencia de fuentes humanas con la capacidad técnica de acceso a sistemas y redes. También, esta "inteligencia" es capaz de ejercer acciones de influencia en el ámbito de las redes sociales y medios de comunicación especializados. Existe ya una tendencia para que la Comunidad de Inteligencia tenga un papel preponderante y significativo en la orientación general de la ciberseguridad.

En tanto que de manera conceptual Seguridad y Defensa conforman un continuo que se debe gestionar integralmente, es evidente que las tecnologías, fundamentalmente las Tecnologías de Información y Comunicaciones que subyacen en esa gestión integral debe ser administradas y consideradas conjuntamente. En el mismo sentido, información, seguridad de la información y la producción de inteligencia en el ámbito de las estrategias de seguridad nacional deben ser gestionadas bajo un prisma interdisciplinario.

Referencias.

Agence nationale de la sécurité des systèmes d'information. 2011. *Défense et sécurité des systèmes d'information, Stratégie de la France*. Disponible en web: http://www.ssi.gouv.fr/IMG/pdf/2011-02-15_Defense_et_securite_des_systemes_d_information_strategie_de_la_France.pdf [Consulta: 17 de junio de 2013]

Alandete, David. 2012. "Obama ordenó un ataque cibernético contra Irán del que perdió el control", *El País*, 1 de junio de 2012. Disponible en web: http://internacional.elpais.com/internacional/2012/06/01/actualidad/1338572841_317814.html [Consulta: 14 de mayo de 2013]

Alperovitch, Dimitri. 2011. *Operación Revealed: Operation Shady RAT*. Disponible en web: http://www.mcafee.com/us/resources/white-papers/wp-operation-shady-rat.pdf [Consulta: 27 de mayo de 2013]

Atlantic Organization for Security. 2012. *Russia's Cyber Strategy*. Disponible en web: http://www.aofs.org/2012/04/15/russia%C2%B4s-cyber-strategy-published/ [Consulta: 14 de mayo de 2013]

Barbería, José L. 2012. "El servicio secreto entra en la 'guerra económica", *El País*, 26 de Julio de 2012. Disponible en web: http://sociedad.elpais.com/sociedad/2012/03/26/actualidad/1332762326_179566.html [Consulta: 3 de mayo de 2013]

Brenne, Susan W. y Leo L. Clarke. 2010. *Conscripts and casualties: civilians in cyberwarfare part I*, Disponible en web: http://works.bepress.com/susan_brenner/2 [Consulta: 3 de mayo de 2013]

Budapest University of Technology and Economics. Department of Telecommunications. Laboratory of Cryptography and System Security (CrySyS Lab). 2012. *sKyWIper (a.k.a. Flame a.k.a. Flamer): A complex malware for targeted attacks v1.05*. Disponible en web: http://www.crysys.hu/skywiper/skywiper.pdf [Consulta: 9 de mayo de 2013]

Caño, Antonio. 2013. "Estados Unidos y China, ante la primera ciberguerra fría", *El País*, 19 de Febrero de 2013. Disponible en web: http://internacional.elpais.com/internacional/2013/02/19/actualidad/1361300185_954734.html [Consulta: 19 de febrero de 2013]

Carr, Jeffrey. 2010. *Inside Cyber Warfare: Mapping the Cyber Underworld*. California: Ed. O´Reilly

Centro Nacional para la Protección de las Infraestructuras Críticas. CNPIC - Guías SCADA. Disponible en web: http://www.cnpic-es.es/Ciberseguridad/4_Guias_Scada/index.html [Consulta: 10 de junio de 2013]

Clark, Robert. M., 2006. *Intelligence Analysis: a Target-Centric Approach.* 2ª ed., Washington: CQPress.

Comisión Europea. 2011. *Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones sobre la protección de infraestructuras críticas de información «logros y próximas etapas: hacia la ciberseguridad global»*, Bruselas, 31.3.2011. Disponible en web: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2011:0163:FIN:ES:PDF [Consulta: 1 de junio de 2013]

Czosseck, Christian., Rain Ottis y Katharina Ziolkowski. (eds.), 2012. "Conference on Cyber Conflict". Disponible en web: http://www.ccdcoe.org/publications/2012proceedings/CyCon_2012_Proceedings.pdf [Consulta: 21 de junio de 2013]

CSIS. *Commission on Cybersecurity for the 44th Presidency*. Disponible en web: http://csis.org/program/commission-cybersecurity-44th-presidency [Consulta: 23 de julio de 2013]

Defense Advanced Research Projects Agency, DARPA. 2010., *Social Media in Srategic (SMISC*). Disponible en web:

http://www.darpa.mil/Our_Work/I2O/Programs/Social_Media_in_Strategic_Communication_%28SMISC%29.aspx [Consulta: 14 de mayo de 2013]

Denmark, Abraham M. 2010. "Managing the Global Commons", *The Washington Quarterly*, Disponible en web: http://csis.org/files/publication/twq10julydenmark.pdf [Consulta: 21 de agosto de 2013]

Department of Defense Strategy for Operating in Cyberspace (Julio 2011)
http://www.defense.gov/news/d20110714cyber.pdf [Consulta:1 de junio de 2013]

Directiva sobre la identificación y designación de infraestructuras críticas europeas y la evaluación de la necesidad de mejorar su protección. Directiva 2008/114/CE del Consejo. Disponible en web: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:345:0075:0082:ES:PDF
[Consulta: 15 de junio de 2013]

E-Gov. 2012. *Declaración de Ciberdefensa del Perú y la informática gubernamental*. Disponible en web: http://www.egov.pe/declaraci%C3%B3n%20-de%20Ciberdefensa%20del%20Per%C3%BA%20y%20la%20inform%C3%A1tica%20gubernament|sal
[Consulta: 17 de mayo de 2013]

eCSIRT.net, Computer Security and Incidente Response Team. 2010. *Incident Classification*. Disponible en web: http://www.ecsirt.net/cec/service/documents/wp4-clearinghouse-policy-v12.html#HEAD6 [Consulta: 15 de mayo de 2013]

El País. 2010. "Las revelaciones de Wikileaks". Disponible en web: http://www.elpais.com/documentossecretos/ [Consulta: 30 de junio de 2013]

Escuela de Guerra Económica. Formación en Inteligencia Económica. Disponible en web: http://www.ege.fr/ [Consulta: 10 de junio de 2013]

ENISA. European Network and Information Security AGency. 2010. *ENISA statement on Wikileaks events*. Disponible en web: http://www.enisa.europa.eu/media/news-items/enisa-statement-on-wikileaks-events [Consulta: 13 de mayo de 2013]

ENISA. European Network and Information Security Agency. 2011. *Estrategias de Seguridad Cibernética de los Países Bajos, Francia y Alemania*. Disponible en web: http://www.enisa.europa.eu/media/news-items/cyber-security-strategies-of-de-nl-presented [Consulta: 13 de mayo de 2013]

European Commission. Digital Agenda for Europe. 2013. *EU Cybersecurity plan to protect open internet and online freedom and opportunity - Cyber Security strategy and Proposal for a Directive*. Disponible en web: http://ec.europa.eu/digital-agenda/en/news/eu-cybersecurity-plan-protect-open-internet-and-online-freedom-and-opportunity-cyber-security [Consulta: 1 de julio de 2013]

Greenwald, Glenn. 2013. "NSA Prism program taps in to user data of Apple, Google and others", *The Guardian*, 6 de junio de 2013. Disponible en web: http://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data [Consulta: el 9 de junio de 2013]

Fox News, 2011. "China Confirms Existence of Elite Cyber-Warfare Outfit the Blue Army", consultado el 12 de enero de 2013, http://www.foxnews.com/scitech/2011/05/26/china-confirms-existence-blue-army-elite-cyber-warfare-outfit/ [Consulta: 12 de julio 2013]

German Federal Ministry of the Interior. 2011. *Cyber Security Strategy for Germany*. Disponible en web: http://www.bmi.bund.de/SharedDocs/Downloads/DE/Themen/OED_Verwaltung/Informationsgesellschaft/cyber_eng.pdf;jsessionid=586A04D370083C12D1DFE3255CAE59BF.2_cid231?__blob=publicationFile [Consulta: 13 de julio de 2013]

Giles, Keir. 2011. *"Information Troops" – a Russian Cyber Command?* 3rd International Conference on Cyber Conflict, NATO Cooperative Cyber Defense Centre of Excellence. Disponible en web: http://www.ccdcoe.org/publications/2011proceedings/InformationTroopsARussianCyberCommand-Giles.pdf [Consulta: 13 de junio de 2013]

Thursday, Guy. 2011. *Cyber security policy will go before cabinet for approval this year*. Disponible en web: http://www.defenceweb.co.za/index.php?option=com_content&view=article&id=13783:cyber-security-policy-will-go-before-cabinet-for-approval-this-year&catid=48:Information%20&%20Communication%20Technologies&Itemid=109 [Consulta: 20 de junio de 2013]

Phahlamohlaka, L. J., Jansen van Vuuren, J. C., y Coetzee, A. J. 2011. *Cyber security awareness toolkit for national security: an approach to South Africa's cyber security policy implementation.* Disponible en web: http://researchspace.csir.co.za/dspace/bitstream/10204/5603/1/Phahlamohlaka1_2011.pdf [Consulta: 20 de junio de 2013]

Instituto Español de Estudios Estratégicos, Ministerio de Defensa. Cuaderno de Estrategia nº 149. 2010. *Ciberseguridad. Retos y amenazas a la seguridad nacional en el ciberespacio.* Disponible en web: http://www.ieee.es/Galerias/fichero/cuadernos/CE_149_Ciberseguridad.pdf [Consulta: 15 de junio de 2013]

IC3 (Internet Crime Compliant Center). *2010 Internet Crime Report.* Disponible en web: http://www.ic3.gov/media/annualreport/2010_IC3Report.pdf [Consulta: 10 de julio de 2013]

Intelligence Advanced Research Projects Activity (IARPA), consultado el 15 de febrero de 2013, http://www.iarpa.gov/MATCHES_Presentations/MATCHES_Proposers_Day_Slides.pdf

International Telecommunications Union. *ITU National Cybersecurity/CIIP Self-Assessment Tool.* Disponible en web: http://www.itu.int/ITU-D/cyb/cybersecurity/projects/readiness.html [Consulta: el 17 de mayo de 2013]

International Telecommunications Union. 2011. *ITU, National Cybersecurity Strategy Guide.* Disponible en web: http://www.itu.int/ITU-D/cyb/cybersecurity/docs/ITUNationalCybersecurityStrategyGuide.pdf [Consulta: el 17 de mayo de 2013]

Joint Publication 2-0. 2007. *Joint Intelligence*. Disponible en web: http://www.fas.org/irp/doddir/dod/jp2_0.pdf [Consulta: el 27 de julio de 2013]

Joint Publication 3-13. 2012. *Information Operations, Chapter I. Principles of Information Operations.* Disponible en web: http://www.fas.org/irp/doddir/dod/jp3_13.pdf [Consulta: el 27 de julio de 2013]

Kerr, Paul K., John Rollins y Caherine A. Theorary. 2010. *The Stuxnet Computer Worm: Harbinger of an Emerging Warfare Capability*. Disponible en web: http://www.fas.org/sgp/crs/natsec/R41524.pdf [Consulta: el 9 de junio de 2013]

Klimburg, Alexander. y Heli Tirmaa-Klaar. 2011. *Cybersecurity and Cyberpower: Concepts, Conditions and Capabilities for Cooperation and Action within the EU.* Study to the European Parliament. Disponible en web: http://www.evi.ee/lib/cyber.pdf [Consulta: el 18 de junio de 2013]

Lee, Jason. 2011. *Markets Analysis and Testing of Contextual Hypotheses Enhancement System (MATCHES).* Disponible en web: http://www.iarpa.gov/Programs/ia/MATCHES/presentations/MATCHES_Proposers_Day_Slides.pdf [Consulta: el 1 de mayo de 2013]

Lewis, James A. 2011. *Cybersecurity: Assessing the Immediate Threat to the United States.* Disponible en web: http://csis.org/files/ts110525_lewis.pdf [Consulta: el 20 de julio de 2013]

Lewis, James A. y Katrina Timlin. 2011. *Cybersecurity and Cyberwarfare. Preliminary Assessment of National Doctrine and Organization.* Disponible en web: http://www.unidir.org/files/publications/pdfs/cybersecurity-and-cyberwarfare-preliminary-assessment-of-national-doctrine-and-organization-380.pdf [Consulta: el 13 de julio de 2013]

Libicki, Martin C. 2009. *Cyberdeterrence and Cyberwar*, RAND, Project Air Force. Disponible en web: http://www.rand.org/pubs/monographs/2009/RAND_MG877.pdf [Consulta: el 13 de julio de 2013]

Lieberthal, K. y Singer, P.W., Febrero 2012, *Cybersecurity and U.S.-China Relations, Brookings*, http://www.brookings.edu/research/papers/2012/02/~/media/Research/Files/Papers/2012/2/23%20cybersecurity%20china%20us%20singer%20lieberthal/0223_cybersecurity_china_us_lieberthal_singer_pdf_english.PDF [Consulta: el 25 de julio de 2013]

Mandiant APT1. 2013. *Exposing One of China's Cyber Espionage Units.* Disponible en web: http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf [Consulta: el 11 de junio de 2013]

Maurer, Tim. 2011. *Cyber Norm Emergence at the United Nations—An Analysis of the UN's Activities Regarding Cyber-security*, Harvard Kennedy School, Disponible en web: http://belfercenter.ksg.harvard.edu/files/maurer-cyber-norm-dp-2011-11-final.pdf [Consulta: el 21 de junio de 2013]

Mcafee. 2011. *Prospective Analysis on Trends in Cybercrime from 2011 to 2020*. Disponible en web: http://www.mcafee.com/us/resources/white-papers/wp-trends-in-cybercrime-2011-2020.pdf [Consulta: el 11 de junio de 2013]

Mercado, Stephen C. 2004. "Sailing the Sea of OSINT in the Information Age," *Studies in Intelligence* nº 48/3. Disponible en web: https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/vol48no3/article05.html [Consulta: el 1 de mayo de 2013]

Meshcheriakov, Vladislav. 2012. *Rusia crea una estrategia de ciberguerra*. Disponible en web: http://rusiahoy.com/articles/2012/03/21/rusia_crea_una_estrategia_de_ciberguerra_16580.html [Consulta: el 3 de julio de 2013]

Ministerio de Defensa de Colombia. 2011. *Colombia presenta estrategia de Ciberseguridad y Ciberdefensa*. Disponible en web: http://www.mindefensa.gov.co/irj/go/km/docs/documents/News/NoticiaGrandeMDN/60a20bd2-8890-2e10-7dab-8a117a5461d8.xml [Consulta: el 3 de junio de 2013]

Ministry of Information and Technology. 2011. *National Cyber Security Strategy of India*. Disponible en web: http://www.mit.gov.in/content/cyber-security-strategy [Consulta: el 8 de junio de 2013]

Ministry of the Interior of the Czech Republic. 2011. *Cyber Security Strategy for the Czech Republic for the 2011 – 2015 Period*. Disponible en web: http://www.enisa.europa.eu/media/news-items/CZ_Cyber_Security_Strategy_20112015.PDF [Consulta: el 8 de junio de 2013]

Ministry of Security and Justice. 2011. *The National Cyber Security Strategy (NCSS)*. Disponible en web: https://www.ncsc.nl/binaries/en/organisation/about-the-ncsc/background/1/National+Cyber+Security+Strategy.pdf [Consulta: el 8 de junio de 2013]

Moore, David. T. 2011. *Sensemaking. A Structure for an Intelligence Revolution*". National Defense Intelligence College, Washington DC. Disponible en web: http://www.ni-u.edu/ni_press/pdf/Sensemaking.pdf [Consulta: el 1 de mayo de 2013]

Muhareb, Mahmoud. 2011. "Israel and Cyber Warfare.", *Doha Institute Book Review*. Disponible en web: http://english.dohainstitute.org/Home/Details/5ea4b31b-155d-4a9f-8f4d-a5b428135cd5/c82f6a5e-6ba7-40c0-ba42-819b34167108 [Consulta: el 7 de junio de 2013]

National Security Information Center. 2010. *Information Security Strategy for Protecting the Nation*. Disponible en web: http://www.nisc.go.jp/eng/ http://www.nisc.go.jp/eng/pdf/New_Strategy_English.pdf [Consulta: el 8 de junio de 2013]

NATO Information Assurance Technical Centre. Disponible en web: http://www.ia.nato.int/ [Consulta: el 1 de mayo de 2013]

NATO. 2009. *Cyber Defence Concept*. Disponible en web: http://www.nato-pa.int/default.asp?SHORTCUT=1782 [Consulta: el 16 de mayo de 2013]

Network Word. 2013. *Deutsche Telekom lanza mapas en tiempo real de ciberataques globales*, Disponible en web: http://www.networkworld.es/Deutsche-Telekom-lanza-mapas-en-tiempo-real-de-ciberataques-/seccion-actualidad/noticia-131125 [Consulta: el 23 de julio de 2013]

New Zealand Government. 2011. *National Cyber Security Strategy.* Disponible en web: http://www.dpmc.govt.nz/sites/all/files/publications/nz-cyber-security-strategy-june-2011_0.pdf [Consulta: el 19 de mayo de 2013]

Nye, Joseph. S. 2010. *Cyber Power*. Belfer Center for Science and International Affairs, Harvard Kennedy School. Disponible en web: http://belfercenter.ksg.harvard.edu/publication/20162/cyber_power.html [Consulta: el 15 de junio de 2013]

O´Dwyer, Gerard. 2011. "Finland to Develop Cyber Defense". *DefenseNews.* Disponible en web: http://www.defensenews.com/article/20111020/DEFSECT04/110200306/Finland-Develop-Cyber-Defense-Counterpunch- [Consulta: el 5 de mayo de 2013]

Sommer, Peter e Ian Brown. 2011. *Reducing Systemic Cybersecurity Risk*. OECD/IFP Project on "Future Global Shocks". Disponible en web: http://www.oecd.org/dataoecd/3/42/46894657.pdf [Consulta: el 5 de mayo de 2013]

Office of the National Counterintelligence Executive. 2011. *Foreign Spies Stealing US Economic Secrets in Cyberspace.*
Disponible en web: http://www.ncix.gov/publications/reports/fecie_all/Foreign_Economic_Collection_2011.pdf [Consulta: el 5 de mayo de 2013]

Office of the Secretary of Defense. 2010. *Annual Report to Congress. Military and Security Developments Involving the People's Republic of China.* Disponible en web: http://www.defense.gov/pubs/pdfs/2010_CMPR_Final.pdf [Consulta: 11 de julio de 2013]

Office of the Secretary of Defense. 2012. *Annual Report to Congress. Military and Security Developments Involving the People's Republic of China.* Disponible en web: http://www.defense.gov/pubs/pdfs/2012_CMPR_Final.pdf [Consulta: 11 de julio de 2013]

Orden Ministerial 10/2013, de 19 de febrero, por la que se crea el Mando Conjunto de Ciberdefensa de las Fuerzas Armadas (MCCD), Boletín Oficial del Ministerio de Defensa 26/02/2013, Disponible en web: http://www.defensa.gob.es/Galerias/ooee/emad/fichero/20130226_CIBERDEFENSA.pdf [Consulta: 21 de julio de 2013]

Pereda, Cristina. F. 2013. "Obama firma una orden ejecutiva para responder a la amenaza cibernética", *El País*, 13 de Febrero de 2013. Disponible en web: http://internacional.elpais.com/internacional/2013/02/13/actualidad/1360731100_027874.html [Consulta: 13 de febrero de 2013]

Presidência da República. Secretaria de Assuntos Estratégicos. 2012. *Segurança e Defesa Cibernética*. Disponible en web: http://www.sae.gov.br/site/wp-content/uploads/Seguranca_Cibernetica_web.pdf [Consulta: 21 de julio de 2013]

Rollins, John y Catherine A. Theorary. 2011. *Terrorist Use of the Internet: Information Operations in Cyberspace*, Congressional Research Service. R41674. Disponible en web: http://www.fas.org/sgp/crs/terror/R41674.pdf [Consulta: 29 de mayo de 2013]

Sánchez Benitez, S. 2011. *La comunicación estratégica como política pública.* Disponible en web: http://www.ieee.es/Galerias/fichero/docs_opinion/2011/DIEEEO21_2011ComunicacionEstrategica.pdf [Consulta: 25 de mayo]

Schillinger, Raymond. 2011. “Social Media and the Arab Spring: What Have We Learned?”, *El Huffingtonpost.com.* Disponible en web: http://www.huffingtonpost.com/raymond-schillinger/arab-spring-social-media_b_970165.html [Consulta: 14 de julio de 2013]

Secretariat of the Security and Defence Comité. 2013. *Finland´s Cyber Security Strategy*. Disponible en web: http://www.yhteiskunnanturvallisuus.fi/en/materials/doc_download/38-finlandas-cyber-security-strategy [Consulta: 14 de julio de 2013]

Seffers, George I. 2011. “U.S. Marines Creating Island for Network Defense”, *Signal Magazine.* Disponible en web: http://www.afcea.org/signal/articles/templates/Signal_Article_Template.asp?articleid=2542&zoneid=285 [Consulta: 25 de mayo]

Sharma, D. (2011), *China’s Cyber Warfare Capability and India’s Concerns*, Disponible en web: http://www.idsa.in/system/files/jds_5_2_dsharma.pdf
[Consulta: 17 de julio de 2013]

South African Government. 2012. *National Cybersecurity Polic Framework For South Africa.* Disponible en web: http://www.info.gov.za/speech/DynamicAction?pageid=461&sid=25751&tid=59794 [Consulta: 16 de julio de 2013]

Symantec. 2012. *Internet Security Treat Report.* Disponible en web: http://www.symantec.com/content/en/us/enterprise/other_resources/b-istr_main_report_2011_21239364.en-us.pdf [Consulta: 23de julio de 2013]

Symantec. 2012. *Flamer: Highly Sophisticated and Discreet Threat Targets the Middle East*, Disponible en web: http://www.symantec.com/connect/blogs/flamer-highly-sophisticated-and-discreet-threat-targets-middle-east [Consulta: 23 de julio de 2013]

Symantec. 2013. *Internet Security Treat Report.* Disponible en web: http://www.symantec.com/content/en/us/enterprise/other_resources/b-istr_main_report_v18_2012_21291018.en-us.pdf [Consulta: 23 de julio de 2013]

The Cyber Hub. N.d. *Cyber Power Index.* Disponible en web: http://www.cyberhub.com/CyberPowerIndex [Consulta: 1 de agosto de 2013]

Trend Micro. 2012. *Informe Trend Micro de la campaña APT y de Ciberespionaje de Luckycat*, Disponible en web: http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp_luckycat_redux.pdf [Consulta: 15 de agosto de 2013]

Tsukayama, Hayley. 2011. "Pentagon puts out a call for the socially savvy". *Washington Post*, 3 de agosto de 2011. Disponible en web: http://www.washingtonpost.com/blogs/faster-forward/post/pentagon-puts-out-a-call-for-the-socially-savvy/2011/08/02/gIQAzP50pI_blog.html [Consulta: 20 de junio de 2013]

UK Cabinet Office. 2009. *Cyber Security Strategy of the United Kingdom.* Disponible en web: http://www.official-documents.gov.uk/document/cm76/7642/7642.pdf [Consulta: 12 de agosto de 2013]

UK Cabinet Office. 2011. *The UK Cyber Security Strategy*. Disponible en web: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60961/uk-cyber-security-strategy-final.pdf [Consulta: 12 de agosto de 2013]

U.S. Army. 2011. *Army social Media Handbook.* Disponible en web: http://www.carlisle.army.mil/dime/documents/Army%20Social%20Media%20Handbook%20VER%202%20AUG%202011.pdf [Consulta: 11 de agosto de 2013]

US Department of State. 2010. *Estrategia de Seguridad Nacional de Estados Unidos de América.* Disponible en web: http://www.whitehouse.gov/sites/default/files/rss_viewer/national_security_strategy.pdf [Consulta: 10 de agosto de 2013]

US Department of State. 2011. *International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World*. Disponible en web: http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf [Consulta: 10 de agosto de 2013]

US Department of Defense. 2011. *Strategy for Operating in Cyberspace*. Disponible en web: http://www.defense.gov/news/d20110714cyber.pdf [Consulta: 8 de agosto de 2013]

Valdez, Adrienne. 2011. *South Korea Outlines Cyber Security Strategy*. Disponible en web: http://www.futuregov.asia/articles/2011/aug/13/south-korea-outlines-cyber-security-strategy/ [Consulta: 18 de agosto de 2013]

Ventre, Daniel. 2009. *Information Warfare*. CNRS, French National Center of Scientific Research, France: Wiley-ISTE.

Ventre, Daniel. 2012. *Cyber Conflict: Competing National Perspectives*. London: Wiley-ISTE.

Verisign iDefense. 2010. *An Excerpt from the iDefense 2011 Cyber Threats and Trends Report*. Disponible en web: http://www.verisigninc.com/assets/whitepaper-idefense-trends-2011.pdf [Consulta: 16 de agosto de 2013]

Verisign iDefense. *Idefense Security Intelligence Services*. Disponible en web: http://www.verisigninc.com/en_US/products-and-services/network-intelligence-availability/idefense/index.xhtml [Consulta: 16 de agosto de 2013]

Villarejo, Esteban. 2013. "El Centro Nacional de Inteligencia recibe 200 ataques importantes en tres meses", *ABC*, 16 de julio de 2013. Disponible en web: http://www.abc.es/espana/20130316/abci-centro-nacional-inteligencia-recibe-201303152049.html [Consulta: 16 de julio de 2013]

Watkins, Jennifer H. and Marko A. Rodriguez. 2008. "A Survey of Web-based Collective Decision Making Systems", in Eds. R. Nayak and L.C. Jain, eds., *Computer Science: Evolution of the Web in Artificial Intelligence Environments*. Berlin: Springer-Verlag, Disponible en web: http://public.lanl.gov/jhw/Jen/Publications_files/LNCSproof.pdf [Consulta: 20 de julio de 2013]

World Economic Forum. 2012. *Global Risks 2012*. Disponible en web: http://www3.weforum.org/docs/WEF_GlobalRisks_Report_2012.pdf [Consulta: el 25 de junio de 2013]