CENTRO SUPERIOR DE ESTUDIOS DE LA DEFENSA NACIONAL


MONOGRAFÍAS
del
CESEDEN

126

# EL CIBERESPACIO. NUEVO ESCENARIO DE CONFRONTACIÓN

MINISTERIO DE DEFENSA

CENTRO SUPERIOR DE ESTUDIOS DE LA DEFENSA NACIONAL

MONOGRAFÍAS
del
CESEDEN

126

# EL CIBERESPACIO. NUEVO ESCENARIO DE CONFRONTACIÓN

Febrero, 2012

**CATÁLOGO GENERAL DE PUBLICACIONES OFICIALES**
**http://publicacionesoficiales.boe.es/**

Edita:

MINISTERIO DE DEFENSA
SECRETARÍA GENERAL TÉCNICA

NIPO: 083-12-024-7 (edición en papel)
NIPO: 083-12-023-1 (libro-e)
ISBN papel: 978-84-9781-723-3
Depósito Legal: M-12287-2012
Imprime: Imprenta del Ministerio de Defensa
Tirada: 500 ejemplares
Fecha de edición: marzo, 2012

NIPO: 083-12-025-2 (edición en línea)
ISBN libro-e : 978-84-9781-724-0

En esta edición se ha utilizado papel libre de cloro obtenido a partir de bosques gestionados de forma sostenible certificada.

# EL CIBERESPACIO. NUEVO ESCENARIO DE CONFRONTACIÓN

## SUMARIO

Página

# INTRODUCCIÓN

# INTRODUCCIÓN

Por José Ramón Casar Corredera

«*Ne Sero Veniam Depugto Proelio*»
(«Que no llegue tarde, con la batalla ya acabada»)

Plauto, *Menaechmi*

*El ciberespacio, nuevo* Global Common *junto con los tradicionales terrestre, marítimo, aéreo y espacial, está siendo objeto común de reflexión y publicación por parte de estudiosos y numerosas agencias e instituciones públicas y privadas nacionales e internacionales, incluyendo la Organización del Tratado del Atlántico Norte (OTAN), Unión Europea, Organización para la Seguridad y Cooperación en Europa (OSCE), etc. El ciberespacio se anticipa o se vislumbra, desde la perspectiva que interesa a esta* Monografía*, como un escenario de conflicto mayor, en el que las actuales escaramuzas, mayoritariamente aún de baja intensidad, pudieran evolucionar a enfrentamientos de mayores dimensiones, que posiblemente combinados con otras actuaciones de fuerza, quizás en otros* Commons*, constituyan una verdadera guerra, la que ha dado en llamarse ciberguerra.*

*Esta* Monografía *se orienta principalmente hacia aspectos relacionados con la ciberdefensa considerada como una cuestión básicamente militar, en el sentido de que se interesa por facetas que involucran a instituciones, organizaciones o profesiones militares, en todo o en parte. No considera sin embargo, al menos explícita y detalladamente, otros aspectos también importantes para el ciudadano, como el robo de datos personales, el ciberdelito económico, etc., y otros, seguramente de interés*

*nacional general, como el ciberespionaje industrial o el uso malicioso de otras herramientas «corrientes» de Internet, como redes sociales,* blogs *o simples portales* web *(o medios de comunicación* on-line*) para hacer apología extremista o sembrar dudas de confianza o reputación de una economía, una nación, una empresa, etc.*

*Los ejemplos recientes (diarios) de ataques premeditados en Internet con notable impacto mediático (por ejemplo, los muy recientes casos de los grupos* Anonymous *o* Lulzsec*), aunque con pocas consecuencias realmente graves (conocidas, al menos de momento), parecen poner de manifiesto que, en muchos casos, el impacto mediático y la alarma social no son siempre proporcionales al grado de la amenaza real. Es literalmente imposible hacer una historia detallada, día a día, de la cantidad de sucesos de ataques (de baja intensidad, diríamos), consistentes en robos de datos, denegaciones de servicio, publicación dolosa de informaciones estrictamente personales, etc. que se han sucedido en los últimos (muchos) meses: Sony, Honda, Citigroup, Paypal, Apple, The Sun, Facebook, el Fondo Monetario Internacional, el Senado de Estados Unidos, la Agencia Central de Inteligencia (CIA) norteamericana, El Pentágono, Inteco, Movistar, y un larguísimo etcétera, que ocuparía varios párrafos, han sido víctimas de ataques a través de Internet. Al margen de consecuencias prácticas que no se han producido, es indiscutible que estos ataques, sean de hacktivismo simple o de otra dimensión, son capaces de generar una sensación de indeseables inseguridad y desconcierto tanto en los ciudadanos como en las economías.*

*El ciberespionaje comercial e industrial es también un elemento de preocupación general, principalmente en Occidente, en relación a algunas grandes potencias. En el año 2010 salieron a la opinión pública varias campañas, aparentemente originadas en algún lugar de China. Quizás dos de las más conocida son la operación* Aurora*, dirigida a diversas empresas con sede en California de los sectores de la Tecnología de la Información y las Comunicaciones (TIC) y Química y la Shadow Network, aparentemente dirigida a comprometer determinados intereses de la India. El ataque a Lockheed Martin y a otros contratistas de Defensa de Estados Unidos, a través de determinados dispositivos de* Rivest Sharmia and Adleman*, es otro ejemplo, de entre tantos, de intentos de intrusión interesada en sistemas de proveedores críticos para la defensa o la economía de una nación. El 4 de noviembre de 2011 se conocía en la prensa española uno de los informes oficiales de inteligencia de Estados Unidos*

*(referido al periodo 2009-2011), que acusaba a China y Rusia de robar (o intentarlo) secretos comerciales. El informe, no obstante, reconoce la dificultad de determinar exactamente quién está detrás de estos ataques cibernéticos (por cierto, una de las dificultades recurrentemente aludidas en varios capítulos de esta* Monografía*).*

*Se puede tener la tentación de intentar restar seriedad práctica a estos intentos, logrados o malogrados, de robo de datos (yo mismo la tengo), pero hay otros indicios y noticias que no pueden dejarnos tranquilos. Podríamos mencionar varios, sin duda; pero, para esta Introducción he retenido dos, basados en dos noticias recientes: la primera, conocida hace unos días, aunque referida a hechos sucedidos en los años 2007 y 2008, descubre que un informe del Congreso de Estados Unidos expone los indicios que hacen sospechar que desde China se tuvo acceso a dos satélites gestionados por la Administración Nacional de Aeronáutica de Estados Unidos (NASA).*

*Se supone que el acceso tuvo lugar a través de un centro de control terrestre de la NASA en Noruega. Sin consecuencia práctica, el suceso ilustra que es posible imaginar capacidades de intrusión en misiones de alto valor estratégico. La segunda noticia es de ayer (escribo estas líneas el 20 de noviembre de 2011) y refiere un ciberataque contra una infraestructura industrial civil de Estados Unidos, en concreto, un servicio de distribución de aguas en Illinois. El incidente habría tenido lugar el 8 de noviembre; los atacantes habrían usado unas claves robadas de una empresa que desarrolla* software *para los Sistemas de Control SCADA, para acceder remotamente e inutilizar una (o varias) bombas de agua. No se sabe a día de hoy acerca de las intenciones del atacante, en su caso, y modo de actuación, pero el incidente demuestra la posibilidad de intervenir remota y maliciosamente en las infraestructuras críticas de un país. Se trazó el ordenador de origen del ataque en Rusia, pero esto, en el ciberespacio, no se puede constituir en prueba alguna de autoría real.*

*Es en este contexto de intrusiones, ataques y provocaciones de menor o mayor envergadura, que se vienen sucediendo cotidianamente, en el que hay que entender la creciente preocupación intelectual, pero también la actualidad del tema en las agendas políticas y de trabajo de los organismos competentes.*

*El Centro Superior de Estudios de la Defensa Nacional (CESEDEN), impulsando ésta que es una de sus líneas de reflexión prioritarias en la ac-*

*tualidad, ha querido contribuir en el debate sobre el estado actual y estrategias de actuación para la defensa de los intereses de los individuos en el ciberespacio, formando un grupo de trabajo sobre el ciberespacio como nuevo escenario de conflicto, que me ha cabido el privilegio de coordinar. Se suma así a otras iniciativas concurrentes o complementarias, algunas extremadamente valiosas, como la que recoge el* Cuaderno de Estrategia*, número 149 del Instituto Español de Estudios Estratégicos, febrero de 2011, dedicada también a la ciberseguridad.*

*El grupo de trabajo ha estado formado por Luis Feliu Ortega, Carlos Enríquez González, Javier López de Turiso y Sánchez, Óscar Pastor Acosta, Manuel Pérez Cortés, Ángel Gómez de Ágreda (que ha ejercido de secretario-coordinador con una eficacia imposible de imitar y sin cuyo concurso este trabajo no se hubiera terminado ni en tiempo ni en forma) y por mí mismo. Hemos dado en titular los capítulos de esta* Monografía*, de los que hago posteriormente una larga (y a veces literal) reseña, de la siguiente forma:*

– *Capítulo 1: «La ciberseguridad y la ciberdefensa».*
– *Capítulo 2: «Estrategias internacionales para el ciberespacio».*
– *Capítulo 3: «La evolución del conflicto hacia un nuevo escenario bélico».*
– *Capítulo 4: «El ciberespacio como escenario de conflictos. Identificación de las amenazas».*
– *Capítulo 5: «Capacidades para la Defensa en el ciberespacio».*
– *Capítulo 6: «Tecnologías para la Defensa en el ciberespacio».*

*Cada uno de los capítulos se debe atribuir a su (único) autor. Sin embargo, tanto la organización, como la orientación, como la formación de algunas ideas es obra colectiva. El grupo se ha reunido para debatir desde aspectos semánticos hasta aspectos doctrinales en seis largas reuniones de trabajo, que han contribuido inevitablemente a conformar la opinión y posición personales de cada uno de nosotros.*

*Junto con los aspectos más defensivos-ofensivos, entendidos desde el punto de vista militar (y, de algún modo, implícitamente, contraterrorista), el grupo de trabajo ha querido tener presente permanentemente, en su reflexión, las herramientas, planteamientos organizativos y fórmulas que aportarían más, a su juicio, a la defensa integral de los intereses civiles de los ciudadanos y comunidades.*

*El capítulo primero, por Luis Feliu Ortega, comienza revisando, con perspectiva histórica, los conceptos de conflicto armado, seguridad y de-*

*fensa, recordando con respecto a estos dos últimos términos, lo que contiene la Doctrina del Ejército de Tierra (2003): La seguridad es el estado deseado por una sociedad, en el que pueda desarrollarse y prosperar libre de amenazas. La Defensa es la adopción práctica de medidas conducentes a mantener la seguridad deseada; y, en relación con esto, compara el uso de la fuerza con el concepto de Defensa Militar, y el de Defensa Nacional, globalmente, con el conjunto de medios y acciones, civiles y militares, tendentes a garantizar la Seguridad Nacional.*

*A continuación se aproxima a los conceptos de ciberespacio, ciberseguridad y ciberdefensa, identificando aquél como un espacio estratégico para el que hay que definir las medidas de prevención, disuasión, protección y reacción de la ciberdefensa. Identificado como nuevo* Global Common, *el ciberespacio posee una serie de características diferenciales del resto de los espacios. Resumidamente:*

1. *El ciberespacio es un entorno único, en el que el atacante puede estar en cualquier parte del globo.*
2. *En la defensa intervienen muchos factores, y no sólo elementos estatales sino también privados. Se exige pues una estrecha coordinación entre todos ellos.*
3. *La confrontación en el ciberespacio presenta frecuentemente las características de un conflicto asimétrico; y es frecuentemente anónimo y clandestino.*
4. *Permite obtener información sobre objetivos sin necesidad de destruir ni neutralizar ningún sistema, y a menudo, sin delatarse.*
5. *Permite también ejercer el chantaje; pero, al mismo, tiempo, la defensa puede utilizarlo para la disuasión.*
6. *Evoluciona rápidamente siguiendo la evolución tecnológica de las TIC.*

*Luego se refiere al concepto de ciberconflicto, para enunciar claramente algo nada irrelevante desde el punto de vista de las implicaciones organizativas, que es que:*

> *«Las confrontaciones y conflictos que tienen lugar en el ciberespacio pueden no ocurrir necesariamente en el contexto de una guerra, ni siquiera en una confrontación general.»*

*A continuación aborda el tema de las estrategias de Seguridad Nacional (incluidas las de ciberseguridad) e identifica algunas coincidencias entre las conclusiones o propuestas de algunas de ellas relevantes, a saber, brevemente:*

1. *Se deben definir claramente las amenazas para la ciberseguridad y como consecuencia, los objetivos a alcanzar, las medidas a tomar y las acciones a ejecutar.*
2. *La ciberseguridad debe enfocarse de forma que integre a las distintas agencias de seguridad e inteligencia del Estado, los centros de investigación tanto públicos como privados, el sector privado empresarial y a los propios ciudadanos.*
3. *A nivel internacional, la ciberdefensa debe incluirse también en las estrategias de defensa colectiva.*
4. *La protección debe incluir la de las infraestructuras críticas, incluidos los Sistemas de Información y Telecomunicaciones (CIS), la de los ciudadanos y la del territorio nacional y sus instituciones.*
5. *Debe incluir la previsión, prevención, disuasión, protección y reacción. No debe limitarse a acciones puramente defensivas o pasivas sino que deben preverse también capacidades ofensivas.*
6. *Debe ser multidimensional; en particular, debe contemplar los aspectos legislativos, los ejecutivos con los organismos encargados de vigilar su cumplimiento y los judiciales. Deberán involucrarse fundamentalmente los Ministerios de Defensa, Interior, Justicia e Industria, investigación y desarrollo debidamente coordinados.*

*Luego, se centra en los ciberataques a infraestructuras críticas (incluidos los cibersabotajes), mencionando algunos ejemplos conocidos, para referirse a continuación a los ciberataques en el ámbito propio de las operaciones militares, como el ataque a los Sistemas de Mando y Control u otros elementos básicos de coordinación.*

*A continuación, se menciona el concepto de superioridad militar en el ciberespacio, definida, citando a Lewis, como «la ventaja operativa en, desde y a través del ciberespacio, para llevar a cabo operaciones en cualquier momento y lugar, sin interferencias que las impidan o limiten, geográfica o temporalmente»; y en relación con ello, el Concepto de Operaciones en Red (CNO), desarrollado por Estados Unidos, la OTAN y la Unión Europea. Nos recuerda la posibilidad de que se desarrolle una carrera ciberarmamentística en pos de la superioridad (y la disuasión consecuente).*

*Tras reflexionar sobre algunos otros elementos, como las ciberarmas o la dificultad, en general, de la atribución del ataque, el autor concluye que:*

> *«Estamos en un nuevo escenario estratégico, en un nuevo campo de batalla o en una extensión del mismo, donde se producen comportamientos o fenómenos ya conocidos, pero que emplean*

*técnicas nuevas; y también fenómenos nuevos que surgen de la propia peculiaridad del ciberespacio en el que la estrategia de seguridad demanda planteamientos nuevos e imaginativos y cambios de mentalidad, de un modo especial en lo que se refiere a la gestión de crisis y resolución de conflictos y a la necesidad de adaptación de la Defensa en general y de las Fuerzas Armadas en particular, a las circunstancias de cada momento.»*

*A continuación se revisan algunos de los antecedentes jurídicos y doctrinales que condujeron a la Estrategia Española de Seguridad (EES), aprobada en el año 2011, una valiosa iniciativa que, sin embargo, no termina de resolver algunos problemas importantes pendientes, afirma que:*

*«España, a diferencia de otros países de nuestro entorno, no ha definido todavía una legislación específica y completa en materia de ciberseguridad. Sí existe legislación distribuida en distintos ámbitos ministeriales, pero no ha sido desarrollada a partir de una política común que refleje el ámbito nacional y estratégico de la ciberseguridad y así las responsabilidades en el ciberespacio están muy fragmentadas en diferentes organismos, dependientes de distintos ministerios que abordan el problema de forma parcial.»*

*La EES prevé la creación de un Consejo Español de Seguridad, dependiente de Presidencia del Gobierno, pero a día de hoy:*

*«Si bien existen organismos con responsabilidades claras en distintos ámbitos de las Administraciones públicas, España no dispone de un órgano único, al más alto nivel, que asuma el valor estratégico que la ciberseguridad tiene para nuestro país y ejerza el liderazgo necesario para que todos esos organismos actúen según una única política nacional. Para ello, sería necesario en primer lugar la creación de una estrategia nacional de ciberseguridad que tratase de forma completa el problema y ayudase a crear, tanto en las autoridades como en las empresas y los particulares, una conciencia de ciberseguridad.»*

*El capítulo termina revisando brevemente aspectos de la actividad y estrategias en el ciberespacio en los ámbitos de la Unión Europea y de la OTAN y reclamando unidad y estrategia.*

*Precisamente el capítulo segundo, por Carlos Enríquez González, se centra casi exclusivamente en la faceta internacional de la ciberseguridad, principalmente en su vertiente militar, pero también en su vertiente civil.*

*Empieza por observar la ausencia de un marco legal mundial o incluso un principio de consenso o acuerdo general en lo que se refiere a la regulación en Internet, en donde se contraponen los partidarios de la autorregulación y los que creen que un cierto grado de intervención mejorará la confianza en los servicios por parte de los usuarios.*

*El capítulo, en todo caso, gira motivado por la afirmación que la Agenda Digital para Europa (2010) hace de que la lucha contra las crecientes amenazas a la ciberseguridad debe desarrollarse en un contexto internacional. La Agenda, recuerda el autor, persigue:*

> *«Promover la internacionalización de la gobernanza de Internet y la cooperación mundial para mantener la fiabilidad de la Red de redes.»*

*Nos recuerda el autor que lo primero parecido a un marco legal internacional se produce en la Convención del Consejo de Europa sobre Cibercrimen en el año 2001, primer tratado internacional sobre delitos cometidos a través de Internet; ciertamente, sólo contempla violaciones de derechos y delitos importantes pero secundarios desde el punto de vista de la Defensa. En el año 2008, en el marco de la OSCE y a iniciativa estona, por razones conocidas (que se mencionan varias veces en esta* Monografía*), se introduce el concepto de ciberseguridad en su dimensión político-militar; a partir de entonces, se han venido sucediendo diversos documentos con recomendaciones de actuación.*

*En lo que respecta a la Unión Europea, Enríquez González hace notar que la Unión mantiene dos instituciones principales y, en consecuencia, dos líneas estratégicas de pensamiento y actuación: por un lado, la de la Agencia Europea de Defensa (EDA), que, en lo que concierne a este trabajo, se ha venido enfocando principalmente en el campo de la colaboración segura en la* Military Cloud*. Por otro, la de la Agencia Europea para la Seguridad de la Información y de las Redes, que trata de acomodar su actividad a lo contemplado en la Estrategia Europea de Seguridad y al plan de acción cuatrienal que ha elaborado la Comisión, uno de cuyos cinco objetivos es precisamente «aumentar los niveles de seguridad de los ciudadanos y de las empresas en el ciberespacio». Para cumplir este objetivo, la Comisión define tres acciones:*

1. *Reforzar la capacidad judicial y policial necesaria para la lucha contra el cibercrimen, principalmente mediante el establecimiento de un Centro de Cibercrimen Europeo.*
2. *Trabajar con la industria para proteger a los ciudadanos mediante la formación y concienciación. Dentro de esta línea de acción también*

*recomienda reforzar la cooperación entre los sectores público y privado a escala europea a través de la Asociación Público-Privada Paneuropea de Resiliencia.*

3. *Mejorar la capacidad para hacer frente a los ciberataques. Sería necesario adoptar una serie de medidas para mejorar la prevención, la detección y la reacción rápida en caso de ataques cibernéticos, estableciendo, mejorando y coordinando Equipos de Respuesta a Emergencias Informáticas (CERT) a nivel europeo.*

*La Organización para la Cooperación y el Desarrollo Económico ha abordado el tema recientemente (2011) en su Informe* Cybersecurity risks and counter-measures*. El autor del capítulo trae a colación dos de las conclusiones del Informe: por un lado, la de que pocos cibersucesos tendrían la capacidad de provocar una conmoción global. Sería improbable la ocurrencia de una verdadera ciberguerra, si bien no descarta la utilización de ciberarmas, virus troyanos,* botnets*, etc., como multiplicadores de fuerza junto a armas convencionales en el contexto de un conflicto. Por otro lado, –según los autores– ya que la mayoría de los objetivos de un ciberataque serían civiles, el papel de las Fuerzas Armadas se limitaría a proteger sus propios sistemas y al eventual desarrollo de capacidades ofensivas.*

*El capítulo dedica unas cuantas páginas luego a revisar hechos y documentos relacionados con las iniciativas y estudios de la Organización de Naciones Unidas (ONU) y de la Unión Internacional de Comunicaciones, que anticipan, por comparación, la que será una de las conclusiones del capítulo: la disparidad de perspectivas de los diversos organismos e instituciones que consideran el tema del ciberespacio.*

*Dentro de la OTAN, el tema del ciberespacio tiene también una trayectoria de creciente interés. El autor la revisa, breve pero rigurosamente, partiendo de los comunicados de sus cumbres, empezando por la de Praga de 2002, en la que se enuncia la necesidad de «fortalecer la capacidad de defenderse de los ciberataques». En el año 2006 (Riga), se acordó «mejorar la protección de nuestros sistemas de información claves, frente a los ciberataques». En el año 2008 (Bucarest), se acordó reforzar los sistemas aliados frente a los ciberataques y se anunció la aprobación de una política aliada de ciberdefensa. En la cumbre de Lisboa de 2010, se aprobó el nuevo Concepto Estratégico, «que eleva los ciberataques a la categoría de amenazas contra la seguridad, estabilidad y prosperidad del área euroatlántica». La nueva política de ciberdefensa fue aprobada*

*por los ministros de Defensa aliados en junio de 2011. En ella se establece que su prioridad principal es la protección de las redes propias de la OTAN y el establecimiento de requisitos para la protección de las redes nacionales en que la OTAN se apoya para llevar a cabo sus misiones esenciales. Por último, el autor termina recordándonos algunas consecuencias de la aprobación de esta política, de entre las que entresaco aquí las siguientes cinco:*

1. *La OTAN deberá elaborar unos requisitos mínimos para los sistemas de información nacionales críticos para el cumplimiento de las misiones esenciales de la OTAN.*
2. *La ciberdefensa se integrará plenamente en el Proceso de Planeamiento de Defensa Aliado, NDPP* (NATO Defence Planning Process), *que identificará y priorizará las necesidades en este ámbito.*
3. *Se definirán los requisitos de ciberdefensa también para las naciones no-OTAN que contribuyen con tropas a las misiones de la Alianza.*
4. *Se mejorarán las capacidades de alerta temprana, de conocimiento de la situación y de análisis.*
5. *Se desarrollarán programas de sensibilización y en los ejercicios de la Alianza se trabajará más el componente cibernético.*

*El capítulo a continuación revisa las estrategias y, en algunos casos, las líneas de actuación para el ciberespacio de algunos países, en particular, de Estados Unidos (y su decisión de crear un mando único específico, el Mando Cibernético (USCYBERCOM), con amplios poderes, del que se escribe también en el capítulo quinto, Reino Unido (y su órgano directivo, la Oficina de Ciberseguridad y de Seguridad de la Información), Francia (y su Agencia Nacional para la Seguridad de los CIS), etc.*

*El capítulo termina con interesantes conclusiones para la reflexión y el debate. Anticipo aquí, breve pero literalmente, dos de ellas:*

1. *Nos encontramos con una aproximación internacional fragmentaria y centrada en el objeto de cada Organización: la OTAN persigue la protección de los sistemas críticos para su misión; la Unión Europea la creación de un mercado digital único soportado por una Internet segura y confiable; la ONU pretende hacer accesibles para todos los beneficios del uso de las Tecnologías de la Información y de Internet. Parece por tanto, que las respectivas estrategias internacionales para el ciberespacio están, por el momento, muy fragmentadas. Incluso cuando un mismo Estado miembro pertenece a varias organizaciones, la representación en cada una de ellas, frecuentemente*

*recae sobre diferentes departamentos que no mantienen posturas ni concertadas ni coherentes.*

2. *Asistimos a una suerte de «afganización» del ciberespacio, con burbujas de seguridad e insurgencia, al igual que ocurre sobre el terreno en ese país centroasiático. Según Innerarity:*

   *«Existen espacios desgobernados allá donde los Estados han cedido soberanía, voluntaria o involuntaria, razonablemente o no, en todo o en parte, a otras autoridades. Si entendemos que los espacios desgobernados son aquellos en los que el poder del Estado es ausente, débil o contestado, entonces –añade el autor–, además de referirnos a los territorios de poder tribal o insurgencia persistente, debemos extender esta perspectiva a los dominios de Internet o a los mercados donde operan los agentes económicos con una regulación pública insuficiente.»*

*El capítulo tercero, debido a Javier López de Turiso y Sánchez, comienza centrándose en el concepto general de conflicto como lucha de intereses, y progresa revisando los tipos, las causas, la dinámica y las fases de la evolución de un conflicto hasta su forma más violenta, que es la guerra.*

*Describe también los escenarios donde actúa «el instrumento de poder militar», identificando el último de ellos como el del ciberespacio (después del terrestre, el marítimo, el aéreo y el espacial). De él hace una breve reseña de sus orígenes y rápida evolución.*

*Luego describe algunas de las características comunes de los escenarios físicos tradicionales de la guerra, y razona que las operaciones en el ciberespacio comparten, en mayor o menor medida, todas y cada una de las características descritas. Luego identifica las características diferenciadoras del ciberespacio, entre las que destaco (resumidamente):*

– *Lo que hace particularmente destacable al ciberespacio es que físicamente se integra en el conjunto de los otros cuatro dominios. Allá donde en cada uno de estos dominios exista un punto de comunicación enlazado con otro, ahí tendrá cabida el ciberespacio.*
– *El ciberespacio evoluciona a una velocidad muchísimo mayor que sus homólogos convencionales. La capacidad de expansión del ciberespacio y su capilaridad dentro del propio espacio físico en el que se expande es prácticamente ilimitada.*
– *Los dominios tradicionales precisan de sistemas de armas para hacer sentir el poder terrestre, naval o aéreo. En el ciberespacio no; las armas*

*no son cinéticas. Aquí también existen armas defensivas y ofensivas, pero son de índole totalmente diferente.*

- *Así como los medios de combate en los escenarios terrestre, marítimo y aéreo normalmente sólo están al alcance de los Estados, los medios del ciberespacio están a disposición de toda la población mundial que disponga de un acceso a la Red.*
- *El principal valor en los entornos terrestre, marítimo y aéreo, aparte del propio ser humano, son los medios materiales, los sistemas de armas, su despliegue, su efectividad y su operatividad. Sin ellos, la lucha en estos entornos carece de sentido. En el ciberespacio el principal valor es la información, la que en la defensiva se ha de proteger y en la ofensiva se ha de negar, alterar o sustraer al enemigo.*
- *Así como los conflictos tradicionales se centran en el campo de batalla, el ciberespacio extiende la zona de combate hasta el mismo corazón de la nación, al ser capaz de entrar en cada una de las casas de los ciudadanos y de cortarle los suministros básicos que éste necesita para su supervivencia.*

*La segunda parte de la contribución de López de Turiso Sánchez aborda el tema de la organización de la ciberdefensa. Comenzando por hacer una reflexión acerca de qué constituye el ámbito de la ciberdefensa y cuáles son las necesarias capacidades para garantizarla, identifica los que denomina subámbitos de control estatal y de control privado, integrando aquél las infraestructuras críticas, las Fuerzas Armadas y las Fuerzas y Cuerpos de Seguridad del Estado. Inmediatamente trae a colación la interesante reflexión acerca de si las Fuerzas Armadas deben ocuparse de sus propias redes o, como cita, también de la base industrial de las empresas tecnológicas de la defensa del país. La opinión de López Turiso Sánchez es que, salvo que se organice de otra manera, que hoy no está definida, «el ámbito de actuación de las Fuerzas Armadas deberá ser exclusivamente sus redes militares».*

*A continuación, el autor se plantea una interesante y oportuna colección de preguntas (sin respuesta) en relación a la organización de la ciberdefensa nacional, que van desde la organización de la red de CERT hasta los aspectos de formación, responsabilidad y coordinación.*

*Luego aborda, más brevemente, aspectos relacionados con la capacidad ofensiva en el ciberespacio, dividiéndola en la capacidad de ciberespionaje y de ciberataque. Califica a esta capacidad como imperativa militarmente, aunque políticamente delicada. De nuevo, el dilema de*

*quién ha de ser la autoridad de control o competencia aparece también como crítico.*

*Finalmente, en la tercera parte de su contribución, el autor reflexiona sobre varias propuestas de organización de las fuerzas de la ciberdefensa en el entorno español.*

*Comienza apelando, en visión retrospectiva, a la evolución de la organización de los medios aéreos en la historia reciente de los conflictos armados. En muchos países a esos medios se les dio la entidad de cuerpo, con la denominación de Cuerpos Aéreos. Luego, se fueron creando fuerzas aéreas independientes con entidad de Ejército, equivalentes a sus homólogos de tierra y mar. De alguna manera, reflexiona, la situación en el ciberespacio es idéntica: es un nuevo escenario que requiere el empleo de nuevas fuerzas, es decir, una cuarta nueva rama militar.*

*López de Turiso y Sánchez reflexiona sobre la entidad de esa nueva rama: parece arriesgado (dice) crear directamente un nuevo ejército; dice que sería lo ideal, pero poco realista. Volviendo a la historia de la fuerza aérea, propone la creación de una fuerza con entidad de cuerpo: el cuerpo de la ciberdefensa. El cuerpo tendría que ser un cuerpo conjunto, porque no cabría ni triplicarlo en cada uno de los tres Ejércitos actuales, ni asignarlo a uno de ellos en exclusiva.*

*Luego se revisan las ventajas de la formación de un cuerpo (independiente) de la ciberdefensa, que resumidamente, se concretarían en los siguientes conceptos: especialización, dedicación, formación, economía, doctrina, organización, operación e imagen. Incluyo un resumen, a continuación, de las cinco primeras:*

1. *La especialización: ésta en ciberdefensa incluiría los conocimientos en técnicas defensivas necesarias para asegurar la confidencialidad, integridad y disponibilidad de los sistemas, así como garantizar la autenticidad de los usuarios y la trazabilidad de sus acciones. Igualmente requeriría conocimientos de técnicas ofensivas, análisis y explotación de vulnerabilidades, penetración en sistemas, descifrado, codificación de* exploits *y aprendizaje de técnicas* stealth*, de evasión y de borrado de huellas, etc.*
2. *La dedicación: una de las grandes ventajas de la creación de un cuerpo de la ciberdefensa sería su dedicación exclusiva. Su personal, a lo largo de toda su trayectoria militar se dedicaría en exclusiva al combate en este entorno. En un cuerpo de la ciberdefensa, su personal*

*especializado se dedicaría a este cometido permanentemente, ya sea sirviendo al Órgano Central, al Conjunto o a cada uno de los Ejércitos.*

3. *La formación: una formación que no esté unificada y que no tenga carácter conjunto, implicaría triplicar los gastos, los esfuerzos y los medios necesarios. La formación única permitiría que todos sus componentes hablasen un lenguaje común y dispusiesen de unos conocimientos homogéneos en todos los campos.*
4. *La economía: en caso de no establecer una única fuerza conjunta, cada uno de los ejércitos iniciarían sus propios movimientos y crearían sus unidades de ciberdefensa para asegurarse este dominio en apoyo a sus operaciones específicas. Esto implicaría tener que detraer medios humanos, materiales y económicos por triplicado de los ya reducidos recursos que tienen los ejércitos para intentar cubrir una nueva necesidad de una manera que probablemente no satisfaga en su totalidad las expectativas de ninguno de ellos.*
5. *La doctrina: es imprescindible disponer de una doctrina específica, una doctrina ciberespacial, que comprenda sus aspectos básico, operativo, táctico y funcional. Una única doctrina conjunta, redactada para esta finalidad desde su origen, orientará sobre cuál deberá ser el empleo de las fuerzas de la ciberdefensa en las operaciones conjuntas.*

*Finalmente, el capítulo concluye con una propuesta de pasos a dar previos a la posible creación de una fuerza permanente. Entre ellos está la creación de una misión conjunta permanente, que bajo la autoridad del Jefe del Estado Mayor de la Defensa (JEMAD), con un carácter permanente, como el que tienen otras misiones específicas permanentes, y con capacidades ofensivas y defensivas, protegería las redes de las Fuerzas Armadas y colaboraría en otras protecciones, si se le encomendase.*

*Esta misión conjunta evolucionaría, a medida que los recursos necesarios lo fueran demandando, hacia la formación de un centro de la ciberdefensa, encuadrado en la misma estructura del Estado Mayor de la Defensa.*

*Finalmente, la evolución podría acabar en la creación de un cuerpo común de la ciberdefensa, independiente de los ejércitos, con entidad propia y autonomía organizativa.*

*Ángel Gómez de Ágreda divide el que es capítulo cuarto de esta* Monografía *en tres temas principales: el ciberespacio desde el punto de vista general, las amenazas en el ciberespacio y las amenazas también desde el ciberespacio.*

*Comienza recordando como posible definición general (que no única) de ciberespacio una del Departamento de Defensa de Estados Unidos que lo definió como:*

> *«Un dominio global dentro del entorno de la información, compuesto por una infraestructura de redes de tecnologías de la información interdependientes, que incluye Internet, las redes de telecomunicaciones, los sistemas de información y los controladores y procesadores integrados junto con sus usuarios y operadores.»*

*Recuerda luego, al igual que otros autores de esta* Monografía*, que el ciberespacio ha sido identificado como uno de los* Global Commons*, cuya singularidad con respecto a los otros tradicionales (físicos) es su naturaleza artificial. Después, introduce las categorías de vulnerabilidades, basándose en una estructura jerárquica del ciberespacio, la de Libicki, que lo organiza en las capas física, sintáctica y semántica. A éstas añade, para explicar el conjunto de las vulnerabilidades, la del componente humano, como probablemente la más débil, como parecen demostrar, o al menos ilustrar, algunos recientes ejemplos de ataques (sabotajes o robos de datos) que han aprovechado precisamente la colaboración (involuntaria o confiada) de usuarios autorizados.*

*Luego, tras recordar que los ataques pueden producirse a las redes informáticas, pero también a los sistemas cibernéticos que controlan determinados procesos industriales y financieros, y en general a los servicios e infraestructuras críticos de un país (tema al que volverá después en el capítulo), Gómez de Ágreda se centra en poner en relación el ciberespacio con el fenómeno (mal comprendido aún) de la globalización, escribe:*

> *«La globalización, entendida en su forma moderna, necesita del ciberespacio porque se basa en su estructura y capacidades para su propia existencia. La descentralización que caracteriza desde su inicio al diseño cibernético influye y condiciona la vida en el mundo real. De este modo, las instituciones que surgieron en las postrimerías de la Segunda Guerra Mundial para garantizar una gobernanza mundial tutelada por las potencias vencedoras y que imponían un modelo centralizado alrededor de Naciones Unidas y del dólar como moneda de referencia (primero basándose en el patrón oro y después por sí mismo) se muestran poco eficientes en estos días en la gestión del mundo global.»*

*La idea que subyace tras esta reflexión quizás sea la cada vez más limitada vigencia del modelo westfaliano del Estado como protagonista único de la vida política internacional, en evolución hacia otro modelo en el que:*

> *«Empiezan a intervenir jugadores no estatales que pretenden suponer un reto al mantenimiento del monopolio estatal en el uso de la fuerza», sigue el autor, citando a Sánchez Medero. En ese contexto, claramente, «Internet y el ciberespacio son intrusos que propician un reequilibrio de fuerzas.»*

*Para terminar la sección general, se revisa, como hiciera Carlos Enríquez González en el capítulo segundo, la disparidad entre los criterios de mayor control de la Red (para proteger determinados derechos sobre la información) frente a mejores mecanismos de autorregulación (para proteger otros derechos del ciudadano).*

*La segunda gran sección de la contribución se dedica a reflexionar sobre las amenazas «en el ciberespacio». Comienza recordando que la principal actividad criminal en el ciberespacio es la «penetración de sistemas de ordenadores conectados en red con la finalidad de acceder a información sensible» y nos recuerda que todos los días, empresas y organismos oficiales sufren intentos de intrusión. Las actividades de los nuevos «piratas» se han trasladado, desde las lúdicas maliciosas de baja intensidad, a las productivas, orientadas a obtener el acceso a un sistema, con un objetivo económico o político. El autor recuerda al lector los casos documentados de los conflictos de Estonia y Georgia.*

*En la siguiente parte de su contribución, como hiciera brevemente Feliu Ortega en el capítulo primero, se recuerda la insalvable actual dificultad de atribuir la autoría de los ataques, especialmente en tiempos útiles para establecer una (siempre lenta) actuación jurídica. Esta dificultad acaba por garantizar, con frecuencia, la impunidad de los agresores.*

*Tras un breve recuento de algunos instrumentos conocidos y grupos de activistas populares (principalmente centrados en el robo de datos y actuaciones de denegación de servicio), en la subsección de «Ser o no ser en la Red», el autor apela a la responsabilidad de los gobiernos, escribe:*

> *«Los gobiernos tienen que comenzar por admitir su limitado papel en la defensa cibernética. Más del 80% de los sistemas críticos para una nación están en manos privadas y su protección es sólo parcialmente responsabilidad de los gobiernos. El papel supervisor y, fundamentalmente, de formación y de concienciación que tienen los*

*gobiernos con respecto a la ciberseguridad en general es, sin embargo, una de sus más importantes e irrenunciables responsabilidades.»*

*La tercera, y última, sección del capítulo se dedica a las amenazas desde el ciberespacio. Comienza enunciando, usando el símil del combate aéreo, que el objetivo de la pugna en el ciberespacio es la supremacía o la superioridad, así, alcanzada:*

> *«El potencial para influir en el exterior del mismo desde las redes digitales es cuantitativa y cualitativamente incomparable con cualquier otro medio conocido hasta la actualidad.»*

*Más adelante en el capítulo, ese potencial «orientador» de Internet lo relaciona (inevitablemente) con las capacidades tradicionales de los medios de comunicación y con las operaciones militares de información y psicológicas. Reconoce que, por desgracia:*

> *«El terreno es igualmente fértil para cualquier otro actor que pretenda desarrollar este tipo de actuaciones; incluso para aquellos para los que estas actividades estaban vedadas o muy limitadas en función de sus recursos.»*

*Para terminar, revisa someramente los efectos de las amenazas sobre la economía, sobre las percepciones y sobre las infraestructuras.*

*En relación con la primera, la economía, escribe:*

> *«Las redes en las que se llevan a cabo los negocios bursátiles, financieros o bancarios son infraestructuras críticas que necesitan ser convenientemente protegidas.»*

*La responsabilidad directa de su gestión y de su defensa está, desde luego, en manos privadas en la mayor parte de los casos pero los efectos de las intrusiones en las mismas son materia, sin lugar a dudas, de Seguridad Nacional al mismo nivel que los sistemas de generación y distribución energética y los de control del tráfico aéreo.*

*Las implicaciones para el mundo económico y financiero no terminan, sin embargo, en los parqués ni siquiera en el ámbito de lo legal. Internet ofrece un sinfín de posibilidades para facilitar la financiación de grupos terroristas a través de transacciones de una elevada opacidad. En ellas influye también la connivencia de actores estatales permisivos –incluso cómplices– de estos grupos y organizaciones que, con su menguada vigilancia o su deliberado volver la vista hacia otro lado, facilitan el aporte de fondos a los terroristas.*

*En relación con la influencia sobre las percepciones, escribe, en relación (a modo de ejemplo) al conflicto entre Rusia y Georgia en el año 2008:*

> *«El mayor perjuicio… fue la incapacidad para hacer sentir su punto de vista en el mundo y para recibir el* feedback *de lo que sucedía en el exterior respecto de los acontecimientos que estaban teniendo lugar. Mayor incluso que el problema que pueda generar en cuanto al establecimiento y mantenimiento del mando y control sobre las unidades y los sistemas mismos es el que supone la desconexión con la opinión pública propia, enemiga o neutral.»*

*Finalmente en la subsección de los efectos sobre las infraestructuras, recordando el conocido «caso de Stuxnet» sobre las infraestructuras nucleares de Irán, el autor sugiere que será ya posible pensar en que la utilización de conceptos similares podrá afectar a infraestructuras o servicios críticos de cualquier país, empresa o particular; será una posibilidad en cualquier escenario; tanto como ataque singularizado y puntual como formando parte de una agresión general.*

*El capítulo quinto es debido a Óscar Pastor Acosta y se centra en las capacidades para una defensa eficaz del ciberespacio, lo que podríamos denominar «Capacidades para la Defensa en el ciberespacio». Comienza por hacer, en la sección primera, una revisión semántica y conceptual de algunos términos relacionados con la ciberdefensa, términos que a veces, comprensiblemente, se usan como sinónimos sin serlo perfectamente. Entre otros, revisa algunas de las acepciones comunes de los términos sajones:* information assurance, infosec y cyberdefense*. Hace notar oportunamente que la OTAN no define como tal:*

> *«El concepto de* cyber security *o ciberseguridad, pero es muy frecuente su uso por parte de las naciones aliadas, algunas veces como sinónimo de ciberdefensa, pero más comúnmente, como nuevo término, para referirse a la seguridad de la información en las TIC, es decir, a* infosec o STIC*.»*

*Cierra Pastor Acosta esta primera sección del capítulo aproximándose al concepto de capacidades, que es lo que importa primordialmente a los efectos de su objetivo temático. Citando a García Sieiro, enuncia que, en términos militares, capacidad es el:*

> *«Conjunto de factores (sistemas de armas, infraestructura, personal y medios de apoyo logístico) asentados sobre la base de unos principios y procedimientos doctrinales que pretenden conseguir*

*un determinado efecto militar a nivel estratégico, operacional o táctico, para cumplir las misiones asignadas.»*

*Por ello concluye que:*

> *«La Capacidad de Ciberdefensa sería el conjunto de sistemas, infraestructuras, personas, medios de apoyo y procedimientos doctrinales, que permiten cumplir con la misión de defender también el ciberespacio.»*

*La segunda sección de su capítulo (la más larga) la dedica a revisar pormenorizadamente las capacidades necesarias para el ciberespacio. Comienza por resumir la visión del JEMAD (sobre ciberdefensa militar) y recordar que, obviamente, está alineada con la de nuestros aliados; en este punto trae a colación la doctrina sobre las Operaciones de Información del Estado Mayor Conjunto de Estados Unidos, que las divide en las de* Computer Network Defense*,* Computer Network Exploitation *y* Computer Network Attack*.*

*Luego, tras recordar algunos aspectos en relación al concepto estratégico para la defensa y seguridad de la OTAN, recuerda que este define:*

> *«La protección de las redes de la OTAN como una responsabilidad fundamental de los aliados, destacando la importancia de cooperar con sus socios y otros organismos internacionales en ciberdefensa, así como la necesidad de integrar las ciberamenazas dentro del proceso de planeamiento de la Alianza.»*

*Posteriormente, nos recuerda la clasificación de las capacidades para la ciberdefensa que este mismo año de 2011 hace la* NATO C-3 Agency*, a instancias del Mando Aliado de Transformación, en su Documento* Multinational Cyber Defence Capability Development Initiative. *La clasificación desglosa las capacidades para la ciberdefensa en seis grandes, que luego detalla:*

1. *Detección de actividad maliciosa.*
2. *Detección, mitigación y terminación de ataques.*
3. *Análisis dinámico de riesgos, ataques y daños.*
4. *Recuperación de ciberataques.*
5. *Toma de decisiones a tiempo.*
6. *Gestión de la información de ciberdefensa.*

*La tercera sección del capítulo se dedica a describir las principales formas de implantación y despliegue de las capacidades enunciadas, que están llevando a cabo naciones y organismos de nuestro entorno. Co-*

*mienza la sección revisando algunos detalles terminológicos en relación a «organismos de respuesta»: CERT, Equipo de Respuesta a Incidentes de Seguridad Informática (CSIRT), Equipo de Respuesta a Incidentes (IRT), Equipo de Respuesta a Incidentes Informáticos (SERT), etc. La OTAN denomina a esa capacidad CIRC de la OTAN o Capacidad de Respuesta ante Incidentes Informáticos de la Alianza (NCIRC). Evidentemente, aparte de las siglas, no todas las capacidades «cibernéticas» que refieren son las mismas, porque responden al servicio, a la comunidad y a la misión. También, en consecuencia, las organizaciones de los equipos y centros son diferentes.*

*Haciendo referencia a un Informe de* Carnegie Mellon University*, el autor estructura los servicios a prestar por estos Centros en: servicios reactivos, proactivos y de gestión de la calidad de la seguridad.*

*El autor concluye que un CIRC esencialmente implementa:*

> *«Las capacidades de Defensa, dentro de la estrategia de ciberdefensa de una nación u organismo internacional, buscando garantizar la prevención, detección, reacción y recuperación frente a ataques, intrusiones, interrupciones u otras acciones hostiles deliberadas, que puedan comprometer la información y los sistemas que la manejan.»*

*La sección tercera de este capítulo se dedica a revisar la traslación del concepto de «Equipo Rojo» al ciberespacio y a su ciberdefensa: es el «Ciberequipo Rojo» una forma de:*

> *«Analizar el modo de pensar del potencial adversario para analizar las fortalezas y debilidades propias, etc. para detectar flaquezas y vulnerabilidades que difícilmente habrían sido alcanzados mediante la inspección tradicional.»*

*Luego, citando a Dandurand, propone estructurar en tres grupos las actividades a realizar por el «Ciberequipo Rojo»:*

1. *Evaluar la eficacia de de las medidas de seguridad, cuyo principal objetivo será el de «evaluar en conjunto la integración de los aspectos técnicos y procedimentales de las medidas de seguridad»,*
2. *Demostrar el impacto del ciberataque en la misión, mostrando el potencial impacto de los ciberataques también en la misión de la organización.*
3. *Mejorar la habilidad de los usuarios y del personal de seguridad para enfrentarse al entorno de crecientes ciberamenazas.*

*La siguiente subsección se dedica al ciberejército, cuyo objeto es el de neutralizar la ciberamenaza implementando los aspectos de explotación y ataque de las capacidades de ciberdefensa.*

*Recuerda que existen numerosas iniciativas para la constitución de ciberejércitos y analiza en detalle el ciberejército norteamericano (cibermando), como aproximación de describir algunas características genéricas de un ciberejército. Resumidamente, el USCYBERCOM será el medio por el que se consiga centralizar el mando de las operaciones en el ciberespacio y se compondrá de cuatro unidades (los cibermandos del Ejército, de la Fuerza Aérea, de la Flota y de Infantería de Marina).*

*Luego, la sección se centra, con más detenimiento, en las capacidades de explotación (especialmente, en la comprensión de la cibersituación) y para la ciberguerra, de las que hace un desglose detallado. El capítulo termina con unas conclusiones a modo de resumen.*

*El último capítulo sexto, por Manuel Pérez Cortés, revisa, desde una perspectiva técnica, la arquitectura y las amenazas y soluciones de seguridad y defensa en el ciberespacio. Se estructura en los siguientes apartados:*

- *Concepción tecnológica del ciberespacio, enfatizando la perspectiva militar y revisando todo ello desde el concepto de interoperabilidad de los sistemas.*
- *Estructura de los ataques en el ciberespacio y descripción de las amenazas desde un punto de vista técnico.*
- *Tecnologías que se utilizan para la prevención de las amenazas.*
- *Tecnologías que se utilizan para la detección de las amenazas, la respuesta y la recuperación.*
- *Herramientas, metodologías y normas disponibles relacionadas con el ámbito de la seguridad en el ciberespacio.*

*El primer apartado, sobre la concepción tecnológica comienza por interpretar el aumento de la complejidad de la infraestructura global por varios aspectos, entre los que menciona:*

- *Su extrapolación a nuevas redes en la que se incluyen otros tipos de dispositivos distintos de los «ordenadores», como teléfonos inteligentes, etc.*
- *La interconexión con las redes de propósito general del ciberespacio de otras redes de propósito específico, como, por ejemplo, los Sistemas de Control Remoto para la supervisión y el mantenimiento de sistemas industriales (Sistemas de Control SCADA, etc.), en algunos*

*casos asociados a infraestructuras críticas de distribución de energía, de telecomunicaciones, etc.*
– *La tendencia creciente a la descentralización de los recursos propios de cálculo y almacenamiento, de manera que también éstos residan de manera compartida en la red* (Cloud Computing).
– *La tendencia creciente a que no sólo las personas, sino también las cosas interactúen a través de la red (internet de las cosas) mediante distintos tipos de dispositivos RFID, con su propia dirección Protocolo de Internet, etc.*

La sección sobre ataques y amenazas revisa interesantes aspectos a considerar sobre las ciberamenazas y describe, ilustrativamente, las distintas etapas que suelen presentarse durante la ejecución de un ataque en el ciberespacio. Menciona el autor las siguientes:

– Recoger datos *en la Red de los objetivos a ser atacados.*
– Escanear sistemáticamente los sistemas*.*
– Ganar el acceso, *identificadas las potenciales vulnerabilidades, el acceso al sistema objeto de ataque, se puede realizar también por diferentes métodos.*
– Aumentar los privilegios, *el aumento de privilegios puede permitir la instalación de puertas traseras, que serán explotadas posteriormente, o la obtención de ficheros de contraseñas y su craqueado en una fase posterior.*
– Explotar los sistemas*.*
– Ciberguerra, *respondería al concepto de un ataque sistemático al más alto nivel, incluyendo ataques de denegación de servicios críticos con el empleo de* botnets*, la mutilación de sitios* web*, el daño a los sistemas, la intrusión en infraestructuras críticas, etc.*
– Denegar el servicio*, la denegación de servicio, que se describe posteriormente con algo más de detalle, es un tipo de ataque que puede no exigir el acceso al sistema a ser atacado.*

*La sección avanza identificando las distintas fuentes de amenaza, sus motivaciones y sus actuaciones típicas.*

*Luego, detalladamente, el autor revisa algunos de los tipos de amenazas en el ciberespacio, desde un punto de vista tecnológico, desde el «abuso de privilegios de acceso» hasta el* phishing*, pasando por hasta 25 elementos.*

*La sección cuarta se dedica a reflexionar sobre las tecnologías para la prevención de amenazas, especialmente:*

1. *Técnicas de análisis y evaluación de riesgos.*
2. *Pruebas de penetración.*
3. *Las medidas de sensibilización y educación.*

*Las primeras, basadas en la identificación-estimación-evaluación de riesgo, tienen el objetivo de analizar dónde, por qué, y cómo pueden surgir los problemas, establecer los objetivos a proteger y el impacto de sus vulnerabilidades, determinar la efectividad de los controles y las consecuencias de la ocurrencia.*

*Las segundas, pruebas de penetración (intrusión) tienen como objetivo poner a prueba los controles que se han implementado para proteger el acceso no autorizado en la Red.*

*Finalmente, las medidas de sensibilización y formación apuntan al, según muchos, el eslabón más débil de la seguridad en los sistemas y redes, que es el factor humano (como ya propusiera Gómez de Ágreda en el capítulo cuarto).*

*La siguiente sección desarrolla los servicios pensados para la detección, respuesta y recuperación de incidentes informáticos. Finalmente, la sección sexta se ocupa de las herramientas, metodologías y normas de aplicación en el ámbito de la seguridad en el ciberespacio: tecnologías de aislamiento en redes, criptografía, detección de intrusiones, protección contra virus y* malware*, ofuscación de la información, y otras tecnologías secundarias, normas y prácticas.*

*El capítulo termina con una sección de conclusiones, que, citando un* White Paper *elaborado por TASC en colaboración con la Universidad de Virginia (mayo de 2011), identifica ocho problemas o retos cuya principal solución está en el desarrollo de soluciones tecnológicas (a diferencia de otros, que requieren principalmente enfoques organizativos, formativos, etc.). Estos ocho problemas son: la atribución de las acciones en el ciberespacio, la monitorización y auditoría de los sistemas, la protección de los datos, la detección eficaz de intrusión, la capacidad de recuperación de los sistemas atacados, la autenticación de* software *y* hardware*, la integración de sistemas de protección basados en tecnologías diferentes y la gestión de los riesgos asociados al* Cloud Computing*.*

*Esta* Monografía*, en su conjunto, no pretende constituir una unidad, ni temática ni doctrinal, ni mucho menos componer un libro para leer página a página, ordenada y secuencialmente. Creemos, sin embargo, que el lector interesado puede encontrar en uno u otro (o en varios) de los*

*capítulos, material sobre una buena parte de los temas básicos de referencia en el ciberespacio, desde los históricos y doctrinales hasta los más genuinamente tecnológicos.*

*Para finalizar, queremos agradecer la confianza depositada en el grupo por parte del CESEDEN y la ayuda prestada por nuestros colaboradores en nuestras respectivas instituciones.*

## CAPÍTULO PRIMERO

# LA CIBERSEGURIDAD Y LA CIBERDEFENSA

# LA CIBERSEGURIDAD Y LA CIBERDEFENSA

Por Luis Feliu Ortega

> «Sé extremadamente sutil hasta el punto de no tener forma. Sé completamente misterioso, hasta el punto de ser silencioso. De este modo podrás dirigir el destino de tus adversarios.»
>
> Sun-Tzu*, El arte de aguerra* hace más de 2000 años

## Conceptos generales

El conflicto armado es inherente a la historia de la humanidad. El ser humano ha tratado siempre de dirimir sus diferencias por medio de la violencia cuando las palabras, las razones y otras acciones han fracasado. Esta violencia la ha ejercido primero, agrediendo sólo con su propio cuerpo, más tarde sirviéndose de otros objetos a los que llamamos armas que se han ido perfeccionando con el tiempo pero siempre con la misma finalidad, la de infligirle un perjuicio de forma tal que se imponga la voluntad propia a la del adversario, el cual se defenderá para tratar de impedir o minimizar este perjuicio y evitar el sometimiento de su voluntad.

Cuando son las colectividades las que se enfrentan así, dan lugar a los conflictos armados que se manifiestan por medio de combates o luchas y que tienen lugar, en principio, en espacios terrestres. Más tarde y al percatarse que desde el mar también es posible imponer esta voluntad surgen los combates navales y las acciones del mar sobre la costa, des-

pués aparecen de forma similar los combates en el aire y en el espacio. Cada vez que aparece una nueva dimensión real o virtual que el ser humano va a utilizar, los contendientes tratarán de dominarlo con objeto de poder emplearlo en su beneficio e impedir o dificultar su uso al adversario. Éste ha sido el caso últimamente del espacio electromagnético o éter y más recientemente aún, del espacio cibernético o ciberespacio que trataremos con más detalle.

Los conflictos armados han ido también evolucionando en la forma de llevarlos a cabo a lo largo de la Historia, constituyendo Ejércitos y Marinas cada vez más numerosos que se enfrentaban por medio de batallas en unos espacios o áreas determinados. Al principio la población civil aunque siempre se veía afectada, no intervenía directamente pero más tarde los conflictos pasaron a ser totales, afectando a toda la población y a todos los espacios. Últimamente los conflictos están revistiendo fundamentalmente la forma de conflictos armados asimétricos en los que un bando mucho más poderoso, en cantidad y calidad tecnológica se tiene que enfrentar a otro netamente inferior pero que es capaz de mantenerlo en jaque, infligirle pérdidas notables y sobre todo impedirle alcanzar su objetivo estratégico, pudiendo llegar también hasta derrotarlo imponiéndole su voluntad.

Se pueden señalar varios hitos que han marcado esta evolución histórica. El primero podría ser la Paz de Westfalia (1648), cuando las naciones firmantes se comprometieron a que los conflictos armados, llamados ya formalmente guerras, sólo deberían tener lugar entre Estados o facciones de un Estado con estructura de tales y mediando normalmente la oportuna declaración de guerra. Otro hito podría ser la firma de los Convenios de Ginebra y La Haya (1899-1907), fuente y principio del Derecho Internacional Público moderno que tratan de reglamentar en cierto modo los usos y costumbres de la guerra, de proteger a la población civil y personal no combatiente así como a los prisioneros de guerra, a los heridos y a los enfermos, lo que se conoce como Derecho Internacional Humanitario y Derecho Internacional del Conflicto Armado.

Otro hito importante lo representa Clausewitz cuando establece que la guerra es la continuación de la política por otros medios. Algo que de hecho ya se producía antes pero que desde ese momento queda perfectamente reconocido. De esta forma confirma también lo que ya dijeran San Agustín y Santo Tomás e incluso nuestro Francisco de Vitoria, cuando distinguían entre guerras justas e injustas. Sin embargo, después

de la Segunda Guerra Mundial, la Carta de Naciones Unidas establece que todos los países firmantes renuncian a la guerra y a la amenaza de la misma para resolver sus diferencias, aunque, aparte del derecho a la legítima defensa, la Organización de Naciones Unidas (ONU) puede autorizar «las medidas necesarias» para garantizar, mantener y también restablecer la paz.

Pero el uso de la violencia no siempre presenta la forma de guerra, declarada o no, sino que como reconocen los protocolos adicionales de los Convenios de Ginebra y La Haya, anteriormente citados, pueden, sin ser guerras, revestir la forma de conflictos armados, frecuentemente asimétricos, que cursan con ataques directos o indirectos y que también afectan a la población civil no combatiente. Finalmente, la violencia, hoy más que nunca, está presente en los conflictos no sólo como violencia física destinada a destruir o neutralizar físicamente las personas, propiedades e instituciones de un Estado con objeto de imponer su voluntad sobre él sino también mediante acciones políticas, económicas, psicológicas, mediáticas, electromagnéticas y actualmente como se verá, cibernéticas (1), siempre con la misma finalidad de imponer la propia voluntad sobre el adversario y forzarle a actuar de forma perjudicial para él.

Todo este tipo de acciones pueden así poner en peligro la seguridad de una sociedad, de una nación, del propio Estado, de su territorio, de sus instituciones, de sus infraestructuras críticas, de sus ciudadanos, de su supervivencia o de su bienestar. Este concepto de seguridad, como se puede observar, ha sufrido una mutación expansiva de su categoría jurídica (2) que desde el concepto clásico de orden público y paz pública, seguridad interior y exterior del Estado, ha ido evolucionando hasta uno más amplio y multidimensional como es el de Seguridad Nacional que se define hoy como «el estado deseado por una sociedad en el que pueda ésta desarrollarse y prosperar libre de amenazas» (3). Entendiendo

---

(1) Por acciones electromagnéticas se entiende aquellas que utilizan la radiación electromagnética en sus diversas formas y frecuencias mientras por acciones cibernéticas se debe entender aquellas que utilizan ordenadores en los sistemas informáticos.

(2) González Cussac, José Luis: *Cuaderno de Estrategia,* número 149, Instituto Español de Estudios Estratégicos (IEEE).

(3) En este estudio hemos preferido por su claridad el utilizar las definiciones que se contienen en la Doctrina del Ejército de Tierra (DO1-001) del año 2003, que establece: «La seguridad se define como el estado deseado por una sociedad, en el que pueda desarrollarse y prosperar libre de amenazas». «La defensa es la adopción práctica de medidas conducentes a mantener la seguridad deseada». Otra definición muy exten-

por amenaza la percepción de la capacidad que un potencial adversario posee para infligirnos un daño o perjuicio, especialmente si no se actúa como él desea. Si bien se suele emplear el término amenaza como sinónimo de riesgo (4) no deben confundirse ambos, puesto que riesgo debería entenderse como estimación del grado de exposición a que una amenaza se materialice a través de vulnerabilidades, sobre uno o más activos propios causando daños o perjuicios en los mismos (5).

Los medios e instituciones de que dispone el Estado para garantizar la Seguridad Nacional de la que es responsable son muy variados y van desde los más livianos, como pueden ser la justicia, la diplomacia o la política económica, hasta los más duros que suponen el uso de la fuerza en sus distintas formas. Estos últimos son los que se engloban tradicionalmente en el concepto de Defensa que en realidad debería llamarse mejor Defensa Militar puesto que Defensa Nacional, en pura lógica, debería comprender todos los medios y acciones, civiles y militares, tendentes a conseguir o garantizar la Seguridad Nacional. Algunos países definen y diferencian perfectamente la Defensa Militar de la Defensa Civil, que no hay que confundirla con la Protección Civil, de la que es sólo una parte. En España, estos conceptos, aunque se intuyen, no están bien definidos y es frecuente mezclarlos e incluso confundir lo que son los objetivos o finalidad a lograr o preservar (la seguridad) con las medidas e instrumentos para lograrla (la defensa) (6), empleando erróneamente se-

---

dida es la de Arnold Wolfers (1952) ampliada por Charles-Philippe David más recientemente: «La seguridad se manifiesta por la ausencia, tanto de amenazas militares, como no militares que pueden introducir el cuestionamiento de los valores centrales que quiere promover o preservar una persona, una comunidad y que suponen un riesgo de utilizar la fuerza».

(4) Aunque, por supuesto supone una falta de precisión, tenemos que admitir que muchos autores, en diversas publicaciones, consideran como sinónimos seguridad y defensa así como amenaza y riesgo o simplemente los asocian sin matizar sus diferencias. En esta *Monografía*, trataremos de utilizarlos con lo que se considera su correcta acepción y no sólo en general sino también cuando se les añade el prefijo ciber, es decir ciberseguridad, ciberdefensa, ciberamenaza y ciberriesgo.

(5) «Seguridad Nacional y ciberdefensa», *Cuadernos Cátedra,* número 6, nota 2, Ingeniería del Sistema de Defensa en España, S. A.-Universidad Complutense de Madrid. A este respecto es interesante también incluir las definiciones que contiene la Estrategia Española de Seguridad (EES): «A los fines de esta Estrategia una amenaza es toda circunstancia o agente que ponga en peligro la seguridad o estabilidad de España. El riesgo es la contingencia o probabilidad de que una amenaza se materialice produciendo un daño».

(6) A estos efectos preferimos la definición de Defensa Nacional que utilizaba la ya derogada Ley Orgánica 6/1980 de Criterios Básicos de la Defensa y la Organización Militar

guridad y defensa como si fuera un concepto único o como si la Defensa fuera sólo la Defensa Militar del territorio y la seguridad todo lo demás. Tampoco parece correcto interpretar por lo tanto que la Defensa (Militar) se refiere sólo a la defensa frente ataques militares o frente a ataques a los sistemas militares (7).

La Defensa se basa fundamentalmente en la disuasión, es decir, en la capacidad de respuesta de forma que el potencial atacante renuncie a materializar su amenaza por los perjuicios que a cambio puede recibir; en la protección, es decir en la capacidad de resistencia a los ataques de forma que los hagan infructuosos o que se minimicen sus efectos y en la prevención o previsión, de forma que se posea libertad de acción para poder tomar las medidas y ejecutar las acciones de protección y en su caso de respuesta en el momento y modo adecuados. En todas ellas pero especialmente en la previsión, juega un papel decisivo la inteligencia sobre las amenazas y los riesgos a que nuestra seguridad está expuesta.

La Seguridad Nacional debe garantizarse pues en todos y desde todos los distintos ámbitos o espacios estratégicos que cada país tiende a dominar o controlar para desde ellos o apoyados en ellos establecer su defensa o conseguir y mantener sus objetivos y donde por lo tanto pueden tener lugar las confrontaciones o conflictos, con otros adversarios cuyos objetivos sean incompatibles con los propios o por el contrario se materialicen acuerdos de cooperación con otros países.

Los Estados y este es el caso de España con la Organización del Tratado del Atlántico Norte (OTAN), no suelen preparar la Defensa de su Seguridad de forma aislada sino que suelen formar parte de organizaciones multinacionales de defensa colectiva. Además suelen estar vinculados mediante tratados bilaterales o multilaterales que en nuestro caso los principales son los que nos ligan con la Unión Europea, la Organización para la Seguridad y Cooperación en Europa y la ONU. Como consecuen-

---

en su artículo 2: «Disposición, integración y acción coordinada de todas las energías y fuerzas morales y materiales de la Nación ante cualquier forma de agresión»… «Tiene por finalidad garantizar de modo permanente la unidad, soberanía e independencia de España, su integridad territorial y el ordenamiento constitucional, protegiendo la vida de la población y los intereses de la Patria, en el marco de lo dispuesto en el artículo 97 de la Constitución». Como puede verse, no la limita sólo a la Defensa Militar.

(7) Como los términos seguridad y defensa van normalmente unidos en muchos documentos y artículos (*véase* nota 4) se tiende a considerarlos sinónimos.

cia de todo ello, la Defensa debe preverse teniendo en cuenta no sólo la Seguridad Nacional sino también la de nuestros aliados.

Hoy en día las amenazas a la seguridad no provienen sola y directamente de otros Estados ni de una facción del propio Estado sino además y principalmente de organizaciones internacionales o transnacionales de crimen organizado, piratería y terrorismo, basadas o provenientes en muchos casos, de Estados inviables que no ejercen el debido control sobre su propio territorio y población o de «Estados canallas» (8) que las utilizan en su propio beneficio. Esto sin contar las catástrofes naturales y los grupos más o menos organizados de personal descontento que existen en todos los países. Amenazas que pueden materializarse en todos o algunos de los espacios estratégicos.

Los Estados organizan la defensa de la seguridad mediante el establecimiento de una Estrategia Nacional de Seguridad. De acuerdo con las amenazas y los consiguientes riesgos se planean y definen unas estrategias de defensa desde los diferentes espacios estratégicos que dan lugar a las distintas facetas de la Defensa como son la defensa territorial, la defensa aérea, la defensa de las fronteras, la defensa económica y como uno de estos espacios es precisamente el espacio de la cibernética o ciberespacio también hoy deberá existir una ciberdefensa que garantice la ciberseguridad (9).

Se conoce con el nombre de ciberespacio al espacio artificial creado por, el conjunto de CIS (10) es decir de redes de ordenadores y de telecomunicaciones interconectados directa o indirectamente a nivel mundial (11). El ciberespacio es sin embargo, mucho más que Internet,

---

(8) Traducción libre del termino inglés *rogue states.*

(9) La OTAN en su MC0571 *(NATO Cyber Defence)* la define como «la aplicación de medidas de seguridad para proteger las infraestructuras de los sistemas de información y comunicaciones frente a los ciberataques».

(10) *Communications and Information Systems*, Sistemas de Información y Telecomunicaciones que utilizan las TIC o Tecnologías de la Información (informática) y las Comunicaciones (telecomunicaciones).

(11) Resulta difícil encontrar una definición clara de ciberespacio pues depende del punto de vista que se considere y del estado de la tecnología. No existe un consenso claro sobre qué es el ciberespacio por no decir de las implicaciones de los conflictos en el espacio. El *Diccionario de Real Academia Española de la Lengua* define al ciberespacio como «ambito artificial creado por medios informáticos». No sólo es pues Internet. Según Fojón, Enrique y Sanz, Ángel: *ARI*, número 101/210, Análisis del Real Instituto Elcano, ciberespacio es el conjunto de medios físicos y lógicos que conforman las

más que los mismos sistemas y equipos, el *hardware* y el *software* e incluso que los propios usuarios, es un nuevo espacio, con sus propias leyes físicas que, a diferencia de los demás espacios, ha sido creado por el hombre para su servicio.

Cuanto más desarrollado sea un país más elementos vulnerables que afecten a su seguridad poseerá y que por lo tanto deberá defender para garantizarla. A este respecto, los Sistemas de Mando y Control son cada vez más dependientes no sólo del espacio electromagnético sino también del ciberespacio y esto no sólo en el ámbito militar sino también en el de las infraestructuras críticas nacionales, tanto estatales como privadas y en el de los propios ciudadanos personalmente.

La ciberseguridad es un componente muy importante de la Seguridad Nacional: si no se controla adecuadamente el ciberespacio, desde allí puede ver una nación amenazada su libertad de acción y su seguridad, no sólo su ciberseguridad sino toda la Seguridad Nacional. El ciberespacio es pues un espacio estratégico a considerar al establecer la Estrategia de Seguridad y como consecuencia, al planear la correspondiente Defensa Nacional por lo que habrá que definir en ella los objetivos a alcanzar y las medidas de prevención, disuasión, protección y reacción de la ciberdefensa.

---

infraestructuras de los CIS. Otra posible definición de ciberespacio es «un ámbito caracterizado por el uso de la electrónica y el espacio electromagnético para almacenar, modificar e intercambiar datos a través de los sistemas en red y la infraestructura fisica asociada». En el Glosario de Términos Informáticos, *Whatis* se dice: «El ciberespacio se puede considerar como la interconexión de los seres humanos a través de los ordenadores y las telecomunicaciones, sin tener en cuenta la dimensión física». La EES más explícita y lo define como «El espacio virtual donde se agrupan y relacionan usuarios, líneas de comunicación, páginas *web,* foros, servicios de Internet y otras redes. Creado por el ser humano, es un entorno singular para la seguridad, sin fronteras geográficas, anónimo, asimétrico, que puede ser utilizado de forma casi clandestina y sin necesidad de desplazamientos Es mucho más que la Red, pues incluye también dispositivos como los teléfonos móviles, la televisión terrestre y las comunicaciones por satélite». El Estado Mayor de la Defensa (EMAD) en su «Concepto de Ciberdefensa Militar» lo define como: «Un dominio global y dinámico dentro del entorno de la información, compuesto por una infraestructura de redes, de tecnologías de información y telecomunicaciones interdependientes –que incluye Internet– los sistemas de información y los controladores y procesadores integrados, junto con sus usuarios y operadores». Es de notar que incluye a usuarios y operadores, en realidad redundante pues los sistemas, por definición ya los incluyen. La definición que se ha incluido en el texto de este trabajo está tomada de la publicación citada en la nota 2.

Para ello y teniendo presente que los principios generales de la Defensa son totalmente aplicables al caso de la ciberdefensa debe tenerse en cuenta también que el espacio cibernético, que se ha convertido en un nuevo *Global Common* (12), posee una serie de características diferenciales del resto de los espacios:

– El ciberespacio es un ambiente único, sin fronteras geográficas. El atacante puede estar en cualquier parte del globo y es difícil localizarlo.
– La Defensa es muy compleja pues intervienen muchos factores. Entre otros hay que considerar que intervienen no sólo elementos estatales sino también privados. Exige pues una estrecha coordinación entre todos ellos.
– La confrontación en el ciberespacio presenta frecuentemente las características de un conflicto asimétrico (13). El atacante puede ser muy inferior al atacado en medios técnicos y con relativamente pocos medios y baratos puede causar tremendos perjuicios. Además es frecuentemente anónimo y clandestino. Así pues, atrae, no sólo a los gobiernos sino también a otros diferentes actores que incluyen los terroristas (14) y las mafias del crimen organizado.
– El ciberespacio no debe considerarse aisladamente a efectos de la Defensa puesto que está interrelacionado estrechamente con los demás espacios.

---

(12) Se conocen como *Global Commons,* aquellos entornos en los que ninguna persona o Estado puede tener su propiedad o control exclusivo y que son básicos para la vida. Un *Global Common* contiene un potencial infinito en lo referente al conocimiento y avance de la biología y la sociedad. Incluye los mares, el aire, el espacio y el ciberespacio, en: *www.twq.com/10july/docs/10jul_Denmark.pdf*. Denmark, Abaham M.: *Managing the global Commons*

(13) Se llama combate asimétrico el que tiene lugar entre dos fuerzas muy diferentes en cuanto a su nivel tecnológico y por lo tanto en su equipo y material. Nuestra Doctrina DO1-001 define el conflicto armado asimétrico como: «Aquel que se produce entre varios contendientes de capacidades militares normalmente distintas y con diferencias sustanciales en su modelo estratégico. Alguno de ellos tratará de vencer utilizando el recurso militar de forma abierta en un espacio de tiempo y lugar determinados y ateniéndose a las restricciones legales y éticas tradicionales. Su oponente u oponentes tratarán de desgastar, debilitar y obtener ventajas actuando de forma no convencional mediante éxitos puntuales de gran transcendencia en la opinión pública, agotamiento de su adversario por prolongación del conflicto, recurso a métodos alejados de las leyes y usos de la guerra o empleo de armas de destrucción masiva. Todo ello con el objetivo principal de influir en la opinión pública y en las decisiones políticas del adversario».

(14) Artículo «Countering the art of information warfare», *Jane's Defence Weekly* de Peter Brookes ex vicesecretario adjunto de Defensa, 2 de octubre de 2007.

– La utilización del ciberespacio permite obtener información sobre objetivos sin necesidad de destruir ni neutralizar ningún sistema y a menudo sin delatarse. Una de sus facetas es el espionaje militar, político o industrial.
– Permite fácilmente también el ejercer el chantaje pero al mismo tiempo, la defensa puede utilizar el ciberespacio para la disuasión.
– Evoluciona rápidamente siguiendo la evolución tecnológica de las TIC (15).

Considerando el ciberespacio como un espacio o una colección de recursos, los actores implicados que incluyen Estados, organizaciones, grupos o individuos, competirán por controlarlo y esto conducirá inevitablemente a conflictos. Así aparece el ciberconflicto (16) como una confrontación entre dos o más partes en que al menos una utiliza los ciberataques contra el otro. La naturaleza del conflicto diferirá según la naturaleza y objetivos de los participantes: los delincuentes buscarán ingresos ilegales, los Servicios de Inteligencia buscarán información, los militares atacarán los CIS enemigos como una forma de debilitar la capacidad del adversario y de apoyar las operaciones propias. Los conflictos pueden ser tan simples como meras disputas por la propiedad de una información o de un dominio o tan complejos como operaciones deliberadas de ciberataques entre Estados tecnológicamente avanzados, aisladamente o como parte de una guerra convencional.

Aunque confunde también la ciberdefensa con la ciberseguridad (17), es interesante incluir aquí lo que la Unión Internacional de Telecomunicaciones (UIT) dice sobre el ciberespacio, al que define como:

> «El lugar creado a través de la interconexión de sistemas de ordenador mediante Internet.»

Define también conceptos como ciberentorno y ciberseguridad (18). El ciberentorno incluye a usuarios, redes, dispositivos, todo el software, procesos información almacenada o que circula, aplicaciones, servicios

(15) Tecnologías de la Información y las Comunicaciones
(16) Caro Bejarano, María José: «Alcance y ámbito de la seguridad nacional en el ciberespacio», *Cuaderno de Estrategia,* número 149, IEEE, febrero de 2011.
(17) *Véase* nota 3.
(18) UIT, Rec UIT-T X.1205. Sector de Normalización de las Telecomunicaciones de la UIT (04/2008). Serie X: Redes de Datos, Comunicaciones de Sistemas Abiertos y Seguridad. Seguridad en el ciberespacio-ciberseguridad. Aspectos generales de la ciberseguridad, abril de 2008.

y sistemas que están conectados directa o indirectamente a las redes. La ciberseguridad es definida como:

> «El conjunto de herramientas, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de gestión de riesgos, acciones, formación, prácticas idóneas, seguros y tecnologías que pueden utilizarse para proteger los activos de la organización y los usuarios en el ciberentorno. Los activos de la organización y los usuarios son los dispositivos informáticos conectados, los usuarios los servicios-aplicaciones, los sistemas de comunicaciones, las comunicaciones multimedios y la totalidad de la información transmitida y/o almacenada en el ciberentorno. La ciberseguridad garantiza que se alcancen y mantengan las propiedades de seguridad de los activos de la organización y los usuarios contra los riesgos de seguridad correspondientes en el ciberentorno. Las propiedades de seguridad incluyen una o más de las siguientes: disponibilidad, integridad, la autenticidad y el no repudio y la confidencialidad.»

De igual forma que en las telecomunicaciones se diferencia lo que es la *infosec*, es decir la seguridad de la información que se transmite, de la *transec* que es la seguridad de la transmisión, la ciberseguridad debe entenderse también que comprende no sólo la confidencialidad de la información que circula *(information security)* sino también la seguridad de los sistemas *(information assurance)*, es decir, de la integridad, disponibilidad, autenticidad y no repudio (trazabilidad) de la información. La seguridad del sistema se consigue cuando éste se encuentra en un estado de riesgo conocido y controlado. Realmente, ambos enfoques, *information security* e *information assurance*, son diferentes pero complementarios, y con mucha frecuencia son utilizados indistintamente de manera errónea. Resumiendo, la ciberseguridad debe formularse proactivamente como un proceso continuo de análisis y gestión de los riesgos asociados (19) al ciberespacio (20).

Es frecuente referirse a los distintos espacios en que tiene lugar la guerra y en los que consecuentemente tienen lugar ataques, explotación y de-

---

(19) Fojón, Enrique y Sanz, Ángel: *ARI*, número 101/210, Análisis del Real Instituto Elcano.

(20) La ciberseguridad consiste en la aplicación de un proceso de análisis y gestión de los riesgos relacionados con el uso, procesamiento, almacenamiento y transmisión de información o datos y los sistemas y procesos usados basándose en los estándares internacionalmente aceptados. *Cuaderno de Estrategia,* número 149, IEEE. Vuelve a confundir ciberseguridad con ciberdefensa y riesgo con amenaza.

fensa, como «guerras» (21) y así aparecen conceptos como guerra naval, guerra aérea, guerra económica, guerra psicológica, cuando quizás mejor se debería decir guerra en la mar, en el aire y así aparece de igual modo en algunos tratadistas el concepto de ciberguerra. Lo que sí es cierto es que las confrontaciones y conflictos que tienen lugar en el ciberespacio pueden no ocurrir necesariamente en el contexto de una guerra, ni siquiera en una confrontación general. Este fue el caso de Estonia donde se produjeron una serie de ciberataques sin que hubiera confrontaciones en otros espacios. Por ello el término ciberguerra es algo más descriptivo y representa la lucha entre dos Estados o facciones de los mismos que tiene lugar en el espacio cibernético o ciberespacio. De igual modo, no se incluyen o no deberían incluirse en la ciberguerra los ciberataques procedentes de individuos u organizaciones con fines de extorsión, estafa o chantaje a ciudadanos u organizaciones privadas. Otros autores describen el concepto de ciberguerrra dentro del ciberespacio como el quinto dominio de la guerra junto a la tierra, el mar, el aire y el espacio (22) y establecen que la expansión de la tecnología digital tiene sus riesgos al exponer a los ejércitos y a la sociedad a los ciberataques o ataques digitales.

La Estrategia de Seguridad Nacional debe definir la forma de proteger el territorio, las infraestructuras críticas y a los propios ciudadanos. Todos los países en mayor o menor medida han desarrollado sus nuevas Estrategias de Seguridad Nacional de acuerdo con las nuevas amenazas y consecuentemente establecido sus planes de Defensa tanto a nivel civil como militar. En ellas ocupa un lugar importante la ciberdefensa que comprende pues todas las acciones y medidas necesarias para garantizar la ciberseguridad es decir la seguridad de todos los CIS tanto militares como civiles y tanto públicos como privados (23). Allí se precisan

(21) Aparte de que los términos anglosajones no son siempre tan precisos como los de las lenguas de origen latino, en castellano no existen como en inglés dos términos tales como *war* y *warfare* y traducimos ambos normalmente como «guerra» cuando algunos autores traducen el segundo como «lucha».

(22) *Revista The Economist,* volumen 396, editorial y *dossier*, julio de 2010.

(23) Es interesante resaltar que el error ya citado de confundir seguridad con defensa no se da en el «Concepto de Ciberdefensa del JEMAD» ya que en él define claramente a la ciberdefensa militar como «conjunto de recursos, actividades, tácticas técnicas y procedimientos para preservar la seguridad de los Sistemas de Mando y Control propios y la información que manejan, así como permitir la explotación y respuesta sobre los sistemas adversarios, para garantizar el libre acceso al ciberespacio de interés militar y permitir el desarrollo eficaz de las operaciones militares y el uso eficiente de los recursos».

los objetivos estratégicos a alcanzar, los órganos competentes y sus responsabilidades, la contribución de las instituciones del país, el nivel tecnológico a alcanzar y en él, los objetivos de Investigación y Desarrollo (I+D). Este es el caso de Estados Unidos, en menor grado el del Reino Unido, que lo ha desarrollado ya a nivel militar y el de Francia que acaba de crear su Agencia de Seguridad de los Sistemas de Información. Corea del Sur e Israel también están desarrollando y perfeccionando su ciberdefensa mientras otros países como: Rusia, China, Irán, Pakistán y Corea del Norte han reconocido su interés estratégico en el ciberespacio (24). Asimismo la OTAN también está a la cabeza y está desarrollando sus planes creando organismos y definiendo responsabilidades y la Unión Europea ha establecido ya las normas para la protección de las infraestructuras críticas y el nivel de seguridad de los CIS. En concreto todos coinciden más o menos en que:

– Se deben definir claramente las amenazas y los riesgos existentes para la ciberseguridad y como consecuencia de ellos, los objetivos a alcanzar, las medidas a tomar y las acciones a ejecutar. En consecuencia se deben incluir los esfuerzos para formación y adiestramiento del personal implicado y las actividades en el campo de I+D para alcanzar el adecuado nivel tecnológico.
– La ciberseguridad y por lo tanto la ciberdefensa deben enfocarse de forma que integren a las distintas agencias de seguridad e inteligencia del Estado, los centros de investigación tanto públicos como privados y que coordine con el sector privado y los propios ciudadanos. El impacto de una amenaza en el ciberespacio tiene implicaciones sociales y económicas en el país que la sufre.
– A nivel internacional, la ciberdefensa debe incluirse también en las estrategias de defensa colectiva.
– La protección debe incluir: la de las infraestructuras críticas, incluidos los CIS, la protección de los ciudadanos y la protección del territorio nacional y sus instituciones.
– Debe incluir la prevision, prevención, disuasión, protección y reacción. No debe limitarse a acciones puramente defensivas o pasivas sino que deben preverse capacidades ofensivas en el ciberespacio o incluso en otros espacios de forma que disuadan de nuevos ataques.
– Debe ser multidisciplinar o multidimensional, es decir que debe contemplar los aspectos legislativos, los ejecutivos con los organismos

(24) Fojón, Enrique y Sanz, Ángel: *opus citada.*

encargados de vigilar su cumplimiento y los judiciales. Deberán involucrarse fundamentalmente los Ministerios de Defensa, Interior, Justicia e Industria (I+D) debidamente coordinados.

Como puede verse, los conceptos de seguridad y defensa se han ampliado últimamente como consecuencia de la aparición de nuevas vulnerabilidades, entre ellas la dependencia creciente de las tecnologías TIC y con ello las consiguientes amenazas y el incremento del riesgo. Hoy en día es prácticamente imposible realizar casi ninguna actividad sin este tipo de tecnologías y tampoco es posible ya funcionar con sistemas de información cerrados y aislados.

De la misma forma que la ciberseguridad está incluida en la Estrategia de Seguridad Nacional, la ciberdefensa no debe ser tampoco una actividad aislada sino que debe estar incluida en la Defensa Nacional y por lo tanto en la Defensa Militar, en la Defensa Civil, en la protección de las infraestructuras críticas y en la lucha contra las organizaciones criminales y terroristas.

Los logros de la ciberdelincuencia y el ciberespionaje, contra los que la ley y la contrainteligencia han encontrado poca respuesta, indican que es sólo cuestión de tiempo el enfrentarse a ciberataques serios contra las Infraestructuras Críticas (IC) (25).

En la seguridad de las IC, la estrategia de la Defensa debe comprender siempre la prevención de posibles ataques, la protección para disminuir la vulnerabilidad y en caso de crisis minimizar los daños y acelerar el periodo de recuperación. Las amenazas enemigas a las IC siempre han existido en tiempos de guerra o conflicto, pero los escenarios de amenazas incluyen ahora también ataques en tiempos de paz por medio ciberataques. Los sucesos actuales, incluyendo los ejemplos de Israel y Estonia, demuestran que se puede alcanzar cierto nivel de disturbio real sólo con paquetes de datos hostiles: los bancos se quedaron sin conexión, los medios de comunicación se silenciaron, se bloqueó el comercio digital y se amenazó la conectividad gubernamental con sus ciudadanos. Véase también el último caso padecido por Irán durante el verano de 2010 (26).

---

(25) Caro Bejarano, Marías José: *obra citada,* nota 16.

(26) *El País:* «Alarma por un virus pensado para el sabotaje industrial y la ciberguerra». *stuxnet* ataca un programa de gestión de centrales eléctricas, oleoductos y con-

Por tanto, es primordial que se evalúe el nivel de dependencia de las IC respecto a las TIC y por lo tanto del ciberespacio para conocer su vulnerabilidad y en definitiva preparar su defensa. Hay que considerar que conforme el control de las IC se desplaza desde redes dedicadas a Internet y se emplean protocolos de red comunes, su vulnerabilidad aumenta aunque el no estar conectados a Internet no las hace inmunes a los ciberataques, especialmente en la forma de cibersabotajes. Los sistemas en red no son los únicos susceptibles en presentar vulnerabilidades y ser atacados; tanto su *software* como su *hardware* pueden ser saboteados antes de ser unidos a un sistema en explotación. El riesgo de manipulación en el proceso de fabricación es totalmente real y es la menos comprendida y más olvidada de las ciberamenazas. El sabotaje es prácticamente imposible de detectar y peor todavía de erradicar.

Debe además tenerse en cuenta que lanzar un ciberataque puede ser más fácil y barato que montar un ataque físico, aunque el nivel y duración de la interrupción que un ciberataque produce es proporcionadamente menor (27). Infligir un daño duradero en una IC sólo mediante ciberataques es poco factible pues las IC se diseñan para poder fallar y ser reiniciadas. Por tanto, más que intentar una protección total, cosa muy difícil, lo que debe preverse es una buena gestión de crisis.

En el ámbito de las operaciones militares, los ciberataques también tienen que ser considerados como una amenaza. Aunque no resulta realista plantear las acciones en el ciberespacio como único medio de una operación militar, sí ha quedado patente su capacidad ofensiva y, en consecuencia, resulta necesario preparar la defensa de los Sistemas de Mando y Control propios para asegurar la libertad de acción en la conducción de las operaciones militares (28). Cada vez resulta más probable que éstas se combinen o integren ataques informáticos con objeto de dejar fuera de servicio las redes y sistemas del adversario u orientar a la opinión pública a favor de uno de los contendientes (29). Éste fue el caso de los ciberataques sufridos por Georgia durante el conflicto con Rusia en Osetia del Sur y Abkhazia. Por primera vez en la historia una

---

glomerados fabriles. Irán admite ser víctima del mismo, en: *http://www.elpais.com/articulo/tecnologia/Alarma/virus/pensado/sabotaje/industrial/ciberguerra*.

(27) Lewis, J. A.: «Assessing the risks of cyber terrorism, cyber war and other cyber threats», Center for Strategic and International Studies, diciembre de 2002.

(28) «Concepto de Ciberdefensa Militar», EMAD, 28 de julio de 2011.

(29) Díaz del Río Durán, Juan José: *Cuaderno de Estrategia,* número 149, IEEE.

operación militar fue acompañada de una serie de ciberataques a los sitios *web* del Gobierno georgiano y otras páginas comerciales, dejándolos fuera de servicio en algunos casos y modificando el aspecto de las páginas en otros, *Defacement* (30).

Las posibles consecuencias de este tipo de ataques pone una vez más de relevancia la necesidad de dotarse de una capacidad de seguridad en el ciberespacio, que garantice una adecuada protección y que a su vez permita conocer y bloquear los sistemas del adversario en caso necesario. En este sentido se está desarrollando, tanto en Estados Unidos como en la OTAN, el concepto Operaciones Cibernéticas en Redes, CNO *(Computer Network Operations)* que se podría definir como las acciones tomadas de forma deliberada para obtener la superioridad en la información y denegarle ésta al enemigo. En España este Concepto se conoce como «Superioridad Militar en el Ciberespacio» definida como:

> «La ventaja operativa en, desde y a través del ciberespacio para llevar a cabo operaciones en cualquier momento y lugar, sin interferencias que las impidan o limiten, geográfica o temporalmente» (31).

La superioridad en la información permite utilizar con seguridad el ciberespacio. Aunque la superioridad total es prácticamente imposible de lograr habrá que obtener y mantener por lo menos una superioridad local durante las operaciones (32).

Las CNO, en combinación con las de guerra electrónica, se utilizan principalmente para interrumpir, perturbar, inutilizar, degradar o engañar los Sistemas de Mando y Control del enemigo, anulando su capacidad para tomar decisiones con eficacia y oportunidad, preservando a la vez los Sistemas de Mando y Control propios y amigos. Las CNO, de acuerdo con la publicación *Joint Doctrine for Information Operations* de Estados

---

(30) *Defacement* es un término usado en informática para hacer referencia a la deformación o cambio producido de manera intencionada en una página *web* por un atacante que haya obtenido algún tipo de acceso a ella, bien por algún error de programación de la página, por algún bug en el propio servidor o por una mala administración de éste. Ataques de *Defacement* conocidos se han hecho sobre los portales de *Twitte*r por el «ciberejército iraní», en el de nuestra última Presidencia de la Unión Europea y en los de los Gobiernos de Georgia y Venezuela, este último «colgando» un recordatorio de la «boda» entre los señores Castro y Chávez, *obra citada,* nota anterior.

(31) *Ibídem,* nota 27.

(32) El mismo documento entiende por superioridad local a la «capacidad de recopilar, procesar y difundir ininterrumpidamente el flujo de información mientras que se deniega esta capacidad al adversario en un área determinada».

Unidos, se subdividen a la vez en tres CND *(Computer Network Defence*), que incluye las acciones tomadas para proteger, monitorizar, analizar, detectar, reaccionar y recuperarse frente a los ataques, intrusiones, perturbaciones u otras acciones no autorizadas que podrían comprometer la información y los sistemas que la manejan CNE *(Computer Network Exploitation),* que incluye las acciones de recolección de información para inteligencia sobre sistemas de información enemigos, así como su explotación y CNA (*Computer Network Attack*), que incluye las acciones tomadas para perturbar, denegar, degradar o destruir información que circula por los sistemas enemigos y es un elemento clave en el concepto NEC *(Network Enabled Capability)* (33).

Algunos líderes militares ven las ciberarmas, es decir las armas informáticas, como armas de destrucción masiva. De hecho, han creado un nuevo término en relación con los ciberataques, las armas de interrupción masiva. El año pasado, el jefe de ciberseguridad de la OTAN avisaba de que los ciberataques y el ciberterrorismo suponen la misma amenaza para la Seguridad Nacional que un misil. Si por ejemplo, decía él, un determinado misil intercontinental tiene un alcance de unos 12.000 kilómetros y viaja a 24.000 kilómetros-hora, una ciberarma tiene un alcance ilimitado y viaja a casi la velocidad de la luz a 297.000 kilómetros-segundo. Respecto a las cibercapacidades, múltiples artículos aparecidos en los últimos años plantean la posibilidad de una carrera ciberarmamentística.

En el campo militar se está trabajando en diseñar estrategias de ciberguerra y la doctrina operacional que necesitan en este entorno único de amenazas. No es tarea fácil dadas las especiales características de las ciberoperaciones. Es preciso no obstante definir las reglas de enfrentamiento y la disuasión frente a estas amenazas pero el principal problema es definir e identificar en su caso si es ciberguerra, ciberespionaje o ciberterrorismo, cuando se produce una ciberagresión. Es muy difícil identificar al agresor y decidir si se trata de una acción de guerra *(casus belli)*, de un acto de terrorismo o de una acción criminal. Consecuentemente es difícil decidir a qué autoridad nacional debe encomendarse la necesaria reacción y por ello ya se dijo que la ciberdefensa debía ser multidisciplinar. El ponerlo en manos de la Justicia, nacional o internacional también

(33) NEC es «la capacidad de integrar todos los componentes del medio operativo (sensores, elementos de decisión y plataformas de armas) desde el nivel político-estratégico hasta el nivel táctico, a través de una infraestructura de información y redes». Díaz del Rio Durán, Juan José: *Cuaderno de Estrategia,* número 149, IEEE.

es difícil pues hasta que se establezca la cooperación internacional en ciberinvestigación, la capacidad de atribuir un ataque a una entidad concreta será difícil.

El análisis necesario para identificar a un atacante puede llevar meses, si es que la identificación es posible finalmente, e incluso, si el atacante es identificado y no es un Estado sino, por ejemplo, un grupo terrorista, puede suceder que no tengamos medios para responder o que incluso aunque la ciberinteligencia acompañada por la recopilación de la inteligencia tradicional pudiera proporcionar la procedencia y el mecanismo, la evidencia necesaria para desencadenar la correspondiente reacción o la causa en un tribunal exigirá mucho más. Para más complicación, los ciberataques a menudo se originan en servidores situados en países neutrales y las respuestas pueden conllevar consecuencias imprevistas a sus intereses, razón por la que el uso de este tipo de reacciones debe estar siempre bajo un mando estratégico que tenga una visión integral y global de la situación.

Por ejemplo, aproximadamente un 32% de los ataques de denegación de servicio distribuido contra Estonia en el año 2007, así como un 35% del tráfico contra Georgia, se originó desde ordenadores comprometidos dentro de Estados Unidos. Recientemente, el Centro de Seguridad de Tecnologías de la Información de Georgia estimó que un 15% de los ordenadores conectados mundialmente han estado comprometidos y han sido parte de *botnets* (34). Esto arrojaría un número de *bots* de aproximadamente 300 millones (35) con lo cual se ilustra el problema de la atribución del ataque.

Finalmente hay que pensar que podría decirse que cibercrimen y ciberamenazas no son categorías equivalentes, pues existen ciberdelitos que no constituyen amenazas a la Seguridad Nacional, ni todas las amenazas a la Seguridad Nacional nacen de la criminalidad cibernética. Ahora bien, en los supuestos de terrorismo y criminalidad organizada, determinadas formas de cibercriminalidad sí representan verdaderas amenazas a la Seguridad Nacional (36).

---

(34) *Botnet (Robot Network)* término que hace referencia a un conjunto de robots informáticos o *bots* que se ejecutan de manera autónoma y automática y que puede controlar todos los ordenadores-servidores infectados de forma remota. *Wikipedia.*

(35) *Véase* nota 16

(36) González Cussac, José Luis: *opus citada,* nota 2.

De todo lo anterior se deduce que el ciberespacio debe ser tenido en cuenta tanto desde el punto de vista de la Defensa Civil como de la militar pues aunque el ciberespacio es un dominio hecho por el hombre, se ha hecho tan crítico para las operaciones militares como la tierra, el mar, el aire y el espacio y su importancia irá en aumento. Estamos en suma en un nuevo escenario estratégico, en nuevo campo de batalla o en una extensión del mismo, donde se producen comportamientos o fenómenos ya conocidos y propios de toda confrontación pero que emplean técnicas nuevas; y también fenómenos nuevos que surgen de la propia idiosincrasia del ciberespacio en el que la Estrategia de Seguridad demanda planteamientos nuevos e imaginativos y cambios de mentalidad, de un modo especial en lo que se refiere a la gestión de crisis y resolución de conflictos y a la necesidad de adaptación de la Defensa en general y de las Fuerzas Armadas en particular, a las circunstancias de cada momento.

En los países occidentales y España no es una excepción, se trata de concienciar a todos los organismos e instituciones de la necesidad de la ciberseguridad. En especial, en las Fuerzas Armadas, todo el personal debe ser adecuadamente concienciado e instruido en la seguridad de la información y la ciberdefensa, realizando ejercicios específicos e incluyendo en todo tipo de ejercicios militares eventos e incidencias de ciberataques.

**La ciberseguridad y la ciberdefensa en España**

En España, los conceptos de seguridad y defensa, están presentes en toda la normativa desde la Constitución de 1978 hasta la EES de 2011. Así en el preámbulo de la citada Constitución ya se indica:

> «La Nacion española, deseando establecer la justicia, la libertad y la seguridad»… Por otra parte, en su sección primera, artículos 18 y 20 se recogen aspectos relativos a los derechos fundamentales y libertades públicas y se especifica el "derecho al secreto de las comunicaciones, limitando el uso de la informática pero garantizando la libertad de expresión e información"».

En el *Libro Blanco de la Defensa* del año 2000 y al definir:

> «El escenario estratégico» se habla de "los prodigiosos avances registrados en los campos de la comunicaciones y sistemas de información"».

En la Revisión Estratégica de la Defensa del año 2003 ya se incluyen claramente como un riesgo para la seguridad los «ataques cibernéticos» y se dice que:

> «La vulnerabilidad estratégica que supone este tipo de amenazas (37) comprende especialmente dos campos. Por un lado, los ataques contra los sistemas que regulan infraestructuras básicas para el funcionamiento de un país –como el sabotaje de los servicios públicos, la paralización de la red de transporte ferroviario o la interrupción de la energía eléctrica a una gran ciudad– suponen un serio quebranto para la normalidad y seguridad de una sociedad avanzada. En consecuencia, todas las infraestructuras básicas deben dotarse de elementos de protección suficientes para poder neutralizar este tipo de agresiones cuando su funcionamiento depende de complejos sistemas informáticos y de comunicaciones. Por otro lado, la penetración en la Red de Comunicación, Mando y Control de las Fuerzas Armadas, en el Sistema Nacional de Gestión de Crisis o en las bases de datos de los Servicios de Inteligencia pueden suponer una amenaza directa a la Seguridad nacional. Por tanto, las Fuerzas Armadas deben dotarse de las capacidades necesarias para impedir cualquier agresión cibernética que pueda amenazar la seguridad nacional.»

En la Ley Orgánica de la Defensa Nacional 5/2005 se habla claramente, aunque no se cite expresamente:

> «Junto a los riesgos y amenazas tradicionales para la paz, la estabilidad y la seguridad surgen otros… y lograr que sea efectiva requiere la concurrencia de la Defensa como uno de los medios necesarios para alcanzarla…»

La Directiva de Defensa Nacional 1/2008, lo mismo que su antecesora de 2004 incluye que:

> «…un sistema de seguridad y defensa español que debe enmarcarse dentro de una Estrategia de Seguridad Nacional»… En ella se contienen los principios de la seguridad y defensa española y da unas directrices de carácter general que se traducen en la Directiva de Política de Defensa 1/2009 (38).

---

(37) No debe extrañarnos una vez más la confusión entre riesgos y amenazas, aquí utilizados como sinónimos.

(38) Esta última Directiva es clasificada.

Finalmente, en la EES, aprobada este año 2011, se incluyen las ciberamenazas como una de las principales amenazas a la seguridad (39) y dice textualmente:

> «Cada vez una mayor parte de nuestra actividad se desarrolla en el ciberespacio, donde las amenazas pueden ocasionar graves daños e incluso podrían paralizar la actividad de un país. Los ciberataques más comunes tienen fines comerciales, pero también estamos expuestos a agresiones por parte de grupos criminales, terroristas u otros, incluso de Estados. Las nuevas tecnologías de información y comunicación ofrecen nuevos y más sofisticados medios para el espionaje y la contrainteligencia. Mejorar la seguridad en el ciberespacio pasa por fortalecer la legislación, reforzar la capacidad de resistencia y recuperación de los sistemas de gestión y comunicación de las infraestructuras y los servicios críticos, y por fomentar la colaboración público-privada con este fin. Es necesaria la coordinación de los diversos agentes involucrados, así como impulsar la cooperación internacional con el objetivo de desarrollar acuerdos de control de las ciberamenazas.»

La EES prevé la creación de un Consejo Español de Seguridad (40), dependiente del presidente del Gobierno, que se añade al ya existente Consejo Nacional de Defensa, Sin embargo España, a diferencia de otros países de nuestro entorno, no ha definido todavía una legislación específica y completa en materia de ciberseguridad. Sí existe, como veremos, legislación distribuida en distintos ámbitos ministeriales, pero que no ha sido desarrollada a partir de una política común que refleje el ámbito nacional y estratégico de la ciberseguridad y así las responsabilidades en el ciberespacio están muy fragmentadas en diferentes organismos, dependientes de distintos ministerios que abordan el problema de forma parcial. Además incluso con la existencia de este marco normativo, su grado de cumplimiento, en algunos casos, es preocupantemente bajo, lo cual supone un aumento del riesgo de nuestro ciberespacio.

La seguridad de nuestro ciberespacio comprende, como en la mayor parte de los países, las infraestructuras críticas, el sector empresarial y los ciudadanos.

---

(39) Aunque no figura con ese título sí se desprende de su contenido que se trata de la Estrategia de Seguridad *Nacional* Española.

(40) Vuelve a eludir otra vez el llamarle *Nacional* como al de Defensa, establecido por la Ley Orgánica de la Defensa. Tampoco queda clara la relación entre estos dos organismos.

Las infraestructuras criticas españolas se pueden agrupar, según el Plan de Protección de infraestructuras Críticas del Centro Nacional de Protección de Infraestructuras Críticas (CNPIC) creado en el año 2007, en 12 sectores: Administración, agua, alimentación, energía, espacio, industria nuclear, industria química, instalaciones de investigación, salud, sistema financiero y tributario, transporte, tecnologías de la información y las telecomunicaciones. Todos estos sectores se apoyan en el ciberespacio tanto para la gestión interna como para la provisión de servicios y su vinculación con otros sistemas. Finalmente, lo anterior queda ya regulado por la Ley 8/2011 donde se establecen medidas para la protección de las infraestructuras críticas y dentro de ellas se refiere, como dice su prólogo, a «... la protección contra ataques deliberados (tanto de carácter físico como cibernético)…»

La mayor parte de las grandes empresas ha incorporado ya la gestión de seguridad en sus redes TIC y a ello dedican parte importante de sus recursos. No así todavía en las pequeñas y medianas empresas que o no se han concienciado debidamente o no disponen de recursos.

Por lo que respecta a las Administraciones públicas el Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración electrónica, constituye un buen punto de partida, pero, como su propio nombre indica, cubre únicamente el sector de las Administraciones públicas, dejando fuera los otros sectores relevantes para la gestión de la ciberseguridad: otras infraestructuras críticas, las empresas y los ciudadanos. Además existen leyes nacionales, europeas e internacionales que abordan la cuestión de la ciberseguridad. Entre éstas, se encuentran la Ley Orgánica de Protección de Datos, la Ley General de Telecomunicaciones y la Ley de la Sociedad de la Información y Comercio Electrónico.

El Real Decreto ya citado establece el Esquema Nacional de Seguridad y consecuentemente la política de de seguridad en la utilización de medios electrónicos por las Administraciones públicas para lograr la protección adecuada de la información. Además dedica un capítulo a la «Capacidad de respuesta a incidentes de seguridad», Equipo de Respuesta de Emergencia Informática (CERT), del Centro Criptológico Nacional (CCN) adscrito al Centro Nacional de Inteligencia (CNI) y señala en su artículo 36 que el CCN:

> «Articulará la respuesta a los incidentes de seguridad entorno a la estructura denominada CCN-CERT que actuará sin perjuicio de las

capacidades de respuesta a incidentes de seguridad que pueda tener cada Administración pública y de la función de coordinación a nivel nacional e internacional del CCN.»

El análisis y gestión de riesgos es un aspecto clave del Real Decreto 3/2010 de 8 de enero por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración electrónica (41). A este respecto es muy útil la Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información (MAGERIT) con lo que se logra identificar, analizar, gestionar los riesgos de amenazas y tener previstos los planes de contingencia. También hay otros CERT a nivel autonómico y nacional como el Instituto de Tecnologías de la Información (INTECO)-CERT para las empresas y ciudadanos y el Servicio de Seguridad (IRIS)-CERT para la red académica y de investigación nacional.

En el año 2008 el CCN-CERT inició el despliegue de un Sistema de Alerta Temprana en la red SARA, puesta a disposición de todas las Administraciones públicas con el fin de detectar las anomalías y ataques a los sistemas de los diferentes ministerios y organismos conectados.

En el año 2007 se creó en el Ministerio del Interior, Secretaría de Estado de Seguridad, el CNPIC con los cometidos de coordinar la información y la normativa; convertirse en el punto de contacto permanente con los gestores tanto públicos como privados, de las infraestructuras críticas; fomentar las buenas prácticas y establecer contactos y mecanismos de colaboración con centros similares de todo el mundo.

El INTECO dependiente del Ministerio de Industria, Turismo y Comercio, promueve un uso adecuado de los servicios que hacen posible la sociedad de la información y la confianza en ellos y asesora a las empresas y a los ciudadanos, especialmente en la prevención y respuesta ante incidentes de seguridad.

El Grupo de Delitos Telemáticos de la Guardia Civil y la Unidad de Investigación de la Delincuencia en Tecnologías de la Información de la Policía Nacional, dependientes ambos del Ministerio del Interior son responsables de combatir la delincuencia que se produce en el ciberespacio.

La Agencia Española de Protección de Datos, dependiente del Ministerio de Justicia, responsable de hacer cumplir la normativa en materia de protección de datos personales.

(41) En: *http://www.csae.map.es/csi/pg5m20.htm*

En el CCN, de acuerdo con el Esquema Nacional de Evaluación y Certificación de la Seguridad de las Tecnologías de la Información (IENECSTI) se pueden certificar los sistemas y productos que cumplen con los criterios, métodos y normas de evaluación de la seguridad, como la Normativa Europea conocida como ITSEC y la normativa internacional conocida como criterios comunes.

Dentro del Ministerio de Industria, Turismo y Comercio, el Plan Avanza para su estrategia de los años 2011-2015 incluye las infraestructuras críticas y el refuerzo policial en delitos informáticos.

En el campo de la Justicia. En la modificación de la Ley del Código Penal de 1995 se establecen penas de prisión para el acceso no autorizado y el daño a sistemas informáticos.

El Ministerio de Defensa ha publicado la política de seguridad de la información, sus normas de aplicación y ha tomado numerosas iniciativas para incrementar la seguridad de su información, tanto en el ámbito de la Red de Propósito General (de orientación administrativa) como en la de Mando y Control (dependiente del Jefe del Estado Mayor de la Defensa (JEMAD) y orientado a las operaciones). La seguridad de la información se estructura en cinco áreas: Seguridad de la Información en las Personas, Seguridad de la Información en los Documentos, Seguridad de la Información en Poder de las Empresas, Seguridad de la Información en las Instalaciones y Seguridad de la Información en los Sistemas de Información y Telecomunicaciones (SEGINFOSIT), designándose director de Seguridad de la Información del Ministerio al secretario de Estado de Defensa, y asignándole, en el ámbito del Departamento, las funciones de dirigir la seguridad de la información, velar por el cumplimiento de la política de seguridad de la información y definir y crear la estructura funcional de la seguridad de la información, incluyendo, en esta última, el Servicio de Protección de Materias Clasificadas.

También se designa al Director General de Infraestructura (DIGENIN) como responsable de las áreas de seguridad de la información en las personas, en los documentos, en los Sistemas de Información y Telecomunicaciones y en las instalaciones y como órgano de apoyo técnico para la realización de estas tareas, se designa a la Inspección General del Plan Director de Sistemas de Información y Telecomunicaciones del Ministerio de Defensa (Inspección General CIS); como Órgano de Coordinación de la Seguridad de la Información del Ministerio. Asimismo se establece, el Consejo de Dirección de la Seguridad de la Información del Ministerio de Defensa.

Como es lógico, también la Directiva de Planeamiento Militar estudia las capacidades relacionadas con el ciberespacio con las que las Fuerzas Armadas deben contar y el concepto de Estrategia Militar, describe el nuevo escenario estratégico, en el que la ciberseguridad es tenida en cuenta y se analizan las tendencias y previsiones en este campo.

En el ámbito militar, el JEMAD ha expresado públicamente la importancia del desarrollo de capacidades relacionadas con las nuevas tecnologías, resaltando la necesidad de desarrollar medidas para mejorar la seguridad de los aliados ante la posibilidad de un ciberataque y definiendo esta amenaza como una de las más complejas a la que cualquier sistema defensivo puede enfrentarse, tanto por sus potenciales efectos sobre la sociedad como por su dificultad de identificar al agresor (42).

En el mismo orden de cosas, el JEMAD publicó el 28 de enero de 2011 la «Visión del JEMAD de la Ciberdefensa Militar» con objeto de difundir su visión sobre la ciberdefensa militar, para orientar la definición, desarrollo y empleo de las capacidades militares necesarias que permitan garantizar la eficacia en el uso del ciberespacio en las operaciones militares. Como consecuencia del Documento anterior, se publicó en julio de 2011 el Concepto de Ciberdefensa Militar cuyo objeto es:

> «Exponer los principios, objetivos y retos de la ciberdefensa en el ámbito militar, definir la terminología, realizar una evaluación de la capacidad y presentar las funciones y responsabilidades para diseñar el marco conceptual que permita establecer un plan de acción para la obtención de la capacidad de ciberdefensa militar en todos sus niveles.»

Su ámbito de aplicación es el de:

> «Los Sistemas Militares de Mando Control, Comunicaciones e Información Nacionales de Nivel Estratégico, Operacional y Táctico (incluidos los Sistemas de Combate y Control de Plataformas); así como los segmentos nacionales de los sistemas de las organizaciones internacionales de seguridad y defensa a las que España pertenece (OTAN, Unión Europea, etc.) en cuanto a la formulación consensuada con nuestros socios y aliados de sus directrices de empleo.»

---

(42) En: *www.uimp.es/blogs/prensa/2009/07/17*

En cualquier caso debe quedar claro que la Ciberdefensa Militar no es la Defensa Militar del Ciberespacio de interés para la Seguridad Nacional sino la Defensa del Ciberespacio de interés militar.

En el campo de la Ciberdefensa Militar, corresponde al JEMAD la elaboración de una Doctrina Conjunta de Ciberdefensa Militar, la dirección, planificación y ejecución de la ciberdefensa en los CIS conjuntos y la dirección, planificación y coordinación de la obtención de la capacidad de ciberdefensa para todos los CIS de las Fuerzas Armadas. Para ello cuenta fundamentalmente con la Sección de Seguridad de la Información del Estado Mayor Conjunto de la Defensa. Como consecuencia de lo anterior se han realizado ya dos ejercicios de ciberdefensa con participación de los Ejércitos, la Armada, el CNI y la Guardia Civil. Por su parte los jefes de Estado Mayor de los Ejércitos y la Armada son responsables de la dirección, planificación y ejecución de la ciberdefensa militar en sus sistemas específicos.

En el Ejército de Tierra y siguiendo las políticas del CNI y OTAN, la Jefatura CIS (JCISAT) ha desarrollado un proyecto denominado Ejército de Tierra-CERT, para cubrir la necesidad de hacer frente a ataques sobre redes clasificadas del Ejército de Tierra, inicialmente en el ámbito de Mando y Control. El Ejército de Tierra-CERT se enfoca a la detección y respuesta ante incidentes de seguridad. El Ejército de Tierra-CERT se compone de sondas desplegadas en cada nodo de un sistema, tanto en territorio nacional como en zonas de operaciones. Las sondas informan a un servidor central de cualquier evento que se produzca en su nodo. El servidor central contiene un motor de inteligencia artificial, capaz de correlacionar enormes cantidades de eventos, ordenarlos, deducir patrones de ataque, dar un punto de situación sobre los sistemas afectados y proponer las soluciones oportunas o, incluso, ejecutarlas automáticamente, todo ello en tiempo real. Esto ayuda a la estructura SEGINFOSIT a llevar a cabo sus cometidos y, sobre todo, a reducir los tiempos de detección y reacción.

La industria española relacionada con la ciberseguridad está en pleno proceso de crecimiento y maduración, tal y como refleja el último «Catálogo de empresas y soluciones de seguridad» del INTECO, cifrando en más de 1.000 las empresas españolas que se dedican a la ciberseguridad. En el año 2009, las principales empresas del sector se agruparon en el Consejo Nacional Consultor sobre Ciber-Seguridad (CNCCS) con el objetivo de fomentar la defensa del ciberespacio, poniéndose a

disposición de entidades gubernamentales o privadas para asesorar en materias de ciberseguridad, y potenciar la innovación tecnológica y el crecimiento económico consiguientes.

España alcanzó en el año 2009 una tasa de penetración en Internet del 71,8%, lo cual representa más de 30 millones de ciberusuarios potenciales. Substrayendo la población preescolar y los mayores de 75 años, este porcentaje, superior al 70% de la población con acceso a los Servicios del Ciberespacio puede interpretarse como que, prácticamente, la totalidad de la población de España accede a tales Servicios. La actual legislación española relacionada con la ciberseguridad hace especial énfasis en la necesidad de formación y concienciación de los ciudadanos en esta materia, así como en el uso responsable del ciberespacio. Sin embargo, la aplicación de estos principios hasta el momento es escasa debido, fundamentalmente, al desconocimiento generalizado de la legislación. El INTECO y el CCN, dentro del ámbito de sus competencias, desarrollan interesantes campañas de concienciación y formación en materia de seguridad TIC, pero aún sin la repercusión deseada. La industria española del sector de la ciberseguridad ha emprendido, igualmente, diversas campañas privadas para la concienciación y formación de determinados sectores de la sociedad como los escolares, jubilados y desempleados.

España forma parte de organizaciones internacionales que promueven la Defensa del Ciberespacio. Destaca nuestra participación en el Centro de Excelencia de Ciberdefensa Cooperativa de la OTAN y en organismos como ENISA *(European Network Information and Security Agency).*

En resumen, si bien existen organismos con responsabilidades claras en distintos ámbitos de las Administraciones públicas, España no dispone de un órgano único, al más alto nivel, que asuma el valor estratégico que la ciberseguridad tiene para nuestro país y ejerza el liderazgo necesario para que todos esos organismos actúen según una única política nacional. De esta forma se evitarían solapes y redundancias entre ellos teniendo en cuenta que además no todos conceden la misma prioridad a los aspectos de la seguridad. Para ello sería necesario en primer lugar la creación de una Estrategia Nacional de Ciberseguridad que tratase de forma completa el problema y ayudase a crear, tanto en las autoridades como en las empresas y los particulares, una conciencia también de ciberseguridad.

## La ciberseguridad y la ciberdefensa en la Unión Europea

Europa, dentro de su Política Común de Seguridad y Defensa (PCSD) del año 1999, ha desarrollado diversos programas y creado órganos para hacer frente a los distintos riesgos y amenazas cibernéticas, tanto corporativamente como a cada uno de sus miembros. Como iniciativas más importantes se pueden citar: la creación de ENISA en el año 2004. Esta Agencia asesora a la Comisión y los Estados miembros en lo relacionado con la ciberseguridad; el Programa para la Protección de la Infraestructuras Críticas y la presentación en 2010 de «Una Agenda Digital para Europa». Esta Agenda (43) constituye un compendio de los problemas y oportunidades actuales y previsibles, y evolucionará a la luz de la experiencia y de las rápidas transformaciones de la tecnología y la sociedad. Por otro lado se plantean un conjunto de iniciativas legislativas (44).

También es interesante señalar que en noviembre del pasado año se realizó el primer ejercicio de simulación de un ciberataque. Este ejercicio, llamado *Cyber Europe 2010* tenía por objeto obtener enseñanzas sobre como mejorar la seguridad comunitaria y de los países. Participaron diversos países de la Unión Europea con el apoyo de ENISA.

Por otra parte, la Unión Europea aprobó en diciembre de 2002 la Estrategia Europea de Seguridad. En ella consideraba la seguridad ante la situación mundial y las principales amenazas (45). Como consecuencia de la apertura cada vez mayor de las fronteras en Europa tras la caída del muro de Berlín es difícil ya separar lo que es la seguridad interior de la exterior. Es además un hecho que ha habido un rápido desarrollo tecnológico que ha incrementado el grado de dependencia de Europa respecto de una infraestructura interconectada en ámbitos como el transporte, la energía o la información, lo que produce un aumento de su vulnerabilidad.

En la revisión de la Estrategia Europea de Seguridad, el llamado Informe Solana, de diciembre de 2008 ya aparece dentro de las nuevas amenazas y riesgos, la seguridad de los sistemas de información y como uno

---

(43) Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones, «Una Agenda Digital para Europa», en: *http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0245:FIN:ES:PDF*, mayo de 2010, fecha consulta: 23 de septiembre de 2010.

(44) Caro Bejarano, María José: *Cuaderno de Estrategia*, *citado.*

(45) EES de 2003, en: *http://www.ieee.es/Galerias/fichero/estrategia_europea_de_seguridad_2003.pdf.*

de los nuevos retos mundiales y principales amenazas menciona el concepto de ciberseguridad:

> «Las economías modernas dependen en gran medida de las infraestructuras vitales como los transportes, las comunicaciones y el suministro de energía, e igualmente de internet. La Estrategia de la Unión Europea para una sociedad de la información segura en Europa, adoptada en 2006, hace referencia a la delincuencia basada en internet. Sin embargo, los ataques contra Sistemas de TIC privadas o gubernamentales en los Estados miembros de la Unión Europea han dado una nueva dimensión a este problema, en calidad de posible nueva arma económica, política y militar. Se debe seguir trabajando en este campo para estudiar un planteamiento general de la Unión Europea, concienciar a las personas e intensificar la cooperación internacional.»

Finalmente, en el año 2010 se aprobó la Estrategia de Seguridad Interior de la Unión Europea (46) que trata de hacer frente a amenazas graves entre las que incluye la ciberdelincuencia.

En el campo de la Defensa, la Unión Europea ha elaborado el CNO y la EDA *(European Defence Agency)* ha publicado el correspondiente contrato para su implementación (47).

Son muchos los pasos dados en el marco europeo pero hace falta más. En el núcleo del desarrollo de una política de ciberseguridad europea se encontraría el desarrollo de una Estrategia Europea de Ciberseguridad. Así lo indicó el director ejecutivo de ENISA, en una conferencia impartida en Madrid sobre protección de infraestructuras críticas afirmando que Europa necesita una estrategia integral de ciberseguridad que integre a las diferentes estrategias nacionales. El Parlamento Europeo recogió esta propuesta en una resolución sobre la aplicación de la Estrategia Europea de Seguridad y la PCSD. Otras propuestas incluyen la creación de un consejo, de un coordinador o de una agencia de ciberseguridad europea (48).

La Unión Europea se ha dotado de una estrategia de seguridad propia. Pero ésta reclama una mayor determinación, recursos suficientes

---

(46) Estrategia de Seguridad Interior de la Unión Europea, en: *http://www.consilium.europa.eu/uedocs/cms data/librairie/PDF/QC3010313ESC.pdf*

(47) *Véase* página 16.

(48) *Véase* nota 39.

y un uso más eficaz y coherente de cuantos instrumentos dispone para la gestión de crisis y la prevención de conflictos; unos requerimientos realmente exigentes a los que ningún país europeo, e incluso Estados Unidos como gran potencia, es capaz de hacer frente en solitario (49).

## La ciberdefensa en la OTAN

Desde el final de la guerra fría la OTAN, está llevando a cabo acciones para dotarse de las capacidades necesarias para poder defenderse y reaccionar adecuadamente frente a las amenazas del ciberespacio.

En la declaración de la cumbre de Riga, 29 de noviembre de 2006, los jefes de Estado y de Gobierno de la OTAN demandaron la mejora de la protección de los CIS claves ante posibles ciberataques.

Sin embargo, el ciberataque de la primavera de 2007 a Estonia fue el que representó un hito y un reto histórico para la OTAN pues fue la primera vez que un Estado miembro solicitó apoyo a la OTAN por un ataque a la infraestructura crítica CIS de su país. Se dio además la paradójica situación de que la mayoría de los expertos en ciberseguridad de la OTAN se enteraron de la noticia en Washington, mientras participaban en el congreso de ciberseguridad (50) que anualmente organiza la Oficina de Seguridad de la Alianza (51).

Como quedó demostrado, la OTAN no disponía de un Plan de Acción en caso de ciberataque a un Estado miembro; hasta entonces se habían detectado problemas de índole nacional, puesto que muchas naciones de la OTAN y en especial Estados Unidos de América recibían y reciben a diario ciberataques –de la misma envergadura y mayor-- contra la infraestructura crítica de información del país, sin que esto constituyera causa de intervención por parte de la OTAN. Pero el caso de Estonia fue diferente, pues debido a la dimensión del país, los ataques le llevaron a una situación de crisis de Seguridad Nacional. La intervención de la OTAN, de alguna manera, era más que justificada. Pero no había un Plan de Acción.

La OTAN se enfrentó con el problema de manera decidida en la cumbre de Bucarest, celebrada entre los días 2 y 4 de abril de 2008. En la reunión

---

(49) Díaz del Rio Duran, Juan: v*éase* nota 39.
(50) Ganuza Artiles, Nestor*: Cuaderno de Estrategia,* número 149, IEEE.
(51) NOS *(NATO Office of Securrity).*

se llegó al acuerdo expresado en la sección 47 de la declaración de la cumbre:

> «La OTAN se mantiene comprometida con el fortalecimiento de los sistemas de información crítica de la Alianza contra ciberataques. Hemos adoptado recientemente la política de ciberdefensa, y estamos desarrollando las estructuras y autoridades para llevarla a cabo. Nuestra política en materia de ciberdefensa subraya la necesidad de la OTAN y de las naciones miembros de proteger los sistemas de información crítica conforme con sus respectivas responsabilidades; compartir las mejores prácticas y establecer una capacidad de apoyo a las naciones, bajo petición, para contrarrestar un ciberataque. Continuamos con el desarrollo de las capacidades de ciberdefensa de la OTAN y con el fortalecimiento de los vínculos entre la OTAN y las autoridades nacionales.»

No sólo los ciberataques a Estonia representaron un caso de reflexión para la OTAN, también otros casos, como el ciberataque a Lituania en julio de 2008, el ciberataque a Georgia en julio de 2008 y el ciberataque a Kirziguistán (52) en enero de 2009. Por ello, en la declaración de la cumbre de Estrasburgo (4 de abril de 2009), afirmaron la vigencia de su compromiso en el fortalecimiento de los CIS de importancia crítica para la Alianza frente a ciberataques, que tanto agentes estatales como no estatales, pueden tratar de explotar, pues cada vez es mayor la dependencia de estos sistemas.

La Revisión del Concepto Estratégico de 1999 también considera la ciberseguridad como un nuevo reto respecto al Concepto Estratégico de la OTAN de 1999.

En el nuevo Concepto Estrategico aprobado en Lisboa en noviembre de 2010 se aclara que:

> «…la defensa y seguridad común… continuará siendo efectiva en un mundo cambiante… incluidas las nuevas amenazas…» y más adelante dentro del entorno de seguridad cita expresamente a los ciberataques dice de ellos que «están siendo más frecuentes, más organizados y más costosos en el daño que infligen en las administraciones gubernamentales, en los negocios, economías y potencialmente en las redes de transporte y abastecimiento y otras

(52) Georgia y Kirziguistán no son países OTAN pero pertenecen al Partenariado por la Paz.

infraestructuras críticas; pueden alcanzar un nivel tal que amenace la prosperidad, seguridad y estabilidad nacional y euroatlántica. Los militares y Servicios de Inteligencia extranjeros, las organizaciones criminales y los grupos terroristas y extremistas pueden ser origen de estos ataques.»

En cuanto a acciones concretas, la OTAN, aparte de adquirir la correspondiente capacidad, NCIRC *(NATO Computer Incident Response Capability)*, para cuyos objetivos se basa principalmente en su Centro Técnico. Ha aprobado, en el año 2008, el concepto y política de ciberdefensa, ha creado la Autoridad de Gestión de la Ciberdefensa, CDMA, *(Cyber Defense Management Authority)* y su correspondiente estructura y organización de apoyo; la ciberseguridad es hoy en día uno de los componentes más importantes de la seguridad, siendo los ciberataques un asunto estratégico del mismo nivel que las armas de destrucción masiva y la *Yihad Global* (53).

En resumen la OTAN necesita actualizarse tecnológicamente para hacer frente a las nuevas amenazas y en consecuencia está desarrollando su política de ciberdefensa. La creación del concepto de ciberdefensa y la inauguración del Centro de Excelencia en Ciberdefensa en Tallin (Estonia), son un ejemplo de ello.

## Conclusiones

El ciberespacio debe ser tenido en cuenta tanto desde el punto de vista de la Defensa Civil como de la militar pues aunque el ciberespacio es un dominio hecho por el hombre, se ha hecho tan crítico como la tierra, el mar, el aire y el espacio y su importancia irá en aumento. Si no se controla adecuadamente, desde allí puede ver una nación amenazada su libertad de acción y su seguridad, no sólo su ciberseguridad sino la Seguridad Nacional. Estamos en suma en un nuevo escenario estratégico, en un nuevo *Global Common,* en nuevo campo de batalla o en una extensión del mismo, donde se producen los comportamientos o fenómenos ya conocidos en todos los conflictos pero que aquí emplean técnicas nuevas; y también fenómenos nuevos que surgen de las propias características del ciberespacio. La Estrategia de Seguridad Nacional deberá tener en cuenta la ciberseguridad y la consiguiente Defensa

(53) En: *www.betanews.com/article/Mr-Obama-Dont-forget-the-cyberwar-threat/1228782845*

Nacional deberá incluir planteamientos nuevos e imaginativos y cambios de mentalidad, de un modo especial en lo que se refiere a la gestión de crisis y resolución de conflictos y a la necesidad en suma de contar con la ciberdefensa.

En la estrategia de ciberseguridad se deben precisar los objetivos estratégicos a alcanzar, los órganos competentes y sus responsabilidades, la contribución de las distintas instituciones del país, el nivel tecnológico a alcanzar y en él, los objetivos de I+D.

En la Seguridad Nacional se contempla la de las infraestructuras críticas y la Estrategia de la Defensa debe comprender siempre la prevención de posibles ataques y la protección para disminuir la vulnerabilidad y en caso de crisis minimizar los daños y acelerar el periodo de recuperación. Las amenazas enemigas a las IC siempre han existido en tiempos de guerra o conflicto, pero los escenarios de amenazas incluyen ahora también ataques en tiempos de paz por medio de ciberataques.

En el ámbito de las operaciones militares, los ciberataques también tienen que ser considerados como una amenaza. Aunque no resulta realista plantear las acciones en el ciberespacio como único medio de una operación militar, sí ha quedado patente su capacidad ofensiva y, en consecuencia, resulta necesario preparar la defensa de los Sistemas de Mando y Control propios de forma que se asegure la libertad de acción en la conducción de las operaciones. Algunos líderes militares ven las ciberarmas, es decir las armas informáticas, como armas de destrucción masiva. De hecho, han creado un nuevo término en relación con los ciberataques, las «armas de interrupción masiva».

En España, los conceptos de seguridad y defensa, están presentes en toda la normativa desde la Constitución de 1978 hasta la EES de 2011, pero es en la Revision Estrátégica de la Defensa de 2003 donde aparece por primera vez el peligro de los ataques cibernéticos. Sin embargo, España, a diferencia de otros países de nuestro entorno, no ha definido todavía una legislación específica y completa en materia de ciberseguridad. Sí existe legislación distribuida en distintos ámbitos ministeriales, pero que no ha sido desarrollada a partir de una política común que refleje el ámbito nacional y estratégico de la ciberseguridad y así las responsabilidades en el ciberespacio están muy fragmentadas en diferentes organismos, dependientes de distintos ministerios que abordan el problema de forma parcial. Además incluso con la existencia de este

marco normativo, su grado de cumplimiento, en algunos casos, es preocupantemente bajo, lo cual supone un aumento del riesgo de nuestro ciberespacio. Se hace necesario la creación de una autoridad nacional de ciberseguridad que defina una estrategia nacional de ciberseguridad y establezca la ciberdefensa coordinando las distintas instituciones, medidas a tomar y acciones a realizar.

Por lo que respecta a las organizaciones internacionales de las que España forma parte es importante reseñar que la Unión Europea se ha dotado de una estrategia de seguridad propia pero necesita una estrategia integral de ciberseguridad que integre a las diferentes estrategias nacionales y en cuanto a la OTAN aunque es consciente del peligro, necesita actualizarse tecnológicamente para hacer frente a las nuevas amenazas y en consecuencia está desarrollando su política de ciberdefensa. La creación del concepto de ciberdefensa y la inauguración del Centro de Excelencia en Ciberdefensa en Tallin (Estonia), en el que España participa, son un ejemplo de ello.

Nos quejamos de que no hay conciencia de Defensa pero todavía la hay menos de ciberdefensa y aunque algo parecido ocurre en nuestro entorno internacional, en nuestro caso es todavía mayor. Si, como dice la EES, la seguridad debe ser responsabilidad de todos, este aserto es todavía, si cabe, más imperioso cuando se trata de la ciberseguridad.

## CAPÍTULO SEGUNDO

# ESTRATEGIAS INTERNACIONALES PARA EL CIBERESPACIO

# ESTRATEGIAS INTERNACIONALES PARA EL CIBERESPACIO

Por Carlos Enríquez González

> «El mundo era tan reciente, que muchas cosas carecían de nombre, y para mencionarlas había que señalarlas con el dedo.»
>
> GabrielGarcía Márquez, *Cien años de soledad*

## Introducción

Tierra, mares y océanos, aire y finalmente, el espacio exterior; explorados y explotados por el hombre, en todos ellos imperan las leyes naturales y sobre ellos hemos impuesto la ley positiva. Donde los Estados no alcanzan, rigen tratados y convenios internacionales, y en su defecto reinan el caos y la ley del más fuerte.

El ciberespacio es el último dominio común en el que el hombre se ha aventurado. Se diferencia de los demás en su creador; en él sus leyes naturales son un conjunto de protocolos lógicos –sustentados por una capa física– creados y acordados por el hombre. Sin embargo, su creador no ha sabido, o no ha querido, imponer una ley positiva sobre su creación. Quizás no lo creyó necesario; posiblemente porque «entonces» no lo fuera. «Entonces» era un tiempo de certidumbres; la tercera guerra mundial en forma de apocalipsis nuclear aniquilaría los principales núcleos de población y las infraestructuras críticas de las potencias enfrentadas.

El éxito pasaba por asegurar la detección, seguimiento e interceptación a tiempo de los bombarderos nucleares enemigos y la supervivencia de las comunicaciones entre centros de poder. Sus usuarios y administradores constituían una pequeña comunidad de interés que no requería vigilancia. Así nació ARPANET (1) y (2) y así evolucionó hacia lo que hoy conocemos como Internet: la Red, una tela de araña que supera los esquemas del viejo mundo westfaliano, que no conoce fronteras, Estados ni naciones y sobre la que no existen ni cuerpo legal ni «gendarmería» universales que garanticen el «buen» funcionamiento de la ingente cantidad de plataformas, equipos, aplicaciones, servicios, contenidos, comunidades de interés y un largo etcétera de mundos convergentes (3).

## Los protagonistas: los Estados, la iniciativa privada y las organizaciones internacionales

En este escenario, los Estados han legislado y han desarrollado estructuras para luchar contra el cibercrimen, como hicieron con la tierra, el mar y el aire. Pero dada la naturaleza global e informe del ciberespacio y el carácter elusivo de aquellos que lo utilizan para delinquir, la acción estatal, aunque necesaria, resulta insuficiente. Así, el sector privado, principal protagonista del ciberespacio tanto por los contenidos y aplicaciones que le proporcionan su valor añadido, como por las infraestructuras que lo soportan, juega un papel de primer orden en esta «partida».

Quizás lo hablado entre el presidente de la República de Francia, Nicolas Sarkozy y Mark Zuckerberg –presidente y director ejecutivo de la red social *Facebook*– antes de la última reunión del G-8 en París, resuma muy

(1) ARPANET: acrónimo de ARPA (*Advanced Research Projects Agency Network*) y NET*work*. ARPA, hoy llamada DARPA, es una Agencia perteneciente al Departamento de Defensa de Estados Unidos de Norteamérica DARPA *(Defence Advanced Research Projects Agency*).

(2) Aunque no existe una versión oficial acerca del origen de ARPANET, ya que incluso la actual DARPA –heredera de ARPA– en su sitio *web* se desvincula de las distintas versiones que circulan, parece que la necesidad de actuar a tiempo contra los bombarderos estratégicos enemigos y garantizar la supervivencia de las comunicaciones en caso de ataque nuclear estaría detrás del origen del Proyecto Lincoln, precursor de ARPANET (Waldrop, 2008).

(3) Hay dos 1.000 millones (*2 billion*) de usuarios de Internet en todo el mundo y casi ocho billones de dólares *(8 trillion*) cambian de manos cada año a través del comercio electrónico (Pélissié du Rausas, Manyika, Hazan, Bughin, Chui & Said, 2011).

bien lo que está en juego. Según Vittorio Collao (4) –consejero delegado del Grupo Vodafone– para el joven Zuckerberg, una Internet sin limitaciones resulta esencial para la innovación y la actividad emprendedora, mientras que Sarkozy, por el contrario sostiene que el éxito de Internet depende de la confianza que nos merezca: necesitamos confiar en Internet y además necesitamos saber que estamos protegidos por la Ley, que se protege nuestra privacidad, que la confidencialidad de nuestros datos personales está asegurada y que nuestros hijos están a salvo en Internet.

Los autores y creadores de contenidos –añade Collao–, necesitan ver sus derechos respetados, por ello los gobiernos deben ser capaces de garantizar la seguridad de los usuarios de Internet, mediante reglas. Zuckerberg, que estaría de acuerdo en la necesidad de preservar la confianza en Internet, sería más partidario de la autorregulación del sector de modo que sean los propios servicios ofertados en la Red los que incorporen los mecanismos de fomento de la confianza que la sociedad demanda. Un ejemplo de esto podría ser el sistema de evaluaciones a los usuarios (compradores y vendedores) que utiliza la plataforma de ventas *eBay*.

Igualmente importantes, dado el carácter global de la materia, son las iniciativas internacionales sobre ciberseguridad; iniciativas que generalmente se enmarcan en el seno de organizaciones internacionales. Pero el concepto ciberseguridad cubre todo el espectro desde el simple delito cibernético a la ciberguerra, desde la protección de los ordenadores personales frente a la acción de un *hacker* aficionado, hasta lo que grupos más organizados pueden hacerle a los equipos que controlan las infraestructuras críticas de un país o incluso a sus Sistemas de Mando y Control Militar. Así cada organización internacional, según su naturaleza, se ha centrado en uno u otro aspecto. Desde la mera protección de sus propios sistemas hasta la actuación directa contra amenazas procedentes del ciberespacio.

*Aproximaciones a la ciberseguridad en el panorama internacional: las organizaciones internacionales y los Estados*

Lo primero que nos llama la atención cuando abordamos la faceta internacional de la ciberseguridad, es la ausencia de esa Ley positiva que

(4) Collao, V.: «¿Es posible que tanto Sarkozy como Zuckerberg estén en lo cierto?», *El País, Ciberp@ís*, 6 de junio de 2011.

decíamos al principio, la falta de un marco legal mundial equivalente a la Convención de Naciones Unidas sobre el Derecho del Mar que delimite responsabilidades y jurisdicciones. Efectivamente, no existe una Convención de Naciones Unidas sobre Derecho del Ciberespacio; ni siquiera uno limitado al –ya de por sí muy amplio– concepto de ciberseguridad. Lo más parecido que encontramos –y con él iniciamos el análisis de algunas aproximaciones internacionales a la materia– es la Convención del Consejo de Europa sobre Cibercrimen (CETS, número 185), también conocida como Convención de Budapest.

## EL CONSEJO DE EUROPA

La Convención del Consejo de Europa sobre Cibercrimen –abierto a la firma por los Estados miembros en Budapest, 23 de noviembre de 2001– es el primer tratado internacional sobre delitos cometidos a través de Internet y otras redes informáticas. Su valor reside en que constituye el único texto legal internacional vinculante hasta la fecha. Por ello, la ratificación de este tratado constituye para muchos expertos la prueba de la seriedad del compromiso de los países en su lucha contra el cibercrimen. Trata principalmente las violaciones de los derechos de autor, el fraude informático, la pornografía infantil y las violaciones de seguridad de la redes. También incorpora una serie de medidas y procedimientos para la inspección de redes y para la interceptación de datos.

Su principal objetivo, tal y como figura en el preámbulo, es aplicar una política penal común encaminada a la protección de la sociedad contra el delito cibernético, mediante la adopción de una legislación adecuada y a través del fomento de la cooperación internacional, incluyendo la extradición de cibercriminales. La Convención es el producto de cuatro años de trabajo de expertos del Consejo de Europa y de otros países como Estados Unidos, Canadá y Japón, entre otros. Recientemente, el tratado se ha complementado con un protocolo adicional que criminaliza la publicación de propaganda racista o xenófoba a través de redes informáticas. Han firmado 48 el tratado hasta el momento, de los cuales 31 lo han ratificado, incluyendo Estados Unidos.

Al hilo de lo que decíamos con anterioridad en cuanto al grado de compromiso con la lucha contra los delitos cibernéticos que supone su firma y ratificación; entre los miembros del Consejo de Europa que ni siquiera han firmado el tratado, aparte de Rusia –país hacia el que a menudo se señala como origen de ataques cibernéticos–, sorprende la presencia de

pequeños países con una fuerte implantación de las tecnologías de la información como son: Andorra, Mónaco y San Marino. Por otra parte, los países que aún habiéndolo firmado, todavía no lo han ratificado son: Austria, Bélgica, República Checa, Georgia, Grecia, Irlanda, Liechtenstein, Luxemburgo, Malta, Polonia, Suecia, Suiza y Turquía.

### LA ORGANIZACIÓN PARA LA SEGURIDAD Y COOPERACIÓN EN EUROPA (OSCE)

Siguiendo dentro del Viejo Continente en el año 2008, durante la Presidencia estonia del Comité Político-Militar de la OSCE, a propuesta del país báltico se introdujo la ciberseguridad como tema a tratar por la Organización dentro de su dimensión político-militar. La postura de Estonia hay que interpretarla desde la óptica de los graves ataques cibernéticos de denegación de servicio sufridos en ese país en el año 2007. Previamente, la OSCE ya venía prestando atención a la lucha contra el delito cibernético y el uso de Internet para fines terroristas o de propagación de odio. En este sentido, tras la masacre cometida el pasado día 22 julio de 2011 en Oslo y en la isla de Utoya por el ultraderechista noruego Anders Breivik, conviene recordar el llamamiento realizado en París en el año 2004 ante el Consejo Permanente de la OSCE, poco antes de su muerte, por el escritor sueco Stieg Larsson –a la sazón director de la Fundación sueca «Expo» y autor de la famosa trilogía *Millennium*– contra la propagación del odio racista, xenófobo, político, etc. a través de Internet. Desde entonces la OSCE ha celebrado numerosos eventos destinados a aumentar la conciencia de ciberseguridad entre los Estados miembros.

Abundando en la política declaratoria emprendida por esta Organización, en la última Conferencia sobre Seguridad Cibernética titulada: *Conferencia de la OSCE sobre una Aproximación Omnicomprensiva a la Seguridad Cibernética: Explorando el Papel de la OSCE*, auspiciada por la Presidencia lituana y celebrada en Hoffburg (Viena), los días 9 y 10 de mayo de 2011, los Estados miembros no han llegado a concretar el papel que debe desempeñar la Organización ni qué actividades se deben emprender en el ámbito de la ciberseguridad. Sí se han emitido, por el contrario, algunas recomendaciones –tan sólo eso, recomendaciones– sobre vías a explorar dentro del pilar político-militar de la Organización.

En particular, se hizo hincapié en la experiencia de la OSCE en relación con las Medidas de Fomento de la Confianza y con las Medidas de Fomento de la Confianza y la Seguridad. Es más, se puso el énfasis en la

utilidad de aplicar esta experiencia al ciberespacio para mejorar la transparencia, la previsibilidad y la estabilidad; reduciendo a la vez los riesgos de falsas percepciones, de escalada y de conflicto. La Presidencia lituana –hay que recordar que Lituania también fue objeto de importantes ataques cibernéticos en verano del año 2008 tras legislar contra la exhibición de simbología soviética– habría incluso arrancado cierto apoyo para aprobar un marco estratégico sobre ciberseguridad en la próxima reunión ministerial de la OSCE a celebrar en su capital, Vilna.

LA UNIÓN EUROPEA

La Unión Europea por su parte, mantiene abiertas al menos dos líneas maestras de trabajo en el campo de la ciberseguridad. Por un lado nos encontramos con el trabajo desarrollado por la Agencia Europea de Defensa (EDA), ubicado dentro de la Política Común de Seguridad y Defensa (PESD) y por tanto bajo la égida del Consejo Europeo. Identificada por la EDA como una de las 10 prioridades en el desarrollo de capacidades, su objetivo es el de progresar en el campo de la colaboración segura en la «nube militar» *(Military Cloud)* y optimizar el uso de las tecnologías de *Cloud Computing* teniendo en cuenta la creciente amenaza cibernética. Aunque es una de las prioridades en el desarrollo de capacidades, no constituye una línea de trabajo «madura» en la que se hayan alcanzado avances dignos de mención. Una de las razones para ello puede obedecer al indudable protagonismo de la otra línea de trabajo que, bajo la autoridad de la Comisión Europea, protagoniza la Agencia Europea para la Seguridad de la Información y de las Redes, ENISA *(European Network and Information Security Agency)*.

ENISA fue creada en marzo de 2004 (5) y, tras un breve periodo de constitución en Bruselas, ocupó su actual sede en la localidad de Heraklion, en isla griega de Creta. Entre sus objetivos están: mejorar la capacidad de la Unión Europea en su conjunto para prevenir, tratar y dar respuesta a las incidencias que afecten a la seguridad de la información y de las redes; desarrollar un alto nivel de conocimiento en la materia; promover la colaboración entre actores de los sectores público y privado, y; apoyar a la Comisión en la elaboración de legislación comunitaria en materia de seguridad de la información y de las redes.

(5) Regulation (EC) número 460/2004 *of the European Parliament and of the Council of 10 March 2004 establishing the European Network and Information Security Agency.*

Así, ENISA, en lo referente a la lucha contra el cibercrimen, ha hecho suyo el mandato que emana de la Estrategia Europea de Seguridad aprobada durante la Presidencia española (6) y que sienta las bases de cómo la Unión Europea debe hacer frente a las amenazas emergentes a su seguridad. Posteriormente, la Comisión ha desarrollado un Plan de Acción cuatrienal (7) para enfrentarse al crimen organizado, al terrorismo y al cibercrimen. En concreto, establece que Europa es un objetivo clave para el cibercrimen debido a su avanzada infraestructura de Internet, el elevado número de usuarios, y a que sus economías y sistemas de pago dependen en gran medida de Internet. Los ciudadanos, las empresas, los gobiernos y las infraestructuras críticas –añade– deben estar mejor protegidos de aquellos delincuentes que se aprovechan de las nuevas tecnologías. Por ello, de los cinco objetivos que establece este Plan de acción, uno de ellos se enuncia así:

> «Aumentar los niveles de seguridad de los ciudadanos y las empresas en el ciberespacio.»

Y para ello, la Comisión establece tres acciones:

1. *Reforzar la capacidad judicial y policial necesaria para la lucha contra el cibercrimen,* principalmente mediante el establecimiento de un centro de cibercrimen europeo que sirva de interfaz entre los Equipo de Respuesta de Emergencia Informática (CERT) nacionales de los Estados miembros.
2. *Trabajar con la industria para proteger a los ciudadanos mediante la formación y concienciación* acerca de: protección de la privacidad en la Red; detección y denuncia de actividades de acoso a menores, suplantación de identidad y sitios *web* falsos; instalación de antivirus y cortafuegos; gestión de nombres de usuario y contraseñas, etc. Dentro de esta línea de acción también recomienda reforzar la cooperación entre los sectores público y privado a escala europea a través de la Asociación Público-Privada Paneuropea de Resiliencia (EP3R). Esta asociación –continúa– debería seguir desarrollando medidas y herramientas innovadoras para mejorar la seguridad, y la resiliencia

(6) Estrategia de Seguridad Interior de la Unión Europea: «Hacia un modelo europeo de seguridad», marzo de 2010, en: *http://www.consilium.europa.eu/uedocs/cms_data/librairie/PDF/QC3010313ESC.pdf*

(7) *The EU Internal Security Strategy in Action: Five steps towards a more secure Europe,* Bruselas, 22 de noviembre de 2010. COM(2010) 673 final, en: *http://ec.europa.eu/commission_2010-2014/malmstrom/archive/internal_security_strategy_in_action_en.pdf*

de la Red y las infraestructuras de información, especialmente las críticas. Asimismo, debería enlazar con otros actores internacionales para reforzar la gestión de las amenazas cibernéticas.

3. *Mejorar la capacidad para hacer frente a los ciberataques*: en esta línea sería necesario adoptar una serie de medidas para mejorar la prevención, la detección y la reacción rápida en caso de ataques cibernéticos. Así, en primer lugar, cada uno de los Estados miembros y las propias instituciones de la Unión Europea deberían disponer, a más tardar en el año 2012, de unos CERT que funcionen adecuadamente. Es importante que, una vez establecidos, todos los CERT y las autoridades policiales cooperen en la prevención y la reacción ante los ciberataques. En segundo lugar, los Estados miembros deberían interconectar sus CERT gubernamentales para mejorar la preparación de Europa ante un ataque cibernético, para lo cual deberá desarrollarse –con el apoyo de la Comisión y de ENISA– un Sistema Europeo de Intercambio de Información y Alerta (EISAS). En tercer lugar, los Estados miembros —conjuntamente con ENISA— deberían desarrollar planes nacionales con urgencia y realizar regularmente ejercicios nacionales y europeos de reacción a los incidentes y de recuperación tras catástrofes. ENISA prestará su apoyo a estas acciones con el objetivo de elevar los niveles de los CERT en Europa.

En el cumplimiento de este Plan de Acción se basa en gran medida en el desarrollo con éxito de la ambiciosa Agenda Digital para Europa (8), una de las siete iniciativas surgida de la Estrategia Europa del año 2020 que la Comisión Europea ha lanzado con el objetivo de salir de la crisis y preparar la economía europea para los retos de la próxima década. En concreto, la meta que persigue la Agenda Digital para Europa —según reza en su introducción— es producir beneficios económicos y sociales sostenibles a través de la implantación de un mercado digital único basado en aplicaciones interoperables soportadas por una Internet rápida ó ultrarrápida. Concretamente persigue maximizar el potencial de desarrollo económico y social que proporcionan las Tecnologías de la Información y las Comunicaciones (TIC) y, muy especialmente, Internet. Así, según el Documento, el sector de las TIC concentra de manera directa el 5% del producto interior bruto europeo, ello sin contar su influencia en el creci-

(8) *A Digital Agenda for Europe*, Bruselas, 19 de mayo de 2010, COM(2010) 245, en: *http://ec.europa.eu/information_society/digital-agenda/documents/digital-agenda-communication-en.pdf*

miento y la productividad de otros sectores económicos y sociales donde juega un papel dinamizador y capacitador de primera magnitud, ya que altera sustancialmente el modo en que las personas se relacionan y hacen negocios entre sí. El gran potencial de las TIC puede verse hecho realidad a través de la estimulación de un «círculo vicioso» consistente en la puesta a disposición de los usuarios de Internet de unos servicios y unos contenidos atractivos soportados por un entorno de red interoperable y sin fronteras. Esto estimulará la demanda de mayores anchos de banda, lo que a su vez sustentará las inversiones en infraestructuras de red cada vez más rápidas y capaces. La implantación de redes más rápidas y capaces, a su vez abre el camino para la explotación de servicios innovadores y contenidos más atractivos, que requerirán velocidades más altas.

Pero para que este «círculo vicioso» funcione correctamente es necesario un entorno empresarial que estimule la inversión y la actividad emprendedora. Además esta suerte de «cuento de la lechera» de la era cibernética debe sortear otros obstáculos que –según la propia Agenda Digital para Europa– son la causa del retraso europeo frente a sus socios y también competidores industriales. Así, para muchos ciudadanos europeos resulta frustrante que el mercado único –esencia constitutiva de la Unión Europea– sea todavía una realidad incompleta en su faceta digital. La consecuencia práctica es que hoy en día, debido a la ausencia de oferta y a la fragmentación de los mercados europeos, hay cuatro veces más descargas de música en Estados Unidos que en la Unión Europea. Asimismo y sorprendentemente –expone la Agenda–, el 30% de los ciudadanos de la Unión Europea nunca ha utilizado Internet. Por si esto fuera poco, la Unión Europea cuenta con tan sólo un 1% de penetración en cuanto a redes de alta velocidad basadas en fibra óptica, mientras que Japón se sitúa en un 12% y Corea del Sur en un 15%. En la misma línea, el gasto comunitario en investigación y desarrollo en el sector de las TIC es un 40% del estadounidense.

En este sentido, la Comisión Europea, basándose en la Declaración de Granada (9) y en la resolución del Parlamento Europeo (10), ha identifica-

(9) *Granada Ministerial Declaration on the European Digital Agenda: Agreed*, 19 de abril de 2001, en: *http://www.eu2010.es/export/sites/presidencia/comun/descargas/Ministerios/en_declaracion_granada.pdf*

(10) El Parlamento Europeo hizo un llamamiento para que los ciudadanos europeos tengan acceso a las nuevas tecnologías digitales, incluyendo Internet de banda ancha,

do siete obstáculos principales para alcanzar su objetivo de maximizar el potencial de desarrollo económico y social que proporcionan las TIC. Estos siete obstáculos –recogidos en la Agenda Digital para Europa– son:

1. *Fragmentación del mercado electrónico*: Europa lejos de presentar un mercado electrónico único, es todavía un conjunto de mercados electrónicos; cada país tiene el suyo.
2. *Falta de interoperabilidad*: las carencias en estandarización y en contratación y coordinación entre autoridades públicas, dificultan que los servicios digitales y los diferentes dispositivos utilizados por los europeos puedan «interoperar» como sería deseable.
3. *El incremento de la cibercriminalidad y la falta de confianza en la Red*: los europeos no se involucrarán en nuevas y más complejas actividades en Internet, a menos que sientan que pueden confiar plenamente en la Red. Por tanto, Europa debe hacer frente y desarrollar mecanismos de respuesta contra el aumento de nuevas formas de delincuencia en Internet, que van desde el abuso de menores a la suplantación de identidad y los ataques cibernéticos.
4. *Escasez de las inversiones en infraestructuras de Red*: se deben proporcionar los incentivos adecuados para estimular la inversión privada, complementada por inversiones públicas bien orientadas –sin volver a los tiempos del monopolio–, así como mejorar la asignación de espectro.
5. *Deficiencias en los esfuerzos en Investigación y Desarrollo (I+D)*: también fragmentados a nivel nacional, se debe ir hacia infraestructuras comunes de investigación y *clusters* de innovación y hacia el desarrollo de estándares abiertos para nuevas aplicaciones y servicios.
6. *Escasez de profesionales bien formados y de conocimientos a nivel general en el campo de las TIC*: carencias que están excluyendo a muchos ciudadanos de la sociedad digital y, por tanto, del mercado de trabajo, limitando así el efecto multiplicador de las TIC sobre el crecimiento económico y sobre el incremento de la productividad.

---

así como la formación y conocimientos necesarios para comprender los contenidos y utilizar estas tecnologías correctamente. La resolución también hizo hincapié en que los usuarios deberían poder acceder libremente a los contenidos y servicios públicos a través de Internet en toda la Unión Europea. También subrayó la necesidad de que los usuarios de Internet conozcan sus derechos y la necesidad de dotarse de un marco jurídico claro para proteger estos derechos, en: *http://europa.eu/rapid/pressReleasesAction.do?reference=IP/10/538&format=HTML&aged=0&language=EN&guiLanguage=en*

7. *Oportunidades perdidas para catalizar el cambio social*: al aprovechar el potencial de las TIC, Europa podría abordar mucho mejor algunos de sus problemas sociales más graves, como el cambio climático; el envejecimiento de la población y el consiguiente aumento de los costes del sistema sanitario; el desarrollo de servicios públicos más eficaces y la integración de personas con discapacidad; la digitalización patrimonio cultural de Europa y su ulterior puesta a disposición de las generaciones presentes y futuras; entre otros.

Para enfrentarse a estos siete inconvenientes la Agenda Digital para Europa se marca ocho áreas de actuación prioritaria; las siete primeras coinciden con las siete áreas problemáticas descritas, mientras que en la octava –de carácter transversal y, por tanto, con presencia en las siete anteriores– explora los aspectos internacionales del reto planteado. Todas ellas se conocen como los pilares de la Agenda Digital para Europa. En beneficio de la concreción y limitándonos al ámbito de la ciberseguridad en el contexto internacional, en este capítulo nos centraremos en el tercer y octavo pilar, la seguridad y confianza en la Red y su dimensión internacional.

En el terreno de la seguridad y confianza en Internet, además de la ya mencionada Estrategia Europea de Seguridad aprobada durante la Presidencia española (11) y el ulterior plan de acción cuatrienal (12) que contempla medidas específicas relativas a la lucha contra el cibercrimen; la Agenda dispone –entre otras medidas– que a partir del año 2010, la Comisión Europea deberá realizar ejercicios para mejorar la capacidad de respuesta de las instituciones europeas y de los Estados miembros frente a eventuales ataques cibernéticos a escala paneuropea. Aquí la Agenda recoge el espíritu y la letra de la Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones sobre Protección de Infraestructuras de Información Críticas, CIIP *(Critical Information Infrastructures Protection)* (13).

---

(11) Estrategia de Seguridad Interior de la Unión Europea: «Hacia un modelo europeo de seguridad», marzo de 2010, en: *http://www.consilium.europa.eu/uedocs/cms_data/librairie/PDF/QC3010313ESC.pdf*

(12) *The EU Internal Security Strategy in Action: Five steps towards a more secure Europe,* Bruselas, 22 de noviembre de 2010, COM(2010) 673 final, en: *http://ec.europa.eu/commission_2010-2014/malmstrom/archive/internal_security_strategy_in_action_en.pdf*

(13) *Communication from the Commission to the European Parliament… on Critical Information Infrastructure Protection «Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience.»* COM/2009/0149 final, Comisión Europea, 2009.

En este sentido, el 4 de noviembre de 2010 tuvo lugar el ejercicio *Cyber Europe*, primer simulacro de ciberataque a nivel paneuropeo en el que se recreó una situación en la que ciudadanos, empresas e instituciones públicas experimentaron dificultades para acceder a servicios esenciales en Internet. Organizado por ENISA en coordinación con los Estados miembros y con apoyo del Centro Común de Investigación de la Comisión Europea, JRC *(Joint Research Centre)* (14), contó con la participación de todos los Estados miembros de la Unión así como con Islandia, Noruega y Suiza.

El simulacro se ambientó en un escenario de conectividad degradada en el que todos los países se fueron enfrentando a problemas de acceso a la Red crecientes, viéndose forzados a cooperar entre ellos para ofrecer una respuesta conjunta y evitar la pérdida completa de conectividad. En resumidas cuentas, se trató de un ejercicio de CIIP cuyo objetivo consistía en fomentar la confianza entre los participantes y en probar la red de contactos, los mecanismos y los procedimientos de comunicación en caso de un ciberataque real a gran escala. Podemos afirmar por tanto, que el ejercicio buscaba establecer una comunicación fluida entre instituciones dentro de cada Estado y entre instituciones de Estados diferentes, así como de todas ellas con las instituciones europeas.

El pasado mes de abril de 2011, ENISA hizo público el informe final del ejercicio (15) basado en el juicio crítico celebrado a su conclusión y en los posteriores informes rendidos por los estados miembros. En él se valora, por una parte, la validez del ejercicio en sí y del escenario propuesto; y por otra, la consecución de los objetivos perseguidos. La principal conclusión extraída la constituye el hecho de que para el 95% de los Estados miembros, el simulacro supuso una eficaz medida de fomento

(14) Organismo de la Comisión Europea de nivel Dirección General cuya misión consiste en proporcionar apoyo científico y técnico para la concepción, desarrollo, implementación y seguimiento de las políticas de la Unión Europea. Dentro del JRC, se encuentra el Instituto de Prospectiva Tecnológica (IPTS) con sede en Sevilla. El IPTS promueve una mejor comprensión de la relación entre tecnología, economía y sociedad. La misión del IPTS, se concentra en las políticas comunitarias que entrañen una dimensión tanto socioeconómica como científico-tecnológica, Centro de Investigación Común de la Comisión Europea.

(15) *Cyber Europe 2010-Evaluation Report. Recommendations and Lessons Identified*, ENISA, en: *http://www.enisa.europa.eu/act/res/cyber-europe-2010/cyber-europe-2010-report/at_download/file*

de la confianza entre los participantes y, por tanto, el objetivo de mejorar la comunicación entre ellos también se alcanzó.

Decíamos antes que la dimensión internacional de la Agenda es transversal a los demás pilares; así, se propone hacer de Europa un centro neurálgico del crecimiento inteligente, sostenible e incluyente y reconoce que la lucha contra las crecientes amenazas a la ciberseguridad debe desarrollarse en un contexto internacional. En este contexto, la Agenda persigue promover la internacionalización de la gobernanza de Internet y la cooperación mundial para mantener la fiabilidad de la Red de redes, todo ello desde una aproximación multilateral. Para ello la Comisión está considerando su apoyo a la financiación del Foro para la Gobernanza de Internet desde este mismo año (2011). También plantea la Agenda trabajar con terceros países para mejorar las condiciones del comercio electrónico internacional de bienes y servicios, teniendo en cuenta los derechos de propiedad intelectual. En la misma línea, el Consejo Europeo ha pedido a la Comisión que promueva la actualización del Acuerdo Tecnológico Internacional (16) de 1996 –en el seno de la Organización Mundial del Comercio– de forma que se eliminen los obstáculos no arancelarios al comercio electrónico y se incluya a los principales productores de las TIC que aún están fuera del Acuerdo, además de aquellos nuevos productos en línea con la evolución experimentada desde su firma en el año 1996.

Pero la Agenda Digital para Europa es además, un Documento vivo; así los días 16 y 17 de junio de 2011 tuvo lugar en Bruselas la I Asamblea sobre la Agenda Digital para Europa. En ella se desarrollaron hasta 24 talleres diferentes (17). De nuevo en beneficio de la concreción nos centraremos tan sólo en uno de ellos; el que lleva por título: *Ciberseguridad: barreras e incentivos*. Con el objetivo invitar a los Estados miembros, el sector privado y representantes del mundo académico a debatir sobre los actuales obstáculos a la inversión y a la participación en actividades y eventos de fomento de la ciberseguridad, la sesión también abordó los posibles incentivos económicos y normativos necesarios para que tanto el sector público como el privado ofrezcan un mayor nivel de seguridad en la Red.

---

(16) *Ministerial Declaration on Trade in Information Technology Products,* Singapur, 13 de diciembre de 1996, en: *http://www.wto.org/english/docs_e/legal_e/itadec_e.pdf*

(17) Resultado de los talleres, disponible en: *http://ec.europa.eu/information_society/events/cf/daa11/workshop-results.cfm*

Las opiniones vertidas durante el taller, confirmaron la utilidad de los partenariados público-privados en el área de la seguridad cibernética, aspecto que fue ilustrado con varios casos de éxito; también se expreso la necesidad de que los sectores público y privado profundicen aún más en el debate sobre los posibles incentivos a la inversión en ciberseguridad en el seno de la Unión Europea, ya que –entre otros problemas– a menudo las organizaciones que están en condiciones de mitigar los riesgos no son necesariamente las mismas que se beneficiarán de su actuación; igualmente, la necesidad de una mejor coordinación y un mayor intercambio de información entre los proveedores de Internet y las Administraciones en la lucha contra los *botnets* (18), apareció como un tema de interés prioritario para futuras discusiones. Finalmente –como no podía ser de otra manera– se llegó a la conclusión de que la Unión Europea sigue siendo uno de los actores clave en seguridad cibernética global, y como tal, debe seguir contribuyendo en el debate a escala internacional, con el fin de definir y defender sus propias prioridades.

Esta asamblea ha estado precedida por la celebración en los Estados miembros de seminarios divulgativos de la Agenda Digital para Europa. Así, por ejemplo, los días 4 y 5 de octubre de 2010, organizado por la Representación Permanente de la Comisión Europea en España, tuvo lugar en Madrid un seminario en el que –en lo referente a las posibles mejoras a la seguridad en Internet– el jefe adjunto de la Unidad de Internet, Redes y Seguridad de la Información de la Dirección General de la Sociedad de la Información de la Comisión Europea (DG INFSO), Andrea Servida, anunció que la Comisión Europea en el año 2013 propondrá reglas jurisdiccionales sobre el ciberespacio a nivel europeo e internacional. Por su parte, Jorge López Hernández-Ardieta, de la División de Seguridad de INDRA y profesor de la Universidad Carlos III de Madrid, apuntó a la gestión de la identidad de los usuarios como una de las principales causas de su falta de confianza en Internet, por lo cual se debería implantar un «ecosistema» de identidad electrónica europea. Por último, Francisco García Morán, director general de Informática de la Comisión Europea (DIGIT), declaró que a lo largo del año 2011 los Estados miembros debe-

(18) *Botnet*: conjunto de ordenadores que han sido infectados con un tipo de *software* malicioso, con funcionalidad de puerta trasera *(backdoor),* que permite al atacante controlar dichas maquinas sin tener acceso físico a ellas y sin el conocimiento del propietario, en: *http://cert.inteco.es/Formacion/Amenazas/botnets/*

rían acordar un catálogo común de servicios electrónicos transfronterizos que respondan a necesidades bien definidas (19).

Como conclusión, la Unión Europea, ese «gigante económico, enano político y gusano militar», con su Agenda Digital para Europa como Documento maestro, ha diseñado dentro de sus competencias, una robusta estrategia para el ciberespacio centrada puramente en el crecimiento económico y sociocultural que lleva aparejada la expansión de las TIC en general y de Internet en particular, pero su aplicación más allá de ciertos estímulos financieros que puedan salir de las arcas europeas, corresponderá a quien tiene los instrumentos para ello: los Estados miembros… paradójico en un ciberespacio que –según decíamos– demanda un enfoque internacional.

### LA ORGANIZACIÓN PARA LA COOPERACIÓN Y EL DESARROLLO ECONÓMICO (OCDE)

Pionera en abordar la solidez de los CIIP entre sus Estados miembros (20), dentro del pilar de gestión de riesgos de su *International Futures Programme* (21), recientemente ha desarrollado el proyecto denominado *Future Global Shocks* del que forma parte el amplio Informe titulado *Cybersecurity risks and counter-measures* (22).

En el proyecto *Future Global Shocks*, expertos de los sectores público y privado exploran cómo incrementar la resiliencia ante futuras conmociones *(shocks)* a escala global. El proyecto busca ofrecer a los gobernantes diversas opciones para mejorar su capacidad de identificar, anticiparse y controlar los grandes desastres, así como contener y mitigar sus efectos. Además el proyecto reconoce que estas conmociones globales pueden brindar oportunidades de progreso, no sólo consecuencias negativas. El informe final se apoyará en varios informes sectoriales sobre, entre otros, los riesgos financieros sistémicos, pandemias, escapes tóxicos, condiciones meteorológicas o geológicas duraderas que interrumpan o

(19) Seminario Agenda Digital para Europa, Madrid, 4 y 5 de octubre de 2010, Informe interno de la representación de la Comisión Europea en España.

(20) OECD (2007: «Development of Policies for Protection of Critical Information Infrastructures», *OECD Digital Economy Papers,* número 130.doi: 10.1787/231008575813

(21) En: *http://www.oecd.org/department/0,3355,en_2649_33707_1_1_1_1_1,00.html*

(22) *Cybersecurity risks and counter-measures, OECD Study, Peter Sommer and Ian Brown Reducing Systemic Cybersecurity Risk,* enero de 2011.

perturben el transporte internacional, revueltas sociales y, el ya citado, sobre riesgos cibernéticos.

Aparte de recomendar a los países que desarrollen estrategias de ciberseguridad adaptadas a las necesidades de todos los ciudadanos y no sólo a las de la Administración Central; expresar la necesidad apoyar con fondos los foros internacionales de CERT; animar a sus Estados miembros a que ratifiquen la Convención de Budapest sobre el Cibercrimen y Desaconsejar la Desconexión de Internet como atajo para solucionar una crisis; la principal conclusión del Informe sobre riesgos cibernéticos podría ser el hecho de que pocos «cibersucesos» tendrían la capacidad de provocar una conmoción global. En esta misma línea –según el Informe– sería improbable la ocurrencia de una verdadera ciberguerra, si bien no descarta la utilización de ciberarmas –virus, troyanos, *botnets*, etc.– como multiplicadores de fuerza junto a armas convencionales en el contexto de un conflicto, de hecho ya lo vimos en el caso de la invasión rusa de Georgia en el año 2008.

Por último, en este sentido –según los autores– ya que la mayoría de los objetivos de un ciberataque serían civiles, el papel de las Fuerzas Armadas se limitaría a proteger sus propios sistemas y al eventual desarrollo de capacidades ofensivas.

### LA ORGANIZACIÓN DE NACIONES UNIDAS (ONU) Y LA UNIÓN INTERNACIONAL DE TELECOMUNICACIONES (UIT): LAS CUMBRES MUNDIALES DE LA SOCIEDAD DE LA INFORMACIÓN (CMSI) Y EL FORO PARA EL GOBIERNO DE INTERNET (IGF)

Pero si hemos afirmado el carácter global del ciberespacio y de su seguridad, nuestro tratamiento de las aproximaciones internacionales no podía limitarse a las iniciativas regionales de nuestro entorno, por importantes y ambiciosas que estas fueran.

En este contexto la principal organización global, la ONU, y la UIT, su Agencia especializada en las TIC, vienen jugando un papel de relevancia indiscutible, sobre todo desde que en el año 2000, en la Declaración del Milenio (23), la Asamblea General de la ONU, respaldase la declaración ministerial del Comité Económico y Social del año 2000 (24) e incluyera

(23) Resolución A/RES/55/2, aprobada el 18 de septiembre de 2000, Declaración del Milenio.

(24) ECOSOC 2000: *Ministerial Declaration: Development and international cooperation in the twenty-first century: the role of information technology in the context of a knowl-*

entre sus medidas para la erradicación de la pobreza la de velar por que todos puedan aprovechar los beneficios de las nuevas tecnologías, en particular de las tecnologías de la información y de las comunicaciones.

Ya en el año 1998, antes de la Declaración del Milenio, la UIT en su conferencia de plenipotenciarios (25) de Minneapolis (Estados Unidos.) resolvió (26) encargar al secretario general de la UIT que consultara con el Comité Administrativo de Coordinación de Naciones Unidas (CAC), la posible celebración de una CMSI que debiera tener lugar antes de la siguiente conferencia de plenipotenciarios. También pidió al secretario general que informara al Consejo de la UIT (27) sobre los resultados de esta consulta. Asimismo encargó al Consejo que, si la consulta resultaba favorable, pidiera al secretario general de la UIT que se ocupase de la coordinación con las demás organizaciones internacionales y con los diferentes actores (Estados miembros, sectores afectados, etc.) y, finalmente; que informase acerca de los resultados de la CMSI en el transcurso de la siguiente conferencia de plenipotenciarios.

Consecuentemente el Consejo de la UIT, tras ser informado por su secretario general de la muy favorable acogida a la celebración de la CMSI por parte de los diferentes actores implicados, resuelve (28) encargarle la preparación y coordinación general de la cumbre, incluyendo la propuesta de temas a tratar y la celebración de las reuniones preparatorias que fueran necesarias.

Para dar cumplimiento al encargo, el secretario general de la UIT presenta al CAC un Plan de Acción que lleva implícita la creación de un Comité

---

*edge-based global economy. Economic and Social Council. Substantive session of 2000.* Nueva York, 5 de julio y 1 de agosto de 2000, Agenda *item*2.

(25) La Conferencia de Plenipotenciarios constituye el órgano supremo de la UIT y en él los Estados miembros deciden el papel que desempeñará la Organización en el futuro y su influencia en el desarrollo de las TIC en el mundo. Celebrada cada cuatro años, en ella se establece la política general de la UIT, se adoptan planes estratégicos y financieros cuatrienales y se eligen los altos cargos de la Organización y los miembros del Consejo, en: *http://www.itu.int/plenipotentiary/2010/about-es.html*

(26) Resolución 73. Conferencia de Plenipotenciarios de la UIT, Minneapolis, 1998.

(27) El Consejo de la UIT lo integran el 25% del total de Estados miembros. En el intervalo entre conferencias de plenipotenciarios trata asuntos generales de política de las telecomunicaciones para garantizar que las actividades, políticas y estrategias de la Unión Europea se actualizan en línea con un entorno tecnológico dinámico y en rápida evolución, en: *http://www.itu.int/council/index-es.html*

(28) Resolución 1158, Consejo de la UIT, 2000.

Organizador de Alto Nivel de la Cumbre (COAN), presidido por el secretario general de la UIT y compuesto por los jefes de los organismos de Naciones Unidas y de otras organizaciones internacionales interesados en participar en el proceso de gestación de la cumbre.

Posteriormente, en el año 2001, el Consejo de la UIT aprueba (29) el marco general del propuesto por su secretario general, según el cual la cumbre ha de organizarse en dos fases, ambas bajo los auspicios del secretario general de Naciones Unidas, asumiendo la UIT un papel rector en su preparación, en coordinación con otros organismos de Naciones Unidas y de otras organizaciones internacionales interesadas, y con los países anfitriones, a saber, Suiza y Túnez para la primera y segunda fase respectivamente.

Pero el apoyo político necesario para la celebración de la CMSI, llegaría de la mano de la Asamblea General de Naciones Unidas cuando en diciembre de ese mismo año respaldó (30) el marco de la CMSI, aprobado por el Consejo de la UIT a propuesta de su secretario general, invitando a la UIT a asumir la función administrativa principal de la Secretaría Ejecutiva de la cumbre y su proceso preparatorio. Igualmente invitó a los gobiernos a participar activamente en el proceso preparatorio y a enviar a la CMSI a representantes del más alto nivel. Así finalmente –no sin antes requerir cierto impulso adicional y ajustes organizativos tanto desde el Consejo como desde la Asamblea de Plenipotenciarios de la UIT (31)–, la primera fase de la cumbre se celebraría en Ginebra del 10 al 12 de diciembre de 2003 y la segunda, en Túnez del 16 al 18 de noviembre de 2005.

Al término de la primera fase se produjo una declaración de principios conocida como Declaración de Ginebra (32). En ella se abordan once aspectos específicos merecedores de atención. Entre ellos destacan los incentivos a la necesaria implantación de infraestructuras de información y comunicaciones adecuadas; las medidas de fomento de la confianza y

(29) Resolución 1179, Consejo de la UIT, 2001.
(30) Resolución A/RES/56/183, aprobada el 21 de diciembre de 2001: primera resolución sobre la CMSI adoptada por la Asamblea General.
(31) Resoluciones 1196 (2002) y 1207 (2003) del Consejo de la UIT y resoluciones PLEN/1 y PLEN/7 de la Conferencia de Plenipotenciarios en Marraquech, 2002 y 2003 respectivamente.
(32) Documento WSIS-03/GENEVA/4-S,12 de mayo de 2004, Declaración de Principios, Construir la Sociedad de la Información: «Un desafío global para el Nuevo Milenio».

seguridad en la utilización de las TIC, evitando que se utilicen para fines criminales o terroristas y abordando los problemas de la ciberseguridad y el correo no deseado *(spam)* en los planos nacional e internacional; la creación de un entorno propicio a nivel nacional e internacional que incluya la intervención gubernamental para corregir los fallos del mercado, mantener una competencia leal, atraer inversiones, intensificar el desarrollo de infraestructura y aplicaciones de las TIC, aumentar al máximo los beneficios económicos y sociales y atender a las prioridades nacionales, y; el aprovechamiento pleno de las oportunidades que ofrecen las TIC para alcanzar los objetivos de desarrollo convenidos internacionalmente, incluidos los que figuran en la Declaración del Milenio.

El subsiguiente Plan de Acción de Ginebra (33), que traduce la Declaración de Principios en once líneas de acción concretas para alcanzar los objetivos de desarrollo acordados a nivel internacional, con inclusión de los consignados en la Declaración del Milenio, el Consenso de Monterrey (34) y la Declaración y el Plan de Aplicación de Johannesburgo (35). De entre estas líneas de acción nos centraremos en la quinta, la creación de confianza y seguridad en la utilización de las TIC, y en la undécima, la cooperación internacional y regional.

En cuanto a la quinta línea de acción, establece que el de la confianza y la seguridad, es uno de los pilares más importantes de la Sociedad de la Información, y propone:

1. Propiciar la cooperación entre los gobiernos dentro de Naciones Unidas y con todas las partes interesadas en otros foros apropiados, para aumentar la confianza del usuario y proteger los datos y la integridad de la Red.
2. Los gobiernos, en cooperación con el sector privado, deben prevenir, detectar, y responder a la ciberdelincuencia y el uso indebido de las TIC, definiendo directrices que tengan en cuenta los esfuerzos existentes en estos ámbitos; estudiando una legislación que permita investigar y juzgar efectivamente la utilización indebida; promoviendo esfuerzos efectivos de asistencia mutua; reforzando el apoyo institucional a nivel internacional para la prevención, detección

(33) Documento WSIS-03/GENEVA/5-S, 12 de mayo de 2004, Plan de Acción.
(34) Resultado de la Conferencia Internacional sobre la Financiación para el Desarrollo, Monterrey (México), 18-22 de marzo de 2002.
(35) Declaración al término de la Cumbre Mundial sobre el Desarrollo Sostenible, Johannesburgo (Suráfrica), 2- 4 de septiembre de 2002.

y recuperación de estos incidentes; y alentando la educación y la sensibilización.

3. Los gobiernos y otros actores interesados deben fomentar activamente la educación y la sensibilización de los usuarios sobre la privacidad en línea y los medios para su protección.
4. Tomar medidas apropiadas contra el envío masivo de correos electrónicos no solicitados *(spam)* a nivel nacional e internacional.
5. Fomentar una evaluación interna de la legislación nacional con miras a superar cualquier obstáculo al uso efectivo de documentos y transacciones electrónicas, incluido también los medios electrónicos de autenticación.
6. Seguir fortaleciendo el marco de confianza y seguridad con iniciativas complementarias y de apoyo mutuo en los ámbitos de la seguridad en el uso de las TIC, con iniciativas o directrices sobre el derecho a la privacidad y la protección de los datos y también de los consumidores.
7. Compartir buenas prácticas en el ámbito de la seguridad de la información y la seguridad de las redes y propiciar su utilización por todas las partes interesadas.
8. Invitar a los países interesados a establecer puntos de contacto para intervenir y resolver incidentes en tiempo real, y desarrollar una red cooperativa entre estos puntos de contacto de forma que se comparta información y también tecnologías para intervenir en caso de incidentes.
9. Impulsar el desarrollo de nuevas aplicaciones seguras y fiables que faciliten las transacciones en línea.
10. Animar a los países interesados a que contribuyan activamente en las actividades en curso de Naciones Unidas tendentes a crear confianza y seguridad en la utilización de las TIC.

Asimismo asegura que la cooperación internacional entre todas las partes interesadas es fundamental para la aplicación del Plan de Acción y que ha de reforzarse con miras a promover el acceso universal a las TIC y cerrar la llamada «brecha digital», entre países ricos y pobres. Para ello propone las siguientes actuaciones:

1. Los gobiernos de los países en desarrollo deben elevar la prioridad relativa que se asigna a los proyectos de las TIC en las solicitudes de cooperación y asistencia internacionales para proyectos de desarrollo de infraestructura que formulen a los países desarrollados y a las organizaciones financieras internacionales.

2. En el contexto del llamado Pacto Mundial de Naciones Unidas (36) y sobre la base de la Declaración del Milenio, fomentar el establecimiento de asociaciones público-privadas para el desarrollo de proyectos y apoyarse en ellas, enfatizando la utilización de las TIC para el desarrollo.
3. Invitar a las organizaciones internacionales y regionales a que utilicen las TIC en sus programas de trabajo y a que ayuden en todos los niveles a los países en desarrollo a participar en la preparación y aplicación de planes de acción nacionales destinados a apoyar la consecución de las metas indicadas en la declaración de principios y en el Plan de Acción, teniendo en cuenta la importancia de las iniciativas regionales.

Para la facilitar la materialización de estas líneas de acción —principalmente en los países pobres— el Plan (de Acción) establece la llamada Agenda de Solidaridad Digital (37), que tiene por objeto fijar las condiciones necesarias para movilizar los recursos humanos, financieros y tecnológicos que permitan incluir a todos los hombres y mujeres en la Sociedad de la Información, entre los que se encuentra el establecimiento de un Fondo de Solidaridad Digital. La Agenda incluye asimismo, una afirmación en aquel momento novedosa, por cuanto que afirma que las ciberestrategias nacionales deben constituir parte integrante de los planes de desarrollo nacionales, incluyendo las estrategias de reducción de la pobreza, para lo que –recuerda la Agenda– deben aplicarse las medidas destinadas a la movilización de recursos para ayuda oficial al desarrollo acordadas en el Consenso de Monterrey (38).

A continuación, el Plan de Acción recoge la necesidad de elaborar un plan realista de evaluación de resultados y establecimiento de referencias (tanto cualitativas como cuantitativas) en el plano internacional, a

(36) En el año 1999, en el Foro Económico Mundial de Davos (Suiza), el secretario general propuso un «Pacto Mundial» entre Naciones Unidas y el mundo de los negocios. El Pacto Mundial pide a las empresas que hagan suyos, apoyen y lleven a la práctica un conjunto de valores fundamentales en materia de derechos humanos, normas laborales, medio ambiente y lucha contra la corrupción (ONU, 2007).

(37) La Agenda de Solidaridad Digital no es un documento aparte sino que está integrada en el «Plan de Acción de Ginebra».

(38) En él se insta a los países desarrollados que aún no lo han hecho, a iniciar actividades concretas para destinar el 0,7% de su Producto Nacional Bruto (PNB) a la Ayuda Oficial al Desarrollo para los países en vías de desarrollo y entre el 0,15 y el 0,20% de su PNB a los países menos adelantados.

través de indicadores estadísticos e investigaciones comparables, para dar seguimiento a la aplicación de los objetivos y metas marcados, teniendo en cuenta las circunstancias específicas de cada país.

Finalmente, concluye que la segunda fase de la CMSI deberá abordar la elaboración de documentos concretos que contribuyan a consolidar el proceso de construcción de una Sociedad de la Información Global y a cerrar la brecha digital, transformándola en oportunidades digitales. La segunda fase –añade– también deberá monitorizar la aplicación del Plan de Acción de Ginebra a escala nacional, regional e internacional y, en particular, a través del sistema de Naciones Unidas, en el marco de un enfoque integrado y coordinado, que invite a la participación de todas las partes interesadas.

Precisamente en esta segunda fase, celebrada –como decíamos– en Túnez del 16 al 18 de noviembre de 2005, es donde se establecen el llamado Compromiso de Túnez y la conocida como Agenda de Túnez para la Sociedad de la Información. El primero, da testimonio de la voluntad de los asistentes para que las TIC constituyan un instrumento eficaz en la promoción de la paz, la seguridad y la estabilidad, así como en la implantación y consolidación de la democracia, la cohesión social, el buen gobierno y el Estado de Derecho en los planos regional, nacional e internacional, afirmación premonitoria del impulso que Internet daría seis años después a la denominada «primavera árabe».

Asimismo subrayaron los concurrentes que las TIC facilitan el crecimiento económico y la actividad emprendedora; por tanto, el desarrollo de infraestructuras, la formación de expertos, la seguridad de la información y la seguridad y confianza en la Red, resultan determinantes para alcanzar esos objetivos. Además, reconocieron los concurrentes la necesidad de afrontar eficazmente las dificultades y amenazas que representa la utilización de las TIC para fines que no corresponden a los objetivos de mantener la estabilidad y seguridad internacionales y que podrían afectar negativamente a la integridad de la infraestructura dentro de los Estados, en detrimento de su seguridad. Es necesario evitar –concluyen– que se abuse de las tecnologías y de los recursos de la información para fines delictivos y terroristas, respetando siempre los derechos humanos.

La Agenda de Túnez, aunque muy centrada en la movilización de recursos para cerrar la brecha digital entre países ricos y pobres en el marco del Fondo de Solidaridad Digital, también aborda las medidas para

fomentar la confianza de los usuarios en la seguridad de las TIC, para lo cual reafirma la necesidad de continuar promoviendo, desarrollando e implementando en colaboración con todas las partes interesadas una cultura mundial de ciberseguridad, como se indica en la resolución 57/239 de la Asamblea General de Naciones Unidas. Esta cultura requiere tanto la actuación a nivel nacional como la intensificación de la cooperación internacional para fortalecer la seguridad mejorando al mismo tiempo la seguridad de la información, la privacidad y la confidencialidad de los datos personales. Pero la principal iniciativa de la Agenda de Túnez la constituye la solicitud al secretario general de Naciones Unidas para que, en un proceso abierto e integrador, convoque para el segundo trimestre del año 2006 una reunión del nuevo IGF con mandato para:

1. Debatir temas de políticas públicas relativos a los elementos claves de la gobernanza de Internet, con objeto de contribuir a la sostenibilidad, la solidez, la seguridad, la estabilidad y el desarrollo de Internet.
2. Facilitar el diálogo entre organismos que se ocupan de políticas públicas internacionales relacionadas con Internet y estimular el debate sobre temas que no se han incluido en el mandato de organismos existentes.
3. Facilitar la comunicación con las organizaciones intergubernamentales apropiadas y otras instituciones en temas de su competencia.
4. Facilitar el intercambio de información y de buenas prácticas y, en este sentido, aprovechar plenamente las competencias de las comunidades académica, científica y técnica.
5. Aconsejar a todas las partes interesadas, sugiriendo soluciones y medios para que Internet esté al alcance de un mayor número de personas en los países en desarrollo.
6. Fortalecer y mejorar la participación de las partes interesadas en los mecanismos de gobernanza de Internet actuales y/o futuros, en particular los de países en desarrollo.
7. Identificar temas emergentes, exponerlos ante los organismos competentes y el público en general, y, en su caso, formular recomendaciones.
8. Contribuir a la creación de capacidad para la gobernanza de Internet en países en desarrollo, aprovechando lo más posible los conocimientos y las competencias locales.
9. Promover y evaluar permanentemente la materialización de los principios de la CMSI en los procesos de gobernanza de Internet.
10. Debatir temas relativos a los recursos críticos de Internet.

11. Ayudar a encontrar soluciones a los problemas que plantea la utilización correcta o incorrecta de Internet, que son de particular interés para el usuario común.
12. Publicar sus actas.

La reunión inaugural del IGF tuvo lugar –según lo solicitado al secretario general de Naciones Unidas– entre el 30 de octubre y el 2 de noviembre de 2006 en Atenas, bajo el lema «Gobernanza de Internet para el desarrollo» y se centró en cuatro aspectos fundamentales:

1. *Apertura o eliminación de restricciones:* libertad de expresión, libre circulación de la información, las ideas y el conocimiento.
2. *Seguridad:* generación de confianza mediante la colaboración, en particular mediante la protección de los usuarios contra el correo basura, la adquisición fraudulenta de información confidencial *(phishing)* y los virus, a la vez que se protege su privacidad.
3. *Diversidad*: promoción del plurilingüismo, incluyendo los contenidos locales.
4. *Acceso:* disponibilidad de acceso a Internet a precios razonables, incluidas cuestiones como costos de interconexión e interoperabilidad.

A esta reunión inaugural siguieron los encuentros de Río de Janeiro en 2007, Hyderabad (India) en 2008, Sharm El Sheikh (Egipto) en 2009 y Vilna (Lituania) en 2010.

La última reunión del IGF bajo el lema «Internet como catalizador para el cambio: el acceso, desarrollo, las libertades y la innovación», se celebró del 27 al 30 de septiembre de 2011 en Nairobi (Kenia) con un récord de asistencia con respecto a ediciones anteriores, ya que se acreditaron más de 2.000 participantes entre los que se encontraban representantes de 125 países. Entre otros aspectos, se abordó la gestión de los recursos críticos de Internet, así como la seguridad y la privacidad en la Red.

Aunque en un principio la seguridad fue un tema marginal –en beneficio de la financiación– a la hora de abordar la expansión de las TIC en general y de Internet en particular, desde que en el año 2006 se celebraran la conferencia de plenipotenciarios de la UIT, la quinta línea de acción del Plan de Acción de Ginebra –el fomento de la confianza y seguridad en Internet y en las TIC–, se ha convertido en una de las funciones principales de la Unión, asunto que ha abordado en sintonía con la undécima línea de acción, la cooperación internacional y regional. Consecuentemente, el 17 de mayo de 2007, con el objetivo proporcionar un marco desde

el que articular y coordinar la respuesta internacional a los crecientes desafíos a la seguridad cibernética, el 17 de mayo de 2007 la UIT hizo pública su Agenda Global sobre Ciberseguridad, GCA *(Global Cybersecurity Agenda).*

La GCA, bajo la dirección técnica y estratégica del denominado Grupo de Expertos de Alto Nivel, HLEG *(High Level Experts Group)* se sustenta en cinco pilares o áreas de trabajo:

1. *Las medidas legales*: la UIT (39), dentro de su Área de Desarrollo (UIT-D), colabora con los Estados miembros en la comprensión de los aspectos legales de la ciberseguridad con el fin de avanzar hacia la armonización de los marcos legales vigentes para permitir y facilitar la cooperación internacional, a la vez que se promueve la idea de que el establecimiento de una legislación adecuada debe ser parte integral de cualquier estrategia nacional de ciberseguridad. Dentro de este área de trabajo la UIT ha publicado el Documento «El cibercrimen: una guía para los países en desarrollo» que tiene como objetivo ayudar a los países en desarrollo a comprender mejor las implicaciones nacionales e internacionales de las crecientes amenazas cibernéticas y ayudarles en el establecimiento de una base jurídica sólida. Otra de las actuaciones de la UIT en este área consiste en la preparación de un «conjunto de herramientas» o *kit* que los países pueden utilizar para la elaboración de su marco jurídico cibernético y de las leyes que lo desarrollen. El *kit* está destinado a los legisladores, abogados, funcionarios gubernamentales, expertos en políticas, y representantes de la industria, proporcionándoles una terminología y unos modelos legales acordes con los marcos vigentes en los países más avanzados en la materia, de forma que les ayude a avanzar en la armonización global de las leyes de lucha contra el cibercrimen.
2. *Las medidas técnicas y procedimentales*: el Área de Normalización de la UIT (UIT-T) se encuentra en una posición única en el mundo de la estandarización, ya que reúne al sector privado y a los gobiernos con el fin de promover la armonización de las políticas y estándares de seguridad a escala internacional. En este sentido, el denominado Grupo de Estudio 17 (SG-17) del UIT-D, es el principal

(39) «La UIT cuenta con tres ámbitos de actividad principales, organizados en "sectores" que desarrollan su labor a través de conferencias y reuniones» (UIT, 2008). Los tres sectores son: Radiocomunicaciones (UIT-R), Normalización (UIT-T) y Desarrollo de las Telecomunicaciones (UIT-D).

foro global –podríamos afirmar que se trata del grupo líder en este ámbito– de análisis de la seguridad de las telecomunicaciones y de gestión de identidad. El SG-17 es, además, responsable de los estudios relativos a la ciberseguridad, la lucha contra el *spam* y de la coordinación de los trabajos relacionados con la seguridad de todos los grupos de estudio de la UIT-T. Asimismo, el SG-17 publica en su sitio *web* un compendio de recomendaciones y un glosario de definiciones relacionadas con la seguridad. El SG-17 también está trabajando en el fomento de la creación de CERT nacionales, especialmente en los países en vías de desarrollo. Desde el SG-17, se lideró la elaboración de una hoja de ruta para promover la colaboración entre los organismos de normalización internacionales en el desarrollo de nuevos estándares de seguridad que tuvieran en cuenta los estándares vigentes y los trabajos de desarrollo en curso ICT *(Security Standards Roadmap)*. La Hoja de Ruta adquirió su condición de verdadero «esfuerzo global» cuando, en enero de 2007, la ENISA y el Grupo Director de Seguridad de la Información, NISSG *(Network Information Security Steering Group)*, de la *ICT Standards Board* se unieron a la iniciativa.

3. *Las estructuras organizativas*: promoviendo la creación de CERT nacionales y regionales y la comunicación, el intercambio de información y el reconocimiento de credenciales más allá de las fronteras nacionales. Además –y sobre todo– la UIT trabaja con actores públicos y privados en la creación de «partenariados» mixtos como la Asociación Multilateral Internacional contra las Amenazas Cibernéticas, IMPACT *(International Multilateral Partnership against Cyber-Threats)*. La participación de la UIT en IMPACT llega al punto de que la GCA comparte con IMPACT su sede de Cyberjaya (Malasia). En IMPACT se encuadra el Centro de Respuesta Global (GRC), diseñado para ser el principal centro de lucha contra la amenaza cibernética a escala mundial, juega un papel fundamental en la aplicación de la tecnología en la lucha contra las amenazas cibernéticas. Los productos estrella del la GRC son el Sistema de Alerta Temprana de la Red, NEWS *(Network Early Warning System)* y la Plataforma Electrónica Segura de Colaboración entre Expertos, ESCAPE *(Electronically Secure Collaboration Application Platform for Experts)*. NEWS ayuda a los países identificar las ciberamenazas en tiempo real y colabora en el establecimiento de un marco conceptual sobre las medidas a tomar para mitigarlos. ESCAPE, por su parte, es una herramienta electrónica que permite a los

expertos de los diferentes países compartir recursos y colaborar entre sí de forma remota dentro de un entorno seguro y de confianza. Mediante la combinación de recursos y la experiencia de muchos países, a corto plazo ESCAPE permitirá a los países de forma individual y a la comunidad internacional en el plano global, responder rápidamente a las amenazas procedentes del ciberespacio.

4. *La creación de capacidades*: como por ejemplo la Herramienta de Autodiagnóstico de la Ciberseguridad Nacional y de Protección de Infraestructuras Críticas de Información *(ITU National Cybersecurity/ CIIP Self-Assessment Tool)* (40), que constituye una importante iniciativa práctica encaminada a ayudar a los países miembros a desarrollar su propia estrategia de ciberseguridad y a diseñar e implantar su propio sistema de protección de infraestructuras de información críticas. Dentro de este pilar se encuentra también el Conjunto de Herramientas para la Promoción de la Cultura de la Ciberseguridad *(ITU Toolkit for Promoting a Culture of Cybersecurity)* que proporciona una serie de directrices para incrementar la conciencia de ciberseguridad en los países en vías de desarrollo principalmente entre los expertos, consumidores y usuarios de las TIC. Asimismo, la UIT está trabajando en una herramienta, la llamada *Botnet Mitigation Toolkit*, destinada a ayudar principalmente a los países en desarrollo, a hacer frente al creciente problema de los *botnets*.
5. *La cooperación internacional*: además de la ya mencionada iniciativa IMPACT en la que se encuadra el Centro para la Cooperación Internacional en Materia de Políticas *(IMPACT Centre for Policy and International Cooperation)* que colabora con organizaciones como el Consejo de Europa, la OCDE y la Interpol; merecen mención la *ITU Cybersecurity Gateway* (41), destinada a dar a conocer las actuaciones nacionales, regionales y globales en materia de ciberseguridad en todo el mundo, y la iniciativa, COP *(Child Online Protection)*.

Asimismo, la GCA se ha marcado siete Objetivos Estratégicos (OE) cuya consecución recae en una o varias áreas de trabajo de las cinco mencionadas:

– OE1: elaboración de estrategias para el desarrollo de un modelo de legislación sobre ciberdelincuencia que sea de aplicación global y compatible con las medidas legislativas nacionales y regionales.

(40) En: *http://www.itu.int/ITU-D/cyb/cybersecurity/projects/readiness.html*
(41) En: *http://www.itu.int/cybersecurity/gateway/*

– OE2: elaboración de estrategias globales para la creación de estructuras organizativas nacionales y regionales adecuadas y de políticas sobre ciberdelincuencia.
– OE3: desarrollo de una estrategia para el establecimiento de criterios mínimos de seguridad y de esquemas de acreditación de sistemas y de aplicaciones de *hardware* y *software*.
– OE4: desarrollo de estrategias para la creación de un marco global de vigilancia, alerta y respuesta a incidentes, capaz de garantizar la coordinación transfronteriza entre las nuevas iniciativas y las ya existentes.
– OE5: desarrollo de estrategias globales para la creación y aprobación de un sistema de identidad digital genérica y universal y de las estructuras organizativas necesarias para garantizar el reconocimiento de las credenciales digitales a través de las fronteras geográficas.
– OE6: desarrollo de una estrategia mundial para facilitar la creación de capacidades humanas e institucionales que permitan mejorar el conocimiento y el «saber hacer» en todos los sectores y áreas antes mencionadas.
– OE7: propuestas para la elaboración de un marco estratégico global y multilateral de cooperación, diálogo y coordinación en todas las áreas antes mencionadas.

Como conclusión, diremos que, la GCA constituye el instrumento internacional que ha ayudado a la UIT a asumir un papel de liderazgo en ciberseguridad, concretamente a través de la quinta línea de acción de la CMSI «la creación de confianza y seguridad en la utilización de las TIC».

### EL eG-8

Los días 26 y 27 de mayo de 2011 tuvo lugar en la villa normanda de Deauville (Francia) la cumbre del G-8. El presidente Sarkozy en calidad de anfitrión y presidente de turno del G-8 y del G-20, tuvo la iniciativa de organizar un encuentro entre los jefes de Estado o de Gobierno del G-8 y los principales «líderes de Internet», como llamó el presidente a los dirigentes de las empresas convocadas. El encuentro, bautizado como eG-8, contó con la presencia de los principales dirigentes de empresas de Internet francesas y algunos –no todos– conocidos empresarios de éxito estadounidenses. Además nos brindó alguna discusión interesante. Así, al principio del capítulo hemos descrito una conversación entre Zuckerberg y Sarkozy que presumiblemente tuvo lugar en los márgenes este foro y que ilustra muy bien el debate sobre el control de la Red.

Pero el aspecto más importante quizá sea el anuncio efectuado por el presidente francés de que el encuentro entre líderes del G-8 y «líderes de internet» –el eG-8– se repetirá cada año. Puede que las sucesivas ediciones nos brinden avances sobre si la balanza se inclina del lado de Zuckerberg (Internet autorregulada) o de Sarkozy (Internet controlada por los Estados) (42).

### LA ORGANIZACIÓN DEL TRATADO DEL ATLÁNTICO NORTE (OTAN)

Para analizar el rumbo seguido por la OTAN a la hora de enfrentarse a las conmociones que han jalonado el camino de la Organización a lo largo de sus más de 60 años de existencia, resulta muy útil analizar los comunicados de sus cumbres. En el caso concreto del ciberespacio, no hace falta irse muy atrás en la Historia, tan sólo hasta Praga en el año 2002, para encontrar la primera mención a la necesidad de la Alianza de «fortalecer su capacidad para defenderse de los ciberataques». Posteriormente, en la cumbre de Riga de 2006, los jefes de Estado y de Gobierno aliados, en el contexto del incremento de capacidades de las fuerzas aliadas para hacer frente a los nuevos retos y amenazas, acordaron «mejorar la protección de nuestros sistemas de información claves frente los cibertataques». Pero no será hasta la cumbre de Bucarest de 2008 –primera, tras los ataques cibernéticos sufridos por Estonia en el año 2007, pero anterior a la crisis de Georgia– cuando la ciberdefensa sea tratada en mayor profundidad.

En Bucarest se renovó el compromiso aliado de reforzar los sistemas aliados claves frente a los ciberataques y se anunció la reciente aprobación de una política aliada de ciberdefensa, así como la creación de las estructuras necesarias para aplicarla. Entre estas estructuras, advierte la declaración en una suerte de «aviso a los navegantes», se encuentra el establecimiento de la capacidad de prestar asistencia a los aliados que lo soliciten en caso de ser víctimas de un ciberataque.

Tras los anuncios de Bucarest y la posterior crisis de Georgia ese mismo verano, en la siguiente cumbre, Estrasburgo-Kehl en el año 2009, la Alianza comunicó la creación de una Autoridad de Gestión de la Ciberdefensa, CDMA *(Ciberdefence Management Authority)*, la activación del

(42) Gómez de Agreda, Ángel: «e-G8: vuelta a Westfalia», *Revista Atenea,* 8 de junio de 2011, en: *http://www.revistatenea.es/revistaatenea/revista/articulos/GestionNoticias_4876_ESP.asp*

Centro de Excelencia para la Cooperación en Ciberdefensa de Tallin (Estonia) y la mejora de su capacidad de respuesta a incidentes cibernéticos, sobre la cual –aseguraba– se acelerarán los trabajos hasta la obtención de su plena funcionalidad. Asimismo –continuaba la declaración– la ciberdefensa será parte integral de los ejercicios aliados y se reforzarán los vínculos entre la OTAN y sus socios; para lo cual proclamaba haber desarrollado un marco de cooperación contra los ciberataques entre la Organización y sus socios. Asimismo la OTAN reconocía la necesidad de cooperar con otras organizaciones internacionales.

Pero el cambio sustancial llegará tras la cumbre de Lisboa, celebrada en noviembre de 2010. Allí los jefes de Estado y Gobierno de la Alianza aprobaron el nuevo Concepto Estratégico, que eleva los ciberataques a la categoría de amenazas contra la seguridad, estabilidad y prosperidad del área euroatlántica. En este contexto, los jefes de Estado encomendaron al Consejo Atlántico la elaboración de una nueva política de ciberdefensa sobre la base de la del año 2008, así como un Plan de Acción para su implementación. La nueva política de ciberdefensa fue aprobada por los ministros de Defensa aliados en junio de 2011, mientras que el Plan de Acción, Documento detallado con cometidos y actividades concretas a desarrollar por las estructuras de la alianza y por las fuerzas aliadas, sería sancionado en la siguiente reunión ministerial celebrada en octubre, constituyendo un Documento vivo y en constante cambio.

La nueva política clarifica tanto las prioridades de la OTAN como las actuaciones en ciberdefensa, incluyendo las redes a proteger y la forma de hacerlo. Así, su prioridad principal es la protección de las redes propias de la OTAN y el establecimiento de requisitos para la protección las redes nacionales en que la OTAN se apoya para llevar a cabo sus misiones esenciales: defensa colectiva y gestión de crisis. En cuanto a las actuaciones en ciberdefensa, se basan en los principios generales de prevención, capacidad de recuperación y no duplicación de esfuerzos.

En cuanto a la repuesta aliada ante un ciberataque, el Concepto Estratégico aprobado en Lisboa, establece que la OTAN defenderá su territorio y su población contra todas las amenazas, incluyendo la cibernética. En esta misma línea, la nueva política sobre ciberdefensa reitera que toda reacción de defensa colectiva está sujeta a las decisiones del Consejo del Atlántico Norte y que la OTAN mantendrá la necesaria ambigüedad estratégica, así como la debida flexibilidad en la forma de responder a

las crisis que incluyan un componente cibernético. Es de esperar por tanto, que en próximas revisiones de su procedimiento de gestión de crisis, la OTAN integre una nueva dimensión cibernética. La forma en que esta dimensión se integre nos dará una idea del mecanismo de toma de decisiones en el contexto de una «cibercrisis».

Asimismo, tras la aprobación de la nueva política, la OTAN prestará asistencia coordinada si un aliado es víctima de un ataque cibernético. Para ello, va a mejorar los mecanismos de consulta, la alerta temprana, el conocimiento de la situación y el intercambio de información entre los Estados miembros. Para facilitar estas actividades, la OTAN quiere concluir acuerdos, MOU *(Memorandum of Understanding)* entre las autoridades de ciberdefensa de todos los aliados y la Junta de Gestión de la Ciberdefensa de la OTAN, CDMB *(Cyber Defence Management Board)*.

En cuanto a la respuesta a incidentes en la infraestructura de información propia de la OTAN, la Organización dispone de un CERT denominado NCIRC *(NATO Computer Incident Response Capability)* cuya capacidad operativa plena –según lo dispuesto por los jefes de Estado y Gobierno en Lisboa– deberá alcanzarse en el año 2012, centralizando la protección de todas las entidades de la Alianza.

En el ámbito de la cooperación internacional, la nueva política establece que tanto la OTAN como los aliados trabajarán con los socios, las organizaciones internacionales, el mundo académico y el sector privado de forma que se promueva la complementariedad y se evite la duplicación. La OTAN –añade, quizás dejando fuera de este ámbito cooperativo a determinados Estados– adaptará su compromiso internacional con arreglo valores compartidos y enfoques comunes. La colaboración en el ámbito de la defensa cibernética –concluye– podría abarcar actividades como la sensibilización y el intercambio de buenas prácticas.

Por último, las consecuencias prácticas de la aprobación de esta política y de su puesta en práctica una vez aprobado el Plan de Acción, suponen que:

– La OTAN deberá elaborar unos requisitos mínimos para los sistemas de información nacionales críticos para el cumplimiento de las misiones esenciales de la OTAN.
– La OTAN ayudará a los aliados que lo soliciten a alcanzar un nivel mínimo de defensa cibernética que reduzca la vulnerabilidad de su infraestructura crítica nacional.

– Se crea un marco para que los aliados, individualmente puedan ofrecer asistencia a otro aliado o a la Alianza en el caso de un ataque cibernético.
– La ciberdefensa se integrará plenamente en el Proceso de Planeamiento de Defensa Aliado, NDPP *(NATO Defence Planning Process)* que identificará y priorizará las necesidades en este ámbito.
– Las autoridades militares de la OTAN evaluarán la forma de incluir la ciberdefensa en el planeamiento de las operaciones.
– Se definirán los requisitos de ciberdefensa también para las naciones no-OTAN que contribuyen con tropas a las misiones de la Alianza.
– Se aplicarán fuertes requisitos de autenticación.
– Se mejorarán las capacidades de alerta temprana, de conocimiento de la situación y de análisis.
– Se desarrollarán programas de sensibilización y en los ejercicios de la Alianza se trabajará más el componente cibernético.

En conclusión, se puede afirmar que la OTAN ha alcanzado una solución de compromiso para disponer de una ciberdefensa efectiva y salvaguardar la soberanía y responsabilidad de las naciones en la protección de sus sistemas de comunicaciones e información. En este sentido –en la línea de prudencia defendida por muchos aliados– no se contempla la implementación de capacidades, ya que no existe ni un marco legal –tropezamos con el problema de la atribución de un eventual ataque–, ni medidas de respuesta a crisis pre acordadas, ni reglas de enfrentamiento. Además, por si fuera poco –en el contexto actual de contracción económica– una tal capacidad requeriría grandes inversiones.

### LOS ESTADOS, ALGUNOS DE NUESTROS ALIADOS

El 14 de julio de 2011 el vicesecretario de Defensa de Estados Unidos, William J. Lynn, presentó de forma oficial la Estrategia para el Ciberespacio del Departamento de Defensa. El Documento publicado se trata de una adaptación sin clasificar de la verdadera estrategia, clasificada, más extensa y que no ha sido distribuida.

La versión publicada comienza señalando la gran dependencia de Estados Unidos con respecto a Internet en lo relativo a redes de comunicaciones, comercio internacional, banca, energía y defensa, entre otros ámbitos; lo que convierte a la Red en potencial objetivo de ataques de impredecibles resultados. Dichos ataques cibernéticos no exigen cos-

tosos sistemas de armas sino tecnologías, en muchos casos, relativamente baratas. El Departamento de Defensa se muestra especialmente preocupado con las amenazas contra la propiedad intelectual, que si bien son menos visibles que las amenazas contra las infraestructuras críticas, tienen un impacto evidente también sobre la vitalidad económica del país.

En el ámbito de la estrategia propiamente dicha, se definen estas cinco iniciativas.

– *Iniciativa estratégica 1*: el Departamento de Defensa declara oficialmente el ciberespacio como campo de operaciones en donde se hace necesario organizarse, equiparse y entrenarse. Por ello, el Mando Estratégico (USSTRATCOM), ha delegado todo lo relativo al ciberespacio al recién creado Mando Cibernético (USCYBERCOM), con responsabilidades para gestionar los riesgos inherentes a la Red, asegurar su integridad y disponibilidad así como el desarrollo de capacidades integradas mediante el trabajo conjunto con otros mandos, servicios y agencias. El comandante del USCYBERCOM es, al tiempo, director de la Agencia Nacional para la Seguridad. La redundancia de sistemas y la capacidad de recuperación en caso de ataque constituyen pilares básicos de esta iniciativa. Para garantizar el adecuado adiestramiento se integraran equipos de ciberguerra en ejercicios realizados por las Fuerzas Armadas.
– *Iniciativa estratégica 2*: el Departamento de Defensa empleará nuevos conceptos operativos de defensa para proteger las redes y los sistemas. Esta iniciativa incluye el concepto de «ciberhigiene», destinado a mitigar uno de los principales puntos débiles: las malas prácticas protagonizadas por usuarios y administradores. Ello pasa por la adecuada formación en el uso de *software* de seguridad, el desarrollo de nuevas arquitecturas o la implantación de sistemas de control, con la finalidad de reducir las amenazas internas mediante la detección, el análisis y la minimización de las amenazas.
– *Iniciativa estratégica 3*: el Departamento de Defensa coordinará sus esfuerzos con otras agencias del Gobierno y con el sector privado. El Departamento constata la gran dependencia del sector privado, que va desde los proveedores de servicio hasta las grandes cadenas de logística y distribución de mercancías y sobre los cuales no tiene ningún tipo de control. Para intentar paliarlo establece una estrecha colaboración con el Departamento de Seguridad Doméstica *(Homeland Security)*. Con ello se pretende reafirmar los límites legales que para

dicha colaboración se encuentran actualmente vigentes, aumentar la efectividad y conservar recursos y presupuestos. Por último, se insta a la colaboración con la industria de defensa para incrementar la protección de la información sensible.

– *Iniciativa estratégica 4*: el Departamento de Defensa establecerá un marco de colaboración robusto con los aliados internacionales de Estados Unidos. El Departamento de Defensa apoyará los esfuerzos de Estados Unidos en el desarrollo y la promoción de reglas internacionales sobre el ciberespacio que promuevan la apertura, la interoperabilidad, la seguridad y la fiabilidad.
– *Iniciativa estratégica 5*: el Departamento de Defensa apoyará el esfuerzo creativo nacional con su personal, tecnología y conocimiento. Se pretende por tanto sostener a las empresas y personal responsable del desarrollo tecnológico al tiempo que se mantiene al personal propio constantemente adiestrado con arreglo a las nuevas tecnologías. Se pretende, por tanto, hacer suficientemente atractivo el trabajo en este campo de forma de forma que se garantice la excelencia y permanencia del personal destinado.

Entrando en valoraciones, nos encontramos con un documento parcial, ya que no incluye aquellos aspectos relativos a las acciones ofensivas o disuasivas. En cualquier caso, la filosofía que desprende está muy lejos del concepto que en la Unión Europea existe de ciberdefensa. Con la creación de OSCYBERCOM, Estados Unidos han «militarizado» la Red al considerar a ésta como el cuarto espacio de batalla. La «doble gorra» de su comandante, como director de la todopoderosa Agencia Nacional para la Seguridad, no hace sino reflejar la importancia creciente que para la Administración americana tiene la ciberseguridad. En esta línea ya se han alzado voces que claman contra lo que se percibe como un ataque directo a la libertad en Internet, al entender que la señalada militarización puede conllevar reacciones no proporcionales contra simples actos de piratería informática.

El Reino Unido también por su parte, en la página *web* del Gobierno manifiesta que:

> «Los riesgos del ciberespacio (…) han sido identificados por el Gobierno como un riesgo de alta prioridad. El Reino Unido se enfrenta a una amenaza constante y persistente de otros Estados, terroristas y criminales, que operan en el ciberespacio.»

Esta alta prioridad queda recogida igualmente en su Estrategia de Seguridad Nacional (43), cuando de entre los 15 riesgos prioritarios señala los cuatro más apremiantes; siendo uno de ellos «los ataques hostiles contra el ciberespacio del Reino Unido causados por otros Estados o el cibercrimen a gran escala». Así –en la línea de señalar a otros Estados como origen de la amenaza– afirma que:

> «Aunque actualmente no nos enfrentamos a ninguna amenaza militar por parte de otro Estado, algunos de ellos siguen intentando obtener ventajas sobre nosotros a través de actividades de espionaje hostil o de ataques cibernéticos.»

La estructura con que el Reino Unido cuenta para hacer frente al riesgo cibernético, cuenta con un órgano directivo, la Oficina de Ciberseguridad y de Seguridad de la Información, OCSIA *(Office of Cyber Security & Information Assurance)* encargada de proporcionar dirección estratégica y coordinación general de las actividades relacionadas con la mejora de la seguridad cibernética y la seguridad de la información en todo el país; y lo hace principalmente a través de un programa cuatrienal de ciberseguridad dotado con 650 millones de libras y en el que, junto con el OCSIA y su órgano de ejecución, el llamado Centro de Operaciones de Seguridad Cibernética, participan: el Ministerio del Interior, el Ministerio de Defensa, la sede de las Comunicaciones Gubernamentales, GCHQ *(Government Communications Headquarters)*, el Centro para la Protección de la Infraestructura Nacional (CPNI) y el Departamento de Negocios, Innovación y Habilidades, BIS *(Bussiness, Innovation and Skills)*. Todos ellos con el objetivo común de hacer progresar el ambicioso Programa de Ciberseguridad.

Este Programa definido en su revisión Estratégica de la Defensa y la Seguridad (44), se fundamenta en los siguientes pilares:

– Revisión del enfoque de la lucha contra la delincuencia cibernética, entre otras cosas mediante la introducción de un único punto de contacto donde los usuarios individuales y las empresas puedan denunciar los delitos cibernéticos.
– Abordar las deficiencias en la capacidad para detectar y defenderse de los ataques cibernéticos, mediante la mejora de la capacidad para

(43) *A Strong Britain in an Age of Uncertainty-The National Security Strategy*, octubre de 2010.
(44) *Securing Britain in an Age of Uncertainty: The Strategic Defence and Security Review,* octubre de 2010.

ofrecer productos y servicios de ciberseguridad, y mediante la mejora de la inversión en capacidades de inteligencia.
– Creación de una nueva organización en el Ministerio de Defensa, el Grupo de Operaciones de Ciberdefensa, que integre la seguridad cibernética y asegure la coherencia de las actividades cibernéticas en todo el espectro de las operaciones de defensa.
– Refuerzo de las infraestructuras críticas, de las redes vitales y de los servicios del Gobierno.
– Establecimiento de alianzas internacionales sólidas, incluyendo el trabajo en un memorando de entendimiento entre el Reino Unido y Estados Unidos que permita el intercambio de información y el planeamiento y ejecución de operaciones de forma conjunta.
– Mejora de la formación y sensibilización en seguridad cibernética a través de iniciativas online tales como *Get Safe Online* (45) y *The Cybersecurity Challenge* (46).
– Colaboración con el sector privado y otras entidades en el patrocinio de investigaciones para mejorar la capacidad de respuesta a los futuros desafíos a la seguridad informática.

Tan ambicioso programa requiere, sin duda, la actualización en primer lugar de la Estrategia de Ciberseguridad en vigor, que data del año 2009. En este sentido, las autoridades británicas se habían propuesto publicar una nueva estrategia en la primavera de 2011, pero su lanzamiento parece que se va a retrasar hasta el otoño.

Por último, entre las principales amenazas que Francia se enfrentaría en los siguientes quince años, el *Libro Blanco sobre Defensa y Seguridad Nacional* de 2008, señaló la posibilidad de un gran ciberataque a la infraestructura nacional.

Esta constatación llevó al Gobierno a disponer el fortalecimiento significativo de la capacidad nacional de ciberdefensa. Así, la creación en el año 2009 de la Agencia Nacional para la Seguridad de los Sistemas de Información, ANSSI *(Agence Nationale de la Sécurité des Systèmes d'Information)*, fue el primer paso en este compromiso al que posteriormente vino a complementar la publicación, en febrero de 2011, de la Estrategia de Francia para la Defensa y la Seguridad de los Sistemas de

(45) En: *http://www.getsafeonline.org/*
(46) En: *https://cybersecuritychallenge.org.uk/*

Información (47), Documento que encarna la ambición manifestada en el *Libro Blanco* de 2008.

La Estrategia francesa se basa en cuatro objetivos:

1. Ser una potencia mundial de la ciberseguridad: mientras mantiene su autonomía estratégica, Francia debe hacer el esfuerzo de pertenecer al restringido club de los principales países en ciberdefensa.
2. Garantizar la libertad de decisión y de acción de Francia, gracias a la eficaz protección de la información sensible para los intereses nacionales: las autoridades gubernamentales, actores en la gestión de crisis, deben tener los medios para comunicarse con seguridad y confidencialidad en cualquier situación. Para ello es necesario retener las habilidades necesarias para diseñar y optimizar el desarrollo y producción de herramientas de seguridad y confidencialidad.
3. Fortalecimiento de la ciberseguridad de las infraestructuras críticas: un ataque con éxito contra un sistema de información crítica puede conducir a graves consecuencias económicas y humanas. Es importante que el Estado, junto con el sector privado, trabajen para asegurar y mejorar la seguridad de los sistemas críticos.
4. Garantizar la seguridad en el ciberespacio: la Administración debe dar ejemplo y mejorar la protección de sus sistemas de información y de sus datos. En lo que respecta a empresas y particulares, debe llevarse a cabo una campaña de información, concienciación y promoción de la ciberseguridad. Además, en la lucha contra el delito cibernético, Francia promoverá el fortalecimiento del derecho y la cooperación judicial internacional.

Para alcanzar estos objetivos, se identifican siete líneas de actuación:

1. Mayor anticipación y análisis del entorno, de forma que permita la toma de decisiones adecuadas.
2. Detección y neutralización de los ataques, alertando y apoyando a las potenciales víctimas.
3. Aumento y sostenimiento de las capacidades científicas, técnicas, industriales y humanas, con el objetivo de mantener también la autonomía necesaria.
4. Protección de los sistemas de información del Estado y de los operadores de las infraestructuras críticas, para lograr una mayor resiliencia nacional.

---

(47) *Défense et sécurité des systèmes d'information, Stratégie de la France,* febrero de 2011.

5. Revisión de las leyes para incorporar los avances tecnológicos y los nuevos usos y costumbres.
6. Desarrollo de la colaboración internacional en materia de ciberseguridad, incluyendo la lucha contra la ciberdelincuencia.
7. Informar y convencer a la población de la importancia de familiarizarse con las técnicas de protección de los sistemas de información y comunicaciones.

Otros países que también han publicado en el año 2011 sus respectivas estrategias específicas para el ciberespacio son: Alemania y Países Bajos y otros muchos han asegurado que pretenden hacerlo próximamente. En el caso de Países Bajos llama la atención su «cesión» a favor de la autorregulación del ciberespacio, cuando en uno de los principios básicos de su estrategia titulado «autorregulación si es posible, legislación si es necesario», establece que:

> «Los sectores público y privado alcanzarán el nivel de seguridad de las TIC que pretenden, principalmente a través de la autorregulación. Si la autorregulación no funciona, el Gobierno examinará la posibilidad de legislar.»

Por parte alemana merece mención su defensa, en el plano de la acción internacional, de un eventual Código de Conducta de los Estados en el ciberespacio, que sea ratificado por tantos países como sea posible y que incluye medidas de fomento de la confianza y de la seguridad.

Pero si hay un factor común en todas ellas, ese es el énfasis en la detección y reacción tempranas, así como en la necesidad de mejorar la resiliencia. Quizás el único elemento llamativo en el panorama, sea la decisión estadounidense de crear un mando específico, el USCYBERCOM para la protección de los sistemas del Departamento de Defensa.

*La iniciativa privada: foros no gubernamentales*

Además de las iniciativas gubernamentales citadas, existen también otros foros no gubernamentales de reconocido prestigio en el campo de la ciberdefensa.

El primero de ellos es el Foro de Equipos de Seguridad y Respuesta a Incidentes, FIRST *(Forum for Incident Response and Security Teams)*. Este Foro reúne a numerosos equipos de respuesta a incidentes cibernéticos (CERT) tanto de organismos gubernamentales, como del sector privado y de la comunidad educativa. Su objetivo es fomentar la cooperación y

coordinación entre CERT en la prevención de incidentes cibernéticos, permitiendo así una rápida respuesta a los incidentes. Para ello organiza diversas actividades entre las que destaca el intercambio de «buenas prácticas» y, sobre todo, su conferencia anual, como la que en el año 2007 tuvo lugar en Sevilla.

Otro Foro «independiente» destacable es el conocido como *Meridian*; iniciativa lanzada en el año 2005 por el Centro de Protección de Infraestructuras Críticas del Reino Unido, con vocación de constituirse en foro de discusión entre gobiernos sobre políticas de CIIP.

*Las amenazas: otros Estados*

Si tuviésemos que agrupar al origen de las amenazas cibernéticas en dos grandes conjuntos, éstos bien podrían ser por una parte, el de los actores estatales y por otra, el de los no-estatales. Aunque la línea que separa ambos grupos puede, en algunos casos, aparecer borrosa debido a la eventual vinculación de determinados activistas «independientes» con algunos Estados, en general podríamos decir que en el grupo se los no-estatales se encontrarían los llamados *hacktivistas* –grupos de protesta en la Red–; los cibercriminales –espionaje, fraude, extorsión, robo, etc.–, y por último los *hackers* aficionados.

En este epígrafe abordaremos solamente los llamados actores estatales. Quizás sean éstos los que recientemente han disparado las alarmas en los gobiernos occidentales –forzándoles a legislar y a crear estructuras de protección gubernamentales–, por las crecientes sospechas de que determinados Estados pudieran encontrarse detrás de los ataques cibernéticos a organismos públicos y privados con el fin de obtener información de relevancia política, industrial o militar.

Esta valoración, junto a la sospecha norteamericana de que China pudiera encontrase tras los ataques cibernéticos a las redes de los fabricantes del avión de combate F-35 (48), podría haber sido determinante en la decisión de crear el USCYBERCOM (49) y de dotarle de los amplios poderes con que cuenta. Así para Andress y Winterfeld (50), la cibergue-

(48) *Ateneadigital.es:* «Preocupación por el espionaje en el ciberespacio», 17 de junio de 2009.
(49) *Ateneadigital.es:* «Estados Unidos crea un *Cyber Command* para hacer frente al espionaje digital de China y Rusia», 26 de junio de 2009.
(50) Jason, Andress and Steve, Winterfeld: «Cyber Warfare: Techniques, Tactics and Tools for Security Practitioners», *Syngress-Elsevier,* 2011, Waltham, MA (Estados Unidos).

rra china estaría protagonizada por su Ejército de Liberación Popular, a través de las secciones tercera y cuarta de su Estado Mayor Conjunto, que dirigirían la actuación de las llamadas Milicias de la Guerra de la Información, posiblemente integradas por expertos en las TIC civiles.

Muy conocidos resultan los episodios de enfrentamiento entre el gigante *Google* y el Estado chino, como consecuencia de la censura gubernamental de las búsquedas ofrecidas por *Google* y la acusación vertida a través de la agencia oficial china de noticias Xinhua, de que:

> «El buscador de Internet mantiene una estrecha relación con los Servicios de Inteligencia estadounidenses, a quienes –según la agencia– provee de registros con los resultados de búsquedas» (51).

Más recientemente, según relata Alandete (52):

> «La consultora de seguridad en Internet McAfee difundió (…) un estudio en el que asegura tener pruebas de que, durante cinco años, una serie de espías cibernéticos se infiltraron en las redes y servidores de instituciones internacionales que abarcan desde el Gobierno norteamericano al Comité Olímpico Internacional y empresas militares.»
>
> «McAfee –continúa Alandete– no dio específicamente el nombre de la mano que se encuentra tras esos oscuros asaltos, pero el tipo de espionaje, que afectó a 72 instituciones en Europa, Norteamérica y Asia, vuelve a proyectar sospechas sobre China. Entre los infiltrados se encuentran rivales tradicionales de ese país, como los Gobiernos de Estados Unidos, Taiwan, Japón y Corea del Sur; diversos comités olímpicos en el contexto de los juegos de Pekín del año 2008, y el grupo de naciones del sureste asiático en la ONU.»

En cuanto a Rusia, país a menudo señalado como origen de graves ciberataques del estilo de los sufridos por Estonia en el año 2007 y Georgia en el año 2008 –crisis que, sin duda, influyeron en la decisión de la OTAN de dotarse de una política de ciberdefensa y de las estructuras necesarias para aplicarla–, en febrero de 2010 su presidente, Medvédev, sancionó la nueva Doctrina Militar en la que prevé la utilización de

---

(51) *BBC Mundo:* «China: *Google* es "herramienta del Gobierno de Estados Unidos"», 21 de marzo de 2010, en: *http://www.bbc.co.uk/mundo/economia/2010/03/100321_china_google_internet_eeuu_jp.shtml*

(52) Alandete, D.: «Una gran operación de espionaje en Internet vuelve a apuntar a China», *El País, vida & artes*, p. 28, 4 de agosto de 2011.

operaciones en la Red en apoyo de las operaciones militares, así como la utilización de las tecnologías de la información para valorar y predecir situaciones y relaciones político-militares, con el objetivo de prevenir y disuadir el desencadenamiento de conflictos militares. Así, para Andress y otros, las capacidades de ciberguerra rusas estarían repartidas entre su Servicio de Inteligencia, el Estado Mayor Conjunto y la Guardia Federal *(Federal Guard Service)*, encargada entre otras cosas, de las TIC utilizadas por el presidente y el Gobierno rusos).

Andress y Winterfeld hablan también de la capacidad de ciberguerra de Israel, cuyos cometidos –según los autores– estarían repartidos entre la Jefatura C4I de las Fuerzas de Defensa Israelíes y la Unidad de Inteligencia de Señales de la Inteligencia Militar.

## Conclusiones

En un mundo en el que las viejas Naciones-Estado se debaten entre dificultades financieras y sus decisiones dependen en gran medida de los dictados de los todopoderosos mercados financieros, las grandes corporaciones globales entre las que se encuentran la mayoría de los «gigantes de Internet», sin tantos problemas financieros y con gran prestigio entre los usuarios de Internet, partirían en posición de ventaja en la batalla entre caballeros que libran con los Estados, las organizaciones internacionales y los ciberdelicuentes, por el control, descontrol o autocontrol del ciberespacio.

Así, por una parte nos encontramos con una *aproximación internacional fragmentaria* y centrada en el objeto de cada organización: la OTAN persigue la protección de los sistemas críticos para su misión; la Unión Europea la creación de un mercado digital único soportado por una Internet segura y confiable; Naciones Unidas pretende hacer accesibles para todos los beneficios del uso de las TIC y de Internet. Incluso cuando un mismo Estado miembro pertenece a varias organizaciones, la representación en cada una de ellas, frecuentemente recae sobre diferentes departamentos que no mantienen posturas ni concertadas ni coherentes. En el nivel estatal, la elaboración de una estrategia nacional para el ciberespacio, acompañada de las estructuras que la implanten, es el primer paso para llevar coherencia a la escena internacional, donde quizás –en línea con el informe sobre ciberseguridad de la OCDE–, el IGF pueda demostrar su valor en la integración de las diferentes estrategias

nacionales e internacionales en una suerte de Convención del Ciberespacio como la que propone Kamal (53).

Por ahora, en cambio, asistimos a una suerte de *afganización del ciberespacio*, con burbujas de seguridad e insurgencia, al igual que ocurre sobre el terreno en ese país centroasiático. Así, para Innerarity (54):

> «Existen espacios desgobernados allá donde los Estados han cedido soberanía, voluntaria o involuntariamente, razonablemente o no, en todo o en parte, a otras autoridades. Si entendemos que los espacios desgobernados son aquellos en los que el poder del Estado es ausente, débil o contestado, entonces –añade el autor–, además de referirnos a los territorios de poder tribal o insurgencia persistente, debemos extender esta perspectiva a los dominios de Internet o a los mercados donde operan los agentes económicos con una regulación pública insuficiente.»

Utilizando la terminología preconizada por el general Petraeus en su doctrina contrainsurgente aplicada en Irak y Afganistán, quizás, con nuestras aproximaciones fragmentarias estemos creando burbujas de seguridad en este espacio desgobernado que es el ciberespacio. Cada empresa, corporación, Estado u organización internacional sería responsable de una «burbuja de seguridad cibernética». La pregunta es si –volviendo al lenguaje del general Petraeus– seremos capaces de ganarnos los corazones y las mentes de los usuarios de Internet, negando espacios a la insurgencia y si lograremos conectar las burbujas para alcanzar un ciberespacio seguro y confiable, porque, al igual que Afganistán, el ciberespacio continúa siendo un lugar peligroso.

Por último y como consecuencia de esa posición de privilegio con que parten los «gigantes de Internet», puede que marchemos *hacia un ciberespacio autorregulado* y en constante y vertiginosa evolución: volviendo a Innerarity, Internet:

> «No se trata de un espacio completamente desgobernado, pues rige en él al menos un partenariado "inoficial" entre Estados y empresas, etc. está claro que la gobernanza de Internet disminuirá la centralidad de la Nación-Estado en la política global.»

---

(53) Ahmad, Kamal: *The Law of Cyberspace,* United Nations Institute for Training and Research (UNITAR), 2005.

(54) Innerarity, D.: «¿Quién manda aquí?», diario *El Correo,* p. 20, 17 de agosto de 2011.

Y si el Estado pierde poder y las organizaciones internacionales no son sino agrupaciones de Estados, quizás el modelo «autorregulatorio» que, según Collao, defiende Zuckerberg, sea el que se acabe imponiendo en un escenario en el que los usos, las modas, las formas de acceso y el delito, evolucionan muy por delante de la capacidad de las burocracias estatales e interestatales para responder a ellas.

**Bibliografía**


ALANDETE, D.: «Una gran operación de espionaje en Internet vuelve a apuntar a China», *El País, vida & artes,* p. 28, 4 de agosto de 2011.

CENTRO DE INVESTIGACIÓN COMÚN DE LA COMISIÓN EUROPEA: *Institute for Prospective Technology,* recuperado el 1 de julio de 2011, de Joint Research Centre (sin fecha), en: h*ttp://ipts.jrc.ec.europa.eu/index_es.cfm*

CMSI: *Agenda de Túnez para la Sociedad de la Información,* 28 de junio de 2006.
— *Compromiso de Túnez,* 28 de junio de 2006.

COLLAO, V.: «¿Es posible que tanto Sarkozy como Zuckerberg estén en lo cierto?» *El País, Ciberp@ís*, 6 de junio de 2011.

COMISIÓN EUROPEA: *Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience,* 2009, recuperado el 1 de agosto de 2011, en: *http://ec.europa.eu/information_society/policy/nis/strategy/activities/ciip/index_en.htm*
— *The EU Internal Security Strategy in Action: Five steps towards a more secure Europe,* 22 de noviembre de 2010, recuperado el 1 de agosto de 2011, en: *http://ec.europa.eu/commission_2010-2014/malmstrom/archive/internal_security_strategy_in_action_en.pdf*

CONSEJO EUROPEO: *Estrategia de Seguridad Interior de la Unión Europea: Hacia un modelo europeo de seguridad,* marzo de 2010, recuperado el 1 de agosto de 2011, en: *http://www.consilium.europa.eu/uedocs/cms_data/librairie/PDF/QC3010313ESC.pdf*

DARPA *(Defence Advanced Research Projects Agency)*: (sin fecha), recuperado el 1 de agosto de 2011, en: *http://www.darpa.mil/*

ENISA: *Cyber Europe 2010-Evaluation Report. Recommendations and Lessons Identified,* abril de 2011.

FORO PARA EL GOBIERNO DE INTERNET: *Internet Governance Forum:* (sin fecha), recuperado el 1 de agosto de 2011, en: *http://www.intgovforum.com/*

GANUZA ARTILES, N.: *Ciberseguridad. Retos y amenazas a la Seguridad Nacional en el ciberespacio: la situación de la ciberseguridad en el ámbito internacional y en la OTAN,* Instituto Español de Estudios Estratégicos-Instituto Universita-

rio «General Gutiérrez Mellado», Dirección General de Relaciones Institucionales, Ministerio de Defensa, Madrid, 2010.

HANS BINNENDIJK, Patrick L. Clawson: «Tuning the Instruments of National Power», *Joint Force Quarter,* invierno, 1996.

INNERARITY, D.: «¿Quién manda aquí?», diario *El Correo,* p. 20, 17 de agosto de 2011.

INSTITUTO NACIONAL DE TECNOLOGÍAS DE LA COMUNICACIÓN, S. A. (INTECO): *Redes Zombi* (botnets) (sin fecha), recuperado el 5 de agosto de 2011, de INTECO-Centro de Respuestas a Incidentes de Seguridad, en: *http://cert.inteco.es/Formacion/Amenazas/botnets/*

NORKUS, E. P.: *Closing Remarks,* «Conference on a Comprehensive Approach to Cyber Security: Exploring the Future OSCE Role», Vilna, 2011.

ONU: *United Nations Global Compact,* 18 de diciembre de 2007, recuperado el 1 de agosto de 2011, en: *http://www.unglobalcompact.org/Languages/spanish/index.html*

ORGANIZACIÓN MUNDIAL DEL COMERCIO: *Ministerial Declaration on Trade in Information Technology Products,* Singapur, 13 de diciembre de 1996.

OSCE: «Reunión del Consejo Permanente sobre la relación entre la propaganda racista, xenófoba y antisemítica en Internet y los crímenes por odio», París, 2004.

PÉLISSIÉ DU RAUSAS, M.; MANYIKA, J.; HAZAN, E.; BUGHIN, J.; CHUI, M. and SAID, R.: *Internet matters: The Net's sweeping impact on growth, jobs and prosperity,* McKinsey Global Institute, McKinsey & Company, 2011.

REPRESENTACIÓN DE LA COMISIÓN EUROPEA EN ESPAÑA: *Informe del Seminario Agenda Digital para Europa,* Madrid, 2010.

UIT: *¿Qué hace la UIT?,* 2008, recuperado el 7 de agosto de 2011, en: *http://www.itu.int/es/about/Pages/whatwedo.aspx*

— *Global Cybersecurity Agenda* (sin fecha), en: *http://www.itu.int/osg/csd/cybersecurity/gca/*

WALDROP, M.: *DARPA: 50 Years of Bridging the Gap. DARPA and the Internet Revolution,* 2008, recuperado el 1 de agosto de 2011, en: *http://www.darpa.mil/WorkArea/DownloadAsset.aspx?id=2554*

## CAPÍTULO TERCERO

# LA EVALUACIÓN DEL CONFLICTO HACIA UN NUEVO ESCENARIO BÉLICO

# LA EVOLUCIÓN DEL CONFLICTO HACIA UN NUEVO ESCENARIO BÉLICO

Por Javier López de Turiso y Sánchez

> «En un cuarto de hora, las 157 mayores áreas metropolitanas fueron colapsadas por un apagón que afectó a toda la nación en plena hora punta. Nubes de gas venenoso flotaban hacia Wilmington y Houston. Las refinerías de varias ciudades eran depósitos en llamas. Los Metros de Nueva York, Oakland, Washington y Los Ángeles habían sufrido accidentes... Los aviones se caían literalmente del cielo como resultado de las colisiones aéreas que se sucedían a lo largo del país... Varios miles de americanos ya habían resultado muertos.»
>
> Richard Clarke, *Cyber War,* 2010

## Introducción

Quizás este fragmento del libro del Richard Clarke describiendo el estado apocalíptico después de un ciberataque a Estados Unidos sea un poco exagerado... ¿o tal vez no? Afortunadamente todavía no hemos tenido la oportunidad de comprobarlo pero lo sea o no, el ciberespacio se ha convertido en un campo de batalla que se verá inundado por las acciones derivadas de los conflictos que el ser humano ha ido teniendo durante siglos y que ahora se extienden a este nuevo escenario.

Pero ¿esto es realmente así? ¿Ha desencadenado el nuevo escenario conflictos distintos o son los conflictos de toda la vida los que se han adaptado al nuevo escenario? ¿Han evolucionado realmente los enfrentamientos o lo que ha evolucionado es tan sólo la manera en que los vivimos?

En la década de los años ochenta se produjeron tres grandes hitos que marcarían definitivamente el futuro de la informática, sus comunicaciones y la seguridad: la aparición del PC, el despegue de Internet y surgimiento del *malware* (1). Hoy día, treinta años después, la utilización de ciberespacio para la comisión de delitos o actividades ilícitas se ha extendido profusamente, lo que está originando una gran alarma social por lo novedoso del escenario utilizado. En realidad no sé por qué nos sorprende, porque si algo nos ha enseñado la Historia es que, debido a nuestra naturaleza, allá donde surja un nuevo escenario con actividad humana, habrá conflictos.

En menos de una generación, la informática ha pasado de ser de una mera herramienta administrativa que facilitaba los trabajos burocráticos de las oficinas, a constituir por sí misma un recurso estratégico nacional para muchas naciones. La evidencia de la importancia que las nuevas tecnologías están adquiriendo en el peso específico de las naciones viene demostrada por el hecho de que Estados Unidos haya desplazado su centro de gravedad hacia el ciberespacio. Considerar al ciberespacio como el centro de gravedad de una nación significa reconocer que constituye el centro neurálgico de todos los poderes del país, el ente del que todo depende (2).

## El conflicto

> «Nuestra estimación es que los ciberataques serán un componente importante de cualquier conflicto futuro, independientemente de que involucre a grandes naciones, estados hostiles o grupos terroristas» (3).

---

(1) Aunque el primer virus informático, el *creeper,* apareció en el año 1972 para el IBM 360, se considera que fue a partir del año 1984 con la difusión del IBM PC y su sistema operativo MS-DOS cuando se empezó a proliferar el *malware.*

(2) Kass, Leni doctora: *A Warfighting Domain,* 2006.

(3) William J. Lynn, III, vicesecretario de Defensa de Estados Unidos.

Miles de años hace que el hombre rivaliza con sus semejantes para obtener todo tipo de ventajas que le aseguraban, en la medida de lo posible, los medios para su subsistencia y la continuidad de su descendencia. Guiados por su instinto de supervivencia, los intereses que movían al ser humano eran meramente primarios: búsqueda de abrigo, alimento y seguridad. Los grupos fueron demarcando sus territorios con el objeto de establecer zonas de exclusión en donde sólo ellos podrían cazar, pescar o recolectar frutos. Los intentos por parte de los miembros de otros clanes de adentrarse en sus territorios para obtener sustento, desembocaban con facilidad en enfrentamientos mortales. Con la evolución afloraron pensamientos y sentimientos, que rápidamente introducirían un nuevo factor de roce en las sociedades: las diferencias de ideas, creencias y valores. Éstos eran adoptados por las sociedades como un signo de identidad frente a otros pueblos y culturas.

Todos los grupos tenían sus cabecillas. Si un líder era muy influyente y lograba imponer su liderazgo sobre un conjunto de varios grupos o aldeas se erigía en jefe (4). La evolución de las grandes jefaturas, dio origen a los Estados (5) los que, con los años, formaron lo que hoy día constituyen las naciones (6). La máxima expresión de un conflicto es cuando se enfrentan militarmente dos o más naciones: la guerra.

El aquí expuesto es lo que probablemente sea el ejemplo más sencillo (y primitivo) de lo que siempre ha sido un conflicto: una pugna por satisfacer los propios intereses.

*Definición*

Existen multitud de definiciones de lo que podría ser considerado como conflicto, tantas como autores. Dentro de la complejidad que esto repre-

(4) Harris, Marvin: *Introducción a la antropología general,* Alianza Universidad Textos, Harris diferencia entre cabecillas y jefes en función del ámbito de dominio del líder, 1991.

(5) El Estado es una forma de sociedad políticamente centralizada cuyos gobernantes tienen el poder de obligar a sus subordinados a pagar impuestos, prestar servicios y obedecer la ley. Carneiro, Robert: «Chiefdom: Precursor of the State», 1981 en Jones, Grant y Kautz, Robert: *The Transition to Statehood in the New World,* Nueva York, Cambridge University Press. Algunas de las grandes civilizaciones del pasado formaron poderosos Estados: persas, egipcios, griegos, romanos, incas, etc.

(6) El concepto de Estado-Nación surgió al finalizar la Guerra de los Treinta Años, en el año 1648 con la Paz de Westfalia en donde el primitivo orden feudal deriva en organizaciones de territorio y población bajo la autoridad de un gobierno que reconoce formalmente sus límites de dominio.

senta, probablemente las más sencillas son las más adecuadas. Probablemente, la que más y mejor puede resumir la idea de conflicto es *una lucha de intereses*.

Así como tenemos encuentros y coincidencias, las diferencias y los conflictos son también parte fundamental de nuestras relaciones cotidianas individuales o grupales. El conflicto es necesario, hace evolucionar al hombre con nuevas ideas y pensamientos (7). Las naciones pueden formar alianzas si sus intereses son comunes y entrar en conflicto en el caso de que sean divergentes.

*Tipos de conflictos*

Aunque una clasificación rigurosa y completa de los conflictos es muy complicada debido al riesgo de realizar una excesiva generalización, vamos a hacer una más sencilla por considerarla adecuada a los fines perseguidos en este capítulo. Esta clasificación se hace en función de los actores implicados, quienes representan las partes en conflicto. Estos podrán ser:

– *Individuos (actor-individuo)*: un conflicto es individual cuando las partes en litigio están constituidas por una o más personas, pero cada una mantiene sus propios puntos de vista (8).
– *Grupos (actor-grupo)*: un conflicto es grupal cuando los mismos intereses son perseguidos por diferentes personas y éstas se agrupan para conseguir de forma colectiva sus objetivos. Estos grupos pueden estar formados por familias, clanes, bandas, tribus (étnicas o urbanas), grupos raciales, grupos religiosos, grupos sociales (lucha de clases), grupos políticos, etc.
– *Naciones (actor-Estado)*: constituyen un tipo particular de los conflictos de grupo cuando al menos uno de sus protagonistas es una nación. Un conflicto se convierte en internacional cuando es el Es-

(7) Sin llegar a identificar conflicto con conflicto bélico, algunos filósofos como Tales de Mileto pensaban que la contradicción era la madre del progreso. Marx creía que el conflicto era una parte importante en la formación de los grupos sociales. Coser afirmaba que el conflicto es una forma constructiva de socialización y continuidad satisfactoria en la vida del grupo.

(8) No hay que confundir los conflictos individuales con los personales. Los individuales se mantienen con otros individuos, mientras que los personales son los conflictos internos de la persona. Algunos autores incluyen dentro de los individuales los que afectan también a unas pocas personas, en: *www.konfliktloesning.dk/files/Conflict_resolution_Spanish.pdf*

tado (9) responsable de la dirección y gobierno de una nación (10) quien promueve, dirige o encabeza la defensa de los intereses de la misma frente a otras naciones o grupos. Puesto que las naciones están representadas por sus Estados, se considerará a éstos como los actores del conflicto.

Para analizar la incidencia de los actores en la ciberdefensa se van a considerar solamente los conflictos en los que una de las partes implicadas sea el *actor-Estado* y en concreto aquellos en que los actores los compongan grupos y Estados (11).

*Causas de los conflictos*

Una profundización sobre las causas de los conflictos (12) no es objeto de este capítulo ya que no interrelacionan con el entorno en el que se desarrollan y su evolución en el ciberespacio es independiente a ellas, al igual que en cualquier otro entorno físico. Sin embargo, se considera conveniente hacer una mención explícita para un mejor entendimiento del conjunto.

Las causas de los conflictos habidos a lo largo de la Historia en los que un actor-Estado se ha visto implicado, se van a tipificar en:

1. Conflictos de intereses o necesidades económicas:
   - T*erritoriales:* luchas por expansión y posesión de territorio, la mayoría de los casos en busca de los recursos que contenían.
   - *Recursos:* materiales (materias primas, riquezas, etc.) o humanos (mano de obra, trata de esclavos, mujeres, etc.).
2. Conflictos de valores, creencias o preferencias:
   - *Políticos:* ideológicos, de estatus, de poder, etc.

---

(9) Estado: conjunto de órganos de gobierno de un país soberano. Real Academia Española, vigésima segunda edición. En las democracias actuales están compuestos por sus tres poderes: Legislativo, Ejecutivo y Judicial.

(10) Nación: conjunto de los habitantes de un país regido por el mismo gobierno. Real Academia Española, vigésima segunda edición.

(11) Se descartan los conflictos entre individuo y Estado por la poca incidencia que tienen éstos.

(12) Las causas generales de los conflictos normalmente se aglutinan en tres grandes grupos: conflictos de comunicación, conflictos de intereses y conflictos de valores. En este capítulo se descartan los primeros ya que raramente un Estado entrará en conflicto con otro debido a problemas de comunicación. La diplomacia es la responsable de evitar que se produzca este tipo de desencuentros entre naciones.

– *Religiosos:* guerras de religión del último milenio.
– *Raciales:* a menudo compañero de cualquiera de los anteriores.
– *Ético-morales (acciones contra Estados opresivos):* Yugoslavia, Irak, Afganistán, Libia, etc.

Los conflictos raramente son debidos a una sola causa. La mayoría de los enfrentamientos entre actores-Estado han sido originados por una combinación de varias de ellas. Sin embargo en un gran número, bien como causa principal abiertamente declarada o bien como secundaria camuflada bajo otros pretextos, siempre ha predominado un factor común: los intereses económicos.

*Dinámica del conflicto*

Por dinámica del conflicto se entiende el proceso de su evolución desde sus orígenes hasta su finalización.

Un conflicto no surge de la nada, ni de la noche a la mañana. Todos tienen sus causas y evolucionan de una manera progresiva desde un Estado inicial de paz hasta el de guerra declarada. Un conflicto no resuelto con los instrumentos de poder pacíficos puede escalar a uno armado y éste a una guerra declarada.

Por norma general, este proceso de escalada de violencia comprende las seis siguientes fases:

1. *Paz*: los países no están enfrentados y luchan por intereses legítimos que no son convergentes.
2. *Paz inestable*: los intereses nacionales de distintos países empiezan a coincidir. Es un periodo en el que la tensión y las sospechas son elevadas pero no hay violencia o ésta es muy esporádica (13).
3. *Tensión*: situaciones de inestabilidad creciente que alteran la vida normal del Estado y la acción de gobierno y que, por su peligrosidad potencial para la seguridad nacional o colectiva, inducen a los gobiernos a tomar medidas preventivas que pueden provocar la activación de sus sistemas de alerta o el empleo de los recursos de la Defensa Nacional (14).

(13) Lund, Michael S.: *Curso de Certificación de Análisis de Conflictos,* U.S. Institute of Peace, en: *http://http://es.scribd.com/doc/61965893/5/Paz-inestable*
(14) Doctrina Aeroespacial.

4. *Crisis*: momentos decisivos dentro de una situación de tensión en los que se produce o prevé un cambio inminente de consecuencias importantes. Suele aparejar la movilización de las Fuerzas Armadas y es posible la aparición de escaramuzas esporádicas también de escasa intensidad.
5. *Conflicto armado*: es la confrontación física entre colectividades organizadas, aunque no necesariamente reconocidas a la luz del Derecho Internacional, caracterizada por el empleo de medios militares de combate con la finalidad de imponer cada una su voluntad (15).
6. *Guerra*: la guerra es la forma más violenta y más desarrollada de enfrentamiento. Consiste en la confrontación entre colectividades políticamente estructuradas con la finalidad de imponer la voluntad de una sobre otra o de defender los propios intereses. Se caracteriza por el empleo masivo y organizado de medios de combate. La guerra tiene connotaciones de carácter legal y normalmente se desencadena cuando un estado la declara a otro. El reconocimiento formal de la situación de guerra tiene implicaciones jurídicas y políticas (16).

La ciberguerra, no se encuentra en la punta de la pirámide de la escalada de un conflicto. La ciberguerra, en su forma de ciberespionaje, tendrá lugar desde las primeras fases del proceso. En su forma de ciberataque dependerá de las tácticas que se adopten en el planeamiento conjunto de las operaciones, si bien normalmente será anterior y/o simultánea a la fase de conflicto. Un ciberconflicto se puede originar de una forma aislada, sin necesidad de que haya una mayor escalada de violencia.

Comparando los conflictos habidos en los últimos años en los que ha existido ciberguerra con los totales del último siglo, se observa que tanto las causas, como los actores implicados o las fases por las que han pasado, se ciñen igualmente a los moldes generales de los conflictos aquí descritos. Se llega, por tanto a la conclusión de que los conflictos han sido y siguen siendo los mismos a lo largo de la Historia, y lo único que han variado han sido los escenarios en los que se llevaron a cabo.

Durante el tiempo que persista un conflicto, las naciones utilizarán todos los instrumentos a su alcance para luchar por la consecución de sus legítimos intereses nacionales. Estos instrumentos son los denominados «instrumentos de poder».

---

(15) *Ibídem*.
(16) *Ibídem.*

## Los instrumentos de poder

> «Estados Unidos se reserva el derecho a responder –a través de medidas diplomáticas, informáticas, económicas o militares– a cualquier amenaza contra la seguridad nacional en el ciberespacio y más allá» (17).

El concepto de «instrumento de poder» es muy abstracto. Desde que se acuñó por primera vez este término en el año 1939 (18) ha habido grandes discusiones sobre su significado y extensión.

En el contexto internacional y diplomático se define *poder* como «la capacidad de influir en el comportamiento de otros para alcanzar el resultado deseado» (19). Aparte de sutilezas conceptuales de lo que para unos o para otros constituyen los instrumentos de poder, con lo que sí parece existir acuerdo es que son las herramientas de las que disponen los Estados para influir y/o presionar a otros estados con el objeto de conseguir sus intereses u objetivos nacionales (20).

Este número de «medios disponibles», de instrumentos de poder, puede ser tan amplio como se quiera considerar. Desde la aparición del concepto hasta hoy, este número ha variado desde tres hasta 15 o más, en función de la época y del enfoque dado. Actualmente parece ser que el número de instrumentos de poder más aceptado se limita a cuatro (21):

1. *Diplomático*: también se le denomina instrumento político; su poder se fundamenta en la persuasión. La diplomacia es el punto de encuentro que lubrica los roces entre los intereses nacionales convergentes de los diferentes países. Abarca todo tipo de acuerdos llevadas a cabo a través de instituciones internacionales, relaciones bilaterales o multilaterales, negociaciones y compromisos con Naciones Unidas,

---

(17) Lt.Col. April Cunningham, portavoz del Pentágono en declaraciones a la BBC, en: *http://www.bbc.co.uk/mundo/movil/noticias/2011/07/110722_eeuu_pentagono_ciberespacio_estrategia_wbm.shtml*

(18) Hallett Carr, Edward: *The Twenty-Years Crisis 1919-1939: Introduction to the Study of International Relation*, Harper Collins, Nueva York, 1964.

(19) Worley, D. Robert: *Orchestrating the Instruments of Power: An Examination of the U.S. National Security System,* 2008, en: *http://www.drworley.org/Pubs/Orchestrating/*

(20) El Departamento de Defensa estadounidense los define como «todos los medios disponibles por el Gobierno para la persecución de los objetivos nacionales». *Joint Publication 1-02,* Department of Defense Dictionary of Military and Associated Terms, 15 de agosto de 2011, en: *http://www.dtic.mil/doctrine/index.html*

(21) *Joint Publication 1-02,* 15 de agosto de 2011.

otros Estados, organizaciones internacionales o no gubernamentales. El producto de las negociaciones suelen ser tratados y acuerdos internacionales. Normalmente este poder es ejercido por los Ministerios de Asuntos Exteriores. Una de las armas fuertes del instrumento diplomático es el poder de reconocimiento de Estados soberanos

2. *Información*: el instrumento de la información difunde y recolecta información al/del público, tanto interno como externo. Es el equivalente a la oficina de relaciones públicas de un país; la que se encarga de dar a conocer al mundo qué es lo que quiere el país y cómo lo quiere conseguir. Este instrumento también recopila información relativa a la historia, cultura y las actitudes de otros países.
3. *Militar*: es el que utiliza la fuerza militar sobre los escenarios físicos para la consecución de objetivos nacionales. Se emplean en operaciones de guerra y en otras diferentes a la guerra, tales como establecimiento de la paz, mantenimiento de la paz, asistencia humanitaria y ayudas en desastres. Hasta ahora las fuerzas militares estaban constituidas conforme al escenario físico en el que operaban: tierra, mar, aire y espacio. Ahora deberán surgir las del ciberespacio.
4. *Económico*: el instrumento económico utiliza el poder de la riqueza de un país para influir en las acciones de los demás. El poder económico de una nación presenta dos caras: la coercitiva, por medio de sanciones económicas, embargos, bloqueos, restricciones a importaciones o exportaciones, políticas comerciales restrictivas, etc. y la colaborativa, que se hace a través de la ayuda exterior, políticas favorables al desarrollo, etc. El instrumento económico es un arma muy potente y coactivo.

Es importante destacar la estrecha interrelación que existe entre todos los instrumentos de poder. El instrumento diplomático negociará sobre temas de seguridad y militares o económicos y sus logros se divulgarán mediante el instrumento de la información. O, por ejemplo, el instrumento de la información será responsable de la difusión de comunicaciones relativas a la política y las acciones militares del país, a sus resultados diplomáticos o a sus negociaciones económicas. Sucesivamente se pueden establecer relaciones entre todos los demás. Para que los instrumentos de poder representen realmente una fuerza en apoyo de la nación tienen que ser fuertes individualmente y estar compensados entre ellos.

De todos los instrumentos de poder sólo uno incide directamente en el mundo físico: el militar. Todos los demás presentan la dicotomía de

mostrar una parte cognitiva, la que le da valor, y otra física, meramente circunstancial. La parte cognitiva representa el valor del significado que tiene un acuerdo diplomático, un embargo económico o una noticia; la parte física es su mera representación en un soporte (documento, cinta, archivo, etc.). Sin embargo, es sobre esta última en la que incide hoy día el ciberespacio. Lo que se roba, lo que se altera o lo que se intercepta en el ciberespacio son los datos que conforman esos archivos o las transmisiones que los mueven. Este hecho es capaz de alterar la parte cognitiva, por lo que su seguridad ha adquirido tanta importancia como su contenido.

El mundo físico tiene, por tanto, una gran transcendencia sobre los instrumentos de poder de una nación, ya sea por incidencia directa (el militar) o circunstancial (diplomático, económico y de información). Este mundo físico tiene su reflejo en los escenarios de conflicto.

## Los escenarios

> «El ciberespacio no es ni una misión ni una operación. Es un escenario estratégico, operacional y táctico» (22).

Un escenario es un lugar donde ocurre o se desarrolla un suceso (23). Un escenario de conflicto es el lugar donde ocurre o se desarrolla un conflicto. La Historia nos revela que a lo largo de los siglos, el ser humano ha ido extendiendo sus zonas de conflicto a aquellos escenarios que progresivamente ha ido dominando, naturales y artificiales.

El hombre es conflictivo por naturaleza y para resolver sus discrepancias utiliza, como se ha visto, los instrumentos de poder que tiene a su disposición. Entre ellos, el poder militar actúa sobre el entorno físico, para cuyos escenarios las naciones han ido formando ejércitos profesionales especializados conforme se fueron progresivamente dominando.

Los escenarios físicos son los llamados escenarios tradicionales de conflicto, los que están delimitados por un entorno físico, natural o artificial, con dimensiones y fronteras, ocupan extensión o espacio y que pueden ser determinados y definidos mediante la utilización de aparatos de medida. Estos escenarios físicos sobre los que se llevan a cabo las opera-

(22) Doctora Lani Kass, directora *del Air Force Cyberspace Task Force* de la USAF.
(23) Real Academia de la Lengua, vigésima segunda edición.

ciones militares constituyen los *entornos operacionales* o *dominios de guerra*.

El instrumento de poder militar, para poder ejercer su fuerza sobre los escenarios, requerirá disponer de unas capacidades militares defensivas y ofensivas y unos medios que permitan alcanzar la superioridad en cada entorno operacional específico.

Los escenarios físicos sobre los que actúa el instrumento de poder militar son cinco: *terrestre, marítimo, aéreo, espacial* y *ciberespacial.*

*El escenario terrestre*

Como animal eminentemente terrestre, el hombre ha desarrollado casi toda su existencia y actividades en la tierra; el acceso a cualquiera de los otros dominios es puramente circunstancial y transitorio. Considerando al *Homo Sapiens* como el origen del hombre actual, durante unos 200 mil años el ser humano ha vivido, cazado, pescado, viajado y peleado sobre la superficie terrestre. El escenario terrestre fue el protagonista de sus disputas, donde se generaban, evolucionaban y resolvían los conflictos. Las diferencias entre individuos, familias, tribus o clanes se solventaban sobre los propios territorios que se querían defender o dominar.

El medio terrestre presenta unas características únicas y diferenciadas. El combate se hace sobre la tierra en todas sus formas y extensiones (bosques, montañas, desiertos, etc.) para lo que requiere unos medios concretos y específicos para el transporte y movimiento de fuerzas, diferentes a los de los otros escenarios: vehículos, tracción animal, etc. así como tácticas y procedimientos específicos. El empleo de las fuerzas terrestres se basa, como en todas las fuerzas, en el fuego y el movimiento, un adecuado reconocimiento previo, la búsqueda de una posición ventajosa y la sorpresa.

*El escenario marítimo*

Los primeros conflictos navales de los que hay constancia en la Historia tuvieron lugar entre los llamados pueblos del mar contra hititas y egipcios entre los siglos XIII y XII a. C. para el control local del Mediterráneo Oriental. Aunque es posible que los hubiera anteriores, éstos no están documentados. Sin embargo, fue con la exploración de las costas de

los fenicios con quienes, a partir del 1200 a. C., se produjo el verdadero dominio de los mares y el transporte y el comercio marítimo tuvieron una mayor expansión.

El escenario marítimo y fluvial se convirtió hasta el siglo XVIII en el medio de transporte principal de mercancías y personas, ya que los medios terrestres eran excesivamente lentos, cansados y caros. Durante las campañas europeas de los siglos XVI, XVII y XVIII, las vías marítima y fluvial eran casi las únicas con las que se abastecían los ejércitos de personal, armamento, municiones y víveres.

El medio marítimo presenta también características exclusivas. El combate se hace sobre o bajo la superficie del medio acuático y en los que es necesario unos medios específicos para el movimiento: barcos, lanchas, submarinos, etc. Este medio precisa también de tácticas de combate propios de su entorno. El empleo de las fuerzas marítimas se rige por los mismos principios que las terrestres, el fuego y el movimiento, reconocimiento previo, posición ventajosa y sorpresa.

*El escenario aéreo*

Durante unos 4.000 años el hombre resolvió sus diferencias entre los escenarios terrestre y marítimo. El dominio de la tercera dimensión, el aire, tan sólo se encontraba en los intentos de algunos aventureros o en la mente imaginativa de ciertos estudiosos.

El descubrimiento del globo aerostático en el siglo XVIII y su posterior aplicación en los enfrentamientos bélicos para observación, estudios topográficos y para la dirección y corrección del tiro de la artillería, introdujeron a los medios aéreos de lleno en la vorágine de los conflictos.

El despegue final tuvo lugar a principios del siglo XX cuando una máquina más pesada que el aire y autónoma se elevaba sobre la superficie terrestre y podía ser controlada y dirigida por el hombre a voluntad. El empleo masivo de este nuevo escenario para su utilización en los conflictos armados no se hizo esperar.

El medio aéreo presenta unas características únicas y diferenciadas, como son el empleo de las tres dimensiones y una mayor velocidad que sus homólogos terrestre y marítimo. El combate en el aire requiere unos medios totalmente diferentes a los necesarios en los otros entornos y unas tácticas y procedimientos específicos.

*El escenario espacial*

Finalizada la Segunda Guerra Mundial, los avances tecnológicos adquiridos en el perfeccionamiento de los motores cohete facilitaron el desarrollo de la era espacial. A finales de los años cincuenta se ponen en órbita los primeros satélites artificiales no tripulados y a los pocos años se consigue que un ser humano orbite en torno a la Tierra. En el año 1969 el hombre alcanza la Luna y en 1971 se lanza la primera estación espacial, la *Salyut* soviética, origen de una serie de estaciones permanentes de diversos países (*Skylab*, MIR, ISS) utilizadas para investigación científica y estudio del espacio. El lanzamiento en los años ochenta de los transbordadores espaciales permitió disponer de una lanzadera reutilizable, lo que abarató los costes de la carrera espacial e incrementó su expansión.

Muchos países disponen en la actualidad de satélites artificiales en órbitas terrestres, propios o compartidos, pero pocos son los que tienen una capacidad militar espacial real. Los enormes costes de Investigación y Desarrollo (I+D) hacen que la mayoría carezcan de fuerzas y medios para el combate en el espacio. Sólo aquellos que sí la tienen se han planteado la utilización del espacio como un escenario de conflicto.

Aparte de en las películas de ciencia-ficción, la utilización real de armamento en el espacio es, por lo que se conoce –debido al celo con que esta información se guarda–, bastante reducida. En los años ochenta, en la época del presidente Ronald Reagan se puso en marcha la Iniciativa de Defensa Estratégica (IDE), sistema basado en tierra y en el espacio que formaba un escudo antimisiles para proteger a Estados Unidos de posibles agresiones soviéticas con misiles balísticos intercontinentales. En la década de los años dos mil, la administración del presidente Bush retomó esta idea con una nueva adaptación reducida del mismo y revitalizó el Programa Militar del Escudo Antimisiles (ABM). Aunque en el año 2009, el presidente Barack Obama renunció a continuar con el desarrollo exclusivo del ABM, uno basado en éste fue adoptado por la Organización del Tratado del Atlántico Norte (OTAN) en el año 2010. ¿Pero es este ABM parte de la guerra en el espacio? Ciertamente es un principio.

*El ciberespacio*

Sin entrar en definiciones rigurosas ni en excesivas complicaciones semánticas, la manera más sencilla de definir Internet es como la interco-

nexión mundial de redes de datos. El lugar físico que ocupan estas redes es el ciberespacio.

Aunque las primeras conexiones entre computadoras se establecieron en los años sesenta, fue en la década siguiente cuando nació ARPANET el primer embrión de la actual Internet.

Tras este despegue, la Red inició una vertiginosa carrera: en la década de los *años setenta* surge la denominación Internet y el protocolo TCP-IP, que facilitó enormemente su expansión. En la década de los *años ochenta*, ARPANET adopta este protocolo; en el año 1984, el escritor William Gibson populariza la palabra ciberespacio en una de sus novelas, término que en breve tiempo se empezó a identificar con Internet; también en esta década se popularizan los BBS (24). A principios de los *años noventa* nace la *web* (*www*) (25), gracias a la creación del lenguaje HTML y a la unión de los enlaces de hipertexto (idea que databa de los años sesenta) con Internet; a finales del año 1991 se crean los primeros servidores *web*, navegadores y editores *web* y las primeras páginas *web*. El lanzamiento definitivo tuvo lugar con la aparición en el año 1993 del navegador Mosaic, cuyo entorno gráfico facilitó enormemente el acceso de los usuarios a la Red y su posterior expansión ha llegado hasta lo que hoy conocemos.

En Internet existen multitud de servicios. Los más conocidos son la *web* y el correo electrónico, pero también presta otros muchos como la transmisión de ficheros, el acceso remoto, chats, mensajería instantánea, telefonía, televisión, etc.

El rápido progreso tecnológico permitió el aumento de las capacidades de los equipos informáticos y de comunicaciones y la facilidad, comodidad y rapidez con la que se accedía a la información fue incrementando la fiabilidad del sistema y la confianza de los usuarios en él, por lo que administraciones, empresas y usuarios volcaron todos sus viejos ficheros y conocimientos en servidores de archivos gestionados por sistemas de información conectados en red.

---

(24) *Bulletin Board System.* Sistema de tablón de anuncios: *software* de redes, principalmente en modo texto, precursor de los actuales foros que permitía el intercambio de mensajes entre usuarios, leer noticias, descarga de *software,* intercambio de ficheros (incluidos los primeros virus), juegos en línea y otras funcionalidades.

(25) No hay que confundir la *web* con Internet. La *web* es tan sólo un servicio más de los que corren por Internet.

Mientras que la industria ha progresado desarrollando sus sistemas poniendo mayor énfasis en su robustez y su interoperabilidad, se ha ido dejando un poco de lado el tema de la seguridad, probablemente guiados por el principio de primar la operatividad sobre la seguridad. A partir de este error surgieron las vulnerabilidades físicas y lógicas, en sistemas operativos, también en aplicaciones y protocolos de comunicaciones.

Aprovechando estas vulnerabilidades, aparecieron como un juego los primeros virus de los que pronto se descubrió su gran potencial maligno, que se convirtieron en las armas del ciberespacio. Los beneficios que esta explotación podría proporcionar a determinados sectores, grupos o mafias impulsaron definitivamente su I+D. Apareció la ciberdelincuencia, los ciberataques, el ciberespionaje, el ciberterrorismo y, lógicamente, la ciberdefensa.

Sin embargo, la capacidad de las naciones para defender sus redes y sistemas siempre quedará por detrás de la habilidad del enemigo para aprovecharse de sus puntos débiles. Siempre existirán vulnerabilidades susceptibles de ser descubiertas por los expertos y siempre se superarán las medidas de seguridad que se impongan para intentar evitar intrusiones. En un entorno eminentemente ofensivo, una mentalidad basada en la mera acción defensiva no tiene futuro.

Nos encontramos ahora en un *nuevo escenario físico*, desarrollado de manera vertiginosa en los últimos 30 años y en el que apenas se ha puesto cuidado en la seguridad, del que nuestra sociedad se ha hecho totalmente dependiente y en el que han surgido importantes amenazas que explotan los fallos de su rápido diseño para obtener pingües beneficios, lo que pone en riesgo nuestro bienestar. Hace falta, por tanto, una fuerza capaz de operar en este nuevo entorno que proteja a la nación de las crecientes amenazas.

### CARACTERÍSTICAS COMUNES DE LOS ESCENARIOS FÍSICOS TRADICIONALES

Los escenarios físicos tradicionales (terrestre, marítimo, aéreo y espacial) presentan en común ciertas características que han hecho que se los considere como un conjunto unificado:

– *Sus actividades se llevan a cabo en un escenario físico único y diferenciado*. El dominio en el que se desenvuelven es un área física gobernada por las leyes de la física. El escenario terrestre está sobre tierra

firme; el marítimo, en el agua; el aéreo, en el aire y el espacial, en el espacio extra atmosférico.

– *Requieren la utilización de medios específicos para moverse, desenvolverse y combatir en él.* Cada escenario requiere sus propios medios de operación, no aptos para su empleo en los otros entornos: vehículos blindados, motorizados, buques, lanchas, aviones, helicópteros, satélites o lanzaderas.
– *Tienen una doctrina de empleo específica* (26). Acorde a las peculiaridades del combate en ese medio. Existen unas doctrinas terrestre, naval, aérea y espacial perfectamente definidas y diferenciadas para cada dominio.
– *Disponen de técnicas y tácticas de combate adecuados al medio en que se desenvuelven*. Las características físicas de cada dominio hacen necesario el disponer de medios específicos para ellos.
– *Se complementan las unas a las otras*. Siendo imposible concebir una defensa global sin la existencia de todos ellos. Hoy día la consecución de los objetivos nacionales son inviables sin considerar la defensa global como un todo y la ejecución de las operaciones militares de manera conjunta.
– *Se rigen siguiendo los principios de la guerra* (27). Objetivo, ofensiva, concentración de fuerzas, economía de esfuerzo, maniobra, seguridad, sorpresa, voluntad de vencer y unidad de esfuerzos.
– *El elemento humano es el factor más decisivo para su empleo*. En cualquiera de los dominios el factor humano es imprescindible para el combate con los medios específicos de que disponga. Actualmente los medios son máquinas y las máquinas son creadas y manejadas por el hombre.
– *El elemento humano exige un área de competencia y experiencia profesional diferenciada al resto de los dominios y requiere una formación específica.* La necesidad de una formación rigurosa y exclusiva del personal que tenga que desempeñar su misión en cada uno de los dominios es, probablemente, uno de los factores más importantes y característicos de cada uno de los entornos.

---

(26) La doctrina es una colección integrada de lecciones aprendidas de experimentos, ejercicios y enfrentamientos anteriores que aceptamos como las mejores prácticas para llevar a cabo la guerra.

(27) Éstos son los más tradicionalmente aceptados en las doctrinas de la mayoría de los países del mundo occidental, sin que su orden implique preferencia alguna. Doctrina Aeroespacial.

APLICACIÓN AL CIBERESPACIO

Para el Departamento de Defensa de Estados Unidos, el ciberespacio se ha convertido un campo de operaciones de igual entidad que la tierra, el mar, el aire o el espacio y por tanto susceptible de ser escenario tanto de maniobras defensivas como ofensivas, lo que podría incluir ataques preventivos y represalias (28).

Pero ¿qué es lo que ha llevado al Departamento de Defensa estadounidense a realizar tal afirmación? ¿Se le pueden aplicar al ciberespacio las características comunes vistas anteriormente?:

– El ciberespacio es un *escenario físico único y diferenciado*. El ciberespacio es un entorno físico incluso de mayor extensión que los tradicionales. Aunque popularmente se le viene denominando «espacio virtual», el ciberespacio de «virtual» tiene bien poco (29). El ciberespacio está compuesto por una tela de araña de equipos informáticos y de comunicaciones, interconectados mediante enlaces físicos (cables) o inalámbricos (Wi-Fi, radio, etc.) formando un enjambre de redes entrelazadas entre sí. Posee, por tanto, una dimensión nítidamente definida que malla los espacios terrestre, marítimo, aéreo y espacial que puede ser medible y observable de una manera precisa mediante los sentidos o instrumentos electrónicos de medida.
– El ciberespacio *requiere la utilización de medios específicos para moverse, desenvolverse y combatir en él*. La lucha en el ciberespacio no precisa de carros de combate, ni fragatas, ni aviones. Al igual que los medios utilizados para el combate terrestre, naval o aéreo son muy diferentes a los empleados en el mundo civil (disponen de defensas, armamento, prestaciones superiores, etc.), los medios en los que se ha de desenvolver la guerra en el ciberespacio tampoco pueden ser los que utilizamos en casa para conectarnos a Internet. Estos deberán estar especialmente diseñados y configurados para combatir en el nuevo escenario: ordenadores, portátiles, tabletas, teléfonos, cortafuegos, Sistema de Detección de Intrusos, Sistema de Previsión de Intrusos, SIEM (30) con componentes *hardware* robustecidos, con sistemas operativos y aplicaciones especialmente diseñados y codi-

(28) *Department of Defense Strategy for Operating in Cyberspace,* julio de 2011.
(29) Definición de la Real Academia de la Lengua, vigésima segunda edición, «virtual», que tiene existencia aparente y no real.
(30) *Security Information Event Management:* son equipos de correlación y gestión de eventos de seguridad de la información.

ficados, con configuraciones reforzadas y con redundancia que les permita tener una alta disponibilidad para asegurarse la supervivencia en caso de ataques contra ellos mismos, que utilicen redes y protocolos de comunicaciones seguros (31), así como todas aquellas otras medidas que hagan a estos sistemas lo más resistentes posibles en un entorno hostil.

– Las operaciones en el ciberespacio requieren *una doctrina de empleo específica*, acorde a las peculiaridades del combate en ese medio. La exclusividad del combate en este nuevo entorno ha originado que numerosos países hayan ya elaborado una doctrina propia e independiente para él. No obstante, al ser un dominio nuevo y encontrarse en una etapa muy inicial de desarrollo, las ciberoperaciones, carecen todavía de la historia y de la experiencia vital necesaria (32) para establecer enunciados de doctrina firmes. Además de la doctrina específica, habrá que desarrollar la nueva doctrina conjunta en la que se tengan presentes las operaciones en el ciberespacio como una parte más de las operaciones conjuntas.
– Las operaciones en el ciberespacio disponen *de técnicas y tácticas de combate adecuados al medio* en que se desenvuelven. Las características físicas de cada dominio modelan sus tácticas y técnicas de combate. Las tácticas del movimiento terrestre son sustancialmente distintas de las del movimiento naval y éstas, de las aéreas; lo mismo es aplicable al combate, a la logística, etc. ¿De dónde extraemos las tácticas y técnicas del combate en el ciberespacio? ¿De la doctrina terrestre, de la naval, de la aérea? De ellas sólo podemos extraer unos cuantos principios básicos que son axiomas doctrinales, pero las tácticas y técnicas del ciberespacio son nuevas, únicas y radicalmente distintas de las de los otros entornos. Al igual que no es lo mismo un vuelo visual realizado por un instructor y su alumno en una avioneta de un aeroclub, que una baja cota sobre territorio enemigo en una misión de combate realizada por un caza, tampoco es lo mismo el acceso a un servidor para ver las noticias en nuestro diario favorito o bajarse unos archivos, que acceder al mismo para penetrar en su red, corrom-

(31) Como el DTN *(Disruption Tolerant Networking).* Es un protocolo de comunicaciones creado para evitar las interrupciones y las demoras en las comunicaciones en el espacio. Su aplicación en las redes terrestres podría tener importantísimas connotaciones de seguridad. Tucker, Christopher K. (dir.): *Certifing Cyberspace,* High Frontier, agosto de 2010.

(32) *Véase* nota 16. Definición de doctrina.

per su base de datos o robar determinados documentos. Las tácticas y las técnicas de la guerra en el ciberespacio son diferentes a las de los otros dominios y son diferentes a las del mismo dominio utilizado con fines pacíficos.

– Las operaciones en el ciberespacio *se complementan a las de los dominios convencionales*, siendo imposible concebir una defensa global sin la existencia de todos ellos. La doctrina conjunta ya determina la necesidad del empleo coordinado de todas las fuerzas militares de una nación para la consecución de los objetivos nacionales. Pero tras la aparición del nuevo entorno, el ciberespacio, es imprescindible contar con sus fuerzas específicas en un nuevo planeamiento conjunto. El dominio del ciberespacio no sólo irá en apoyo y en beneficio de las acciones de los ejércitos y la fuerza naval, sino que será prioritario e imprescindible para el eficaz empleo de las fuerzas convencionales.
– Las operaciones en el ciberespacio *se rigen igualmente siguiendo los principios de la guerra* (33): Disponen de un objetivo único estratégico, operacional o táctico; precisa de la acción ofensiva súbita que le proporcione la iniciativa; demanda concentración de fuerzas con una distribución de recursos eficiente, tanto en ofensiva como en defensiva; se maniobra con seguridad, mediante acciones de ciberespionaje, para obtener una posición ventajosa sobre el adversario y todo ello bajo la dirección de un mando único al más alto nivel.
– *El elemento humano es el factor más decisivo para el empleo del ciberespacio*. Más que en ningún otro entorno, el elemento humano es importante en la lucha en el ciberespacio. El ciberespacio es un medio artificial, creado por el hombre, por lo que éste es un factor crítico en su desarrollo y evolución. En el extremo final de toda máquina ubicada en el ciberespacio, siempre habrá una persona que la controle, la administre, la configure, la programe o la repare y, sobre todo, una persona que tome las decisiones y ordene las acciones oportunas en función de los datos que las máquinas le presenten.
– *El elemento humano en el ciberespacio exige un área de competencia y experiencia profesional diferenciada al resto de los dominios y requiere una formación específica*. El combate en cada uno de los entornos presenta unas peculiaridades que requieren una exhaustiva formación específica para su personal. Así como la formación de un piloto co-

(33) Éstos son los más tradicionalmente aceptados en las doctrinas de la mayoría de los países del mundo occidental, sin que su orden implique preferencia alguna. Doctrina Aeroespacial.

mercial no es la misma que la de un piloto de combate, en el ciberespacio también se necesita una formación muy específica y desarrollar unas competencias muy diferenciadas sobre el resto de combatientes y sobre el resto de internautas. El combate en el ciberespacio requiere profundos conocimientos y experiencia en seguridad informática, redes, protocolos de comunicaciones, sistemas operativos, bases de datos, programación, herramientas y tecnologías de seguridad, que permitan al combatiente desenvolverse con soltura en un mundo complejo y extremadamente veloz.

CARACTERÍSTICAS DIFERENCIADORAS DEL CIBERESPACIO

Al igual que los espacios terrestre, marítimo, aéreo y espacial mantienen evidentes diferencias entre sí, diferencias que les hace únicos, el ciberespacio también presenta determinadas singularidades:

– El ciberespacio es un dominio casi infinito. Los dominios terrestre, marítimo y aéreo están perfectamente delimitados físicamente unos de otros. El dominio espacial es más amplio, pero abarca tan sólo hasta donde sea capaz de llegar el ser humano con sus medios materiales. Lo que hace particularmente destacable del ciberespacio es que físicamente se integra en el conjunto de los otros cuatro. Allá donde en cada uno de estos dominios exista un punto de comunicación enlazado con otro, ahí tendrá cabida el ciberespacio.
– El ciberespacio evoluciona a una velocidad muchísimo mayor que sus homólogos convencionales. La evolución del ciberespacio ya no sólo es debido al progreso tecnológico, sino también a la evolución del código *software* y de los algoritmos, al número de recursos que lo conforman y al de usuarios que lo utilizan. La capacidad de expansión del ciberespacio y su capilaridad dentro del propio espacio físico en el que se expande es prácticamente ilimitada (34).
– Los dominios tradicionales precisan de sistemas de armas para hacer sentir el poder terrestre, naval o aéreo. En el ciberespacio no; las armas no son cinéticas. Aquí también existen armas defensivas y ofensivas, pero son de índole totalmente diferente. Las armas defensivas están

(34) Con la implantación definitiva de IPv6, las direcciones del Protocolo de Internet (IP) que habrá disponibles para la conectividad de equipos ascenderá a la escalofriante cifra de 340 sextillones (34 por 1.036), lo que permitiría asignar, aproximadamente, unos 670.000 billones de direcciones a cada milímetro cuadrado de la superficie de la Tierra.

compuestas por dispositivos de análisis y control de tráfico de red, *hardware* y *software* de seguridad, configuraciones correctas, procedimientos, y por la formación y concienciación de técnicos y usuarios. Las armas ofensivas se construirán en base a la investigación, generación de código, unos conocimientos adecuados y unas tácticas y técnicas especializadas.

– Así como los medios de combate en los escenarios terrestre, marítimo y aéreo normalmente sólo están al alcance de los Estados, los medios del ciberespacio están a disposición de toda la población mundial que disponga de un acceso a la Red.
– El principal valor en los entornos terrestre, marítimo y aéreo, aparte del propio ser humano, son los medios materiales, los sistemas de armas, su despliegue, su efectividad y su operatividad. Sin ellos, la lucha en estos entornos carece de sentido. En el ciberespacio el principal valor es la información, la que en la defensiva se ha de proteger y en la ofensiva se ha de negar, alterar o sustraer al enemigo. La calidad de la información que se posea es más importante que la cantidad.
– Aunque el ciberespacio es un escenario físico y está gobernado por las leyes de la física dimensional, no le son de aplicación las mismas leyes que a los escenarios convencionales. En éstos, los sistemas de armas han de tener en cuenta pesos, volúmenes, rozamientos y otras características físicas. En el ciberespacio, su principal valor, la información, es realmente inmaterial, no pesa, carece de masa, no ocupa más que lo que ocupe su sistema de almacenamiento (del cual además se puede independizar), se puede modificar y alterar y convertirse de favorable en desfavorable en décimas de segundo.
– El ciberespacio se ha convertido en la primera línea de batalla, el primer escenario de combate de cualquier acción bélica moderna, por delante de las acciones realizadas en los escenarios tradicionales.
– Así como los conflictos tradicionales se centran en el campo de batalla, el ciberespacio extiende la zona de combate hasta el mismo corazón de la nación, al ser capaz de entrar en cada una de las casas de los ciudadanos y de cortarle los suministros básicos que éste necesita para su supervivencia.

### CAUSAS POR LAS QUE LOS CONFLICTOS SE EXPANDEN AL CIBERESPACIO

Pero ¿cuáles son las causas que hacen del ciberespacio un entorno en el que tienden a generarse y evolucionar, cada vez con mayor intensidad,

las situaciones de conflicto? ¿Por qué los conflictos se están trasladando o tienen como primera etapa la lucha en el ciberespacio?

*Por las características físicas del entorno*

Por su *capilaridad y ubicuidad*. Porque puede tener acceso a él cualquier persona desde cualquier lugar del mundo.

Por su *anonimato*. Porque este acceso puede ser totalmente anónimo y transparente en la Red y hacerse mediante acciones que hagan muy difícil saber, si no imposible, quién está realmente detrás de ellas. En un conflicto convencional, es fácil imputar un hecho determinado a un individuo, grupo o Estado, pero mientras un acto puntual no pueda ser atribuido a algún actor concreto, el ciberespacio facilitará inmunidad al atacante.

Por su *seguridad*. La dificultad de la localización del atacante le proporciona seguridad. Aun existiendo la posibilidad de ser descubierto de manera fehaciente, la característica de su ubicuidad y movilidad haría que el riesgo físico del agresor fuera mínimo, puesto que la posibilidad de una respuesta cinética a un ataque cibernético, si bien factible, es muy improbable.

*Por sus características económicas*

Por su *eficiencia*: un ordenador, utilizado como arma en una acción ofensiva por personal especializado es de resultados muy rentables, por ser económica y efectiva. Estas armas son indudablemente más baratas que sus homólogas cinéticas y su destrucción no representa ventaja militar alguna para el enemigo, puesto que fácilmente se puede disponer de miles de ellos.

Por su *rendimiento*: un pequeño ordenador hoy día es capaz de realizar muchos millones de operaciones por segundo. Teniendo en cuenta que un ciberataque se puede llevar a cabo de manera efectiva con unos cuantos cientos de líneas de código, el rendimiento de estas pequeñas máquinas puede llegar a ser altísimo. Con un simple equipo, un atacante preparado puede llegar a originar y sostener de manera individual acciones devastadoras con suficiente potencia como para paralizar un país.

Por su *mantenibilidad*: en un conflicto convencional, destruir el material es casi tan importante como neutralizar al adversario. En el ciberespa-

cio, destruir el material es prácticamente inútil por lo extremadamente sencillo que resulta su reposición. La mayoría de los equipos actuales tienen piezas intercambiables que les hace extremadamente flexibles en cuanto a configuración y reposición.

*Por sus características propagandísticas*

Por su *difusión:* un atacante puede buscar y obtener rápidamente adhesiones a su causa (voluntarias –por convencimiento– o involuntarias –mediante propaganda, engaños o *malware*–) gracias a la fácil difusión pública que puede hacer de ella por la Red y a la sencillez con que podrá obtener apoyos por parte de los internautas. Los riesgos físicos del que se adhiere a una causa son pocos o nulos. Por ejemplo, en el año 2008, tras el asalto israelí a la flotilla que intentaba romper el bloqueo de Gaza, Israel sufrió una serie de ataques cibernéticos de *Defacement* y denegación de servicios distribuidos contra alguna de sus instituciones por parte de grupos y personas que se adherían voluntariamente a la causa palestina y que, tras visitar una determinada página *web*, se descargaban un *malware* que hacía que el equipo del visitante quedara integrado en una *botnet*, que era la que ordenaba los ataques de denegación de servicio contra los sitios israelíes (35).

Por su *divulgación*: antes de la existencia del ciberespacio, la divulgación de las noticias era más lenta y siempre dependía de terceros para una rápida y exitosa difusión. Los resultados de las acciones que se hagan en el ciberespacio, cuando han sido exitosas, se divulgan a gran velocidad por la Red, lo que hace poner en evidencia y en conocimiento de todos las capacidades ofensivas o defensivas de los agentes implicados. Si éstas son buenas, la propaganda será positiva y potenciará el efecto disuasorio. En el caso de ser negativas se harán públicas las debilidades existentes, lo que puede originar posteriores explotaciones por otros atacantes.

Por su *impacto*: los ataques con éxito (aunque tan sólo sean denegación de servicios distribuidos o *Defacements* (36) y más aún si son robo o mo-

---

(35) En: *http://www.europapress.es/tecnologia/internet-00446/noticia-web-banco-israel-cerrada-dos-dias-ciberataque-islamista-20080428184547.html* y *https://cert.s21sec.com/index.php?option=com_content&view=article&id=279:los-hackers-se-sirven-del-conflicto-de-gaza-para-difundir-malware&catid=53:otros&Itemid=69*

(36) Cambio o alteración no autorizada intencionada que se produce en una página *web* mediante la explotación de una vulnerabilidad del sitio *web.*

dificación de datos) tienen un fuerte efecto psicológico desmoralizador sobre los atacados debido a la sensación de vulnerabilidad y de impotencia que producen, especialmente si ya se habían adoptado ciertas medidas de seguridad.

*Por sus características operativas*

Por su *velocidad*: una de las mejores características del poder aeroespacial es su velocidad. La velocidad permite realizar operaciones y desarrollar un mayor número de ataques en menor tiempo. La velocidad facilita la sorpresa, disminuye los tiempos de reacción, aumentando las posibilidades de supervivencia (37). En el mejor de los casos, la máxima velocidad que pueden alcanzar los medios aeroespaciales es de varios miles de kilómetros por hora. Los ciberataques se producen a velocidades cercanas a la de la luz. En el ciberespacio, todas las ventajas y beneficios mencionados anteriormente para el poder aeroespacial quedan multiplicados por un millón.

Por su *alcance*: el alcance del poder militar convencional depende de su autonomía y de su capacidad de reabastecimiento. El alcance en el ciberespacio depende de la infraestructura de red disponible, que hoy día, gracias a los satélites de cobertura global, se puede considerar ilimitada. Desde cualquier lugar del mundo se puede tener acceso instantáneo a cualquier otro lugar, siempre que exista un terminal conectado a la Red, ya sea mediante conexiones cableadas o inalámbricas.

Por su *fácil acceso*: en la mayoría de los países civilizados adquirir un arma ofensiva exige un riguroso registro por parte de las autoridades. Para adquirir alguna fuera de este control hay que ir al mercado negro, que suele estar más o menos vigilado y perseguido por los Cuerpos y Fuerzas de Seguridad del Estado. Las armas ofensivas en el ciberespacio están compuestas por código al que, con los conocimientos adecuados, puede tener acceso toda persona desde cualquier lugar. Si bien es cierto que parte de este código empieza a ser controlado por las mafias y bandas organizadas con el objeto de sacar de él un beneficio económico, otro se encuentra libremente en Internet y también siempre existirá la posibilidad de que cualquiera, desde el salón de su casa, pueda generar y extender un código de catastróficas consecuencias.

(37) Doctrina Aeroespacial.

Por su *facilidad de coordinación*: las acciones, una vez conjuntadas y coordinadas pueden ser devastadoras. Tomada la decisión de perpetrar un ataque, hay que conjuntarlo y coordinarlo, acción ésta que en el ciberespacio se suele conseguir por medio de *botnets*. En el caso de no existir el control por medio de *botnets*, las características de la comunicación en el ciberespacio hacen que la coordinación de un ataque en un tiempo y lugar determinado sea relativamente fácil de llevar a cabo.

Por su *disuasión*: un ciberataque fulminante previo a un ataque convencional puede dejar paralizada o muy incapacitada a una nación. La prueba se tuvo en Georgia en el año 2008. La mera posibilidad de que esto ocurra, junto con la capacidad conocida de una nación adversaria para poder llevarlo a cabo es suficiente como para que represente un importantísimo factor de disuasión.

Por el *factor miedo*: el sentimiento de vulnerabilidad e indefensión que produce el hecho de saber que se están sufriendo ataques y desconocer de dónde provienen o comprobar que no están focalizados en una zona concreta, sino que se encuentran dispersos a lo largo de la geografía mundial, generan una sensación de impotencia que produce un terrible efecto desmoralizador. Otra acción que incrementa este factor miedo es el hecho de que los atacantes vayan difundiendo en directo la consecución de sus diferentes objetivos, como pasó en agosto de este año con los ataques de *Anonymous* a países suramericanos en la denominada operación *Andes Libres* que iba siendo anunciada por *Twitter* y *Facebook*.

Por su *difícil atribución*: cuando un ciberataque está bien hecho, es prácticamente imposible saber su origen; en el caso de que no esté tan bien hecho, puede llevar días, incluso meses descubrirlo. Esta situación proporciona grandes ventajas al atacante sobre el defensor, que verá claramente mermada su capacidad para tomar acciones decididas e inmediatas de contraofensiva.

Por su *potencia*: un ciberataque bien organizado, coordinado y dirigido a la línea de flotación de un país puede dejar inutilizado sus sistemas de comunicación, sus infraestructuras críticas o su capacidad de mando y control, tanto civil como militar. Esto puede hacer que se desestabilice su centro de gravedad y le produzca graves consecuencias políticas, económicas o sociales.

Por la *criticidad del objetivo*: siempre se ha dicho que la información es poder y todos los países requieren información en cantidad y en calidad.

Aparte de la vida humana, el mayor valor que tiene hoy día nuestra sociedad es la información. Ésta mueve todo, las decisiones políticas, las económicas, las militares, las sociales, las industriales. La información controla nuestras vidas, nuestras máquinas, nuestro pasado, presente y futuro. Hasta hace bien poco esta información se almacenaba en documentos en soporte físico, pero el desarrollo de las redes de comunicaciones y los sistemas de información han hecho que en la actualidad la mayoría haya sido confiada y volcada en estos sistemas para su mejor y más eficiente almacenamiento, procesamiento, transmisión y explotación. Los dirigentes y mandos necesitan información para su toma de decisiones; los sistemas de armas requieren información para obtener una mayor precisión o ser más efectivos. Unos y otros dependen inexorablemente de los sistemas de información y de las comunicaciones, que actualmente constituyen el centro de gravedad de los países más desarrollados. Esto hace que se hayan convertido en objetivos críticos. El movimiento de la información de un sistema a otro a través de las redes de comunicación representa una vulnerabilidad explotable en cualquiera de las fases de su recorrido, lo que le convierte en objetivo primordial para cualquier acción ofensiva.

## Organización de la ciberdefensa

*En busca del potencial necesario*

El Departamento de Defensa de Estados Unidos, a través de su subsecretario, William Lynn, ha hecho público la decisión de abordar una estrategia defensiva cibernética en el que contará con recursos militares. Según sus palabras, esto supone que si se considera un ataque informático peligroso para la vida de civiles o para la Seguridad Nacional, el presidente podrá responder con los medios que tenga a su alcance, incluyendo el militar.

¿Es esto lo que se quiere? ¿Es esto lo que políticamente se está dispuesto a aceptar? ¿Buscamos tan sólo proteger nuestras redes o realmente queremos una capacidad que permita el empleo a voluntad del poder militar para obtener la superioridad local en el ciberespacio cuando sea necesario para la defensa de los intereses nacionales?

Estas serían tan sólo las primeras preguntas a las que deberíamos darnos respuesta. El Jefe del Estado Mayor de la Defensa (JEMAD) en su

«Concepto de Ciberdefensa Militar» sí que define las capacidades militares que se deberán tener en el ámbito de los Sistemas de Mando y Control. Pero ¿y en el resto de los sistemas del Ministerio de Defensa? ¿Están definidos? ¿Por quién? ¿Con qué capacidades? ¿Y en el resto de la Administración? ¿Está definido el ámbito que hay que defender? ¿Y qué hay de las infraestructuras críticas?

Desgraciadamente la ciberdefensa no es sólo ciberdefensa militar. Si así fuera, sería algo más sencillo. La ciberdefensa ha de ser nacional y la militar tan sólo deberá ser una parte más de ella. España, ¿qué capacidades en el ciberespacio quiere tener? Y no hablamos sólo de capacidades militares, sino de capacidades nacionales de ciberdefensa. ¿Sólo defensivas? ¿También ofensivas? ¿Quién ha de tener estas capacidades? ¿Para qué? ¿En qué ámbito de actuación trabajarán cada uno de ellos?

Las capacidades nacionales (no sólo militares) que se pueden (y deben) tener en el ciberespacio son:

1. Capacidad defensiva.
2. Capacidad ofensiva.

*Capacidad defensiva*

Muchas veces se ha dicho que seguridad y operatividad son como el agua y el aceite, que no terminan de casar bien. Para empezar, la seguridad absoluta en la Red no existe y una operatividad insegura no es una verdadera operatividad. Por tanto habrá que definir el punto de la balanza en el que se obtengan una adecuada operatividad y una buena seguridad a un coste razonable. Esta decisión implicará aceptar riesgos y tomar decisiones.

Por todos es sabido que lo primero que tenemos que hacer cuando queremos defender algo es tener claro qué es lo que hay que defender. Se dice que el ciberespacio es uno de los cuatro *Global Commons* y que es difícil de delimitar. Pero sí el aire, que es otro de los cuatro, ha sido delimitado por las naciones en forma de espacio aéreo ¿qué nos hace pensar que no podría definirse igualmente un *ciberespacio nacional*, del mismo modo que también están definidas las fronteras o las aguas jurisdiccionales en la que cada país considera que es competente? Llegado el caso de que se hubiera podido concretar, el *ciberespacio nacional* sería inmenso, compuesto por todas y cada una de las ramificaciones de redes interconectadas entre sí y sus equipos como puntos intermedios

o finales. Querer defender todo el ciberespacio de un país sería como querer defender una casa con cientos de miles de puertas: una tarea casi imposible. Es preciso, por tanto, acotar más el *ámbito* que se consideraría necesario defender para asegurar el bienestar de los habitantes de la nación.

El problema con el que nos enfrentamos es que el ciberespacio de un país no es como sus fronteras terrestres, aguas jurisdiccionales o espacio aéreo, que son de todos los ciudadanos y que para su defensa colectiva se crea una fuerza determinada, esto es, ejércitos y fuerzas navales. El ciberespacio es igualmente de todos, pero lo que le diferencia es que está formado por una multitud de pequeñas posesiones individuales. Cada individuo, empresa, organismo, institución es propietario de una o varias de esos cientos de miles de puertas de la casa que hay que defender.

Para ejercer un control efectivo de cada individuo en la Red sería necesaria la implantación de algo parecido a un NAC (38) a nivel mundial, lo cual es bastante improbable, por no decir imposible. Para ello debería existir un organismo internacional que lo gestionara y definiera las políticas de acceso y rechazo en la Red. Sin duda el deseo de controlar este instrumento de gigantesco poder sería un nuevo motivo de enfrentamiento entre las naciones.

Para establecer la acotación del *ámbito de la ciberdefensa* de manera que diera protección a los intereses nacionales prioritarios, habría que establecer dos subámbitos de actuación:

1. El subámbito de control estatal: sería aquel sobre el que el Estado tiene la dirección y coordinación de la ciberdefensa. Este abarcaría:
   - Las infraestructuras críticas del país: administraciones, organismos e instituciones y empresas públicas o privadas consideradas como infraestructuras críticas del país.
   - Las Fuerzas Armadas (39).
   - Los Cuerpos y Fuerzas de Seguridad del Estado.

(38) *Network Access Control* (Control de Acceso a Red).

(39) La Ley 8/2011 que establece las medidas para la protección de las infraestructuras críticas en su artículo punto dos, excluye expresamente en su ámbito de aplicación a las infraestructuras del Ministerio de Defensa y de los Cuerpos y Fuerzas de Seguridad del Estado.

2. El subámbito de control privado: resto de empresas, organismos e instituciones privadas y particulares, en el que cada uno de ellos deberá tener su propio control de ciberdefensa.

La Ciberdefensa Nacional y la definición del ámbito completo de la ciberdefensa (subámbitos estatal y privado) deberá estar determinada, dirigida, organizada y coordinada *al más alto nivel* posible por un cargo, institución u organismo que tenga autoridad sobre todos los ministerios implicados en la Ley de Protección de Infraestructuras Críticas (Presidencia, Defensa, Interior, Economía, Industria, Fomento, Sanidad, etc.) y con potestad para promulgar una exhaustiva documentación legislativa que defina, entre otras cosas:

– La organización que cubra todo el abanico del ámbito a proteger.
– El reparto de cometidos y la definición de responsabilidades.
– La coordinación entre organismos.
– Requisitos mínimos y recomendaciones.
– Asignaciones presupuestarias y posibles subvenciones de apoyo a empresas, etc.

El determinar el ámbito completo de la Ciberdefensa Nacional, siendo un cometido de crucial importancia, no es tarea fácil y tendríamos que respondernos, entre muchas otras, a las siguientes preguntas:

– ¿Cómo se va a organizar la Ciberdefensa Nacional? ¿Mediante múltiples Equipos de Respuesta de Emergencia Informática (CERT)? ¿De alguna otra manera? ¿Quién coordinará todas las acciones? ¿Los CERT serán autónomos o estarán organizados en una estructura jerarquizada que incluya tanto públicos como privados, civiles y militares? ¿Se va a designar una figura o autoridad máxima (cargo, organismo o institución) responsable de la dirección, control y ejecución de toda la ciberdefensa con potestad sobre organismos públicos y privados? ¿Cómo será el flujo de información entre los CERT y cómo se van a distribuir las responsabilidades de control? ¿Qué tipo de tecnologías se van a emplear y cuáles serán los procedimientos de trasvase de información y alerta? ¿Habrá que procedimentar el tipo de defensa para cada organismo o institución en función de su criticidad y habrá que definir qué tipo de respuesta se asignan dentro de las defensas proactivas (40) y qué organismos tendrán la capacidad de defensa activa y bajo qué reglas de enfrentamiento? ¿Quién se va a encargar de

(40) *Véase* página siguiente.

la ciberdefensa de las estructuras críticas del país? ¿El Centro Criptológico Nacional (CCN)-CERT? ¿Y las del subámbito privado?
– ¿El Instituto de Tecnología de la Comunicación (INTECO)-CERT? ¿Cada empresa o particular lo suyo? ¿Deberán las empresas tener sus propios CERT? ¿Con qué guías u orientaciones los crearían? Si uno de los aspectos críticos es la formación ¿quién va a proporcionar formación a empresas y ciudadanos?
– Y otras preguntas relacionadas con las Fuerzas Armadas: ¿Cómo se van a coordinar las acciones de las Fuerzas Armadas, CCN y empresas privadas? Llegado el caso de que las Fuerzas Armadas tengan que tomar el control del ciberespacio nacional ¿tienen capacidad real para ello? ¿Cómo podría ejercerse?

Una vez que se consiga definir el ámbito nacional de la ciberdefensa, especificar el papel que deberán desempeñar las Fuerzas Armadas en él, requiere precisar si su ámbito defensivo de actuación se ha de circunscribir a sus propias redes o, por el contrario, tal y como opina el comandante del Mando Cibernetico (USCYBERCOM) (41), el Ministerio de Defensa tendrá mucho que opinar cuando el objetivo primario de los ataques se produzcan contra la base industrial de las empresas tecnológicas de defensa del país.

La ciberdefensa militar ha de estar integrada en la Ciberdefensa Nacional pero, sea como fuere la organización nacional que políticamente se decida, lo que es indudable es que las Fuerzas Armadas deberán asegurar sus propias redes y prepararlas para un posible conflicto cibernético. Y mientras no se le asigne otra misión específica o tenga que actuar bajo lo dictado por lo que determinan los estados de alarma, excepción y sitio, el ámbito de actuación de las Fuerzas Armadas deberá ser exclusivamente sus redes militares. Si luego, las Fuerzas Armadas entran a formar parte de un entramado nacional de ciberdefensa que, como se ha dicho, deberá definirse a muy alto nivel y que cohesione, coordine y dirija los dos subámbitos mencionados anteriormente, es una cuestión que aunque es muy necesario definir, se escapa a las intenciones de este capítulo.

Las capacidades defensivas que se definan deberán establecer una defensa en profundidad, en función del momento de la acción ofensiva

(41) Alexander, Keith B. general: U.S. «Cybercommand Commander and NSA Director. Building a New Command in Cyberspace», *Strategic Studies Quarterly,* invierno de 2011.

enemiga. A modo de ejemplo, y sin entrar mucho en detalle, ya que son objeto de otro capítulo de esta *Monografía*, se podrían determinar:

1. *Defensas preactivas*: son las que se ejecutan antes de que se produzca el ataque enemigo. Entre ellas están la concienciación y formación de usuarios y técnicos, la definición de normas y procedimientos, la instalación y la configuración correcta de *hardware* y *software* y las acciones de disuasión.
2. *Defensas proactivas*: son las que se ejecutan en el momento que se detecta el posible ataque enemigo. Estarán basadas principalmente en normas y procedimientos (análisis de eventos, determinación de atribuciones, desconexión de sistemas, lanzamiento de contraataques, etc.). Dentro de las defensas proactivas se pueden distinguir tres tipos de reacciones defensivas; para comprenderlas se va a establecer un símil pugilístico:
   – *Reacción pasiva*: es en la que tan sólo se ponen defensas, protecciones, guardas, pero no se toma ninguna acción. Es el boxeador que lo único que hace es encajar golpes y confiar en su resistencia para vencer al adversario por agotamiento o disuasión (42).
   – *Reacción semiactiva*: en las que las defensas establecidas toman pequeñas acciones no agresivas, como cortar comunicaciones o bloquear direcciones IP. Nuestro boxeador, aparte de encajar golpes, puede pararlos y bloquearlos voluntariamente.
   – *Reacción activa (defensa activa):* son los contraataques, en los que se toman acciones contra los agresores. Es cuando nuestro boxeador, después de bloquear, puede golpear.
3. *Defensas reactivas*: son las que se deberán ejecutar una vez que se haya producido el ataque enemigo, diferentes en función de si éste ha tenido éxito o no. Serán las acciones encaminadas a la recuperación y aumento de la disponibilidad de los sistemas o a averiguar en qué sistemas se ha producido un daño o robo de información, cómo ha sucedido y poner los medios para evitar su repetición.

Todas estas dudas sobre la organización de la Ciberdefensa Nacional y la distribución de capacidades defensivas son, al fin y al cabo, cuestiones que deberían plantearse en estudios analíticos mucho más profundos pero que sirven de referencia para mostrar todo el camino que nos queda por andar.

(42) Disuasión ante la fortaleza y la evidencia de la imposibilidad de acceder a nuestros sistemas.

*Capacidad ofensiva*

Algunos expertos en temas cibernéticos, como Jun Isomura, asesor del Instituto Hudson, opina que las medidas defensivas por sí solas no son suficientemente eficaces para proteger a un país y que es necesario aplicar acciones ofensivas. Isomura afirma que en los últimos 10 años la tecnología de los atacantes ha avanzado muy rápidamente, pero las herramientas para la defensa no lo han hecho en la misma proporción, lo que origina una clara desventaja a la posición defensiva frente a la ofensiva y aboga por que se desarrollen maniobras de contraataque para destruir electrónicamente los equipos agresores que hayan sido utilizados en la penetración de nuestros sistemas, aún siendo de uso privado.

Ante estas afirmaciones, el doctor Martin C. Libicki, analista experto en temas cibernéticos de la Rand Corporation, cree inútil este tipo de medidas encaminadas a destruir un ordenador de unos pocos cientos de dólares, por el mero hecho de que esto implica llevar a cabo un acto de agresión que podría legitimar una ciberguerra, además de la dificultad que conlleva la atribución del ataque, lo que representa el riesgo añadido de ocasionar los tan poco deseados daños colaterales.

Definir una capacidad ofensiva no es políticamente correcto. Pero lo que resulta evidente es que no existe capacidad de defensa sin capacidad de ataque y como determina uno de los principios de la guerra, la acción ofensiva es la que permite obtener la iniciativa a nuestras fuerzas.

La capacidad ofensiva es un aspecto crítico y políticamente delicado. Militarmente es un imperativo. Ahora bien, la decisión de tener esta capacidad, o no, en otros organismos ajenos al Ministerio de Defensa, Cuerpos y Fuerzas de Seguridad del Estado para lucha contra el ciberterrorismo y ciberdelincuencia), deberá ser adoptada a este nivel. Tener una capacidad ofensiva implica tener capacidad para conocer al adversario, poder tomar la iniciativa cuando sea necesario y tener la posibilidad de contraatacar después de un ataque. Desde que se adopta la decisión de penetrar en un sistema ajeno sin autorización, ya es una acción ofensiva.

Las dos acciones que se pueden hacer en ofensiva en el ciberespacio y que implican capacidades, son:

1. Capacidad de ciberespionaje.
2. Capacidad de ciberataque.

Una acción de ciberespionaje y una de ciberataque son inherentemente lo mismo. Para ejecutar ambos se requiere:

1. Un *acceso* a un sistema que permita.
2. *Explotar una vulnerabilidad*.
3. *Inocular una carga dañina*. La diferencia entre uno y otro radicará en el contenido de la carga que se inocule.

En el primero, el código inoculado tendrá como misión la sustracción y envío de información y en el segundo será la destrucción o alteración de datos o la degradación o inutilización de un sistema:

1. *Acceso a un sistema*: los accesos a los sistemas podrán ser:
   – Accesos remoto: vía Internet, módem o inalámbrico.
   – Accesos locales: accesos voluntarios o involuntarios de usuarios comprometidos, terceros no enemigos (proveedores, mantenimiento, limpieza, etc.), agentes secretos, etc.
2. *Explotación de vulnerabilidades*: las vulnerabilidades explotables pueden ser, como se especifican en otro capítulo, en cualquiera de las tres capas, la física, la sintáctica o la semántica, esto es, canales de comunicación, *hardware*, *firmware*, *software*, configuración, usuarios y operadores y proveedores de servicio.
3. *Inoculación de carga dañina*: el contenido de la carga inoculada es lo que realmente va a diferenciar un tipo de acción ofensiva de otro. La carga define lo que se puede hacer una vez que la vulnerabilidad ha sido explotada: ocultarse, reproducirse, retransmitir datos, destruir o alterar ficheros, bloquear un sistema, etc.

Pero la resolución de decidir si se ha de disponer de capacidad ofensiva o no, no es la única decisión importante que habrá que adoptar.

Otro de los problemas existentes está en determinar si la ciberseguridad ha de estar bajo el control civil o militar y hasta dónde el mundo civil se ha de subyugar a la autoridad militar. Este problema ya lo han tenido en Estados Unidos y todavía está sin resolver. Howard Schmidt, coordinador para la ciberseguridad del presidente Obama, estima que el término medio está en no dar demasiada autoridad a una agencia u otra y asegurarnos de que se comparte información entre todos.

La solución a este problema vendría de analizar detenidamente el abanico de tareas y competencias que hay que acometer en el tema de la

defensa del ciberespacio y definir exactamente las responsabilidades que se le ha de asignar a cada organismo y cada vez que surja una nueva tarea, asignar su responsabilidad inequívocamente a alguno de ellos.

Como siempre conviene aprender de los problemas que han sufrido los que nos llevan la delantera, probablemente uno de los mayores imperativos en la estructuración de la ciberdefensa, sea precisamente esta: la necesidad de una *clara definición de responsabilidades.* La inexistencia de ésta en la asignación de cometidos ante las diferentes agencias estatales de Estados Unidos (mar 2009) ha originado más de una crisis institucional en el país, así como problemas de competencias, duplicidades, enfrentamientos y roces entre organismos y servicios, entre ellas la supuesta intromisión de la Agencia Nacional para la Seguridad en las redes del DHS y el control de sus operaciones. La crítica se basaba principalmente en el temor de que se pusiera en peligro los principios democráticos del país en el caso de que una sola Agencia controlara toda la seguridad del conjunto de redes de alto nivel de la nación.

## Fuerzas de la ciberdefensa

Como se ha demostrado nos encontramos frente a un nuevo entorno operacional, un nuevo ámbito de combate de la misma entidad que el terrestre, naval o aéreo, que sin duda alguna será empleado en los conflictos venideros por los países contrincantes con la misma intensidad, si no más, que las fuerzas convencionales (43).

Este nuevo entorno, demanda unas nuevas necesidades, entre las que destacan la de una fuerza especializada para operar en él, compuesta por medios dedicados, humanos, físicos y económicos. Pero ¿qué fuerzas? ¿De qué tipo? ¿De dónde las sacamos?

### *Un poco de historia*

Si echamos la vista atrás en una visión retrospectiva de nuestro pasado más reciente, nos daremos cuenta de que esta situación no es novedosa. La Historia nos cuenta como conforme evolucionaron los escenarios

(43) En los futuros conflictos, el ciberespacio será siempre el primer escenario en ser utilizado; el ciberespacio se extiende y tiene influencia sobre todos los escenarios anteriores y su falta de control puede impedir la utilización efectiva y el desarrollo de las operaciones en el resto de escenarios.

de conflicto, los países fueron configurando nuevas fuerzas especializadas capaces de sacar todo el provecho de sus características.

Hace aproximadamente 100 años surgió el escenario aéreo, tras su conquista por el hombre. Cuando aparecieron los primeros medios aéreos nadie, por aquel entonces, fue lo suficientemente visionario como para comprender el grandísimo potencial que éstos representarían. Las fuerzas existentes (Ejército y Armada) comprendieron la gran utilidad que el empleo de medios aéreos podría significar en el apoyo a sus operaciones. Para ello crearon, dentro de sus propias estructuras, unas fuerzas que se especializarían en su uso. En la mayoría de los países se les dio a estas fuerzas una entidad de cuerpo, con la denominación de Cuerpos Aéreos *(Royal Flying Corps, Aéronautique Militaire, Fliegentruppen y US Army Air Corps).* En España, dentro del Cuerpo de Ingenieros del Ejército, se conformó el Servicio de Aeronáutica Militar compuesta por dos ramas, la de aerostación y la de aviación.

En la Primera Guerra Mundial los medios aéreos demostraron plenamente su capacidad y utilidad muy por encima de la inicialmente prevista para ellos. A partir de este punto de inflexión y siendo las naciones conscientes del futuro que prometían los medios aéreos, a lo largo de las décadas siguientes se fueron creando en todos los países fuerzas aéreas independientes con entidad de Ejército, equivalentes a sus homólogos de tierra y mar.

Así, en el año 1918 se crea la RAF *(Royal Air Force)*, independizándose del *British Army* y de la *Royal Navy.* En el año 1933, *l'Armée de l'Air* tras separarse del Ejército francés. Alemania, que durante la Primera Guerra Mundial dispuso de una potente fuerza aérea dependiente del Ejército *(Luftstreitkräfte)*, en el año 1935 rompió la prohibición del Tratado de Versalles que le impedía disponer de una fuerza aérea propia y formó una de nueva creación, independiente del *Heer* alemán (Ejército). España crea en el año 1939 el Ejército del Aire, como Ejército independiente que se escinde definitivamente del Cuerpo de Ingenieros del Ejército. La más tardía fue la Fuerza Áerea de Estados Unidos, que no se crea hasta después de la Segunda Guerra Mundial, tras independizarse del *US Army* en el año 1947.

*La Historia se repite*

Siempre se ha dicho que la Historia se repite. La sensatez nos obliga a aprender de los aciertos de la Historia, pero también a no caer en los errores cometidos.

El nuevo escenario aéreo exigió la creación nuevas fuerzas integradas en Cuerpos Aéreos dentro de las estructuras de los ejércitos que entonces existían; cuerpos que más tarde derivarían a ejércitos completos. Ahora la situación es idéntica: surge un nuevo escenario, el ciberespacio, que requiere el empleo de nuevas fuerzas con unos cometidos que son radicalmente distintos de los específicos de las fuerzas actuales, por lo que es necesario crear una nueva rama militar que explote todo el potencial que esto representa.

El desarrollo de una cuarta rama militar dedicada a la lucha en el ciberespacio ya es algo más que una mera idea en otros países. China (44) y Corea del Norte (45) ya disponen de fuerzas regulares para la lucha en el ciberespacio y Estados Unidos ha creado un USCYBERCOM, bajo la dependencia del Mando Estratégico (USSTRATCOM).

Sí, hace falta una nueva fuerza militar, pero ¿de qué entidad? Ya sabemos lo que es el ciberespacio; ya sabemos hacia dónde va; ya sabemos el potencial que tiene en el futuro y sabemos que, probablemente, desemboque en una fuerza de la misma entidad que la que tienen los actuales entornos operacionales: una ciberfuerza, un ciberejército o un ejército de la ciberdefensa; en fin, un ejército independiente.

Pero aun así, ante lo novedoso del escenario, parecería un tanto arriesgado crear directamente un nuevo ejército. Como se ha dicho, esto sería lo ideal. Pero seamos realistas. España no está en condiciones de sostener la creación de un nuevo ejército manteniendo simultáneamente las capacidades que se le exigen en la actualidad al resto de las Fuerzas Armadas, que son imprescindibles. La necesidad de defender nuestro ciberespacio está ahí, real, latente, progresiva ante unas amenazas cada vez más peligrosas y agresivas. De poder tener cubierta cuanto antes esta necesidad dependerá en un futuro inmediato la operatividad, no sólo del resto de la Fuerzas Armadas, sino prácticamente de la nación entera. Por lo que la necesidad hay que cubrirla: es imperioso.

Pero, como se ha visto, el ciberespacio es un dominio que engloba a la totalidad de los escenarios tradicionales, tierra, mar, aire y espacio e influye en el empleo de todos los Ejércitos por igual, afecta a su seguri-

---

(44) En: *http://defensetech.org/2008/05/08/chinas-cyber-forces/*

(45) En: *http://defensesystems.com/articles/2010/11/17/digital-conflict-north-korean-cyberwarfare-capabilities.aspx* y *http://www.jewishpolicycenter.org/blog/2011/06/cyberspace-the-next-battlefield*

dad y a sus operaciones. Todas las Fuerzas Armadas precisarán, tarde o temprano, de las acciones en el ciberespacio para asegurarse el éxito de las que se lleven a cabo en sus escenarios físicos. Para determinar la entidad de la fuerza, convendría de nuevo volver la vista atrás y pensar en lo que históricamente se ha visto eficaz y suficiente para las fuerzas emergentes: en los orígenes de las fuerzas aéreas se crearon tan sólo Cuerpos Aéreos dentro de las estructuras existentes, por lo que no sería nada descabellada la idea de la creación de una fuerza de la ciberdefensa con entidad de cuerpo: el Cuerpo de la Ciberdefensa.

*Encuadramiento*

Surge ahora una segunda pregunta: este Cuerpo de la Ciberdefensa, ¿dónde se encuadraría? ¿A qué ejército se le asignaría? Cada uno de los Ejércitos y la Armada dispone de potentísimos sistemas de información y comunicaciones que les son absolutamente imprescindibles para el cumplimiento de sus misiones específicas y poseen información valiosísima que almacenan y transmiten por estos medios. Sistemas que han de proteger del ciberespionaje y de los ciberataques procedentes de países o grupos hostiles. Por otro lado, el combate en el ciberespacio se escapa a las formas de acción propias de cada uno de los Ejércitos ya que el ciberespacio tiene, como se ha visto, las suyas particulares. En consecuencia, la ciberdefensa es una necesidad de todos y un cometido que no es atribuible a ninguna fuerza en concreto.

Absurdo sería, por tanto, pensar que podría o debería estar asignada a uno solo de los tres Ejércitos actuales. Y más absurda sería la idea de crear tres cuerpos con la misma función en cada uno de los ejércitos. La ciberdefensa es conjunta de nacimiento. Por consiguiente, sólo cabe una opción: crear un cuerpo conjunto, un *Cuerpo Conjunto de la Ciberdefensa*.

*Ventajas de un Cuerpo de la Ciberdefensa independiente*

Las características comunes del ciberespacio con el resto de entornos físicos le hacen acreedor de una fuerza de combate independiente; las características exclusivas y diferenciadoras le hacen merecedor de una fuerza preparada y dedicada. No es aconsejable, ni bueno, ni deseable que la lucha en este entorno no esté altamente especializada, del mismo modo que lo está el combate en los entornos terrestre, naval y aéreo.

La formación de un cuerpo independiente de la ciberdefensa presentaría múltiples ventajas:

1. La *especialización*: de igual modo que el combate en los entornos terrestres, naval y aéreo requieren una especialización propia, el combate en el ciberespacio demanda unos conocimientos y un entrenamiento exclusivo. La especialización en ciberdefensa incluiría los conocimientos en técnicas defensivas necesarias para asegurar la confidencialidad, integridad y disponibilidad de los sistemas, así como garantizar la autenticidad de los usuarios y la trazabilidad de sus acciones, lo que incluiría conocimientos de instalación y configuración de equipos, sistemas y redes, criptografía, disponibilidad, detección y análisis de intrusiones, rastreo y eliminación de códigos dañinos, restauración de sistemas, etc. Igualmente requeriría conocimientos de técnicas ofensivas, análisis y explotación de vulnerabilidades, penetración en sistemas, descifrado, codificación de *exploits* y aprendizaje de técnicas *stealth*, de evasión y de borrado de huellas, etc. Pero no sólo eso; la especialización podría también hacerse cargo de otros aspectos de la ciberseguridad en los que habitualmente, debido a su complejidad, los usuarios de sistemas tienen desconocimiento, como son los análisis de riesgos, desempeño de los cargos en la organización de seguridad de los sistemas de información, elaboración de documentación de seguridad de sistemas, análisis forenses, recuperación de datos, auditorías, inspecciones y evaluaciones y resto de facetas relativas a la seguridad de los sistemas de información y las comunicaciones que no se han enumerado.
2. La *dedicación*: una de las grandes ventajas de la creación de un Cuerpo de la Ciberdefensa sería su dedicación exclusiva. Ya no sólo es que sea necesario, que lo es, un servicio permanente las 24 horas, los 365 días del año, al estilo del prestado en la defensa aérea, sino que su personal, a lo largo de toda su trayectoria militar se dedicaría en exclusiva al combate en este entorno. Del mismo modo que un piloto de caza no está unos años volando un F-18 y luego pasa a misiones de transporte y menos aún a mandar una compañía de carros o una patrullera, difícilmente sería permisible el tener a un personal formado en ciberdefensa que no tuviera continuidad en este cometido y que al cabo de unos años pudiera pasar destinado a otros destinos en sus Ejércitos de origen que nada tengan que ver con los conocimientos adquiridos. En un Cuerpo de la Ciberdefensa, su personal especializado se dedicaría a este cometido permanentemente, ya sea sirviendo al Órgano Central, al Conjunto o a cada uno de los Ejércitos.

3. La *formación*: una buena formación y entrenamiento en el campo de la ciberdefensa son vitales. Los conocimientos necesarios para desenvolverse en este medio son muy complejos, abarcan muchos conceptos y requieren largo tiempo y dedicación. El tiempo necesario y la alta especialización hacen que la formación en ciberdefensa sea costosa y que se considere prioritario optimizar al máximo su rendimiento. Una formación que no esté unificada y que no tenga carácter conjunto, implicaría triplicar los gastos, los esfuerzos y los medios necesarios. La formación única permitiría que todos sus componentes hablasen un lenguaje común y dispongan de unos conocimientos homogéneos en todos los campos. La realización de ejercicios de ciberdefensa rutinarios fomentarían la competitividad de los componentes e incrementarían su nivel de habilidad y conocimientos.
4. La *economía*: el dominio del ciberespacio es imprescindible para el desarrollo de las operaciones militares. En caso de no establecer una única fuerza conjunta, cada uno de los ejércitos iniciarían sus propios movimientos y crearían sus unidades de ciberdefensa para asegurarse este dominio en apoyo a sus operaciones específicas. Esto significaría el tener que detraer medios humanos, materiales y económicos por triplicado de los ya reducidos recursos que tienen los ejércitos para intentar cubrir una nueva necesidad de una manera que probablemente no satisfaga en su totalidad las expectativas de ninguno de ellos. Los presupuestos disponibles que tienen asignados los ejércitos son para el cumplimiento de sus misiones actuales, por lo que dedicar las mismas fuerzas o recursos a nuevas responsabilidades va en detrimento del cumplimiento de sus cometidos fundamentales y de la eficacia de su personal.
5. La *doctrina*: la guerra en el ciberespacio es radicalmente diferente a la guerra en el resto de escenarios. Esto implica que exige disponer de una *doctrina específica* para su uso, una doctrina ciberespacial, que comprenda sus aspectos básico, operativo, táctico y funcional. Pero también se ha comentado que la ciberdefensa tiene que ser conjunta desde su nacimiento. Una única *doctrina conjunta*, redactada para esta finalidad desde su origen, orientará cuál deberá ser el empleo de las fuerzas de la ciberdefensa en las operaciones conjuntas y permitirá realizar el planeamiento conjunto a todos los niveles, estratégico, operacional y táctico.
6. La *organización*: la fuerza de la ciberdefensa es necesaria. Una integración en la estructura de los ejércitos llevaría otros problemas

añadidos: ¿dónde se integrarían? ¿en los cuerpos generales? ¿en el de Ingenieros? ¿en las tres escalas? ¿con qué especialidad fundamental? ¿y complementaria? Si esto representa un problema, el asignárselo a los ejércitos lo multiplicaría por tres. Un Cuerpo de la Ciberdefensa independiente tendría que acometer igualmente estas cuestiones, pero sería una única estructura nueva la que asumiría el proceso, liberando a los ejércitos de estos esfuerzos.

7. La *operación*: la fuerzas de la ciberdefensa podrá llevar a cabo las operaciones específicas que, en base a su doctrina, tengan encomendadas. Estas podrán ser defensivas y/u ofensivas en función de las capacidades que se le asignen. Igualmente podrán realizar operaciones conjuntas con el resto de las otras fuerzas o en apoyo a ellas. Por otro lado proporcionarían seguridad lógica a los sistemas de información y comunicaciones conjuntos o específicos de los ejércitos, medios que son imprescindibles para el ejercicio de sus formas de acción.
8. La *imagen*: la existencia de una organización clara y definida de la ciberdefensa militar española, con responsables, con medios definidos y diferenciados, con programas de formación y entrenamiento y con capacidades suficientes, daría un importante peso específico a las Fuerzas Armadas dentro de la ciberdefensa nacional e internacional y potenciaría su visión ante la sociedad española y del resto de países.

*Propuesta de futuro* (46)

Como ya se ha visto, la creación de un ejército de la ciberdefensa es un reto difícilmente asumible por España. Las implicaciones de índole política, social y económica lo hace de compleja viabilidad.

Para una solución perdurable en el tiempo, el desarrollo de la idea de un cuerpo de la ciberdefensa es de más fácil realización. Políticamente evitaría tener que modificar la Constitución, en su artículo octavo (47) y el nuevo cuerpo podría ser creado por Ley, tal y como determina el artículo

(46) Esta propuesta es una de las varias posibles para la constitución de las fuerzas de ciberdefensa. Otros autores podrán tener otras diferentes.

(47) Artículo 8: «1. Las Fuerzas Armadas, constituidas por el Ejército de Tierra, la Armada y el Ejército del Aire, tienen como misión garantizar la soberanía e independencia de España, defender su integridad territorial y el ordenamiento constitucional. 2. Una ley orgánica regulará las bases de la organización militar conforme a los Constitución española principios de la presente Constitución.»

25 de la Ley 39/2007 de la Carrera Militar. Socialmente no es lo mismo anunciar la creación de un nuevo ejército que la formación de un nuevo cuerpo que se encargue de la ciberdefensa; la sociedad seguramente lo percibiría como algo necesario y que ocasionaría un gasto notoriamente inferior. Finalmente, es evidente que el coste económico de la creación de una entidad tipo cuerpo siempre será mucho más asumible que una de tipo ejército.

La creación del nuevo cuerpo tampoco se puede hacer de la nada, requiere su tiempo, disponibilidad de recursos y una planificación minuciosa. Sin embargo, el hueco de la ciberdefensa hay que taparlo y convendría hacerlo cuanto antes. Las ciberacciones contra otras naciones, empresas y organizaciones se suceden día tras día (48). Es sólo cuestión de tiempo que nuestras instituciones, organizaciones, Fuerzas Armadas y empresas se conviertan en objetivos, si no lo están siendo ya. Mientras la organización de la ciberdefensa se decide a nivel nacional, las Fuerzas Armadas tienen que blindar sus sistemas; mejor antes, que después. La entrada no autorizada, el robo de información clasificada o la inutilización de algunos de nuestros sistemas o servicios pueden significar un importante problema para la Defensa Nacional.

Hasta llegar a disponer de la fuerza permanente necesaria, se podrían dar otros pasos previos de más fácil realización y de segura efectividad:

1. Creación de una misión conjunta permanente. La idea de una misión conjunta permanente fue expuesta por el General Jefe de la Jefatura de Sistemas de Información y Comunicaciones (GJSTCIS) del Ejército del Aire en las «Jornadas de Ciberdefensa» convocadas por el Estado Mayor de la Defensa (EMAD) y la empresa INDRA del pasado mes de septiembre en León. Alrededor de esta propuesta está conformándose la postura oficial del Ejército del Aire.

   La misión consistiría en la generación y operación de una Fuerza Operativa Conjunta (FOC), bajo la autoridad del JEMAD y del Centro de Operaciones del EMAD, como las demás fuerzas que están desplegadas pero con un carácter de permanencia en el tiempo como el de las misiones específicas permanentes asignadas a los Ejércitos y la Armada, tendría capacidades defensivas y ofensivas y actividad H24/365, desplegada básicamente en territorio nacional, que se encargaría de proteger las redes de las Fuerzas Armadas y colaborar,

(48) En: *http://blogs.mcafee.com/mcafee-labs/revealed-operation-shady-rat*

cuando fuera necesario y así se le encomendase, con los Cuerpos y Fuerzas de Seguridad del Estado u otros organismos en operaciones contra ciberterrorismo y ciberdelincuencia.

El personal necesario, del que se deberán definir sus especialidades, estaría encuadrado en sus respectivos ejércitos y pasaría a formar parte de la misión por el tiempo que operativamente se determine. Uno de los aspectos críticos sería el de la formación del personal que, para evitar multiplicidad de esfuerzos y para unificar conocimientos, sería recomendable que fuera desde su inicio responsabilidad conjunta, a cargo del EMAD.

2. Creación del Centro de Ciberdefensa de las Fuerzas Armadas. Como es muy probable que los conflictos en el ciberespacio vayan incrementándose en número, frecuencia, intensidad y complejidad en los próximos años, no habría que descartar que la misión conjunta permanente fuera demandando cada vez más recursos y más preparados, por lo que llegará el momento en que sea necesario dar el siguiente paso en la escalera del desarrollo de las fuerzas de la ciberdefensa. La lógica evolución sería encaminarlo hacia formación de un Centro de la Ciberdefensa de las Fuerzas Armadas, de carácter conjunto, con una entidad similar a la del Centro de Inteligencia de las Fuerzas Armadas (CIFAS) y encuadrado igualmente en la misma estructura del EMAD.

   La existencia de este centro presentaría sus ventajas, especialmente en lo relativo a la permanencia del personal, que ya no serían designados por turno, sino que pasarían destinados al nuevo organismo con dedicación exclusiva a la ciberdefensa. La creación de un centro permitiría además la definición de una estructura permanente y de la delimitación de las dependencias y relaciones existentes con los otros organismos del EMAD y con el resto de los Ejércitos y la Armada, así como facilitaría la formación del personal, su reciclaje y entrenamiento. En el entorno de la ciberdefensa la dedicación, la permanencia y la especialización son factores críticos en un mundo tan técnico y que evoluciona tan rápidamente.

3. Creación del Cuerpo Común de la Ciberdefensa. La tecnificación de las Fuerzas Armadas y la dependencia de los sistemas de información y comunicaciones es una realidad imparable. Hoy día se considera impensable un estancamiento en la evolución tecnológica de

las fuerzas de ningún país, lo que hace pensar que las operaciones del futuro se basarán o se apoyarán más aún en estos sistemas. El crecimiento de la necesidad de fuerzas de la ciberdefensa es incuestionable.

El Centro de la Ciberdefensa de las Fuerzas Armadas proporcionaría a las Fuerzas Armadas las capacidades de ciberdefensa que necesita, definidas por el JEMAD en su «Concepto de la Ciberdefensa Militar». No obstante ¿quién proporciona la seguridad lógica en las redes y sistemas de información de las Base Antártica Española y Unidad Central Operativa de cada uno de los ejércitos? ¿Los propios Ejércitos y la Armada? ¿Necesitan seguir formando personal para estos cometidos, cada vez más complejos? Ya que se están creando las fuerzas de ciberdefensa ¿no sería más sensato disponer de personal especializado en estas funciones en cada unidad que lo requiera, independientes del ejército en el que estuvieran encuadrados? Si buscamos una fuerza que cumpla con los cometidos asignados al Centro de Ciberdefensa de las Fuerzas Armadas y que además sea capaz de hacer esto, es necesaria la creación del ya mencionado Cuerpo de la Ciberdefensa.

Puesto que el ciberespacio es un entorno que engloba, abarca y afecta igualmente a la operatividad de todo el conjunto de las Fuerzas Armadas, ¿dónde y cómo creamos el nuevo Cuerpo de la Ciberdefensa? ¿Sería factible que las fuerzas necesarias fueran satisfechas del mismo modo que lo han sido otras necesidades comunes a las Fuerzas Armadas, tales como las médicas o las jurídicas, mediante la creación de un nuevo *Cuerpo Común de la Ciberdefensa* (49), independiente de los Ejércitos, con entidad propia, con autonomía en cuanto a su organización y formación y que preste sus servicios y apoyo, como el resto de los cuerpos comunes, a la totalidad del Ministerio de Defensa, integrado en la estructura de los Ejércitos de la manera y para los cometidos que se determinen reglamentariamente? ¿No podría estar el Centro de la Ciberdefensa de la Fuerzas Armadas compuesto por personal de este cuerpo y además disponer de personal que fuera capaz de hacerse cargo de la seguridad de las redes y sistemas de información en

(49) Compuesto por Escala de Oficiales, Suboficiales y Tropa, con titulación previa (oficiales de Ingeniería Informática o de Telecomunicaciones; suboficiales de Formación Profesional de grado superior de la rama informática; Tropa de Formación Profesional de grado medio en sistemas informáticos y redes). Los primeros cuadros de mando tendrían que proceder necesariamente de los Ejércitos y la Armada.

todas las unidades de las Fuerzas Armadas, conformaran las estructuras de seguridad de los Sistemas de Información (implantación: ASS, ASS-D, ASS-L y verificación: SSTIC, SSTIC-D) y responsables de toda la documentación de seguridad de los sistemas, de los análisis de riesgos y de todo lo que sea necesario en las unidades relativo a la seguridad de las Tecnologías de la Información y las Telecomunicaciones? ¿Utópico? El futuro dirá.

## Conclusiones

El conflicto, algo inherente al ser humano surgido como consecuencia de una lucha de intereses, ha existido desde el principio de la humanidad. Los motivos y actores han sido los mismos; los medios empleados por los Estados para solventarlos, también. Lo único que han evolucionado han sido los escenarios en los que se han llevado a cabo.

La evolución de los escenarios se ha ido produciendo conforme el hombre los dominaba. Los más históricos han sido el terrestre y el marítimo; los más novedosos el aéreo y el espacial. A éstos se les ha unido recientemente uno artificial, de manufactura humana: el ciberespacio.

Para resolver los conflictos en estos escenarios, los países formaron sus fuerzas militares. Fuerzas que son específicas para cada uno de ellos: fuerzas terrestres, navales, aéreas y espaciales. Pero para el nuevo escenario artificial no se habían creado fuerzas específicas hasta ahora. Los enfrentamientos que ya se están produciendo en él las exigen. La necesidad se impone y ante nuevas necesidades se requieren nuevos medios.

Las fuerzas del ciberespacio deberán disponer de capacidades ofensivas y defensivas y su objetivo será permitir el libre uso del ciberespacio a los ciudadanos de cada nación e impedirlo, si fuera necesario, a sus enemigos. Para conseguir este objetivo, las fuerzas deberán estar especializadas, ser permanentes y tener dedicación exclusiva a la ciberdefensa. Esto sólo se consigue con fuerzas conjuntas con adiestramiento conjunto desde el inicio o mejor aún, con fuerzas independientes de los actuales ejércitos. La complejidad del entorno y su rápida evolución no permiten otra opción.

**Bibliografía**


ADAM FRASER, Nicolas Lt.Col. USAF; KAUFMAN III, Robert J. Lt.Col. USAF and RYDELL, Mark R.: *Es hora de defenderse: «operacionalización» de la defensa de redes.*

ALEXANDER, Keith B. Gen. Commander US Cyber Command and Director NSA: *Building a New Command in Cybersapace. Strategic Studies Quarterly,* verano de 2011.

ANDRUES, Wesley R.: «What US Cyber Command Must Do», *Joint Force Quarter,* número 59, cuarto trimestre de 2010.

BURGHARDT, Tom: *Cyberspace, the Battlefield of the Future: Pentagon Ramps-Up Cyberwar Plans,* agosto de 2011, en: *http://www.globalresearch.ca/index.php?*

«Ciberseguridad. Retos y amenazas a la seguridad nacional en el ciberespacio», Instituto Español de Estudios Estratégicos (IEEE), Ministerio de Defensa, Madrid, 2010.

CIMBALA, Stephen J.: «Nuclear Crisis Management and Cyberwar. Phishing for Trouble?» *Strategic Studies Quarterly*, primavera de 2011.

CLARK, David D. and LANDAU, Susan: *Untangling Attibution,* President and Fellows of Harvard College, 2011.

CORNISH, Paul; LIVINGSTONE, David; CLEMENTE, Dave and YORKE, Claire: *Cyber Security and the UK's Critical National Infraestructure,* Chathman House, septiembre de 2011.

CROSSTON, Matthew D.: *World Gone Cyber MAD. How «Mutually Assured Debilitation» Is the Best Hope for Cyber Deterrance,* Strategic Studies Quarterly. verano de 2011.

«Defending Against Cyberattacks», en: *http://www.nato.int/cps/en/natolive/75747.htm.*

DEMCHAK, Chris C. and DOMBROWSKI, Peter: *Rise of Cybered Westphalian Age. Strategic Studies Quarterly,* primavera de 2011.

DEPARTMENT OF DEFENSE STRATEGY FOR OPERATING IN CYBERSPACE: julio de 2011.

«Deterring CyberAttacks: Informing Strategies and Developing Options for U.S. Policy», National Research Council, 2010, en: *http://www.nap.edu/catalog/12997.html.*

DOCUMENT 3-12: *Cyberspace Opeations. Air Force Doctrine*, julio de 2010.

DOCTRINA AEROESPACIAL: IG 00-1, 2002.

DOCTRINA EMPLEO DE LAS FUERZAS TERRESTRES: DO1-001, tercera edición, 2004.

DUNLAP, Charles J. Jr. Maj. Gen. USAF: *Perspectives for Cyber Strategists on Law for Cyberwar.*

FIELD MANUAL: *100-20-Military Operations in Low Intensity Conflict,* USAF and US Army.

FRANZ, Timothy Lt.Col. USAF: *The Cyber Warfare Professional. Realization for Developing the Next Generation.*

GOODMAN, Will: «Cyber Deterrance. Tougher in Theory tan in Practice?», *Strategic Studies Quarterly,* Fall, 2010.

GRAU, Abel: *La nube digital también amenaza tormenta,* agosto de 2011, en: *http://www.elpais.com/articulo/sociedad/nubedigital*

GUÍA DE LA RED SARA: Ministerio de Administraciones Públicas, Madrid, 2008.

HAYDEN, Michael V. Gen. USAF. Former NSA and CIA Director: «The Future of Things "Cyber"»*, Strategic Studies Quarterly*, verano de 2011.

*High Frontier,* volumen 5, número 3, «Cyberspace».

— Volumen 6, número 4, «Cyber and Space. A Way Ahead. The Cyber Kill Chain: A Foundation for a New Cyber Security Strategy».

— Volumen 7, número 1, «National Security Fundamental in the Space and Cyver Domains».

— Volumen 7, número 3, «Cyber Defense. Protecting Operations in an Evolving Domain».

HOLLIS, David M. Lt.Col. Katherine Hollis: *U.S. Cybersecurity must-do's,* Armed Forces Journal, febrero de 2011.

— *Cybersecurity Policies We Need,* Armed Forces Journal, junio de 2011.

HUGHES, Rex B.: *NATO and Cyber Defense,* Mission Accomplished, 2009.

HUNTER, Robert E.; GNEHM, Edward and JOULWAN, George: *Integrating Instruments of Power and Influence,* Rand Corporation, 2008.

JABBOUR, Kamal: «Cyber Vision and Cyber Force Development»*, Strategic Studies Quarterly*, primavera de 2011.

JOYNER, John: *The next battlefield: Cyberspace and military readiness,* julio de 2011, en: *http://www.techrepublic.com/blog/security*

JP 1-02: *Department of Defense Dictionary of Military and Associated Terms,* agosto de 2011.

KOCZIJ, David: *Cybersecurity: Is Technology Moving Faster Than Policy?* Security & Defense Agenda, febrero de 2011.

KRISTAL L. M. Alfonso, Lt.Col. USAF.: *A Cyber Proving Ground. The Search for Cyber Genius.*

KURTH CRONIN, Arthur: *Cyber-Mobilization: The New Levée en Masse,* 2006.

LAMBETH, Benjamin S.: «Airpower, Spacepower and Cyberpower», *Joint Force Quarter,* número 60, primer trimestre de 2011.

Ley 39/2007 de la Carrera Militar.

Ley 8/2011 de Medidas para la Protección de Infraestructuras Críticas.

Libicky, Martin C.: *Chinese Use of Cyberwar as an Anti-Access Strategy,* Rand Corporation, 2011.

— *Cyberdeterrance and Cyberwar,* Rand Corporation, 2009.

— «Cyberwar as a Confidence Game», *Strategic Studies Quarterly*, primavera de 2011.

Lin, Herb: *Cyberspace: The New and Evolving Global Battlefield,* National Academies, junio de 2011.

Lloyd, Mike: *The Silent Infiltrator,* Armed Forces Journal, junio de 2010.

Lynn III, William J. secretario adjunto de Defensa de Estados Unidos: *Defendiendo un nuevo ámbito. La ciberestrategia del Pentágono.*

Miller, Robert A. and Kuehl, Daniel T.: *Cyberspace and the First Battle in 21st Century War,* Defense Horizons, septiembre de 2009. Molist, Mercè: *Las doctrinas de vigilancia informática han quedado obsoletas,* en: *http://www.elpais.com/articulo/Pantallas/doctrinas,* junio de 2006.

Owens, William A.; Dam, Kenneth W. and Lin, Herbert S.: *Technoligy, Policy, Law and Ethics Regarding US Acquisition and Use of Cyberattack Capabilities,* National Academies Press, 2009.

Proyecto Miló: *El conflicto: definición, elementos y tipos,* Compañía de María.

Preventing and Defending Against Cyber Attacks: octubre de 2011, en: *http://www.dhs.gov/xlibrary/assets/preventing-and-defending-against-cyber-attacks-october-2011.pdf*

Ramírez Valle, Elisabet: *El porqué de la guerra,* en: *http://academia.edu/Papers/in/Origin_of_war*

Real Decreto 704/2011 del *Reglamento de Protección de las Infraestructuras Críticas.*

Romero Gálvez, Antonio: *Teoría del conflicto social.*

Sádaba Rodríguez, Igor y Roig Domínguez, Gustavo: *Internet: nuevos escenarios, nuevos sujetos, nuevos conflictos,* en: *www.uned.es/ntedu/asignatu/5-Nodo50.htm.*

Savage, John E.: *Cybersecurisy and International Ralations,* Brown University, junio de 2011.

Sheldon, John B. «Deciphering Cyberpower», *Strategic Studies Quarterly,* verano de 2011.

Sofaer, Abraham D.; Clark, David and Diffie, Whitfield: *Cybersecurity and International Agreements,* National Academy of Sciences, en: *http://www.nap.edu/catalog/12997.html*

Solce, Natasha: *The Battlefield of Cyberspace: The Inevitable New Military Branch-The Cyber Force,* Albany Law Schoo, 2008.

Sterner, Eric: «Retaliatory Deterrence in Cyberspace», *Strategic Studies Quarterly,* primavera de 2011.

Stone, Lauren: *Cyberspace: The Next Battlefield,* junio de 2011, en: *http://www.jewishpolicycenter.org/blog/2011/06/cyberspace-the-next-battlefield.*

Worley, Robert D.: «Orchestrating the Instruments of Power: An Examination of the U.S», National Security System, 2009, en: *http://www.drworley.org/Pubs/Orchestrating/*

*Páginas web*

En: *http://escolapau.uab.cat/conflictosypaz/definiciones.php*

En: *http://www.campogrupal.com/conflicto.html*

En: *http://www.beyondintractability.org/action/essay.jsp?id=28816&nid=1068*

En: *http://www.gmu.edu/programs/icar/pciberespacio/sandole.htm*

En: *http://www.usc.edu/dept/LAS/ir/cews/html_pages/conflictdatabase.htm#narratives*

En: *http://www.beyondintractability.org/essay/conflict_stages/*

## CAPÍTULO CUARTO

# EL CIBERESPACIO COMO ESCENARIO DEL CONFLICTO. IDENTIFICACIÓN DE LAS AMENAZAS

# EL CIBERESPACIO COMO ESCENARIO DE CONFLICTOS. IDENTIFICACIÓN DE LAS AMENAZAS

Por Ángel Gómez de Ágreda

> «Las amenazas cibernéticas han sido, simultáneamente, infra y sobreestimadas: su alcance se ha minusvalorado mientras que el papel que juegan los actores malvados se ha sobrevalorado.»
>
> Michael Dell

## Introducción

Hace unos años que vivimos en dos mundos de forma simultánea. Seguimos con nuestra vida normal en un mundo físico con amigos a los que vemos y estrechamos la mano y abrazamos y con los que vamos de compras a lugares concretos en los que adquirimos bienes materiales que abonamos con dinero contante y sonante. Un mundo en el que los acontecimientos se suceden unos a otros de un modo ordenado y secuencial.

Quizás no todos, pero muchos viven también en un mundo digital en el que puede ser que veamos a nuestros amigos pero a los que rara vez estrechamos la mano y en el que la información y el dinero se «mueven» a la velocidad de la luz. En este mundo los acontecimientos no se suceden sino que se simultanean y se influyen mutuamente creando una red de interferencias que hace que todo sea distinto a cada instante.

El mundo digital nos permite –pero también nos exige– inmediatez. Todo es accesible y todo está disponible pero la misma acumulación de datos

e información genera un ruido que dificulta tremendamente su gestión. En este espacio cibernético «de tanto navegar y buscar terminamos sacrificando nuestra capacidad de contemplación e introspección» (1) y hasta nuestra memoria, confiados como estamos en él. Es un ámbito irreal y, sin embargo, confiamos a él nuestros conocimientos y nuestros ahorros, nuestras relaciones sociales y profesionales; nuestra vida, en suma, discurre entre los unos y ceros del ciberespacio tanto como entre las calles y plazas de nuestras ciudades y pueblos.

A este mundo virtual también ha llegado el conflicto como un avatar de su equivalente en la vida «real». Las batallas en el ciberespacio y desde el ciberespacio no son tan distintas de las que se libran en los campos de batalla y, aunque al no ser cruentas parezcan menos violentas, sirven los mismos propósitos que las que libran entre sí los blindados, la fragatas y los cazabombarderos. El entorno virtual sirve de escenario a guerras muy reales entre las grandes potencias en las que están implicados todos los campos del saber y todas las actividades humanas, desde la actividad económica hasta la que se libra por hacerse con los «corazones y las mentes» de los ciudadanos:

> «En el siglo XXI los *bits* y los *bytes* podrán ser tan amenazantes como las balas y las bombas», en palabras del vicesecretario de Estado de Defensa estadounidense en la presentación en julio pasado de la «Estrategia de Operaciones en el Ciberespacio» (2).

## El ciberespacio

### *La definición del ciberespacio*

Cada quién concibe el ciberespacio como conviene a sus intereses o como se percibe desde su óptica según las necesidades que tenga en su organización. La Publicación Conjunta 1-02 del Departamento de Defensa de Estados Unidos lo definía como:

---

(1) Carr, N.: *Superficiales. ¿Qué está haciendo Internet con nuestras mentes?*, 2010, se puede consultar una sinopsis en: *http://www.editorialtaurus.com/es/libro/superficiales/.* También sobre el mismo tema y comentando el libro se puede leer de Celis, B.: «Un mundo distraído», diario *El País,* 29 de enero de 2011, en: *http://www.elpais.com/articulo/portada/mundo/distraido/elpepuculbab/20110129elpbabpor_3/Tes*

(2) Según recoge la «Reseña de la primera "Estrategia de Operaciones en el Ciberespacio"» del Instituto Español de Estudios Estratégicos (IEEE), Madrid, 14 de julio de 2011.

> «Un dominio global dentro del entorno de la información, compuesto por una infraestructura de redes de tecnologías de la información interdependientes, que incluye Internet, las redes de telecomunicaciones, los sistemas de información y los controladores y procesadores integrados junto con sus usuarios y operadores.»

La traemos aquí por lo completa que resulta y el modo en que desglosa los distintos componentes que abarca. Cuando lo que se plantea es estudiar el ciberespacio como nuevo escenario de conflicto, será preciso, no obstante, ponerlo en relación con el uso estratégico que se puede hacer de él.

El ciberespacio ha quedado definido, desde el punto de vista geoestratégico, como uno de los cuatro *Global Commons*. Los *Commons* son una figura que recogía el Derecho medieval británico y que hacía referencia a aquellos terrenos que, sin ser propiedad de ninguno de los vecinos del municipio, son explotados por el conjunto de la comunidad para beneficio de todos. Los *Commons* globales son aquellos espacios que, normalmente sin estar sujetos a la soberanía de país alguno, son utilizados por las naciones para transportar personas o bienes y servicios o para transmitir datos. Al ámbito tradicional de las aguas internacionales (en realidad, sólo la superficie hasta este momento) se han venido añadiendo el espacio aéreo y el espacio exterior según las capacidades humanas permitían su tránsito y explotación. Por último, recientemente se ha empezado a hablar del ciberespacio como cuarto bien común por el que transitan datos e ideas.

La diferencia fundamental del espacio cibernético respecto de los tres *Commons* preexistentes es su *naturaleza artificial*. Así como en los espacios marítimo, aéreo y espacial el entorno es algo que existe en la Naturaleza y al que el ser humano tiene que adaptar medios artificiales para su utilización, en el ciberespacio tanto el continente como el contenido son creados por el hombre y, por lo tanto, su diseño –incluidas sus imperfecciones– son fruto del esfuerzo humano y responden a unas circunstancias concretas que se dieron en el momento de su diseño y desarrollo.

La alusión que hemos hecho a las imperfecciones del ciberespacio no es casual ni gratuita. Mientras que en el resto de los espacios que hemos comentado el medio es una creación con una naturaleza fija e inmutable –si bien sometida a avatares meteorológicos y de otro tipo que los hacen sólo parcialmente previsibles– y el hombre debe diseñar los vectores que

se adapten a dicha naturaleza para aprovechar sus características, *en el espacio cibernético el medio es de factura tan humana como el vehículo que se mueve por él* y, por lo tanto, la cantidad de variables a considerar es mucho mayor ya que el entorno puede variar de naturaleza. Igualmente, tanto espacio como vector incluyen errores de diseño que serán la puerta de acceso que utilizarán aquellos que pretendan agredirnos.

*La estructura del ciberespacio*

Tradicionalmente, siguiendo a Martin C. Libicki (3), se viene dividiendo el ciberespacio en tres capas, cada una de las cuales presenta sus vulnerabilidades y es objeto de un tipo concreto de ataques: *la capa sintáctica, la capa semántica* y *la capa física.*

De este modo, los datos, los programas que introducimos para gestionarlos, todo el conocimiento acumulado en los servidores y en los discos constituye *la capa semántica.* La estructura con que se almacenan estos datos sigue criterios uniformes que permiten su intercambio y es conocida por los expertos. Los *terabytes* de información que supuestamente fueron sustraídos de los ordenadores de la Lockheed Martin con datos altamente sensibles sobre el cazabombardero de quinta generación F-35, el conocido *Joint Strike Fighter*, forman parte de esta capa (4).

El *espionaje* es la actividad más frecuente en la guerra que tiene lugar en el ciberespacio. De todos los datos que se extraen, la propiedad intelectual es sólo una parte, como veremos en el siguiente apartado. Casos de tanta relevancia como la operación *Shady Rat* (5) que desvela el espionaje continuado a 70 empresas y organismos oficiales durante cinco años son sólo la punta del iceberg que sobresale al mar de secretismo que se guarda en torno a estos asuntos.

Los protocolos, los sistemas operativos y demás lenguajes que sirven para hacer funcionar los programas y legibles los datos constituyen, a su vez, *la capa sintáctica* del ciberespacio. Contiene las instrucciones que los diseñadores y usuarios introducen en los sistemas y es básica para permitir que los terminales se comuniquen entre ellos. Los sistemas ope-

(3) Libicki, M. C.: *Cyberdeterrence and Cyberwar,* RAND Corporation, 2009.

(4) Gorman, S.; Cole, A. and Dreazen, Y.: «Computer Spies Breach Fighter-Jet Project», *The Wall Street Journal,* 21 de abril de 2009, en: *http://online.wsj.com/article/SB124027491029837401.html*

(5) En: *http://www.mcafee.com/us/resources/white-papers/wp-operation-shady-rat.pdf*

rativos son uno de sus elementos críticos. Su diseño constituye una de las vías de acceso más frecuentes para *hackers* e intrusos. La imperfección de su programación o la intencionada apertura de puertas traseras que permitan un acceso fácil y rápido para efectuar retoques y modificaciones se utiliza por los expertos para instalar programas o rutinas que les habilitan para controlar subrepticiamente los sistemas. Posteriormente veremos algunos ejemplos de intrusión utilizando las vulnerabilidades propias de la capa sintáctica, la más ampliamente utilizada para ello.

Por último, tanto una como otra capa de datos tiene que ubicarse físicamente en algún tipo de soporte. Solemos pensar que *la capa física* del ciberespacio es aquello que podemos ver y tocar en nuestro ordenador: discos duros, monitores, teclados y ratones, etc. Si ampliamos el círculo, incluimos hasta la impresora y, quizás, el enrutador pero en muchas ocasiones olvidamos que buena parte de la capa física está muy alejada de nosotros y, probablemente, nunca llegaremos a verla o tocarla. Servidores ubicados en otros países, cables submarinos o satélites por los que se mueve la información y otros elementos son perfectamente vulnerables a ataques de una naturaleza tan física como la suya. El caso de los cables submarinos está empezando a ser considerado un elemento crítico por cuanto un número limitado de ellos permite las comunicaciones entre los terminales de todo el mundo constituyendo cuellos de botella de paso obligado de la información que son controlables o neutralizables con relativa facilidad.

La externalización en la fabricación de componentes añade vulnerabilidades a esta capa que son cada vez más explotadas. La introducción de alteraciones en componentes fabricados en terceros países es una técnica con un alto potencial en la manipulación de los sistemas informáticos y el control de los componentes que pasan a formar parte de aquellos considerados críticos es –al menos siguiendo los protocolos habituales de actuación establecidos– muy exhaustivo. La dependencia de un mercado global de componentes supone un riesgo importante para la seguridad de nuestros equipos y la información que contienen. Son numerosos los informes de sospechas de que elementos fabricados en algunos países puedan contener un programa durmiente que pudiera ser activado a voluntad de forma remota en caso de conflicto o, simplemente, para poder acceder a la información contenida en una red o a su control (6).

(6) En: *http://www.revistatenea.es/RevistaAtenea/REVISTA/articulos/GestionNoticias_4591_ESP.asp#*

*El elemento humano: sujeto y objeto del ciberespacio*

Sin embargo, a estas tres capas tradicionales tenemos que añadir el componente humano que interactúa con *hardware* y *software* tanto como creador o mantenedor como en el papel de explotador del mismo. Sin lugar a dudas, esta *capa humana* es la más vulnerable de todas como demuestran los más recientes y sofisticados ataques (7). Técnicas como el *phishing* y el *spear phishing* pretenden –y consiguen en muchos casos– explotar la debilidad de la misma (8).

Los ataques que se dirigen contra la capa humana del ciberespacio pretenden explotar vulnerabilidades surgidas de las deficiencias en la formación de los usuarios, el exceso de confianza o, simplemente, la buena fe (9). Diversos estudios realizados por empresas especializadas en seguridad informática insisten en la sorprendente facilidad con que se pueden obtener los datos reservados de algunos usuarios y, a través de ellos, acceso a redes supuestamente protegidas.

No hay que olvidar que la mayor parte de las técnicas diseñadas para atacar la parte «blanda» del ciberespacio, es decir, sus capas sintáctica y semántica, lo son para acceder a sistemas conectados a Internet y, por lo tanto, accesibles de algún modo a través de los diversos servidores y enrutadores que los conectan. El sabotaje o el robo de datos de terminales o redes aisladas suele requerir de la participación física de algún usuario autorizado. Éste colaborará con o sin su conocimiento en la intrusión y con o sin inteligencia de las consecuencias de sus acciones. La *concienciación de los usuarios* de todos los niveles y el diseño de sistemas «a prueba de necios» están en la base de la seguridad informática tanto como en la de cualquier otro.

En este sentido, los desarrollos tecnológicos y las barreras lógicas que podamos establecer serán sólo tan válidos como lo sea el usuario encargado de gestionar el sistema. La seguridad es una cadena que se rompe siempre por el eslabón más débil por lo que el diseño de la misma debe basarse en un incremento progresivo y equilibrado de todos los com-

(7) En: *http://www.securelist.com/en/analysis/204792104/Patching_human_vulnerabilities*

(8) Lozano Prieto, A.: *Análisis teórico-experimental de técnicas y herramientas de* phishing *y delitos electrónicos*, proyecto de fin de carrera Universidad Complutense de Madrid, Departamento de Ingeniería Telemática, octubre de 2009.

(9) En: *http://www.securitypark.co.uk/security_article26485.html*

ponentes que forman parte de la misma. Un *desarrollo inarmónico* sólo supondría un derroche de medios ya que el potencial intruso buscará dicho eslabón débil para obviar la resistencia que ofrece el resto de un sistema construido de una forma mucho más robusta.

Cada una de las cuatro capas que conforman el espacio cibernético presenta potenciales *vulnerabilidades* explotables por los posibles intrusos. Las más suculentas son, por su carácter crítico, aquellas que consiguen adentrarse en los sistemas operativos que gestionan los sistemas mismos y en las herramientas diseñadas para su protección como los antivirus y cortafuegos. El acceso ilimitado que estos programas tienen al conjunto del sistema les permite acceder a cualquier parte del mismo evitando, al mismo tiempo, generar alarmas que permitan al usuario adoptar medidas defensivas ya que éstas también deberían partir de ellos mismos.

El sonado caso del robo de datos del contratista del Departamento de Defensa de Estados Unidos *Rivist, Shaning* y *Adleman* (10) es muy ilustrativo de estos peligros. La empresa es la encargada de fabricar y mantener los *token* o generadores de claves que utilizan los funcionarios y militares del Departamento para acceder a las bases de datos del mismo (11). La sustracción de los algoritmos de generación de los códigos supondría la virtual inutilización del sistema ya que la seguridad de los mismos se encontraría comprometida por definición.

*Las amenazas dentro de y procedentes del ciberespacio* (12)

Como vemos, las redes informáticas son susceptibles de recibir multitud de ataques distintos; éstos formarían parte de las amenazas que el ciberespacio puede tener que soportar como ámbito de comunicación y transmisión de información.

Además de estas amenazas, el control que los sistemas cibernéticos ejercen sobre determinados procesos industriales y financieros proporciona un potencial inmenso de agresión *desde* el ciberespacio aunque el objetivo esté situado fuera de él. En este sentido cabe enfatizar el riesgo a que están sometidos los *servicios e infraestructuras críticos* –principal-

(10) En: *http://www.rsa.com/*

(11) En: *http://www.defensenews.com/story.php?i=6862639*

(12) Gómez de Ágreda, Á.: «Riesgos y amenazas en y desde el ciberespacio», *Seguridad Global,* número 1, Instituto Choiseul España, 2011.

mente las instalaciones energéticas– de los países desarrollados. Estos sistemas, incluso cuando están convenientemente protegidos y aislados, son un blanco especialmente apetitoso para los intrusos y su potencial, como demostró el virus *stuxnet*, es equivalente al de un ataque convencional masivo.

La posibilidad de hacer daño del ciberespacio no se limita a las acciones ofensivas. La utilización de sus potencialidades por parte de *organizaciones terroristas* o, simplemente, criminales les proporciona un instrumento multiplicador de sus propias capacidades que los convierte en particularmente peligrosos y les da un alcance muy superior al que podrían haber soñado de no contar con estos instrumentos. La notoriedad que buscan estas organizaciones está garantizada por la repercusión mediática que tienen los incidentes informáticos, especialmente cuando se combinan con acontecimientos de gran relevancia cuya seguridad física haría muy difícil actuar contra ellos directamente (13).

La utilización de las redes informáticas para la *captación, propaganda, financiación, instrucción y entrenamiento* es mucho más beneficiosa para este tipo de redes criminales que para organizaciones estatales con un mayor potencial propio. El ciberespacio es un elemento igualador de capacidades y reductor de asimetrías (14).

*Globalización y ciberespacio*

> «La globalidad es, esencialmente, un fenómeno de simultaneidad de flujos y nuevas formas de poder, en el que la información, los capitales y las mercancías, así como los individuos atraviesan –mediante la informática– las fronteras sin ningún límite, lo cual produce una nueva modalidad de identidad: nómada y fragmentada, desligada de las tradiciones nacionales cerradas» (15).

Los conceptos de *globalización* y de *ciberespacio* van necesariamente unidos en el mundo moderno. Son numerosos los autores que argumentan que el fenómeno de la globalización existe desde tiempos remotos

---

(13) En: *http://www.bbc.co.uk/mundo/noticias/2011/01/110120_0957_juegos_olimpicos_ciberataques_ 2012_londres_dc.shtml*

(14) En: *http://harrel-yannick.blogspot.com/2011/08/le-cyberespace-est-un-champ-de-bataille.htm*

(15) Pozas Horcasitas, R.: «*Globalidad» en Léxico de la Política*, Baca Olamendi, Laura *y otros* (comp.): editorial Fondo de Cultura Económica, México, 2004.

en mayor o menor medida, sin embargo, el fenómeno global según lo experimentamos en nuestros días es algo cualitativamente distinto y no una mera evolución del conocido «efecto mariposa» según el cual el humilde batir de las alas de una de ellas en algún lugar del mundo se trasladaba y tenía sus efectos sobre cualquiera otro.

La definición del profesor Pozas pone el énfasis en la utilización de los medios informáticos para construir el mundo global. Puede existir un mundo interconectado en el que los acontecimientos se influyan mutuamente con relativa independencia de las distancias a que sucedan, pero eso difícilmente puede calificarse de globalización. Es la *simultaneidad de la presencia virtual* de los actores, la creación de una sociedad paralela que vive en la Red, lo que permite la interacción en tiempo real de los acontecimientos y su mutua influencia.

Pozas pone al mismo nivel los flujos que recorren la Red y la aparición de nuevas formas de poder derivadas de la *capacidad de esos flujos* para viajar libres de impedimentos y de llegar a los más remotos confines. Si «la información es poder», la capacidad para hacer llegar esa información –en la forma que nosotros deseemos– hasta un número virtualmente ilimitado de receptores y en tiempo real supone una nueva forma de poder que va mucho más allá de los medios de comunicación de masas «clásicos».

La diferencia fundamental entre la televisión o la radio, que eran los que principalmente cumplían con la función difusora de información hasta hace pocos años e Internet no reside exclusivamente en la cantidad de posibles receptores del mensaje sino que hay otros aspectos mucho más importantes que convierten el ciberespacio en algo totalmente distinto. Prueba de ello es el efecto potenciador que pretenden conseguir las emisoras de radio y televisión colocando sus contenidos en la Red para buscar una audiencia más amplia y un acceso no restringido por los horarios de emisión a que se ven constreñidos en sus medios.

Por un lado está la *universalidad del acceso*. Mientras que la difusión de las señales de televisión o de radio ha estado condicionada a su retransmisión mediante repetidores hasta la aparición de los satélites y las antenas parabólicas (con la excepción de determinadas gamas de frecuencia de radio), el acceso a Internet –salvo que sea intencionada y puntualmente restringido– tiene un carácter universal con independencia del lugar desde el que nos conectemos. La capacidad para restringir, manipular o dirigir la información en la Red se ve más limitada para el

gran público que su equivalente para televisión o radio. La pluralidad y el volumen de la información accesible en Internet sobrepasan, con mucho, a la que hay en cualquier otro medio de comunicación.

Aún más importante que esta pluralidad y que el mismo volumen de información es la *interactividad* que permite el mundo digital. La posibilidad de participar activamente en la generación de noticias, de comentar, añadir, desmentir e interactuar de cualquier otro modo que tiene Internet le otorgan una ventaja notable desde el punto de vista psicológico por la diferencia en el grado de aceptación de la información en él contenida. De hecho, si bien el porcentaje de páginas *web* en inglés parece haber disminuido según la Organización de Naciones Unidas para la Educación las Ciencias y la Cultura (UNESCO) en los últimos años hasta el entorno del 42% (desde una proporción cercana al doble 15 años atrás), la lengua de Shakespeare ha vivido su mayor expansión gracias a la informática y al deseo de la gente de tomar parte activa en la Red.

La definición del profesor Pozas hace también referencia al *tránsito de capitales* y mercancías *(sic)* por el ciberespacio. Sería demasiado prolijo detenerse en los efectos que Internet ha tenido y tiene en el mundo financiero aunque tocaré el tema más abajo. Baste apuntar que, gracias a la creación de algoritmos que automatizan las transacciones bursátiles y a la velocidad en las gestiones, cada día se opera con el equivalente a docenas de veces el Producto Interior Bruto (PIB) mundial. La mayor parte de la riqueza del mundo no llega nunca a salir de los circuitos de los ordenadores y de los servidores de los bancos.

Y, aún así, el profesor Pozas coloca en la definición la capacidad de influencia que tiene el ciberespacio sobre las percepciones por delante de su valor financiero o comercial.

Vemos que el ciberespacio no altera solamente las rutas de los flujos y permite el acceso irrestricto de datos, ideas e información. *La principal característica de la globalización no está en el espacio, sino en el tiempo*. La influencia de esas ideas, de esos datos y de esa información se produce de forma inmediata y simultánea en todo el mundo. Lo que es más, su vigencia se reduce en función de la capacidad de la Red para aportar nuevos datos, de actualizar la información o de rebatir o debatir las ideas según están siendo plasmadas. Mucho más trascendental que el alcance físico de la Red son los *tempos* que impone. No basta con que los diarios digitales sean capaces de hacernos llegar las noticias con unos minutos de retraso (si acaso),

los titulares tienen que adelantarse incluso antes de ser susceptibles de ser editados e, incluso, abrir el debate público para los miles de usuarios que están permanentemente enganchados a su «gotero» de titulares.

El mundo global es un mundo gestionado por los usuarios en tiempo real en el que los datos influyen de forma simultánea e instantánea en todos los rincones del orbe y son sustituidos por otros que dejan obsoletos a los anteriores de forma casi instantánea y, muchas veces, demasiado rápida como para que podamos seguir su evolución paso a paso. Pensar en el ciberespacio como en un mundo físico en el que todo va más rápido, llega más lejos y actúa con mayor fuerza es un grave error equiparable a confundir un ordenador con una máquina de escribir electrónica o un teléfono móvil con un teléfono que no necesita cables.

La globalización, entendida en su forma moderna, necesita del ciberespacio porque se basa en su estructura y capacidades para su propia existencia. La descentralización que caracteriza desde su inicio al diseño cibernético influye y condiciona la vida en el mundo real. De este modo, las instituciones que surgieron en las postrimerías de la Segunda Guerra Mundial para garantizar una gobernanza mundial tutelada por las potencias vencedoras y que imponían un modelo centralizado alrededor de Naciones Unidas y del dólar como moneda de referencia (primero basándose en el patrón oro y después por sí mismo) se muestran poco eficientes en estos días en la gestión del mundo global.

*Control y descontrol en las redes*

En este contexto y partiendo de la *concepción westfaliana* que rige en la política de los Estados-Nación, Internet y el ciberespacio son intrusos que propician un reequilibrio de fuerzas en que la asimetría se convierte en una estrategia por sí misma. En el mundo virtual las fuerzas están mucho más equilibradas que en el físico y cada usuario es individual e independiente. El reto que supone este desafío al poder estatal está siendo motivo de preocupación entre las naciones más poderosas que, por un lado, ven como su ventaja diferencial se reduce considerablemente respecto de otros actores estatales y, por otro, como empiezan a intervenir jugadores no estatales que pretenden suponer un reto al mantenimiento del monopolio estatal en el uso de la fuerza (16).

(16) Sánchez Medero, G.: «Los Estados y la ciberguerra», *Boletín de Información del CESEDEN*, número 317, 2010, en: *http://www.ceseden.es/centro_documentacion/boletines/317.pdf*

Hete aquí otro de los aspectos más significativos del ciberespacio. El ejercicio de la fuerza ya no lleva necesariamente aparejados grandes desembolsos ni una cuidada preparación bélica sino que las agresiones pueden provenir de individuos o de grupos con algunos conocimientos rudimentarios de informática. Así, la figura del *hacker* se ha convertido en un icono de la modernidad digital y grupos como *Anonymous* (17) o *Lulzsec* acaparan un protagonismo reservado en otro tiempo a complejas organizaciones estatales. No quiere decir esto que haya llegado el momento de deshacerse de los arsenales militares y continuar su labor por medios electrónicos pero, desde luego, *las Fuerzas Armadas deberán tomar en consideración el potencial que tiene el ciberespacio como escenario de los conflictos presentes y futuros* e incluir en sus arsenales y especialidades suficiente material y personal capacitado para cubrir las necesidades que impone este nuevo campo de batalla.

El ciberespacio vive en un *estado permanente de agresión* en el que todos los usuarios, sea cual sea su nivel, son susceptibles de recibir ataques con relativa independencia de su grado de protección. El sueño que acompañó la caída del muro de Berlín de un mundo sin guerras –al menos entre las grandes potencias– ha dejado, apenas se asentó el polvo, un despertar en el que cada una de esas potencias está sometida a un incesante bombardeo. Si bien estas agresiones no son cruentas de por sí, sus efectos sobre las vidas de las personas y de las organizaciones son absolutamente reales.

El efecto igualador que ejerce el ciberespacio sobre sus usuarios al que aludíamos con anterioridad amplía hasta el infinito el número de agresores potenciales mientras que las dificultades en la trazabilidad en tiempo real (o, al menos, útil) de dichos ataques hace que sus autores sean *relativamente invulnerables a medidas disuasorias* como las que marcaron la guerra fría y, en muchos casos, escapen también de posibles represalias ante la dificultad de su identificación positiva y la inconveniencia de escalar conflictos fuera del entorno digital.

Esta situación amenaza la concepción westfaliana que sitúa al Estado en el centro de la vida política internacional. El Derecho Internacional está tremendamente mal dotado para responder a situaciones como ésta y

(17) Morcillo, C. y Muñoz, P.: «Anonymous, más allá de la máscara», diario *ABC,* 19 de junio de 2011, en: *http://www.abc.es/20110619/medios-redes/abci-anonymous-201106182338.html*

la atribución de responsabilidades –pilar sobre el que se sostiene todo el sistema– se lleva a cabo más con criterios políticos que científicos o jurídicos. Ni puede tenerse la certeza de que un ataque efectuado desde un servidor estatal tiene respaldo de la nación a que pertenece ni una intrusión llevada a cabo desde un cibercafé tiene porqué ser obra de un adolescente aislado. Unas normas jurídicas que establecen que un espía es aquel que actúa sin vestir el uniforme que le identifica como combatiente perteneciente a un Estado –y que se diseñaron antes de la existencia misma del espacio virtual– difícilmente pueden servir para regularlo (18). Los dispares intereses de las naciones en este terreno amenazan con que se cree una *indefinición jurídica* similar a la de otros asuntos como el terrorismo.

Precisamente por ello, con anterioridad a la cumbre del G-8 celebrada el pasado mes de mayo, el presidente de la República Francesa organizó una cumbre a la que invitó a las más relevantes figuras de la industria digital de la información. La respuesta que recibió por su parte fue bastante tibia y los creadores y organizadores de las redes sociales, buscadores y demás mostraron la diversidad de puntos de vista existentes sobre la necesidad y la conveniencia de establecer mayores controles sobre la Red.

Si bien los argumentos del Elíseo se basaban en la necesidad de proteger la propiedad intelectual, la libertad, la seguridad, la transparencia y la confidencialidad de forma genérica, los asaltos sufridos por la Administración francesa en fechas previas (19) y otros que se han hecho públicos desde entonces revelan que el alcance de la amenaza trasciende desde hace ya bastante tiempo el aspecto lúdico para adentrarse en el de la Seguridad Nacional incluyendo campos como el energético, el financiero y el de defensa (20).

*Los Estados reclaman un ambiente «favorable, transparente, estable y predecible»* para los usuarios y para ellos mismos, en palabras del presidente francés. Buena parte de la industria y de los usuarios abogan por un ciberespacio libre de la interferencia de los estados y autocontrolado;

---

(18) En: *http://www.theregister.co.uk/2011/02/04/cyberwar_rules_of_engagement/*

(19) En: *http://www.lavanguardia.com/20110420/54143326402/un-intento-de-estafa-pone-en-evidencia-la-seguridad-de-la-presidencia-de-francia.html*

(20) Rushkoff, D.: «*Internet is easy prey for Governments»,* CNN, 8 de febrero de 2011, en: *http://edition.cnn.com/2011/OPINION/02/05/rushkoff.egypt.internet/index.html?hpt=C1*

con sus limitaciones, desde luego, pero abierto y en constante evolución como hasta el momento.

Para el mes de noviembre estaban previstas distintas conferencias en Londres y Aviñón y un Foro de Gobierno de Internet cuyas conclusiones no podremos ya recoger en este capítulo pero que, con toda seguridad, apuntarán en la dirección expuesta. En cualquier caso, la navegación por el ciberespacio tal y como la conocemos y disfrutamos ha llegado a su punto actual de desarrollo precisamente por su carácter inestable e impredecible. Una modificación de este carácter podrá dar lugar a un espacio más «habitable» pero lo hará a costa de perder la vitalidad que lo creó y desarrolló. Un *ciberespacio estable y predecible* podrá ser más útil a determinados usuarios pero no necesariamente, como piensa Sarkozy, lo que el mundo necesita.

La necesidad de establecer *mecanismos de autorregulación* que coarten lo menos posible la iniciativa de desarrolladores y de innovadores se plantea como una alternativa a la creación de una red paralela en la que estarían ubicados los sitios que necesitan primar la seguridad sobre las demás consideraciones. Las posiciones respecto al tema están muy polarizadas y no faltan quienes entienden que el objetivo de la reciente presencia mediática del tema es proporcionar una excusa a los gobiernos para hacerse con el control de Internet (21).

## Amenazas en el ciberespacio

La *capacidad para dominar la generación, gestión, uso y manipulación de información* con la ayuda de las tecnologías cibernéticas tiene un tremendo potencial para aquellos que la posean. Ese potencial está permitiendo desarrollar el periodo más productivo de la historia de la humanidad. Sin embargo, el poder que supone significa, al mismo tiempo, una amenaza para aquellos sobre los que se ejerza. Como hemos visto, a diferencia de otras ocasiones históricas, el ciberespacio permite que pequeñas potencias, empresas e, incluso, particulares estén en condiciones de adquirir esas capacidades en una medida suficiente como para lograr grandes desarrollos, pero también para suponer una amenaza desproporcionada para su entidad tradicional.

(21) Shields, M.: «La ciberguerra es una exageración que podría militarizar internet», *BBC Mundo*, 16 de febrero de 2011, en: *http://www.bbc.co.uk/mundo/noticias/2011/02/110216_ciberguerra_exageracion_mt.shtml*

Diversos informes hacen ya un estudio histórico de la amenaza cibernética y su evolución a pesar de que no cuenta todavía con el medio siglo de vida. Sin embargo, los *tempos* que se manejan en el ciberespacio –sobre los que volveremos más tarde– son absolutamente distintos de los de otros ámbitos y, efectivamente, el ritmo evolutivo del mismo hace que las amenazas que hace unos pocos años ocupaban portadas en la prensa por su incidencia a nivel mundial sean hoy poco menos que inocuas. De hecho, incluso los objetivos perseguidos por los atacantes han variado a lo largo de los años y, de algún modo, se han profesionalizado. De las intrusiones de carácter «deportivo» en la que un adolescente buscaba demostrar su dominio de la tecnología o poner en evidencia a su víctima hemos pasado a ataques coordinados que pretenden obtener información sensible; muchas veces con *finalidades económicas* o *políticas.*

La difusión de los ataques cibernéticos se produce tras la fusión de los medios informáticos con los de telecomunicaciones que permiten a los primeros conectarse entre distintos terminales y compartir información. El fenómeno, que tiene lugar a finales de los años setenta y principios de la década de los ochenta, viene a coincidir con la introducción del ordenador personal, el popular PC. La reducción del tamaño y, más aún, del precio de los terminales da paso a una generación de jóvenes apasionados por los nuevos «juguetes» que se dedican a estudiar sus entrañas físicas y lógicas. La relativa *simplicidad de las estructuras* del momento permite un conocimiento profundo de las mismas en poco tiempo y anima a muchos usuarios a bucear en *la capa sintáctica* tanto como en *la capa física*.

Fruto de esta pasión fue una rapidísima *evolución de los sistemas* de la época que se sucedían unos a otros en el espacio de meses. También resultó en la aparición de los primeros ataques cibernéticos que aprovechaban las vulnerabilidades que estos incipientes «genios» de la informática iban detectando. Estando el fenómeno bastante restringido en cuanto a su difusión, el usuario final de un vector de ataque solía ser el mismo que lo había diseñado ya que apenas había mercado para estos productos. Buena parte de los desarrolladores de virus, gusanos y troyanos de los primeros tiempos terminaron por engrosar las nóminas de las compañías del sector donde continuaron su labor detectando las mismas vulnerabilidades y desarrollando los parches pertinentes.

La expansión del fenómeno y la *inclusión de componentes informáticos en otros dispositivos como los teléfonos móviles* de última generación

han ampliado el número de terminales susceptibles de ser atacados y el número de vulnerabilidades disponibles para hacerlo. La interconexión existente entre muchos de estos terminales y las redes hace que se utilicen muchas veces como puerta de entrada para atacarlas. La proliferación de tabletas y dispositivos móviles conectados de forma inalámbrica en los últimos tiempos supone un paso más en la pretensión de conexión universal –que ha supuesto la necesidad de modificar el modelo de direcciones del Protocolo de Internet (IP)– pero también mayor vulnerabilidad global.

Los *hackers* de «sombrero blanco» –aquellos que dedican sus esfuerzos a detectar las vulnerabilidades sin ánimo de explotarlas delictivamente– se han agrupado en asociaciones y comunidades para ayudar a la protección del ciberespacio. El diario *El País*, publicaba (22) que, en el ámbito de una de estas comunidades, DEFCON (23), se había dado a conocer el descubrimiento, por parte de una niña de 10 años de una vulnerabilidad en un juego para teléfono móvil.

*El poder de la información*

Nacido dentro del ámbito militar, la primera preocupación que surgió en un Internet abierto a millones de potenciales usuarios fue la seguridad de la información contenida en la Red. La *penetración de sistemas* de ordenadores conectados en red con la finalidad de acceder a información sensible se convirtió en una de las principales actividades criminales dentro del ciberespacio. De hecho, continúa siendo la «operación» bélica o criminal que se produce más asiduamente. Todos los días, millones de empresas y organismos oficiales reciben intentos de intrusión que comprometen ingentes cantidades de datos.

No entraremos a describir aquí las características técnicas de virus, gusanos, troyanos y demás *malware* destinado a los ataques contra la es-

(22) *CyberPais* del día 8 de agosto de 2.011, página consultada el mismo día, en: *http://www.elpais.com/articulo/tecnologia/nina/anos/descubre/vulnerabilidad/juegos/moviles/elpeputec/20110808elpeputec_2/Tes*

(23) DEFCON es el acrónimo que define una condición de defensa (*DEFense CONdition*), es decir, el grado de alerta a que están sometidas las fuerzas de la Alianza en función de la amenaza. Esta comunidad de *hackers,* en: *http://www.defcon.org/,* toma su nombre de la abreviatura.

tructura misma del ciberespacio (24). Otro capítulo de esta *Monografía* tiene ese cometido. Nos limitaremos en las siguientes líneas a incidir en los efectos que tienen estos ataques y a ilustrar cada caso con algunos ejemplos recientes que pongan de relieve la magnitud de la amenaza. Lógicamente, el incremento más que exponencial que se ha venido produciendo en el papel que la Red juega en la generación, almacenamiento y distribución de datos en los últimos años supone que la magnitud de la misma se ha incrementado, al menos, en la misma proporción.

Sí podemos adelantar que aquellos virus, como el famoso *Iloveyou*, que hace apenas una década eran la gran preocupación de los encargados de la seguridad por su potencial destructor de los contenidos de los ordenadores han dejado de ser el principal quebradero de cabeza de la actualidad. En primer lugar porque la seguridad de los sistemas es ahora mucho mayor y la sofisticación necesaria para acceder a los mismos, cuando están convenientemente protegidos, se ha multiplicado. Pero también porque *los esfuerzos de los piratas se dirigen a actividades mucho más productivas*, para ellos, que la mera destrucción de información o programas.

La actividad ofensiva que prima en la actualidad tiene mucho más que ver con conseguir *ganar acceso a un sistema* que con su destrucción o inhabilitación. La destrucción lógica de bases de datos, sin embargo, puede seguir considerándose como una posibilidad a contemplar en un conflicto cuando no es posible la extracción de la información para su explotación por parte de las fuerzas propias o cuando ésta no va a ser viable por la premura de tiempo disponible.

Conviene siempre tener presente la realidad con la que estamos conviviendo hasta el momento en la relativamente corta historia de los *conflictos* que se han librado, total o parcialmente, en el ciberespacio. No obstante, conflictos más o menos abiertos como las agresiones que los servidores de la República de Estonia sufrieron en el año 2007 o la utilización del técnicas cibernéticas durante la confrontación entre la Federación Rusa y la República de Georgia en el verano del año 2008 –o conflictos de la misma naturaleza en Lituania y Kazajistán– no son, ni mucho menos, la única actividad que se lleva a cabo ni siquiera la principal de ellas.

---

(24) En: *http://www.bbc.co.uk/mundo/noticias/2011/02/110216_ciberguerra_exageracion_mt.shtml*

*Los casos de Estonia y Georgia*

Muy brevemente, haremos una descripción de las acciones que tuvieron lugar durante ambas confrontaciones para poder extraer las conclusiones pertinentes sin pretender, en cualquier caso, que éstas vayan a ser definitivas e inmutables. La guerra en el ámbito cibernético está en un estado demasiado embrionario como para considerar nada lo bastante evolucionado como para establecerlo como paradigma.

Estonia era, ya a primeros de este siglo, pionera en la utilización de las redes informáticas en multitud de aspectos de su vida cotidiana. Desde el mismo año 2000 su Administración comenzó a poner en marcha una cultura de ausencia de papel y a mantener la correspondencia y las reuniones –incluidas las del Consejo de Ministros– sobre bases de datos comunicadas. La presencia de la cibernética permea todos los aspectos de la vida estonia, desde la mencionada Administración hasta la educación pasando por su utilización para todo tipo de servicios. Entre estos últimos, los bancarios emplean de forma particularmente profusa los medios informáticos y telemáticos de forma que la cantidad de dinero en metálico que se mueve en el país es mínima ya que la mayor parte de las transacciones se efectúan de forma electrónica. Su nivel de dependencia de las nuevas tecnologías hace que haya recibido el apodo de *E-stonia* entre la comunidad digital.

El conflicto del año 2007 comenzó como una cuestión urbanística que se politizó en el contexto de las tensiones existentes entre la comunidad estonia de origen ruso y la autóctona. El traslado de un monumento que honra la memoria de los soldados rusos caídos en las batallas libradas en el país desde su ubicación habitual en el centro de la ciudad, a un cementerio desencadenó una serie de críticas de los rusos de ambos lados de la frontera.

Las críticas dieron lugar a ataques, más o menos organizados en principio, sobre las páginas *web* y los servidores del país báltico. La situación se escaló hasta que eran miles de terminales los que servían como lanzadera para los ataques de denegación de servicio distribuida que terminó por colapsar la capacidad de los servidores estonios. Durante semanas ningún servicio telemático funcionaba en un país que, como hemos visto, es altamente dependiente de los mismos. Los ataques por saturación procedían, en su mayor parte, de ordenadores situados al otro lado de la frontera aunque no se detectó ninguna dependencia estatal de los

mismos. De hecho, las redes sociales jugaron un papel importante en la coordinación de los mismos si bien se podría suponer un instigador de naturaleza institucional por la naturaleza política del ataque.

La gravedad de la situación llevó a Estonia a considerar la petición de activación del artículo V del Tratado de Washington que establece el principio de defensa mutua dentro del ámbito de la Alianza Atlántica. Si bien no llegó a implementarse la medida, su mera consideración es digna de reseñarse como un hito en la naturaleza bélica de la utilización también del ciberespacio.

Estonia puso en marcha una serie de medidas con ayuda internacional para contrarrestar la parálisis que estaba sufriendo. Cerró el acceso exterior de sus servidores para permitir solamente su uso desde territorio nacional y contrató los servicios de empresas de *routing* que le permitiesen incrementar su capacidad y restablecer sus conexiones externas por vías alternativas. La medida se demostró eficaz aunque sólo pueda considerarse válida cuando la mayor parte de las conexiones se establezcan desde terminales ubicados más allá de las fronteras del país objetivo.

Un año después de los incidentes se inauguraba en Tallin el Centro de Excelencia de Ciberdefensa Cooperativa (CCDCOE) de la Organización del Tratado del Atlántico Norte (OTAN) (25) para fomentar la investigación y la formación del personal de la Alianza en temas de seguridad cibernética y contribuir a la cultura de la colaboración en dicho campo.

El caso estonio es de difícil clasificación dentro de la gama de conflictos. No existe ninguna prueba de implicación estatal en los ataques ni de que éstos fueran siquiera organizados por un grupo político o de presión concreto. La escala, coordinación y magnitud de los mismos lo sugiere pero sin que se pueda atribuir la autoría a nadie ni a ningún país. Se considera por parte de los expertos que ésta será una constante en los conflictos en el ciberespacio.

Estos conflictos no llegarán a alcanzar, previsiblemente, un grado de intensidad equivalente al de las guerras convencionales cuando se produzcan por separado pero mantendrán una incidencia constante de un nivel medio o bajo. Sin embargo, en los conflictos armados «clásicos» es de esperar que, a partir de ahora, uno de los frentes de batalla siempre esté en el ámbito cibernético y telemático.

(25) En: *http://www.ccdcoe.org/*

Es el caso del conflicto que libraron la Federación Rusa y la República de Georgia en agosto de 2008. De forma paralela a la campaña bélica que llevaron a cabo las fuerzas regulares –y algunas no tanto– de ambos países se produjeron acciones paralelas en el ciberespacio por parte de ambos contendientes. Curiosamente, también en este caso resulta prácticamente imposible atribuir la autoría a los gobiernos de ambas naciones a pesar de que el estado de guerra *de facto* en que se encontraban habría justificado el recurso a los medios cibernéticos como parte de la campaña.

Los ataques sobre Georgia se organizaron desde seis *botnets* (redes de ordenadores que actúan coordinadamente bajo un control centralizado) distintas que implicaban terminales de todo el mundo y que, supuestamente, habrían sido obra de *hacktivistas*. Richard A. Clarke y Robert K. Knake, en su libro: *Guerra en la red. Los nuevos campos de batalla* (26) llegan a asociar las *botnets* con los Servicios de Inteligencia rusos aunque éstos negaron siempre estar implicados en el caso.

Los combates físicos se originaron con ocasión de una serie de disturbios en las regiones independentistas de Osetia del Sur y de Abjasia y dentro del contexto general de la expansión hacia las antiguas repúblicas soviéticas tanto de la Alianza Atlántica como de la Unión Europea. En cuestión de pocas horas, fuerzas rusas y georgianas tomaron posiciones convergiendo sobre la capital de Osetia del Sur. Las acusaciones mutuas de inicio de las hostilidades y la opacidad de la información hicieron muy difícil la determinación del agresor inicial.

Estas informaciones y falta de transparencia son, precisamente, uno de los efectos principales conseguidos con la interferencia sobre las redes informáticas de ambos adversarios. Si bien Georgia utilizó sus propios recursos para atacar a los rusos, su limitada capacidad se vio todavía más reducida desde semanas antes de comenzar abiertamente las hostilidades y casi totalmente anulada durante la duración del conflicto. En contra de lo que podría llegar a pensarse, la incidencia en la capacidad de mando y control de las Fuerzas Armadas georgianas se vio menos afectada de lo que cabría esperar ante la magnitud del ataque ya que su dependencia de las tecnologías de la información era mucho menor que la que tenía, por ejemplo, Estonia en la crisis del año previo.

---

(26) En: *http://fernandorgenoves.blogspot.com/2011/04/guerra-en-la-red-de-richard-clarke.html*

Durante la campaña llegó incluso a anularse el dominio *.ge* perteneciente a la República de Georgia. Las *webs* de distintos ministerios de la república caucásica estuvieron colapsadas permanentemente después de haber sufrido ataques menores –como *Defacements*, alteraciones de la apariencia de la página, normalmente con fines propagandísticos o críticos– en el trascurso de las semanas previas. La paralización de la actividad económica y mediática tuvo repercusiones serias en Tiblisi. Como queda apuntado, la incapacidad de los georgianos para comunicarse con el exterior de forma fluida toda vez que sus servidores estaban colapsados y la falta de referencias internacionales crearon un vacío informativo desde Georgia en ambos sentidos –entrada y salida– cuyos efectos fueron mayores que los producidos sobre el propio sistema de mando y control.

Grupos rusos de simpatizantes de las provincias secesionistas y de nacionalistas cargaron, supuestamente, con el peso de la distribución del *software* necesario para formar las redes de ordenadores cautivos que se utilizaron como vectores en los ataques. La capacidad de movilización a través de las redes sociales, con independencia de quién estuviera realmente detrás, se puso de manifiesto aquí bastante antes de los sucesos de la «primavera árabe» de principios del año 2011 o los del Reino Unido que han tenido lugar este mismo verano.

*Armas insidiosas, guerreros anónimos*

Común a estas dos acciones y a la práctica totalidad de las que se producen a diario fuera de contextos tan definidos es el hecho de que la posibilidad de *atribución de los ataques*, sobre todo en tiempo útil –ya que no real– es, hoy por hoy, casi imposible de conseguir en la mayor parte de los casos. La Ingeniería Forense Informática, encargada de investigar y determinar la trazabilidad de los ataques tiene un largo camino por delante antes de poder proporcionar a los juristas las pruebas que necesitan para actuar contra estos esquivos adversarios.

La imposibilidad de atribución de las acciones ofensivas que se desarrollan en el ciberespacio es uno de los motivos que se esconden detrás de la reunión convocada por el presidente Sarkozy antes de la cumbre del G-8 de mayo pasado (27). Como hemos comentado, esta dificultad para

(27) Gómez de Ágreda, Á.: «eG8. Vuelta a Westphalia», *Revista Atenea Digital,* 8 de junio de 2011, en: *http://www.revistatenea.es/RevistaAtenea/REVISTA/articulos/GestionNoticias_4876_ESP.asp*

el rastreo del origen de las agresiones supone en la práctica la *impunidad* de terroristas y criminales que se amparan en una larga cadena de saltos y en un servidor final ubicado en países que no pueden o no quieren colaborar en su rastreo.

Para la actividad de estos individuos o grupos es particularmente útil la creación de *botnets* o redes de terminales «esclavizados» que colaboran con sus recursos a las acciones de su controlador. En contra de lo que pueda pensarse entre los usuarios casuales, la extensión de estas redes de ordenadores alcanza los millones de terminales y su potencia combinada es lo que permitió ataques como los que hemos descrito anteriormente en Estonia y en Georgia.

Los virus y, sobre todo, los gusanos y troyanos modernos tienen, muchas veces, la misión de actuar como transmisores de instrucciones o de abrir puertas traseras en aquellos sistemas que infectan para colocarlos «a las órdenes» de su creador y distribuidor. En muchos casos, los usuarios pueden ser perfectamente inconscientes de la existencia de estos *malware* durante un tiempo indefinido durante el cual su equipo está siendo utilizado para la distribución de correos electrónicos o para saturar la capacidad de los servidores de un gobierno. Acciones relativamente simples y aparentemente tan poco agresivas como visitar repetidamente una página *web* se convierten en ataques de *denegación de servicio* cuando consiguen saturarla y evitar que sea utilizable por el público o por los clientes en general.

Cuando el ataque de denegación de servicio se hace utilizando los recursos de varios sistemas dirigidos o controlados desde uno central o coordinados de alguna manera estamos hablando de una *denegación de servicio distribuida*. Las formas de coordinación pueden ser tan poco sofisticadas como la distribución de correos electrónicos o mensajes de texto entre un grupo de colaboradores para ejecutar las acciones, de forma más o menos manual, cada uno desde su propio terminal. Diversos grupos de *hacktivistas* (28) han conseguido una gran notoriedad en los últimos años utilizando técnicas de este estilo.

(28) El *hacktivismo* es la utilización de las herramientas informáticas para la acción política «no violenta». Entre sus actividades incluye los sabotajes de páginas *web* y otras agresiones que cuestionan el concepto de violencia que emplean en su propia denominación.

De entre estos grupos, sería interesante destacar los dos que más éxitos han conseguido: *Anonymous* y *Lulzsec*. Ambos tienen una larga lista de intrusiones en diversos sistemas de seguridad (29) y, al menos el primero, apoyó a Julian Assange tras su detencón posterior a la publicación en su página *WikiLeaks* de docenas de miles de cables confidenciales extraídos de un servidor del Departamento de Defensa por un usuario con acceso autorizado en un caso, todavía pendiente de juicio, que se ha convertido en un ejemplo paradigmático de explotación de una vulnerabilidad en la capa humana de un sistema aislado y considerado seguro.

Los ataques de denegación de servicio y de robo de datos (30) llevados a cabo por estos grupos organizados han puesto en jaque a diversas industrias (31) y organismos nacionales e internacionales (32) Sólo en los últimos meses se ha empezado a actuar policial y judicialmente contra sus supuestos integrantes (33). Una de las reclamaciones que presentan, bastante en línea con otras protestas juveniles contemporáneas como el Movimiento 15-M, es la libertad de utilización de la Red sin interferencia de actores estatales. La postura, antagónica a la mantenida por varios gobiernos como hemos visto, aspira a una virtualización de la sociedad mediante el uso de las redes sociales y a implantar la democracia directa y abierta.

*Ser o no ser en la Red*

El robo de identidades (34) de datos, de contraseñas y accesos no son, como afirman Peter Sommer e Ian Brown (35) acontecimientos ciber-

---

(29) En: *http://www.eluniversal.com.mx/notas/784150.html*

(30) En: *http://www.huffingtonpost.com/2011/04/03/epsilon-hack_n_844212.html?utm_source=DailyBrief&utm_campaign=040411&utm_medium=email&utm_content=NewsEntry&utm_term=Daily%20Brief*

(31) En: *http://alt1040.com/2011/07/lulzsec-anonymous-rupert-murdoch*

(32) En: *http://www.itespresso.es/lulzsec-y-anonymous-ponen-al-descubierto-informacion-del-fbi-y-la-otan-52128.html*

(33) En: *http://www.lavanguardia.com/internacional/20110720/54188738736/detienen-a-14-hackers-de-anonymous-en-ee-uu.html, http://www.abc.es/20110727/internacional/abci-detenido-lulzsec-201107271802.html*

(34) En: *http://ingame.msnbc.msn.com/_news/2011/04/26/6539290-why-the-playstation-network-breach-is-scary* y, sobre el mismo tema, en: *http://www.lavanguardia.com/internet/20110429/54147434582/a-la-venta-en-internet-los-datos-de-dos-millones-de-tarjetas-de-credito-robados-a-playstation.html*

(35) Sommer, P. and Brown, I.: «*Reducing Systemic Cybersecurity Risk», Project on Future Global Shocks,* OECD/IFT, enero de 2011, en: *http://www.oecd.org/dataoecd/57/44/46889922.pdf*

néticos individuales que puedan ocasionar, por si mismos, un fallo catastrófico del sistema. Sin embargo, su utilización diaria –sobre todo teniendo en cuenta la velocidad a la que se mueve la información en el ciberespacio y la recurrencia que puede alcanzar con algoritmos automatizados– produce un desgaste que va drenando las reservas de las víctimas. En este sentido, Sommer y Brown sólo detectan en su estudio dos posibilidades de *fallo catastrófico del sistema* (36) en su conjunto: un ataque que acertase a alterar los protocolos técnicos subyacentes de los que depende Internet (que, ciertamente, no afectaría a los sistemas desconectados aunque limitaría mucho su utilidad) o bien la destrucción física de los componentes en que se basan las comunicaciones por una masiva erupción solar (o una serie de pulsos electromagnéticos).

Las propias características del ciberespacio, como hemos venido diciendo, nos aseguran que el resto de los ataques se seguirán produciendo en mayor o menor medida. Por experiencia sabemos que *las brechas anteceden a los parches* igual que los delitos a la legislación por lo que siempre existirán nuevas formas de ataque. Ni la seguridad absoluta en este campo es posible ni lo es la represalia en tanto no se consiga determinar con certeza la fuente de los ataques.

Otra consecuencia que puede extraerse, principalmente del ataque sobre los servidores de Estonia, es que la seguridad de una nación constituye un todo indisoluble. Cada día con mayor frecuencia las Administraciones externalizan parte de sus servicios; aquellos considerados no propiamente característicos de su actividad principal. La *externalización*, si bien está demostrado que sirve para ahorrar costes y generar un tejido empresarial alrededor de los aparatos gubernamentales, supone igualmente la subcontratación de una serie de garantías que, previamente, venían asumiendo los mismos organismos gubernamentales. Entre ellos está la seguridad de los sistemas que emplean y que, en multitud de ocasiones, comparten o están ligados con los del organismo al que sirven.

Es necesario exigir a las compañías que trabajan como contratistas del Gobierno los mismos niveles de concienciación, al menos, que los que existan dentro de la Administración. La *falta de concienciación* a este respecto no sólo supone un riesgo añadido para la seguridad de los

(36) Más sobre el tema, en: *http://www.bbc.co.uk/mundo/noticias/2011/01/ 110117_ciberguerra_ocde_ataques_tecnologia_dc.shtml*

Estados sino una dilapidación de los recursos públicos empleados en la protección de los medios propios si se permite que queden «ventanas» abiertas a través de compañías civiles.

Los gobiernos tienen que comenzar por admitir su limitado papel en la defensa cibernética. Más del 80% de los sistemas críticos para una nación están en manos privadas y su protección es sólo parcialmente responsabilidad de los gobiernos. Salvo que se quiera reformar completamente la arquitectura del ciberespacio –puede hacerse, teóricamente, ya que es un diseño humano– para habilitar un ámbito más seguro y restrictivo lo mismo es cierto del resto de los sistemas informáticos. El *papel supervisor* y, fundamentalmente, *de formación y de concienciación que tienen los gobiernos* con respecto a la ciberseguridad en general es, sin embargo, una de sus más importantes y también irrenunciables responsabilidades.

La buena noticia es que, al tiempo que los métodos de intrusión y de ataque se van haciendo más sofisticados, también las técnicas de detección y defensa lo hacen. Cada día es más difícil para un *hacker* «lobo solitario» acceder a las redes de mayor *complejidad y capacidad de autoprotección*. Esta circunstancia deja en manos de grupos organizados –normalmente con un Estado o una gran corporación detrás proporcionando el apoyo financiero y los medios necesarios– la mayor parte de los ataques significativos. Cualquier pirata que quiera acceder de forma continua y eficaz (o lucrativa, en su caso) un sistema moderno deberá:

1. Disponer de los vectores adecuados para explotar las *vulnerabilidades «de día-cero»*, esto es, nuevas y desconocidas para los operadores y los diseñadores. Del mismo modo que siempre existen nuevas vulnerabilidades que explotar, también las empresas de seguridad están resolviendo muchas de ellas a diario por lo que la «oferta» de vulnerabilidades se mantiene más o menos constante y tiene una caducidad muy limitada.
2. Estar en condiciones de *diseñar nuevos vectores* una vez que la primera versión haya sido detectada y contrarrestada. Este hecho puede darse incluso antes de que llegue a utilizarse por ser descubierta la vulnerabilidad o por utilizarse el vector por otro agente
3. Conocer con el mayor lujo de detalles posible la *estructura del sistema* a atacar
4. Diseñar el método de ataque para conseguir *escapar a la detección y seguimiento.*

Como veremos también para las amenazas que provienen del ciberespacio pero que se materializan fuera de él, debemos aspirar a ser capaces de minimizar los efectos provocados por los mismos y a recuperar cuanto antes nuestra capacidad para operar. A eso se ha denominado *resiliencia*, una *resistencia adaptativa* que va reconfigurando nuestro sistema para sufrir los menos daños posibles y recuperar la operatividad con el menor coste para el usuario. Del mismo modo que es muy difícil que un arma cibernética pueda ser decisiva en un conflicto es previsible que estén presentes, en mayor o menor medida, en todos los que se combatan en el futuro previsible.

Válido tanto para las amenazas dentro del ciberespacio como para aquellas originadas desde el mismo es también el principio de que la defensa tiene que hacerse, necesariamente, con una *visión integral*. Se deben incluir sistemas públicos y privados, civiles y militares, empresariales y particulares bajo un mismo paraguas, con distintos grados de protección en función de su exposición pero de manera que formen un conjunto coherente. De nada sirve a la seguridad de una nación que sus Fuerzas Armadas tengan una red informática impenetrable si su sistema bancario está expuesto o si sus comunicaciones quedan bloqueadas porque ha sido atacado su proveedor de servicios. En un mundo interconectado e interdependiente, la protección de los elementos periféricos es tan vital como cualquier otro elemento porque los sistemas ceden siempre por su eslabón más débil.

**Amenazas desde el ciberespacio**

Igual que en el combate aéreo, la pugna dentro del ciberespacio busca obtener la supremacía –la absoluta *libertad de acción* para ejecutar las operaciones que se deseen y asegurar que los rivales no pueden hacer otro tanto– o, a lo menos, la superioridad en el enfrentamiento, limitando la situación de supremacía a un espacio o tiempo determinado. A pesar del lenguaje con connotaciones marineras que habla de navegar o surfear en las redes, el medio aéreo y el cibernético comparten muchas más afinidades; muy especialmente la de que ambos tienen una enorme capacidad para influir sobre otros ámbitos.

Tanto el espacio aéreo como el ciberespacio engloban de alguna manera a los demás *Commons* rodeándoles y siendo capaces de acceder a los mismos desde la privilegiada posición elevada que mantienen. La velo-

cidad de los procesos en ambos medios es otra de las características comunes. El salto que se produce desde los plazos que se manejan en las operaciones terrestres o navales y aquellos a los que acostumbran a manejar los responsables de las operaciones aéreas es de varios órdenes de magnitud. Sin embargo, el abismo que separa cualquiera de dichas velocidades con la cuasi ubicuidad resultante del espacio cibernético es todavía mayor. Es por este motivo que, alcanzada la deseada supremacía o superioridad en el espectro digital, el *potencial para influir en el exterior* del mismo desde las redes digitales es cuantitativa y cualitativamente incomparable con cualquier otro medio conocido hasta la actualidad.

De este modo, mientras que es bastante difícil obtener la supremacía aérea –por mucho que haya sido el caso en las últimas guerras y operaciones de la Alianza– se me antoja casi imposible obtener la digital. Igualmente, mientras que el dominio del aire siempre supondrá no sólo una ventaja para el que lo ostenta sino un serio revés para el que lo sufre, *el dominio del ciberespacio no tiene porqué afectar negativamente a un adversario que carece de medios cibernéticos* por mucho que seguirá mejorando las capacidades de sus enemigos.

Conviene comenzar por hacer una reflexión sobre el *concepto de la velocidad* aplicado al ciberespacio. El hombre ha sido capaz de irse adaptando a los diferentes *tempos* impuestos por sus avances en la navegación en los distintos medios naturales. De hecho, las sociedades menos desarrolladas y con menos capacidad para acceder a comunicaciones más rápidas y fluidas mantienen pautas de comportamiento radicalmente diferentes a las que sí pueden permitirse su utilización.

No se trata sólo de los medios de comunicación y de la capacidad de transporte sino, fundamentalmente, de los medios de transmisión de datos que nos permiten ampliar el ámbito de nuestras interacciones a prácticamente cualquier otro punto del globo que tenga acceso a tecnologías equivalentes. El ritmo de vida de las grandes ciudades, sin ir más lejos, refleja el mayor uso que se hace de estos medios. El mundo globalizado es, ante todo, un mundo interconectado, un *mundo intercomunicado*, en que cada individuo se va volviendo cada vez más dependiente del resto de la comunidad mundial. Thomas P. Barnett divide al mundo en dos mitades en función de que pertenezca a la comunidad global «conectada» o no. Algo muy parecido a la división entre el «mundo-que-importa» y el que no.

Sin embargo, la capacidad de adaptación que había demostrado el hombre cuando se trataba de acomodarse a los ambientes naturales se ve drásticamente reducida cuando hablamos del entorno digital. Los *tempos* que impone la velocidad de la luz a la que se desplazan los datos realizados por procesadores enlazados por todo el mundo se escapan a la comprensión humana o, al menos, a su capacidad para atenderlos personalmente. *El ciberespacio tiene que volarse con el piloto automático conectado* porque somos incapaces de dirigir sus pasos de forma manual sin limitar las posibilidades del sistema.

Eso no quiere decir que el ser humano haya perdido el control sobre los procesos que se realizan en el mundo digital sino que su capacidad se limita a ponerlos en marcha confiando en haber definido correctamente los algoritmos y así obtener el resultado apetecido.

Pero no todo tiene que ver con los procesos lógicos en el ciberespacio. Internet se ha convertido, ante todo y sobre todo, en una gigantesca *red de comunicaciones* que ha cambiado las pautas de comportamiento de las sociedades desarrolladas. El hombre contemporáneo es un ser conectado permanentemente y que recibe una abrumadora cantidad de información a un ritmo difícilmente digerible; es un hombre hiperinformado pero con una menguante capacidad de análisis. Mario Vargas Llosa lo describe con su prosa precisa en su artículo «Más información, menos conocimiento» (37) cuando habla del «mariposeo cognitivo». El ser humano se ha convertido en un devorador de titulares y de información premasticada (38).

El *potencial orientador* –incluso manipulador– de los medios de comunicación tradicionales, la cara perversa de la prensa, recibe con la llegada de Internet un impulso insólito y un efecto multiplicador potencialmente peligroso. Las tradicionales Operaciones militares de Información (InfOps) y Psicológicas (PsyOps, terminología militar) encuentran en el ciberespacio un terreno fértil donde desarrollarse. Por desgracia, el terreno es igualmente fértil para cualquier otro actor que pretenda desarrollar este tipo de actuaciones; incluso para aquellos para los que estas actividades estaban vedadas o muy limitadas en función de sus recursos.

---

(37) Vargas Llosa, M.: «Más información, menos conocimiento», *La Cuarta Página*, p. 27, *El País*, 31 de julio de 2011.

(38) Fanjul, S.: «Atentos a todo… y a nada», diario *El País* 12 de mayo de 2011, en: *http://www.elpais.com/articulo/sociedad/Atentos/todo/nada/elpepusoc/20110512elpepusoc_3/Tes*

Finalmente, el ciberespacio no sólo transmite información para el consumo directo de nuestros ojos sino que *conecta sistemas e instalaciones industriales*. La asignación de las tareas de rutina y de supervisión a programas informáticos y sistemas cibernéticos incrementa la eficiencia de las instalaciones y mejora el rendimiento general de las empresas. No obstante, el incremento de capacidades –como en todos los casos– viene acompañado de un aumento similar de las vulnerabilidades que tiene implícitas. Cuanto más complejo sea un sistema, mayor será el número de errores que puede contener. Esto, que es cierto para los programas informáticos que contienen millones de líneas de instrucciones, es perfectamente válido para cualquier sistema industrial.

A las amenazas que se cernían sobre cualquiera de las estructuras críticas para el funcionamiento de una nación se deben añadir ahora las que puedan provenir de los ataques a través de las redes digitales e, incluso, de la paralización de éstas.

*Sobre la economía*

Existe una limitada, aunque variable, cantidad de dinero en circulación. Mucho más limitada es la cantidad disponible para una persona o para una empresa en un momento dado y, sin embargo, las oportunidades de invertir esas cantidades, disponiendo de la información adecuada, son prácticamente infinitas. Los mercados han buscado tradicionalmente la forma más ágil de mover el dinero disponible para poder utilizarlo allá donde sea más rentable y tantas veces como sea posible en el menor lapso de tiempo. La aparición de mercados secundarios donde las posiciones se adoptan y se deshacen a gran velocidad ha incrementado el potencial para utilizar *algoritmos informáticos* para tomar las decisiones y transmitirlas.

Hoy los mercados mueven cada día el equivalente a varias veces el PIB mundial anual. Es decir, cada día se negocia en los parqués la producción real de riqueza del mundo entero equivalente a varios años de trabajo. Esta actividad tiene un potencial enorme de generación de riqueza al efectuar miles de operaciones de compra y venta de activos cada día con el mismo dinero una y otra vez (o, muchas veces, sin dinero real respaldando la transacción).

Cuando el 11 de septiembre de 2001 los terroristas de Al Qaeda estrellaron los aviones que habían previamente secuestrado contra las Torres

Gemelas del World Trade Center en pleno barrio financiero de Manhattan estaban atentando contra los símbolos del poder de lo que llamaban el «enemigo lejano», el Occidente representado, en este caso, por Estados Unidos de América. Son sobradamente conocidos los efectos producidos por los impactos, tanto a corto como a largo plazo.

Sin embargo, a pocas manzanas de allí se encuentran, entre otras, las centrales del Bank of New York y de Citigroup. Entre las dos entidades negociaban, en aquel momento, con un equivalente diario a cerca de la mitad del PIB anual estadounidense. Es evidente que la destrucción física de los bancos no habría volatilizado dicho capital (entre otras razones porque, como se ha dicho, muchas veces el dinero ni siquiera existe en la realidad y, cuando lo hace, se utiliza muchas veces cada día) que tampoco estaba físicamente en los bancos, pero la pérdida económica que se habría generado en ese día y en los siguientes habría sido tremendamente superior y apenas si se habría perdido en simbolismo en el ataque.

El hecho ilustra bastante bien la importancia de la seguridad –tanto física como lógica– de los sistemas informáticos de las entidades financieras. Es *en su capa semántica donde se encuentra muchas veces la riqueza de individuos y naciones* mucho más que en las cajas acorazadas de los bancos y reservas nacionales. El valor real de los billetes en circulación ha dejado hace tiempo –como sucedió con el oro en su día– de representar el monto total de la economía de un país.

Otros hechos, aparentemente inconexos, se han venido repitiendo últimamente con una frecuencia inusual en los mercados bursátiles. En determinados momentos de la cotización se vienen produciendo una serie de operaciones que hacen que, puntualmente, los mercados sufran fuertes recortes en sus cotizaciones que, con la misma rapidez como ocurrieron, se recuperan a continuación. Estos hechos, provocados por la fallida actuación de un algoritmo que gestiona las transacciones de compra-venta de derivados o acciones, no parecen tener detrás más que un error en alguna de la líneas de la programación pero plantean la posibilidad de que un acto así se llevase a cabo de forma intencionada causando el caos en las Bolsas –y las economías– del mundo.

El alcance del ciberespacio dentro del mundo de las transacciones financieras no parece tener límite. Donde hay una oportunidad de negocio, allí están los delincuentes cibernéticos para aprovecharla. El escasamente

conocido mercado de derechos de emisión de dióxido de carbono también fue víctima en repetidas ocasiones de robos a través de la Red (39). Estos actos están muy lejos de ser gamberradas perpetradas por adolescentes insomnes. Las cantidades sustraídas distan mucho de ser insignificantes.

Pero, mucho más que los efectos directos sobre la economía, estos ataques ponen de relieve la vulnerabilidad de nuestros mercados financieros y, por ende, del conjunto de nuestro sistema económico. Las redes en las que se llevan a cabo los negocios bursátiles, financieros o bancarios son infraestructuras críticas que necesitan ser convenientemente protegidas (40).

La responsabilidad directa de su gestión y de su defensa está, desde luego, en manos privadas en la mayor parte de los casos pero los efectos de las intrusiones en las mismas son materia, sin lugar a dudas, de Seguridad Nacional al mismo nivel que los sistemas de generación y distribución energética y los de control del tráfico aéreo. El sistema informático del *National Association of Securities Dearles Autorited Quation*, el índice bursátil tecnológico estadounidense, ya ha sido penetrado en ocasiones sin que se haya determinado el alcance de la intrusión aunque el potencial desestabilizador de la mera sospecha puede resultar altamente significativo (41).

Las implicaciones para el mundo económico y financiero no terminan, sin embargo, en los parqués ni siquiera en el ámbito de lo legal. Internet ofrece un sinfín de posibilidades para facilitar la financiación de grupos terroristas a través de transacciones de una elevada opacidad. En ellas influye también la connivencia de actores estatales permisivos –incluso cómplices– de estos grupos y organizaciones que, con su menguada vigilancia o su deliberado volver la vista hacia otro lado, facilitan el aporte de fondos a los terroristas.

Estos fondos proceden de distintas fuentes; algunas de ellas, legales. El azaque o *zakat* que constituye uno de los pilares del islam y que ha sido

---

(39) En: *http://www.elmundo.es/elmundo/2011/01/20/ciencia/1295542768.html?a=MULB2ef582227a566373f9e6d88cc4a84c5b&t=1295557745&numero=*

(40) En: *http://www.reuters.com/article/2010/03/03/us-crime-hackers-idUSTRE6214ST20100303*

(41) Barret, D.: «Hackers penetrate NASDAQ computers», *The Wall Street Journal,* 5 de febrero de 2011, en: *http://online.wsj.com/article/SB10001424052748704709304576124502351634690.html?mod=WSJEurope_hpp_LEFTTopStories*

traducido en español como «limosna» es una obligación de todo musulmán de contribuir al sostenimiento de los más desfavorecidos de la comunidad con un porcentaje fijo de su riqueza. En ocasiones se ha utilizado la cobertura legal que supone este impuesto religioso para financiar actividades terroristas aprovechando la facilidad que ofrece la Red para su distribución.

Internet también supone un apoyo para las formas tradicionales de transferir fondos entre países o individuos en muchos países asiáticos. La *hawala* es un sistema de transferencia de fondos basado en la confianza similar al que se empleaba en Europa durante la Edad Media entre los banqueros. Si bien no necesita del ciberespacio para desarrollarse como demuestra su larga historia, la inmediatez que proporciona el mismo supone un aliciente adicional para su utilización permitiendo su proliferación y aprovechamiento por grupos y organizaciones terroristas de todo el mundo; incluso en países occidentales entre ciudadanos procedentes de aquellas comunidades.

Las interacciones que se producen entre terroristas y organizaciones criminales trasnacionales han permitido a los primeros acceder a los sistemas de movimiento de capitales que emplean los segundos con fines distintos. Mientras que los delincuentes pretenden blanquear las ganancias obtenidas por medios ilícitos enmascarando su procedencia a través de múltiples transacciones por cuentas sitas en paraísos fiscales, los segundos únicamente están interesados en mantener el anonimato de emisores y receptores con la finalidad de evitar su localización y captura por parte de los Cuerpos y Fuerzas de Seguridad del Estado.

*Sobre las percepciones*

Afirman los expertos que el mayor perjuicio que sufrió Georgia como consecuencia de los ataques a su dominio en Internet durante las semanas previas y la duración misma del conflicto que le enfrentó a la Federación Rusa en agosto de 2008 y que resultó en la pérdida de control sobre las regiones de Abjasia y Osetia del Sur fue la incapacidad para hacer sentir su punto de vista en el mundo y para recibir el *feedback* de lo que sucedía en el exterior respecto de los acontecimientos que estaban teniendo lugar.

Mayor incluso que el problema que pueda generar en cuanto al establecimiento y mantenimiento del mando y control sobre las unidades y los sistemas mismos (como es el caso con los aviones no tripulados

norteamericanos) (42) es el que supone la desconexión con la opinión pública propia, enemiga o neutral. Tanto las fuerzas regulares como los grupos insurgentes y terroristas utilizan el ciberespacio para sus InfoOps y PsyOps, que incluyen, en las ocasiones más benignas, la alteración de la apariencia de una página hostil conocido como *Defacement*.

Entre estas actuaciones no podemos olvidar la función que desarrolla internet en las labores de propaganda, captación, formación y adoctrinamiento entre los grupos y organizaciones terroristas. Significativamente, el mayor crecimiento porcentual en la utilización de internet en el mundo durante la década pasada se ha producido en el mundo árabe.

En ese entorno se ha pretendido ver la influencia de las tecnologías asociadas al ciberespacio en la llamada «primavera árabe» (43). Muchos analistas atribuyen a las redes sociales (44) un papel fundamental en la difusión de mensajes incendiarios en una forma más eficiente aún a la que permitían, hace apenas unos años, los mensajes cortos de móviles SMS. Con independencia de su grado real de responsabilidad que se le pueda atribuir a estas tecnologías, lo cierto es que Egipto acordó la suspensión total del servicio proporcionado por las cinco compañías que daban cobertura al país en un intento por atajar la difusión de los mensajes.

No es necesario irse al mundo musulmán para encontrar ejemplos de la utilización del ciberespacio para estos fines; ni es su utilización, ni mucho menos, exclusiva de los mismos. En los graves incidentes que se produjeron en algunas ciudades inglesas durante el pasado verano del año 2011 se hizo un amplio uso de estas tecnologías por parte de los saqueadores y, posteriormente –como hemos visto en el artículo del profesor Calvo– por la misma Policía.

De nuevo, la implicación emocional que supone la participación (inter) activa en los foros o en las discusiones sobre las noticias proporciona a internet una mayor influencia sobre los comportamientos y las percepciones de sus usuarios respecto de los medios de comunicación «unidireccionales» como la radio o la televisión.

---

(42) Alandente, D.: «Un virus se infiltra en la red de aviones teledirigidos de Estados Unidos», diario *El País,* 7 de octubre de 2011, en: *http://internacional.elpais.com/internacional/2011/10/07/actualidad/1318022326_060512.html*

(43) En: *http://www.renesys.com/blog/2011/01/egypt-leaves-the-internet.shtml*

(44) Calvo i Cristina, A.: «London Riots: Decentralized Intelligence Collection and Analysis», *Small Wars Journal,* 9 de agosto de 2011, en: *http://smallwarsjournal.com/jrnl/art/london-riots-decentralized-intelligence-collection-and-analysis*

*Sobre las infraestructuras*

Los primeros meses del año 2010 mantuvieron a algunos analistas de Defensa ocupados con especulaciones sobre las opciones que Estados Unidos e Israel tenían disponibles para intentar retrasar o liquidar el enriquecimiento de uranio que, incumpliendo lo establecido en el Tratado de No-Proliferación, estaba –y está– llevando a cabo la República Islámica de Irán. Se barajaron docenas de opciones en las que se tuvieron en cuenta las posibles represalias que el régimen de los ayatolás podrían emplear contra los intereses del agresor: el cierre temporal del estrecho de Ormuz, la potenciación de los ataques a Israel a través de sus *proxys Hezbollah* y *Hamás*, el incremento de la desestabilización o ataques a las fuerzas aliadas en Irak y Afganistán, atentados terroristas, etc.

Las infraestructuras a neutralizar se encontraban dispersas y protegidas a pesar de la negativa rusa de vender a Irán sus Sistemas S-300 antiaéreos. Un ataque aéreo con armamento convencional podía ser insuficiente y muy costoso; una operación con armamento nuclear elevaba las apuestas más allá de lo aceptable y una operación terrestre estaba fuera de toda consideración. El problema de los sobrevuelos de Irak o Arabia Saudí comprometía diplomáticamente a aliados importantes y el establecimiento de destacamentos en esos países –de los que se llegó a hablar– no era menos perjudicial.

De un día para otro, sin embargo, cesaron todas las especulaciones. El ataque se había producido hacía meses y estaba ya dando sus resultados. No se sabe a ciencia cierta quién está detrás del ataque (45). Esa es, precisamente, una de las características más notables del uso de estos medios: no había agresor sobre el que tomar represalias; es más, ni siquiera era conveniente admitir la existencia del ataque y su éxito. La ciencia forense cibernética sigue midiendo en plazos inasumibles desde el punto de vista práctico político y diplomático los resultados de sus investigaciones.

No es este el lugar para desarrollar a fondo la naturaleza de *stuxnet* (46) ni las implicaciones que su mera existencia supone (47). Un gusano introducido por medio de una llave *Universal Serial Bus* –probablemente

(45) En: *http://www.revistatenea.es/RevistaAtenea/REVISTA/articulos/GestionNoticias_4194_ESP.asp*

(46) En: *http://www.simonroses.com/stuxnet-worm-art-of-cyber-warfare/*

(47) En: *http://www.revistatenea.es/RevistaAtenea/REVISTA/articulos/GestionNoticias_4203_ESP.asp*

sin siquiera el conocimiento del autor– fue capaz de sobrecargar los ciclos de funcionamiento de las centrifugadoras de uranio mientras los indicadores seguían manteniendo lecturas correctas. El resultado es difícil de establecer desde fuera de Irán, pero hasta las estimaciones menos optimistas cifran en meses o años de trabajo el retraso que supondrá la infección.

Parece evidente que, una vez abierta la «caja de Pandora» que contenía los gusanos que afectan al funcionamiento de los Sistemas de Control SCADA (48) la utilización de los mismos para afectar a infraestructuras o servicios críticos de cualquier país, empresa o particular tendrá que ser considerada una posibilidad en cualquier escenario; tanto como ataque singularizado y puntual como formando parte de una agresión multidisciplinar.

No podemos más que atisbar qué nos aguarda en el futuro (49). El foco, desde luego, pasará a los contenidos, a la capacidad para compartirlos y relacionarlos y a la inmediatez. En palabras del profesor Juan A. De Castro, hemos pasado de la acumulación de información a la generación de conocimiento.

Nos hemos colocado en una situación de dependencia del ciberespacio para el mantenimiento de nuestro ritmo de crecimiento. De alguna manera, nos hemos condicionado a nosotros mismos a seguir el mismo ritmo de desarrollo que sigue la tecnología en aspectos tales como sus implicaciones legales, sociológicas y psicológicas.

Hemos desarrollado un instrumento extraordinario que nos está permitiendo alcanzar fronteras que nunca habríamos siquiera soñado sin él. El potencial del ciberespacio es fabuloso e irrenunciable pero deberemos, como en el resto de los ámbitos en los que nos movemos, establecer unas reglas de comportamiento, unos marcadores que las verifiquen y un mecanismo de control que nos permita su utilización buscando el eterno compromiso entre la libertad y la seguridad.

---

(48) *Supervisory Control and Data Adquisition*, Sistemas de Control de Pocesos Industriales y de muestra de resultados a través de procesos informáticos.

(49) En: *http://www.clasesdeperiodismo.com/2011/04/25/seis-tendencias-que-marcaran-el-futuro-del-mundo-conectado/*

## CAPÍTULO QUINTO

# CAPACIDADES PARA LA DEFENSA EN EL CIBERESPACIO

# CAPACIDADES PARA LA DEFENSA EN EL CIBERESPACIO

Por Óscar Pastor Acosta

> «El hombre superior, al descansar seguro, no olvida que el peligro puede venir. Cuando la seguridad es estable, él no olvida la posibilidad de la ruina. Cuando todo está ordenado, él no olvida que el desorden puede llegar. Así, no pone en peligro su persona, preservando sus Estados y a todos sus clanes.»
>
> Confucio, (551-479 a. C)

## Introducción

No cabe duda de que el ciberespacio, como:

> «Entorno virtual donde se agrupan y relacionan usuarios, líneas de comunicación, páginas *web*, foros, servicios de Internet y otras redes» [1].

Se ha convertido en un nuevo ámbito, que junto con los tradicionales de tierra, mar, aire y espacio, es el medio dónde se desarrollan las actividades económicas, productivas y sociales de las naciones modernas:

> «El ciberespacio toca prácticamente todo y a todos. Proporciona una plataforma para la innovación y la prosperidad y los medios para mejorar el bienestar general de todo el mundo» [2].

Por ello, no es de extrañar que los gobiernos de dichas naciones manifiesten su intención de defender sus activos e intereses estratégicos en dicho ámbito. Así, en la recientemente publicada «Estrategia Internacional para el Ciberespacio», suscrita por el presidente estadounidense Barack Obama, podemos leer:

> «Todos los Estados tienen el derecho inherente a la propia defensa y reconocemos que ciertos actos hostiles llevados a cabo en el ciberespacio podrían obligar a tomar acciones en el marco de los compromisos que tenemos con nuestros aliados militares. Nos reservamos el derecho a utilizar todos los medios necesarios: diplomáticos, informativos, militares y económicos, adecuados y coherentes con el Derecho Internacional aplicable, con el fin de defender a nuestra Nación, nuestros aliados, nuestros socios y nuestros intereses» [3].

Conviene, por tanto, analizar cuáles son las capacidades para llevar a cabo una defensa eficaz del ciberespacio, que las naciones más avanzadas propugnan conseguir cada vez con mayor ahínco, para responder con prontitud a la creciente amenaza cibernética, que pone en riesgo la prosperidad de nuestra sociedad moderna. En este capítulo, nos centraremos en analizar las capacidades para la ciberdefensa, que permitan hacer frente eficazmente a las ciberamenazas, cuyo análisis ya se ha abordado en detalle en otros capítulos de la presente *Monografía*.

En primer lugar, abordaremos el análisis conceptual del término «ciberdefensa», que no siempre es entendido del mismo modo, máxime cuando nos adentramos en el ámbito internacional. Sin pretender una definición formal del término, sí intentaremos ubicar su significado en relación con otros términos, muy relacionados y con los que a veces se solapa parcialmente, como son ciberseguridad, seguridad de la información, STIC (1), etc.; para estudiar mejor las capacidades que son necesarias en su correcto desarrollo.

Posteriormente, intentaremos mencionar la mayoría de las capacidades para la ciberdefensa, que actualmente se contemplan en el cuerpo doctrinal de los países tecnológicamente más avanzados, estructurándolas según el grado de oposición (defensa, explotación y respuesta) frente a la ciberamenza que pretenden combatir. Las describiremos someramente,

(1) Seguridad de las Tecnologías de la Información y las Comunicaciones.

para comprenderlas mejor, pero evitaremos entrar en detalles tecnológicos, que serán abordados en otro capítulo de la presente publicación.

A continuación, abordaremos el análisis y la descripción de las principales formas de implantación y despliegue de estas capacidades, que se están llevando a cabo en las naciones y organismos internacionales de nuestro entorno, lo que nos permitirá detectar diferentes modelos, compromisos y alcances, no excluyentes unos de otros, a la hora de disponer de una adecuada capacidad de ciberdefensa. Para concluir, incluiremos unas breves conclusiones sobre el análisis realizado.

## Marco conceptual de la ciberdefensa

Antes de poder adentrarnos en el análisis y la definición de lo que supone una capacidad para la defensa del ciberespacio, debemos concretar qué entendemos por ciberdefensa.

Con frecuencia, en nuestro día a día, nos encontramos con un conjunto de términos (*ciberseguridad*, *seguridad de la información*, s*eguridad de las tecnologías de la información*, *ciberdefensa*, etc.), cada vez más presentes en los medios de comunicación en general (ya no sólo en las revistas técnicas especializadas), que en ocasiones se usan como si fueran sinónimos, pero en los que subyacen matices semánticos que nos hacen intuir diferencias entre los mismos.

Así por ejemplo, si leemos ciberseguridad en un medio, podríamos asociarlo mentalmente a los Cuerpos y Fuerzas de Seguridad del Estado (Policía, delitos informáticos, etc.), pero si el término analizado es ciberdefensa, seguramente lo asociaremos a Fuerzas Armadas (ejércitos, operaciones militares, etc.). Si nos preguntaran la definición de cada término, no tendríamos muy clara la diferencia, y seguramente el autor del artículo o reseña que leemos tampoco la tenga, por lo que los estará usando indistintamente. Sin embargo, hay alguna connotación que nos hace intuir sus diferencias de significado.

Esto se complica todavía más cuando dichos términos mezclan su aparición, cada vez con más frecuencia, con sus semejantes en lengua inglesa (*information assurance*, *cyber security*, *infosec*, *computer security*, *computer networks security*, *computer networks defence*, *cyber defence*, *critical information infrastructure protection*, etc.) [4], cuyo significado no siempre concuerda con la traducción directa de los términos anglosajo-

nes que los componen, por lo que tenemos una nueva fuente de ruido en la determinación de lo que quieren decir.

La Real Academia Española (RAE) nos indica que «ciberespacio» es:

> «El *ámbito artificial creado por medios informáticos*» [5], mientras que cibernauta es la *persona que navega por ciberespacios*.»

No encontraremos en el *Diccionario* de la RAE la definición de «ciberseguridad» o «ciberdefensa», pero sí podemos encontrar que el prefijo *ciber*» es un elemento compositivo que significa *cibernético* y proviene de la palabra «cibernética». Ésta, a su vez, hace referencia al:

> «Estudio de las analogías entre los Sistemas de Control y Comunicación de los seres vivos y los de las máquinas; y en particular, el de las aplicaciones de los mecanismos de regulación biológica a la tecnología.»

Etimológicamente nos llega del francés *(cybernétique)*, que a su vez lo tomó del inglés *(cybernetics)*, aunque originalmente viene del griego (κυβερνητικ), dónde hacía referencia al «arte de gobernar una nave». Así podemos concluir que «ciberdefensa» hace referencia a la «defensa cibernética». Seguramente este es un nivel suficiente de definición para un *Diccionario de la Lengua*, pero intentemos profundizar un poco más en el análisis y la compresión de lo para nosotros supone este término hoy día.

Como ya hemos apuntado, a nivel internacional se suelen utilizar los términos en inglés, aunque normalmente su significado tiene diferentes matices dependiendo del país de origen de quien los usa. Para poder disponer de un mínimo común denominador, en el correcto entendimiento del contexto de la ciberdefensa, podemos acudir al cuerpo normativo de la política de seguridad de la OTAN (2), donde se definen los términos *information assurance* (3), *infosec* y *cyber defence*.

De los tres términos antes citados, el que tiene un significado más amplio es el de *information assurance* y se encuentra definido en la política de gestión de la Información de la OTAN (4) como:

---

(2) Organización del Tratado del Atlántico Norte.

(3) *Information assurance* suele traducirse como *seguridad de la información*, aunque seguramente sería más adecuado traducirlo como *garantía* o *aseguramiento de la información* [6], para poder diferenciarlo de *information security*, que normalmente tiene un significado más restringido cuando se habla en inglés.

(4) NIMP *(NATO Information Management Policy).*

> «El conjunto de medidas para alcanzar un determinado grado de confianza en la protección de los sistemas de comunicaciones, los sistemas de información y otros sistemas electrónicos y no electrónicos, así como de la información que está almacenada, procesada o transmitida en estos sistemas con respecto a la confidencialidad, integridad, disponibilidad, no repudio y la autenticación.»

Como vemos, es una definición compleja y que abarca la protección de la información en su sentido más amplio, tanto cuando es manejada en Sistemas de las TIC (5) como fuera de ellos, es decir, cuando la información reside en las personas, en las instalaciones o en documentos u otros soportes físicos de información.

En cambio los términos *infosec* (6) y *cyber defence* hacen referencia a la protección de la información cuando es manejada por Sistemas TIC. Así, *infosec* [7] se define como:

> «La aplicación de medidas de seguridad para proteger la información procesada, almacenada o transmitida en los sistemas de comunicación, información u otros, contra la pérdida de confidencialidad, integridad o disponibilidad, ya sea accidental o intencionada, y para evitar la pérdida de la integridad o la disponibilidad de los propios sistemas.»

Por otro lado, *cyber defence* [8] sería:

> «La aplicación de las medidas de seguridad para proteger los componentes de la infraestructura TIC contra ataques cibernéticos», siendo éstos «una forma de guerra cibernética, ya sea en combinación con un ataque físico o no, que está destinada a perturbar los sistemas de información de un adversario.»

Parece, por tanto, que el concepto *infosec*, que en España denominamos STIC [9], es más amplio y abarca al de *cyber defence*, que traduciremos como ciberdefensa, pues este último sólo contempla los acciones hostiles deliberadas, mientras que el primero contempla también los daños accidentales. Además, entendemos que los ataques cibernéticos, o ciberataques, son ataques a la infraestrucutra TIC originados desde el propio ciberespacio, excluyendo por tanto los ataques físicos a las TIC.

---

(5) Tecnologías de la Información y las Comunicaciones.
(6) *Infosec* es el acrónimo de *INFormation SECurity*.

Finalmente, la política de seguridad de la OTAN no define como tal el concepto de *cyber security* o ciberseguridad, pero es muy frecuente su uso por parte de las naciones aliadas, algunas veces como sinónimo de ciberdefensa, pero más comúnmente como nuevo término para referirse a la seguridad de la información en las TIC, es decir, a *infosec* o STIC. En definitiva, parece lógico pensar que las capacidades necesarias para implementar adecuadamente la ciberdefensa son un subconjunto de las capacidades de ciberseguridad.

Pero llegados a este punto deberíamos concretar qué entendemos por «capacidad» y, acudiendo nuevamente a la RAE, obtendríamos que la afección que mejor se ajusta es la que indica que «capacidad» es:

> «La aptitud, talento, cualidad que dispone a alguien para el buen ejercicio de algo» [5].

Pero si hablamos en términos militares, «capacidad» es:

> «El conjunto de factores (sistemas de armas, infraestructura, personal y medios de apoyo logístico) asentados sobre la base de unos principios y procedimientos doctrinales que pretenden conseguir un determinado efecto militar a nivel estratégico, operacional o táctico, para cumplir las misiones asignadas» [10].

Por tanto, podríamos concluir que la capacidad de ciberdefensa sería:

> «El conjunto de sistemas, infraestructuras, personas, medios de apoyo y procedimientos doctrinales, que permitan cumplir con la misión de defender el ciberespacio.»

Una vez enmarcado conceptualmente su significado, estamos mejor preparados para, a continuación, analizar con un poco más de detalle cuáles son esas capacidades para la ciberdefensa a las que nos estamos refiriendo.

## Capacidades para la ciberdefensa

En enero del año 2011, el JEMAD (7) indica, en su «Visión de la Ciberdefensa Militar», que las Fuerzas Armadas requieren de un conjunto equilibrado de capacidades en el ciberespacio, que contribuyan a garantizar

(7) Jefe de Estado Mayor de la Defensa.

la libertad de acción en las operaciones militares y proporcionen un adecuado nivel de seguridad en el empleo de los sistemas propios.

Así, en una primera clasificación de lo que se debe contemplar se citan las capacidades de:

– *Defensa,* que incluya las medidas para la prevención, detección, reacción y recuperación frente a ataques, intrusiones, interrupciones u otras acciones hostiles deliberadas, que puedan comprometer la información y los sistemas que la manejan.
– *Explotación*, que permita la recopilación de información sobre sistemas de información de potenciales adversarios.
– *Respuesta*, que incluya las medidas y acciones a tomar ante amenazas o ataques.

Además, el JEMAD establece que la amenaza en el ciberespacio requerirá una respuesta coordinada entre diferentes actores, tanto nacionales como internacionales, en especial con las organizaciones de las que España forma parte, como la OTAN y la Unión Europea (8).

El JEMAD finaliza su «Visión de la Ciberdefensa Militar» estableciendo como líneas de acción a corto plazo la realización de un análisis de la situación de la seguridad en el ciberespacio, la identificando de los riesgos y las capacidades necesarias para hacerles frente, así como la elaboración del «Concepto de Ciberdefensa Militar», para definir un plan de acción para la obtención armonizada de las Capacidades de Ciberdefensa.

Como vemos, la Visión del JEMAD está alineada con la doctrina tradicional de nuestros aliados, como es la del Departamento de Defensa de Estados Unidos (9), cuyo Estado Mayor Conjunto indica, dentro de la Doctrina de las Operaciones de Información [11], que las capacidades de las *Computer Network Operations* (10) se componen de:

– *Computer Network Defense* (11): que incluye las medidas adoptadas a través del uso de redes de ordenadores para proteger, controlar, analizar, detectar y responder a la actividad no autorizada en los sistemas de información y comunicaciones. Las acciones CND no sólo buscan

(8) Unión Europea.
(9) *United States Department of Defense.*
(10) CON *(Computer Network Operations),* lo que se podría traducir como operaciones de la red de ordenadores.
(11) CND *(Computer Network Defense),* lo que se podría traducir como defensa de la red de ordenadores.

proteger los sistemas de un adversario externo, sino también de su explotación desde dentro de la propia organización.
– *Computer Network Exploitation* (12): que incluye las capacidades de recolección de inteligencia llevadas a cabo a través del uso de redes de computadoras para recopilar datos de los sistemas de información y comunicaciones del posible adversario.
– *Computer Network Attack* (13): que se compone de las medidas adoptadas a través del uso de las redes informáticas para interrumpir, negar, degradar o destruir la información manejada por los sistemas de información y comunicaciones (del posible adversario), o los propios sistemas de información y comunicaciones.

Asimismo, el JEMAD detalla posteriormente en su «Concepto de Ciberdefensa Militar» lo ya adelantado en su Visión sobre las capacidades de la ciberdefensa (de *defensa*, de *explotación* y de *respuesta*) que deberán ser desarrolladas considerando los siguientes aspectos o dimensiones:
– *Material*: para garantizar la concordancia de los procesos de adquisición de material con la rapidez de los cambios tecnológicos y la adecuación a la normativa de protección de la información, prestando especial atención a las garantías de seguridad de toda la cadena de suministros (del *hardware* y del *software*).
– *Infraestructura*: para que las instalaciones y componentes de los sistemas de información y comunicaciones cuenten con las adecuadas medidas de seguridad física y de emisiones electromagnéticas no deseadas (TEMPEST) (14).
– *Recursos humanos*: para disponer de personal formado técnicamente y con continuidad adecuada para garantizar la eficacia y la eficiencia de la ciberdefensa, donde el personal militar podrá ser complementado con personal civil cualificado, que forme parte de equipos multidisciplinares en donde se potencien las sinergias.

---

(12) CNE *(Computer Network Exploitation),* lo que se podría traducir como explotación o aprovechamiento de la red de ordenadores.
(13) CNA *(Computer Network Attack),* lo que se podría traducir como ataque a la red de ordenadores.
(14) *Transient Electromagnetic Pulse Surveillance Technology* [9] hace referencia a las investigaciones y estudios de emanaciones comprometedoras (emisiones electromagnéticas no intencionadas, producidas por equipos eléctricos y electrónicos que, detectadas y analizadas, puedan llevar a la obtención de información) y a las medidas aplicadas a la protección contra dichas emanaciones.

– *Adiestramiento*: para que el personal esté adecuadamente concienciado e instruido en la seguridad de la información y en la ciberdefensa. Para ello, los ejercicios de ciberdefensa son fundamentales, debiéndose potenciar su realización a nivel nacional y fomentar la participación a nivel internacional. Además, se deberán incluir eventos e incidencias de ciberdefensa en todo tipo de ejercicios militares.
– *Doctrina*: puesto que la naturaleza de la ciberdefensa requiere de una doctrina conjunta y alineada con las de la OTAN y Unión Europea, para proporcionar a los mandos las bases tácticas, técnicas y de procedimiento, que les permita ejercer su misión de forma eficaz y eficiente.
– *Organización*: para permitir la implementación de una seguridad dinámica, en contra de la actual estructura de los Sistemas TIC orientada hacia la protección estática, y el ejercicio de las actividades de explotación y respuesta. Además, la necesidad de una dirección, planificación y coordinación centralizada requiere adaptar la organización para alcanzar la adecuada eficacia de las capacidades necesarias.
– *Colaboración público-privada* (15): para fomentar acuerdos, nacionales e internacionales [12], entre los sectores público y privado, que permitan el intercambio de información y una adecuada coordinación de las acciones.

A nivel internacional, los jefes de Estado y de Gobierno de la OTAN aprueban, en la cumbre de Lisboa de noviembre de 2010 [13], el *concepto Estratégico para la Defensa y Seguridad de los miembros de la Alianza*, en el que se comprometen a:

> «Desarrollar aún más la capacidad de la Alianza para prevenir, detectar, defenderse y recuperase de los ataques cibernéticos, incluyendo la coordinación y mejora de las capacidades de ciberdefensa de las respectivas naciones, mediante el uso del proceso de planificación de la OTAN, llevando a todos los organismos de la OTAN a una protección cibernética centralizada y mejorando la integración de la concienciación, alerta y respuesta cibernéticas de la OTAN con los países miembros.»

(15) En inglés PPP, P3 o P3 *(Public–Private Partnership)*. Un ejemplo de este tipo de colaboración es el EP3R *(European Public-Private Partnership for Resilience)*, que tiene como objetivo proporcionar un marco de gobierno flexible a nivel europeo, para involucrar a actores relevantes, públicos y privados, en las políticas públicas y toma de decisiones estratégicas para fortalecer la seguridad y la resiliencia en el contexto de la CIIP *(Critical Information Infrastructure Protection),* en: *http://ec.europa.eu/information_society/policy/nis/strategy/activities/ciip/ep3r/index_en.htm*

Además, en esa misma cumbre de Lisboa, se realiza una declaración de los jefes de Estado y de Gobierno en la que se afirma que:

> «Las amenazas cibernéticas se están incrementando rápidamente y evolucionando en su sofisticación. Por ello, a fin de asegurar el acceso libre y permanente de la OTAN al ciberespacio y la integridad de sus sistemas críticos, haremos todo lo posible para acelerar al año 2012 la Capacidad Plena Operativa (FOC) (16) de la capacidad de respuesta ante Incidentes Informáticos de la OTAN y la reunión de todos los organismos de la OTAN bajo una ciberprotección centralizada.»

En esa misma declaración se confirma el compromiso para:

> «Utilizar los procesos de planificación de la defensa de la OTAN con el fin de promover el desarrollo las capacidades de ciberdefensa de los aliados, así como para ayudar bajo demanda a cada país aliado y optimizar el intercambio de información, la colaboración y la interoperabilidad. Para hacer frente a los riesgos de seguridad que emanan desde el ciberespacio, vamos a tener en cuenta la dimensión cibernética de las conflictos modernos en la doctrina de la OTAN y vamos mejorar sus capacidades para detectar, evaluar, prevenir, defenderse y recuperarse en caso de un ataque cibernético contra los sistemas de importancia crítica para la Alianza, trabajando para ello en estrecha colaboración con otros actores, tales como la Organización de Naciones Unidas (ONU) y la Unión Europea.»

En esa misma cumbre, se encomiendan al Consejo Atlántico desarrollar una profunda revisión de la política de ciberdefensa de la OTAN y preparar un Plan de Acción para su aplicación, teniendo en cuenta las estructuras internacionales existentes, y tenerlo disponible en junio de 2011.

En este sentido, los ministros de Defensa de la OTAN aprueban en marzo de 2011 el nuevo «Concepto de Ciberdefensa de la Alianza» [14], en el que se define la protección de las redes de la OTAN como una responsabilidad fundamental de los aliados, destacando la importancia de cooperar con sus socios y otros organismos internacionales en ciberdefensa, así como la necesidad de integrar las ciberamenazas dentro del proceso de planeamiento de la Alianza.

---

(16) *Full Operational Capability.*

En este nuevo Concepto de Ciberdefensa, la Alianza realiza el siguiente tipo de actividades:

– Coordinación y asesoramiento en ciberdefensa.
– Asistencia a las naciones.
– Investigación y formación.
– Cooperación con socios de la Alianza, como la Unión Europea y la OSCE (17).

Tal y como había sido establecido, la Alianza dispone en junio de 2011 de una nueva política de ciberdefensa, revisada y alineada con el Concepto antes citado, así como un Plan de Acción que permita la rápida implementación de las capacidades de ciberdefensa que los países aliados precisan para hacer frente a este grupo de amenazas emergentes.

En este contexto, la Agencia C3 de la OTAN (18) lanza su Iniciativa Multinacional para el Desarrollo de la Capacidad de Ciberdefensa (MN CD2) (19), como respuesta al reto de desarrollar las nuevas capacidades de ciberdefensa en tiempos de importantes restricciones financieras, lo que exige una aproximación inteligente y eficiente para conseguir rápidamente las capacidades necesarias tanto en la OTAN como en cada una de las naciones aliadas.

La NC3A entiende que la ciberdefensa, como aplicación de medidas de seguridad para la protección y reacción frente a ataques cibernéticos contra las infraestructuras TIC, requiere una capacidad de preparación, prevención, detección, respuesta, recuperación y extracción de lecciones aprendidas de los ataques que podrían afectar a la confidencialidad, integridad y disponibilidad de la información, así como a los recursos y servicios de los Sistemas TIC que la procesan.

---

(17) *Organization for Security and Co-operation in Europe.*

(18) *NATO Consultation, Command and Control Agency.* La NC3A es una Agencia de la OTAN que comparte la personalidad jurídica de la Alianza. Sus estatutos fueron aprobados por el Consejo del Atlántico Norte y opera bajo un régimen de financiación al 100% de sus clientes, que son habitualmente organismos de la propia OTAN. La NC3A es parte de la estructura C3 de la OTAN, junto con el NATO C3 Board y la NCSA *(NATO CIS Service Agency).* La misión de la NC3A es facilitar la cosecucución de los objetivos de la Alianza a través de la prestación imparcial de las capacidades de Consulta, Mando y Control, Comunicaciones, Inteligencia, Vigilancia y Reconocimiento (C4ISR).

(19) *Multinational Cyber Defence Capability Development .*

Dentro de la iniciativa MN CD2, y para apoyar una obtención coordinada e interoperable de las capacidades de ciberdefensa entre los países aliados, el Mando Aliado de Transformación (ACT) (20) encarga a la NC3A realizar una desglose, clasificación o taxonomía de las capacidades de ciberdefensa [15], con el objeto de dar una idea clara de sus aspectos operativos y dividir el esfuerzo de desarrollo u obtención en piezas manejables que puedan ser tratadas de forma independiente. Esta clasificación desglosa la ciberdefensa en seis grandes áreas de capacidad, cada una de las cuales, a su vez, se divide sucesivamente en otras capacidades subyacentes, y así sucesivamente hasta llegar a un nivel de detalle suficiente.

Dicha clasificación puede servir como guión de un análisis más detallado de las capacidades necesarias para la ciberdefensa. Veamos cada una de ellas:

1. *Detección de actividad maliciosa*: capacidad que se implementa a través de la recopilación de información de una amplia gama de sensores, base para el análisis que separe los flujos de tráfico entre entidades maliciosos, que permita una evaluación de la situación. Ésta se logra relacionando entidades maliciosas entre sí y con las entidades de origen y destino, además de tener en cuenta el histórico de actividades entre ellas. Por tanto, esta capacidad se compone a su vez de:
   - *Recopilación de datos de sensores*: capacidad para recoger en un repositorio global los datos sobre todas las actividades en curso, a través de la utilización de sensores y la alineación de la sintaxis de los datos. Los sensores incluyen los sistemas de detección de intrusos, escáneres de vulnerabilidad e informes de registros de eventos de dispositivos como cortafuegos, servidores y *proxies*, entre otros. Además de la recolección de datos de los sensores, estos datos tienen que ser preprocesados para unificar la sintaxis y los puntos de referencia.
   - *Evaluación de entidades*: capacidad para fusionar las observaciones de los sensores en entidades asociadas, con propiedades comunes, clasificando éstas según sean dañinas o no. En el ciberespacio, las entidades pueden ser cualquier conjunto de datos relacionados de alguna manera, tales como por ejemplo los datos asociados a una descarga de una página *web*, una llamada

(20) *Allied Commander Transformation.*

de voz sobre Protocolo de Internet (IP) o un ataque denegación de servicios distribuidos. A su vez se compone de:

- *Normalización de los datos de sensores*: capacidad para unificar el significado de los datos recopilados de diferentes sensores, de forma que expresiones distintas con un mismo significado se estructuren en un mismo formato, obteniendo puntos de referencia comunes que faciliten la correlación entre ellos.
- *Correlación de datos de sensores:* capacidad de reconocer trazas de datos provenientes de diferentes sensores, pero que pertenecen a una misma entidad, como puede ser un servidor o un flujo de datos concreto.
- *Asignación de atributos a las entidades:* capacidad para asignar atributos (como ancho de banda consumido o tipo de páginas *web* descargadas) a cada entidad, basados en los datos recopilados de los sensores, que permitan caracterizar a ésta.
- *Caracterización de entidades:* capacidad de determinar el tipo de entidad, basándose en sus atributos y el conocimiento previo de lo que ellos significan. Así por ejemplo, una forma muy simple de caracterización sería establecer que el tráfico al puerto 80 se corresponde con un tipo de entidad que denominaremos «descarga de página *web*».
- *Evaluación de la situación*: capacidad para reconocer actividades, entendidas como relaciones entre entidades, sus actores, así como su significado y su contexto. A su vez se compone de:
  - *Correlación de entidades:* capacidad de identificar relaciones entre entidades, que permitan formar actividades. Estas relaciones pueden ser patrones de tiempo, que identifiquen acciones secuenciales o en paralelo.
  - *Localizar la fuente t*écnica de *ataque:* capacidad para identificar el servidor desde el que el ataque se ha originado o es controlado, que normalmente va más allá de identificar la IP de origen, pues habitualmente habrá sufrido un ataque de *spoofing* (21) o será un nodo de una ruta de múltiples saltos también usada por el atacante.

(21) *Spoofing,* en el contexto de seguridad TIC, suele referirse al uso de técnicas de suplantación de identidad, normalmente con intención maliciosa. Según el elemento identificador que se suplante hablaremos de IP *spoofing,* ARP *spoofing,* DNS *spoofing, web spoofing o email spoofing.*

– *Interpretar la actividad:* capacidad de interpretar cada actividad y su origen técnico para comprender la extensión y los detalles de la misma.
– *Interpretar el contexto:* capacidad para identificar relaciones entre actividades, tanto en sistemas de información propios como ajenos, por medio del intercambio de información. Las actividades ya interpretadas son puestas en contexto mediante información histórica de patrones de actividad, que pueden ser contrastados con actividades similares en Sistemas TIC ajenos, para dar una visión global de si nos enfrentamos a un ataque genérico o específico.
– *Visualización para el análisis*: capacidad de presentar visualmente actividades, entidades y sensores para facilitar el trabajo de los analistas humanos, que deben tratar con cantidades ingentes de datos, y son los encargados de detectar acciones maliciosas.

2. *Prevención, mitigación y terminación de ataques*: esta capacidad se compone a su vez de:
   – *Reconfiguración de la topología de los sistemas*: capacidad para modificar la estructura de los sistemas de información y comunicaciones, incluyendo sus servicios, su *software* y su *hardware*, su interconexión, así como la configuración de cualquiera de sus módulos o componentes. A su vez se compone de:
     – *Reubicación de los servicios de información:* capacidad para mover servicios y su información asociada a infraestructura TIC alternativa.
     – *Compartimentación de sistemas:* capacidad de separar y aislar ciertas partes de un Sistema TIC. Lo que es crucial cuando un ataque es inminente o está en curso para limitar el impacto y preservar la integridad y la continuidad de las operaciones del resto del sistema.
     – *Cierre de componentes y servicios:* capacidad para cerrar ordenadamente componentes o servicios de un sistema, como servidores o interfaces de red, lo que puede ser una medida eficaz para mitigar un ataque, pero que puede impactar negativamente en la operación, por lo que siempre deberá ser evaluada previamente su aplicación.
     – *Revocación de credenciales:* capacidad de retirar los permisos de acceso a entidades que habían sido previamente acreditadas, pero cuyas credenciales han sido también comprometidas o mal utilizadas.

– *Actualización del* hardware*, del* software *y de su configuración:* capacidad para modificar el *hardware*, el *software* y su configuración para prevenir y mitigar posibles ataques. Así, por ejemplo, las vulnerabilidades del *software* exigen actualizaciones periódicas de sus versiones, para prevenir su explotación por parte de posibles atacantes.
– *Control del flujo de tráfico*: capacidad para terminar o limitar a un cierto ancho de banda o con un cierto retraso el flujo de datos, así como para cambiar la ruta de comunicación o interferir en el flujo de datos, modificándolo con el fin de detener o mitigar un ataque.
– *Decepción:* capacidad de crear de forma estática y dinámica áreas del Sistema TIC en las que el ataque pueda desarrollarse sin impacto en la operativa normal del sistema.
– *Defensa activa:* capacidad de utilizar técnicas de ataque con el único propósito de parar o mitigar un ataque en curso. Pueden tener como objetivo retomar el control sobre los recursos propios o sofocar ataques neutralizando la fuente de los mismos.
– *Coordinación de la respuesta externa:* capacidad para coordinar la aplicación de medidas con terceras partes, como son los proveedores nacionales o internacionales de servicios TIC, para parar o mitigar los ataques.

3. *Análisis dinámico de riesgos, ataques y daños*: esta capacidad se compone a su vez de:
   – *Análisis dinámico de riesgos*: capacidad de evaluar el riesgo de manera continua y automática para poder proyectar la situación actual en el futuro y predecir el posible impacto. Este tipo de análisis de riesgo se diferencia del tradicional, que normalmente se efectúa en la fase de diseño y en otras fases del ciclo de vida del sistema, pero que carece de su carácter automático y continuo. Hace uso de uno o varios métodos de cálculo, que toman como entrada ciertas variables de entorno del Sistema de Información y Comunicaciones, cuyos valores hay que poder estimar, como son:
     – *Valoración de activos*: entendido como el valor de los servicios que proporciona el Sistema TIC para la organización a la que sirve. Conocer todos los activos y su importancia relativa es fundamental a la hora de poder evaluar el impacto de un ataque y de priorizar las acciones encaminadas a reducir el riesgo que soporta el sistema.

- *Evaluación de la amenaza*: incluyendo tanto información general de amenazas, que se irá actualizando con productos de inteligencia genéricos, como información obtenida mediante los propios sensores de actividad maliciosa.
- *Análisis de vulnerabilidades*: que incluirá todas las vulnerabilidades detectadas en el sistema, descubiertas mediante el uso de sensores de vulnerabilidades tanto activos como pasivos.
- *Estructura del sistema*: entendida como una imagen actualizada y completa del Sistema TIC, incluyendo sus dispositivos, conexiones, *software*, la configuración de cada módulo, así como la información procesada y almacenada en el mismo.
- *Valoración de ataques*: capacidad de permitir que un ataque progrese, para analizarlo y monitorizarlo con el fin de comprender mejor la intención y capacidad del atacante. A su vez se compone de:
  - *Análisis de los ataques en curso:* capacidad para analizar las características de un ataque, y su originador, mientras éste se está desarrollando, con el fin de hacer un mejor análisis de la amenaza que supone.
  - *Coordinación de la monitorización externa:* capacidad de coordinar medidas con terceras partes, como son colaboradores o proveedores de servicios, para monitorizar y analizar los ataques en curso.
- *Evaluación de daños*: capacidad para valorar el daño causado por un ataque, una vez ha sido confirmado y detenido. El daño puede producirse sobre el sistema propiamente o sobre la información que almacena y procesa. A su vez se compone de:
  - *Análisis de malware* (22): capacidad de entender el funcionamiento del código malicioso.
  - *Identificación de los sistemas afectados:* capacidad para identificar si un sistema está funcionando como debería o si ha sido afectado por un ataque.
  - *Verificación de la integridad de la información:* capacidad para chequear que la información almacenada o procesada en el sistema no ha sido modificada de forma maliciosa.

(22) *Malware* proviene de la fusión de las palabras inglesas *malicious software* y hace referencia cualquier tipo de código o programa cuya intención sea acceder sin autorización o causar daño en un sistema ajeno.

  - *Identificación de información comprometida:* capacidad para identificar cualquier información cuya confidencialidad haya sido comprometida, por ejemplo, mediante su descarga sin autorización por parte de un atacante.
  - *Medida de la disponibilidad del servicio:* capacidad para detectar si los servicios proporcionados han sido afectados por un ataque. Para ello, debe medirse de forma continua la disponibilidad de los servicios, identificando aquellos servicios que se prestan de forma degradada o que se han dejado también de prestar por completo.
- *Concienciación sobre la situación*: capacidad para concienciar de forma visual y rápida a los usuarios y operadores del sistema sobre la situación del mismo, incluyendo información sobre las actividades y componentes del sistema, sus objetivos y prioridades, así como sus amenazas y vulnerabilidades.

4. *Recuperación de ciberataques*: capacidad para recuperarse de un ataque mediante la restauración del sistema y la información a su estado original y a sus propiedades de seguridad. Esta capacidad se compone a su vez de:
   - *Restauración de la integridad del sistema:* capacidad de restaurar el sistema a un estado en el que tanto la plataforma como los servicios que corren sobre ella garantizan su funcionamiento bajo los requisitos de seguridad. Esto puede requerir una reinstalación completa de los mismos, o desde una copia de seguridad cuya integridad haya sido verificada.
   - *Restauración de la integridad de la información:* capacidad para restaurar la información almacenada o procesada por el sistema, de forma que se pueda confiar en que dicha información es la correcta y carece de modificaciones no autorizadas. Esto puede requerir la recuperación de la información desde una copia de seguridad cuya integridad haya sido verificada, o la eliminación de cualquier pieza de información no fiable.
   - *Restauración de la disponibilidad del servicio:* capacidad de hacer los servicios nuevamente disponibles tras un ataque. Requerirá la restauración tanto de la integridad de la información como del propio sistema, así como la reconfiguración del sistema para prevenir nuevos ataques.
   - *Registro de la información comprometida:* capacidad de mantener un registro de toda la información cuya confidencialidad haya sido

comprometida para poder informar convenientemente a todas a las partes interesadas.

5. *Toma de decisiones a tiempo*: capacidad de decidir sobre las acciones a ser implementadas de manera oportuna. Dado que en el ciberespacio los eventos pueden desarrollarse de forma vertiginosa, esto implicará que en muchas ocasiones la respuesta sea automática, para garantizar que es suficientemente rápida. En cualquier caso, será preciso la toma de decisiones por humanos, para coordinar los resultados de diferentes respuestas y elegir la mejor vía a seguir en el proceso de defensa. Esta capacidad se compone a su vez de:
   – *Identificación de opciones:* capacidad para identificar las diversas alternativas de respuesta a un ataque, evaluando las opciones y priorizándolas de acuerdo al efecto y al impacto deseados, identificando también a las personas responsables de tomar las decisiones oportunas para llevarlas a cabo.
   – *Coordinación de la decisión:* capacidad de coordinar una decisión con las diferentes partes implicadas, que pueden ser diferentes organizaciones en un entorno de redes y sistemas federados, de forma que pueda ser implementada de manera adecuada.
   – *Diseminación de la decisión:* capacidad para comunicar una decisión a todas las partes implicadas, incluyendo tanto a organizaciones externas, que colaboran con la nuestra, como a nuestros propios usuarios y operadores de los Sistemas TIC.

6. *Gestión de la información de ciberdefensa*: capacidad de recopilar y compartir información de forma que permita un intercambio rápido y fiable de la misma entre diferentes partes. Entre la información de referencia sobre ciberdefensa a compartir se encontrará una estimación de la intención del adversario y de su capacidad, así como información acerca de las vulnerabilidades conocidas, *software* malicioso y las evaluaciones y certificaciones de los diferentes productos de *software* y *hardware*. Esta capacidad se compone a su vez de:
   – *Recopilación y compartición de la información de ciberdefensa:* capacidad para recopilar información de diferentes fuentes y compartirla con diversos colaboradores, incluyendo la información propia recogida de los incidentes en curso. Esto permitirá una mejor evaluación del riesgo y la implementación de medidas preventivas. El intercambio de información debe basarse en un modelo de confianza entre las partes y debe diseñarse de forma que permita una

rápida distribución de la información, en coherencia con los requisitos de toma de decisión a tiempo.
- *Garantía de calidad de la información de ciberdefensa:* capacidad de gestionar la confiabilidad de la información de ciberdefensa recibida, dado que ésta puede provenir de diferentes fuentes, incluyendo desde fuentes abiertas en Internet a informes de la comunidad de inteligencia.
- *Recopilación y explotación del histórico de datos:* capacidad para registrar información en almacenes de datos de corta y larga duración, para apoyar en futuras acciones. El histórico de datos incluirá tráfico de red, información de sensores, etc. Esta información puede ser utilizada, por ejemplo, con nuevos algoritmos de detección, de forma que, aplicados sobre datos históricos, se pruebe su validez, conociendo lo que ocurrió previamente.

## Implementación de la ciberdefensa

Una vez enumeradas y definidas cada una de las capacidades necesarias para una adecuada defensa del ciberespacio, y para que los árboles no nos impidan ver el bosque, abordaremos a continuación la descripción de las principales formas de implantación, que están llevando a cabo en las naciones y organismos internacionales de nuestro entorno, para el despliegue operativo de dichas capacidades.

### *Capacidad de respuesta ante incidentes informáticos*

Nuevamente debemos comenzar este apartado con una aclaración terminológica, pues son muchas las siglas (formadas a partir de los términos en inglés), que se usan como sinónimos o con un significado muy similar, para referirse a la capacidad de respuesta ante incidentes informáticos.

Seguramente la más ampliamente usada a nivel internacional es CERT (23), o Equipo de Respuesta a Emergencias Informáticas, ya que fue la primera en aparecer a finales de los años ochenta, tras el ataque del gusano

(23) *Computer Emergency Response Team.* Aunque éste es el significado original del término CERT, y así lo mantiene la Universidad Carnegie Mellon, conviene indicar, para evitar confusiones, que con posterioridad el Departamento de Seguridad Nacional de Estados Unidos, en su US-CERT, usa esta misma sigla pero modificando el sentido de la letra *R,* que ya no corresponderá a *Response* sino a *Readiness.* Seguramente esta denominación es más acorde con la realidad del servicio que se presta.

*morris* [16], que se propagó rápidamente por todo el mundo, infectando una gran cantidad de sistemas. Unos días después de su aparición, la Agencia DARPA (24), perteneciente al Departamento de Defensa americano, creó el primer Centro de Coordinación de Equipo de Respuesta a Emergencias Informáticas (CERT-CC) (25), ubicado en la Universidad Carnegie Mellon, en Pittsburgh (Pensilvania).

Poco después, el Departamento de Energía de Estados Unidos formó la CIAC (26), o Capacidad de Asesoramiento ante Incidentes Informáticos, con similar objetivo dentro de su ámbito.

Al cabo de un tiempo, el modelo es adoptado también en Europa, pero en este caso usando la denominación CSIRT (27) o Equipo de Respuesta a Incidentes de Seguridad Informática, puesto que el término CERT había sido protegido como marca registrada por la Universidad Carnegie Mellon (28).

De esta forma van apareciendo otras muchas siglas para referirse a este mismo tipo de capacidad, como IRT (29), Equipo de Respuesta a Incidentes, o CIRT (30), Equipo de Respuesta a Incidentes Informáticos, o SERT (31), Equipo de Respuesta a Emergencias de Seguridad, pero todas ellas son mucho menos frecuentes que las mencionadas anteriormente.

Finalmente, la OTAN también se compromete a desplegar una capacidad similar a un CERT, a raíz de las decisiones tomadas en las cumbres de Praga (2002) y Estambul (2004), pero en este caso la denomina CIRC (32) de la OTAN o NCIRC (33), que podríamos traducir como capacidad de respuesta ante incidentes informáticos de la Alianza.

---

(24) *Defense Advanced Research Projects Agency*

(25) *Computer Emergency Response Team-Coordination Center,* en: *http://www.cert.org./*

(26) *Computer Incident Advisory Capability.*

(27) *Computer Security Incident Response Team.*

(28) En todo caso, la Universidad Carnegie Mellon permite el uso de la marca CERT a todos los CSIRT que compartan su compromiso con la mejora de la seguridad de las redes conectadas a Internet, debiendo solicitar para ello la correspondiente autorización para utilizar marca CERT junto al nombre de cada CSIRT.

(29) *Incident Response Team.*

(30) *Computer Incident Response Team.*

(31) *Security Emergency Response Team.*

(32) *Computer Incident Response Capability*.

(33) *NATO Computer Incident Response Capability.*

Aunque podemos concluir que los términos CERT, CSIRT o CIRC (34) se utilizan para referirse al mismo tipo de capacidades cibernéticas, no podemos pensar que éstas son siempre las mismas. En función de la comunidad a la que deban dar servicio, o la misión a la que van a responder, habrá diferentes tipos de CIRC [17], entre los que podemos citar: académicas, comerciales, para la Protección de las Infraestructuras Críticas de la Información (CIIP) (35), del sector público, de defensa, nacionales, para la PYME (36), etc.

Según su tipo, cada CIRC estructurará su funcionamiento de diversas formas, que en general seguirán uno de los siguientes modelos organizativos [18]:

– *Independiente*: es una CIRC que actúa como una organización independiente, con sus propios responsables y recursos. Éste es el modelo que mejor se ajusta a los CERT comerciales, que se constituyen como empresas independientes para prestar sus servicios.
– *Integrado:* en este modelo, la CIRC está incrustado en la organización a la que presta servicio o que lo patrocina, funcionando como un departamento, más o menos autónomo, de la misma. Suele estar dirigido por un responsable de las actividades, que además de trabajadores propios del CIRC, es capaz de reclutar al personal técnico preciso para la resolución de un incidente, acudiendo si fuera necesario a otras áreas de la organización para solicitar asistencia especializada. Éste es el modelo de CIRC más habitual.
– *Campus:* es el modelo que surge en las universidades y entornos de investigación, de ahí su nombre, en los que existe una sede central, que se denomina CERT principal o madre, y muchas sedes distribuidas dependientes del principal, o CERT hijos, que son más pequeños y cuentan con una gran autonomía de acción. Éste sería el modelo que

(34) A partir de este punto, y en el resto del capítulo, se intentará primar el uso de la sigla CIRC para referirnos a este tipo de capacidades, pues parece ser la que mejor se ajusta al concepto estudiado, al hablar explícitamente de «capacidad» en lugar de «equipo» y, además, es el término usado en la OTAN, estableciendo así un léxico común para los entornos de Defensa. En cualquier caso, conviene tener presente que nos estaremos refiriendo básicamente al mismo concepto que CERT o CSIRT, siglas que también se usarán en el capítulo cuando el contexto así lo aconseje para su mejor comprensión.
(35) *Critical Information Infrastructure Protection.*
(36) Pequeña y Mediana Empresa.

mejor se ajusta a empresas y organizaciones multinacionales, con un elevado grado de descentralización.
– *Voluntario:* en este modelo la capacidad CIRC se constituye *ad hoc*, formada por un grupo de especialistas que se unen de forma voluntaria para apoyarse entre sí y prestar servicio a una comunidad. Las redes WARP (37) son un ejemplo de este modelo.

Según el tipo y modelo organizativo de cada CIRC, encontraremos un número y perfil diferente de personas trabajando en él, pero en general siempre se dispondrá de personal con una alta cualificación técnica y una serie de rasgos de su personalidad, que lo hagan apto para trabajar en este tipo de entornos tan exigentes. En general, el personal de una CIRC deberá ser [19]: dedicado, innovador, detallista, flexible, paciente, analítico, buen comunicador, tolerante al estrés, orientado a la resolución de problemas y, sobre todo, íntegro.

Aunque, como se ha expuesto, la composición de cada CIRC variará mucho de uno a otro, en general nos encontraremos los siguientes roles [20]:
– Gerente o líder de equipo.
– Subgerentes, supervisores, o líderes de grupo.
– Personal de ayuda en una situación de crisis.
– Personal para la gestión de incidentes.
– Personal para el análisis de vulnerabilidades.
– Personal de análisis de dispositivos.
– Especialistas de diferentes plataformas.
– Formadores.
– Investigadores.

Aunque con menos frecuencia, también se pueden encontrar este otro tipo de roles en una CIRC:
– Personal de soporte.
– Redactores técnicos.
– Administradores de red o de sistemas de la infraestructura propia.
– Programadores o desarrolladores de herramientas específicas.
– Desarrolladores y mantenedores *web*.
– Responsable de relaciones con los medios.

(37) *Warning, Advice and Reporting Points.* Se trata de un tipo de comunidades de intercambio de información de seguridad, ampliamente extendidas en el Reino Unido, que se han desarrollado para proporcionar un método eficaz para apoyar la defensa frente ataques a pequeñas organizaciones.

– Personal legal.
– Personal de los Cuerpos y Fuerzas de Seguridad del Estado.
– Auditores o personal de aseguramiento de la calidad.
– Personal de comercialización.

Las capacidades CIRC se implementan para prestar una serie de servicios, que varían de unas a otras, pero que podemos estructurar en los siguientes tipos [21]:

1. *Servicios reactivos*: servicios que son activados por un evento o una solicitud, como un informe de un servidor comprometido, código malicioso ampliamente difundido, vulnerabilidades de *software* o algo que fue identificado por un sistema de detección de intrusos o un registro de eventos. Los servicios reactivos constituyen el componente central del trabajo de una CIRC. Este tipo de servicios incluiría:
   – Alertas y advertencias.
   – Tratamiento de incidentes. Que incluirá:
      – Análisis de incidentes.
      – Apoyo a la respuesta a incidentes.
      – Coordinación de la respuesta a incidentes.
      – Respuesta a incidentes *in situ*.
   – Tratamiento de vulnerabilidades.Que incluirá:
      – Análisis de vulnerabilidades.
      – Respuesta a vulnerabilidades.
      – Coordinación de la respuesta a vulnerabilidades.
   – Tratamiento de dispositivos o artefactos.Que incluirá:
      – Análisis de dispositivos o artefactos.
      – Respuesta a dispositivos o artefactos.
      – Coordinación de la respuesta a dispositivos o artefactos.
2. *Servicios proactivos*: estos servicios proporcionan asistencia e información para ayudar a preparar, proteger y asegurar los sistemas protegidos en previsión de ataques, problemas o acontecimientos. La prestación de estos servicios va directamente dirigida a reducir el número de incidentes futuros. Este tipo de servicios incluiría:
   – Comunicaciones y anuncios.
   – Observatorio de tecnología.
   – Evaluaciones o auditorias de seguridad.
   – Configuración y mantenimiento de herramientas, aplicaciones e infraestructuras de seguridad.

- Desarrollo de herramientas de seguridad.
- Servicios de detección de intrusiones.
- Difusión de Información relacionada con la seguridad.

3. *Servicios de gestión de la calidad de la seguridad*: son servicios orientados a potenciar el resto de servicios existentes y suelen ser independientes de la gestión de incidentes. Tradicionalmente son prestados por otras áreas de la organización, diferentes de la CIRC, como el Departamento TIC, el de auditoría o el de formación. La implicación del personal CIRC en estos servicios ayudará a mejorar la seguridad general de la organización, identificando sus riesgos, amenazas y debilidades. En general, se trata de servicios proactivos y contribuyen indirectamente a reducir el número de incidentes, pero se diferencia del grupo anterior porque sus objetivos son a más largo plazo. Este tipo de servicios incluiría:
   - Análisis de riesgos.
   - Continuidad del negocio y recuperación ante desastres.
   - Consultoría de seguridad.
   - Sensibilización-concienciación.
   - Educación-formación.
   - Evaluación o certificación de productos.

A la vista del catálogo de servicios que compone una CIRC, y recordando que las capacidades de ciberdefensa podían clasificarse en tres tipos o grupos: de *defensa*, de *explotación* y de *respuesta*; podemos concluir que mediante una CIRC se implementan fundamentalmente las Capacidades de Defensa, dentro de la estrategia de ciberdefensa de una nación u organismo internacional, buscando garantizar la prevención, detección, reacción y recuperación frente a ataques, intrusiones, interrupciones u otras acciones hostiles deliberadas, que puedan comprometer la información y los sistemas que la manejan.

Por otro lado, ya habíamos mencionado anteriormente que en la Alianza Atlántica su NCIRC constituye un elemento clave de la política de ciberdefensa aliada, tal y como se indica en la declaración de los jefes de Estado y de Gobierno que se produce tras cumbre de Lisboa celebrada a finales del año 2010, en la que se comprometen a acelerar su implementación y despliegue hasta alcanzar la capacidad plena operativa de la NCIRC durante el año 2012 [22]. Analicemos pues con un poco más de detalle la NCIRC, como muestra de referencia de esta capacidad en los entornos de Defensa.

La NCIRC se diseña para ser capaz de dar una serie de servicios de apoyo técnico y legal, que puedan responder a incidentes de seguridad informática dentro de la OTAN, implantando de forma centralizada estos tres grupos de medidas [23]:

1. *Medias preventivas:* que incluía, entre otros, la publicación de boletines de seguridad, la distribución de actualizaciones de *software*, la disponibilidad de equipos de análisis de vulnerabilidades, etc.
2. *Medidas reactivas*: que incluía el soporte y la respuesta ante incidencias o intentos de intrusión.
3. *Asesoramiento legal:* que incluía el análisis forense, la investigación y la actualización normativa.

El diseño de la NCIRC debía responder a los siguientes requerimientos:

– Capacidad para coordinar la respuesta global de la OTAN durante un incidente.
– Base de conocimiento centralizada en apoyo de los administradores de sistemas locales.
– Centralizar los servicios en línea y los *in situ.*
– Centralizar los acuerdos de apoyo forense y también de asesoramiento legal.
– Optimización de recursos.
– Servir de punto de contacto de la OTAN con otros CERT externos.

Para ello, la NCIRC se estructura en tres capas o niveles:

1. *NCIRC CC* (38): compuesto por la NOS (39) y el C3 (40) *staff,* es el nivel de coordinación de la NCIRC y constituye el punto central de contacto tanto para otros organismos internos de la OTAN, como para los interlocutores externos, como otros CERT, etc.
2. *NCIRC TC* (41): Constituido por el SOC (42), es el nivel técnico operativo de la NCIRC.

---

(38) *NATO Computer Incident Response Capability-Coordination Centre.* El Centro de Coordinación Técnico del NCIRC es el primer nivel del NCIRC.

(39) *NATO Office of Security.*

(40) *Consultation, Command and Control*.

(41) *NATO Computer Incident Response Capability-Technical Centre.* El Centro Técnico del NCIRC constituye el segundo nivel, en: *http://www.ncirc.nato.int/index.htm*

(42) *Security Operation Centre.* El Centro de Operaciones de Seguridad suele hacer referencia a la ubicación física, y por extensión a las personas y sistemas TIC que se incluyen en ella, desde la que se gestiona la seguridad de una organización. Suele formar parte de cualquier CERT, aunque pueden existir SOC limitados que no consti-

3. Administradores de sistemas y de red de toda la OTAN: que en su conjunto formarán el nivel tercero de la NCIRC.

Finalmente, el catálogo de servicios de la NCIRC incluía los siguientes:

– Gestión de incidentes.
– Información de vulnerabilidades y amenazas.
– Análisis de vulnerabilidades *(on-line-in situ)*.
– Servicios de consultoría (tecnológica y forense).
– Recopilación y monitorización de información de diversas fuentes: IDS (43), antivirus, cortafuegos, etc.
– Soporte en línea de actualizaciones automáticas, descargas *software* o procedimientos operativos estándar.
– Análisis de incidente y pruebas de seguridad.

*«Ciberequipo Rojo»*

El término «Equipo Rojo» (44) es ampliamente utilizado en los entornos militares, en los que su significado se entiende sin gran dificultad. Analicemos un poco más este sentido para facilitar la comprensión de su aplicación al ciberespacio.

Históricamente, parece que la idea se le debe atribuir al mariscal de campo británico Bernard Montgomery [24], quién, en el transcurso de la Segunda Guerra Mundial, asignó a varios oficiales subalternos la misión de estudiar las estrategias del mariscal de campo alemán Irwin Rommel en África y Europa, con el fin de contrastar la viabilidad de los planes de los aliados.

Esta idea fue después ampliamente utilizada por las Fuerza Armadas norteamericanas en sus ejercicios de adiestramiento durante el periodo de la guerra fría (45). En ellos, habitualmente había dos equipos [25]: el «Equipo Azul», formado por las participantes en el ejercicio actuando

---

tuyan una capacidad CIRC propiamente dicha. También puede aparecer referido por su sigla en español COS.

(43) *Intrusion Detection System.*

(44) Proviene del inglés *Red Team.* Muy a menudo aparece en su forma verbal *Red Teaming* para referirse a la acción de crear, utilizar o implementar «Equipos Rojos».

(45) En su acepción moderna, se entiende que abarca el periodo comprendido entre el año 1947, poco después de la finalización de la Primera Guerra Mundial, hasta el año 1991, año en el que se produjo la desintegración de la antigua Unión de Repúblicas Socialistas Soviéticas (URSS).

como fuerzas propias de Estados Unidos, y el «Equipo Rojo», constituido por los participantes de dicho ejercicio que tomaban el rol del adversario, normalmente la extinta URSS, de dónde se deriva su nombre.

Esta práctica de asumir el modo de pensar del potencial adversario para analizar las fortalezas y debilidades propias, obtiene unos resultados excelentes al detectar flaquezas y vulnerabilidades que difícilmente habrían sido alcanzados mediante una inspección tradicional. Por ello, se extiende rápidamente su uso a nivel internacional y algunos países, como Estados Unidos [26] o el Reino Unido [27], lo incluyen y formulan dentro de sus cuerpos de doctrina militar, diseñando incluso cursos de formación específica [28] dentro también de sus programas de estudios militares.

A partir de aquí, podemos establecer una definición más elaborada de lo que sería utilizar un «Equipo Rojo» como el arte de aplicar un pensamiento estructurado, independiente y crítico, además de sensible a alternativas culturales [29], desde diferentes perspectivas, para cuestionar los supuestos propios y analizar a fondo los resultados potenciales, con el fin de reducir los riesgos y aumentar las oportunidades. Por tanto, el concepto de «Equipo Rojo» incluye no sólo «jugar» a ser adversarios o competidores, sino también intentar actuar como «abogados del diablo», ofreciendo interpretaciones alternativas y retos al pensamiento establecido dentro de una organización [30].

Por tanto, tal y como decíamos al comienzo de este capítulo, si anteponemos el prefijo *ciber-* al concepto de «Equipo Rojo», para formar el nuevo término «Ciberequipo Rojo», estaremos hablando de un «Equipo Rojo» cibernético, es decir, estaremos aplicando el concepto antes definido a la defensa del ciberespacio.

Así, diversos países y organismos internacionales de nuestro entorno, entre ellos la propia OTAN [31], han reclamado la necesidad de disponer de esta capacidad de ciberdefensa, como medio más eficaz de detectar las vulnerabilidades propias antes de que los adversarios las puedan aprovechar para infringirnos un impacto negativo, anunciado asimismo su intención de implementarlas en un futuro próximo.

En este contexto, la misión de un «Ciberequipo Rojo» sería la de evaluar la eficacia general de las medidas de seguridad de los sistemas de información y comunicaciones operativos, que apoyan el cumplimiento de la misión, a través de la ejecución controlada y sin previo aviso de

ciberataques verosímiles, demostrando a las partes interesadas, y en especial a los responsables en la toma de decisiones, el posible impacto negativo en la misión, mejorando la capacidad del equipo de seguridad de detectar y responder a dichos ataques.

Por tanto, para cumplir con su misión, el «Ciberequipo Rojo» deberá realizar una serie de actividades que podemos analizar estructurándolas en tres grupos principales [32].

EVALUAR LA EFICACIA DE LAS MEDIDAS DE SEGURIDAD

Que incluirá todas aquellas acciones encaminadas a medir la eficacia real de las medidas de seguridad implementadas en el sistema de la organización bajo evaluación. Esta actividad deberá realizarse únicamente bajo petición del jefe de la propia organización, que será el encargado de definir su alcance y objetivos. Por su naturaleza, el principal objetivo es evaluar en conjunto la integración de los aspectos técnicos y procedimentales de las medidas de seguridad, objetivo que normalmente no es asumido en los métodos convencionales de evaluación y auditoría. Teniendo en cuenta la naturaleza humana y la importancia relativa que el factor humano juega en la eficacia de casi todas las medidas de seguridad, una evaluación realista de la integración global de los procesos y las soluciones tecnológicas sólo puede lograrse si dicho examen se realiza sin previo aviso. Además, la evaluación no debe concentrarse en las medidas de seguridad propiamente dichas, sino en el impacto que los ataques cibernéticos pueden producir en la misión, por la falta de eficacia de las citadas medidas de seguridad.

Por otro lado, conviene tener en cuenta que la evaluación realizada por el «Ciberequipo Rojo» no es un análisis de vulnerabilidades, ni tampoco un test de penetración, tal y como se entiende dichas actividades tradicionalmente (46). Para la mayoría de las organizaciones, el análisis de vulnerabilidades se realiza de manera colaborativa con el objetivo de detectar todas las vulnerabilidades existes en un sistema, utilizando para ello herramientas automatizadas. Estas herramientas suelen mostrar sólo las posibles vulnerabilidades de los sistemas evaluados, en su

(46) Evidentemente, la definición de las acciones realizadas en un análisis de vulnerabilidades, en un test de penetración o por un «Equipo Rojo» variarán de una organización a otra y, por tanto, puede haber un cierto solapamiento de los objetivos y las metodologías que se utilizan en cada una de ellas, en función de la definición que se utilice en cada caso.

contexto y configuración, pero no indican si la explotación de dichas debilidades es realista, teniendo en cuenta la topología de la Red, las medidas de seguridad o el nivel de monitorización que dicho sistema tiene implementado. Tampoco ofrecen ninguna idea de los posibles impactos que un atacante podría realizar si ha sido capaz de explotar dichas vulnerabilidades.

Con respecto al test de penetración, en este caso generalmente sí se incluye el intento de explotar las vulnerabilidades de un sistema, tras un examen integral para detectar todas ellas [33], generalmente usando herramientas altamente especializadas y programas desarrollados específicamente para el sistema objetivo. Pero, normalmente, se centra en un servicio o aplicación específico, en lugar de en el sistema de información en su conjunto, y se hace de forma colaborativa, casi siempre antes de la entrada en producción del nuevo servicio TIC. Por tanto, el servicio proporcionado por un «Ciberequipo Rojo» sería complementario al análisis de vulnerabilidades y al test de penetración tradicionales.

### DEMOSTRAR EL IMPACTO DEL CIBERATAQUE EN LA MISIÓN

El segundo grupo de actividades buscará demostrar el posible impacto negativo que los ataques cibernéticos pueden provocar en los objetivos de negocio de la organización o en las operaciones militares en curso. Los objetivos de la demostración serán determinados por el responsable de la organización objeto de evaluación, y buscarán mostrar el potencial impacto de los ciberataques específicos en la misión de la organización, dada la dependencia que ésta tiene de la funcionalidad proporcionada por los Sistemas TIC.

Se incluirá la demostración a los altos responsables en la toma de decisiones de la organización, que no suele ser un aspecto contemplado en las actividades tradicionales de evaluación de la seguridad, dado que en su mayoría se centran en el análisis del funcionamiento técnico de los componentes del sistema. Al eliminar la incertidumbre, a través de la demostración real del posible impacto, se permite a los responsables de la implementación de los sistemas decidir de forma más objetiva cómo equilibrar las medidas de seguridad con los requisitos que compiten con éstas, tales como la facilidad de uso o el incremento de la funcionalidad, así como con las restricciones económicas o de plazos de tiempo. La única limitación a las demostraciones del «Ciberequipo Rojo» será la necesidad de mantener el control sobre los efectos que éstas puedan cau-

sar, directamente o como consecuencia de los efectos que se deriven de las actividades del ciberequipo.

### MEJORAR LA HABILIDAD DE LOS USUARIOS Y DEL PERSONAL DE SEGURIDAD

Dado que el correcto funcionamiento de las medidas de seguridad depende en gran medida de su correcta utilización por parte del personal de seguridad y de los usuarios, incrementar la habilidad de éstos para enfrentarse al entorno creciente de las ciberamenzas conformará también un objetivo del «Ciberequipo Rojo». Normalmente, los usuarios de los Sistemas TIC reciben formación sobre cómo llevar a cabo procedimientos habituales que suponen un riesgo para la seguridad de estos Sistemas (como por ejemplo, sobre riesgos asociados a la transferencia de archivos a través de dispositivos extraíbles) y programas de concienciación sobre cómo detectar signos reveladores de los ciberataques y la forma en que deben manejarlos.

Por otro lado, los administradores de seguridad suelen estar capacitados para detectar y tratar los ataques cibernéticos, mediante la operación de herramientas especializadas, con el objeto de detenerlos, reportarlos y tomar las acciones oportunas para la recuperación del Sistema. Parte de esta formación se realizará a través de cursos, mientras que otra parte se llevará a cabo mediante ejercicios. Los cursos se utilizarán generalmente para capacitar al personal de seguridad en el uso de herramientas, mientras que los ejercicios se utilizan principalmente para entrenarlos en la ejecución de procesos.

Sin duda alguna, estos programas de formación, concienciación y sensibilización están disponibles y contribuyen a la mejora de la seguridad TIC de la organización, pero normalmente no tienen lugar en el entorno de los sistemas en producción y están fuera del ambiente normal en el que trabajan tanto los usuarios como el personal de seguridad. Además, habitualmente estos cursos o ejercicios parten de premisas o situaciones de contexto que no son reales, simplemente por limitaciones o necesidades de eficiencia en la ejecución del evento formativo.

La ejecución controlada de los ciberataques en contra de Sistemas TIC operacionales proporcionará una oportunidad clara, tanto a los usuarios como al personal de seguridad, para perfeccionar sus habilidades con las herramientas que se utilizan para manejar ciberataques reales. Se pueden definir objetivos específicos para cubrir determinadas lagu-

nas de formación y para asegurarse de que todo el personal es capaz de ejecutar correctamente los procesos de gestión de incidentes críticos.

El incremento de la habilidad de los usuarios y del personal de seguridad es un beneficio clave proporcionada por un «Ciberequipo Rojo», ya que la calidad de la formación obtenida de los cursos y ejercicios tradicionales es muy limitada, debido principalmente a que el entorno en que se celebra la formación o el ejercicio está muy alejado de la realidad operativa.

Como hemos expuesto, las actividades que realiza un «Ciberequipo Rojo» pueden producir importantes beneficios para la organización objetivo de las mismas, pero conviene tener en cuenta que también conllevan ciertos riesgos, que deberán tratarse mediante salvaguardas con el fin de limitarlos al mínimo. Veamos a continuación algunos de los citados riesgos, así como las medidas que pueden tomarse para minimizarlos:

1. Impacto sobre los sistemas informáticos de la organización con un perjuicio grave que afecte a la continuidad de la misma:
   – Se deberán recoger en un documento firmado por el director de la organización objeto de la evaluación, los sistemas que deban ser probados y las actividades que se realizarán sobre ellos.
2. Actividades ilegales o en contra de derechos de terceros:
   – Toda actividad que deba realizar el «Ciberequipo Rojo», en la que esté involucrada una organización objetivo, deberá ser revisada por un asesor legal y deberá ser autorizada por el responsable del «Ciberequipo Rojo».
3. Riesgos de integridad y disponibilidad:
   – El responsable del «Ciberequipo Rojo» deberá garantizar que todos los programas desarrollados al efecto han sido probados correctamente conforme procedimiento que tenga definido el «Ciberequipo Rojo».
4. Respuesta imprevista o arriesgada por parte del personal de la organización ante una situación de ataque:
   – Designar personal de confianza dentro de la organización contra la que va a actuar el «Ciberequipo Rojo», de forma que estén prevenidos en todo momento sobre las acciones de éstos y puedan orientar a los operadores del sistema cómo actuar durante un ataque.
5. Actuación maliciosa de algún miembro del «Ciberequipo Rojo» o riesgos de acceso no autorizado.
   – El personal de confianza de la organización objetivo revisará en todo momento las acciones que realizan los miembros del «Ciberequipo Rojo», de manera que puedan reportar a sus responsables

cualquier acción no permitida. Además, se deberá realizar en todo momento una auditoría integral de accesibilidad, tráfico de red y acceso al sistema, por parte de un tercero ajeno al «Ciberequipo Rojo» y a la organización cliente.

6. Fuga de información de las evaluaciones realizadas por parte del «Ciberequipo Rojo»:
   - Dicha información deberá ser tratada por parte de la organización como información sensible y se aplicarán las medidas acordes a la política de la organización y a la normativa del país en la que esté situada la misma.

Finalmente, parece claro que para abordar adecuadamente las actividades que deber realizar el «Ciberequipo Rojo», controlando a su vez los riesgos que se derivan de las mismas, no vale cualquier tipo de estructuración, sino que es necesario diseñar una organización alineada con los objetivos y responsabilidades del mismo. Algunos autores [32] propugnan que dicha organización debería incluir al menos los siguientes elementos:

1. *Director de equipo*: estará situado a nivel estratégico y será el encargado de dirigir el «Ciberequipo Rojo», guiándole en su evolución y mejora continua. Las responsabilidades principales con las que cuenta serían:
   - Establecer los objetivos, prioridades, hitos y comportamiento ético del equipo.
   - Asegurar que las actividades que se desarrollan están bajo un marco legal.
   - Asegurar la financiación y los recursos adecuados.
2. *Comité de Inspección*: por debajo del director se establecerá un Comité de Inspección, que estará compuesto por un experto en seguridad y un representante de la organización contra la que va actuar el «Ciberequipo Rojo».
   - El representante de la organización aceptará el riesgo y asesorará al experto en seguridad sobre los posibles impactos en su organización que supondrá cada actividad realizada también por el «Ciberequipo Rojo».
   - El experto en seguridad tendrá poder de veto sobre las actividades del «Ciberequipo Rojo» y será el máximo responsable del éxito de la actividad propuesta. Además, si por algún motivo se produjera una consecuencia imprevista, el experto en seguridad será quién responda ante el representante de la organización.

3. *Jefe del equipo de ataque*: por debajo del Comité de Inspección, y ya a nivel operativo, existirá el jefe del equipo de ataque, que será el responsable de garantizar que todas las personas del equipo de ataque están capacitadas para realizar las actividades que se proponen.
4. *Grupo de ataque*: normalmente, dentro de este grupo existirán varios equipos de ataque, cada uno compuesto por un jefe de equipo y un número razonable de analistas, que son los responsables de realizar los ataques buscando la manera de lograr los objetivos dentro de los límites definidos. Los analistas requieren de una mezcla de habilidades y experiencia, así como un conocimiento experto de técnicas de ciberdefensa, de los entornos de sistemas y de red, de los protocolos comunes de Internet, etc.
5. *Jefe del equipo de soporte*: subordinado del jefe del equipo de ataque, cuya función será garantizar el desarrollo y el buen funcionamiento de los programas informáticos que se implementen para su uso en el equipo de ataque.
6. *Grupo de soporte*: el grupo de soporte es el responsable directo del desarrollo de las diversas herramientas que necesita el grupo de ataque, así como del mantenimiento de los sistemas de éstos. Por ello, este grupo debe estar compuesto por personal especializado en desarrollo (bases de datos, *web*, *software*, sistemas y red, etc.) y en seguridad (vulnerabilidades, ingeniería inversa, *malware*, etc.).

Para concluir el análisis realizado sobre el «Ciberequipo Rojo», y a la vista de la estructura y actividades que desarrolla, debemos reconocer que un «Ciberequipo Rojo» incrementa fundamentalmente la Capacidad de Defensa, dentro de los tres grupos en los que se clasifican las capacidades de ciberdefensa, puesto que al centrar su actividad únicamente en los sistemas propios, se excluyen por definición las actividades de *explotación* y *respuesta*.

En cualquier caso, también conviene establecer que un «Ciberequipo Rojo» es una capacidad complementaria y potenciadora de una CIRC, analizada anteriormente, aportando capacidades no incluidas en ésta. Además, el adiestramiento y forma de operar de un «Ciberequipo Rojo» está muy próximo al que recibirían los componentes de un ciberejército, que analizaremos posteriormente, diferenciándose de éste fundamentalmente en su doctrina y también en los objetivos de su misión.

*Ciberejército*

Hasta ahora hemos analizado las formas de implementar las capacidades de ciberdefensa que se limitan a los aspectos defensivos de las mismas, pues centran fundamentalmente su actividad en la protección de los sistemas propios.

Sin embargo, cada vez con más frecuencia, y en mayor número de países, ha ido surgiendo la opinión de que el crecimiento [34] y la sofisticada [35] evolución de la ciberamenaza hacen necesario enfrentarla con medidas más activas, que busquen no sólo prevenir, detectar, reaccionar y recuperar las infraestructuras propias, sino neutralizar la ciberamenaza desde su origen, implementando los aspectos de explotación y ataque de las capacidades de ciberdefensa. Surgen así los conceptos de ciberguerra [36] y ciberejército, así como las reglas de enfrentamiento [37] que permitan a éstos pasar al ataque.

De esta forma, podemos encontrar numerosas iniciativas en diferentes países, para crear y estructurar un cibermando militar (47) o ciberejército, entre los que se encuentran: Estados Unidos [38], Reino Unido [39], China [40], Rusia [41], Irán [42], India [43], Pakistán [44], Corea del Norte [45], Corea del Sur [46], Israel [47] y un largo etcétera.

Seguramente sea el Mando Cibernético (USCYBERCOM) de Estados Unidos el que disponga de un cuerpo doctrinal más avanzado y conceptualmente elaborado, además de ser el que con mayor transparencia informa del avance en la implementación de sus capacidades. Analicemos, por tanto, el ciberejército norteamericano como forma de describir las características genéricas que cualquier otra nación implementa, implementará, o pretenderá implementar dentro de sus posibilidades, para sus respectivos ciberejércitos.

El 23 de junio de 2009, el secretario de Defensa norteamericano ordenó al jefe del Mando Estratégico (USSTRATCOM) (48) de Estados Unidos

(47) Es muy habitual encontrar el término *Cyber Command,* en los documentos escritos en inglés, para referirse a la capacidad militar para la defensa del ciberespacio. Sin embargo, su traducción directa por cibercomando no tiene el mismo significado en español, por lo que en el presente capítulo utilizaremos los términos ciberejército o cibermando militar, pues consideramos que su comprensión se aproxima más al significado original del término en inglés.

(48) *U.S. Strategic Command.*

establecer el USCYBERCOM de Estados Unidos (49), con la misión [48] de planificar, coordinar, integrar, sincronizar y llevar a cabo actividades para:

– Dirigir las operaciones y la defensa de las redes de información específicas del Departamento de Defensa.
– Preparar y, cuando así se indique, llevar a cabo todo el espectro de las posibles operaciones militares en el ciberespacio, con el objetivo de facilitar las acciones en todos los ámbitos.
– Garantizar libertad de acción de Estados Unidos y sus aliados en el ciberespacio, y negar la misma a sus adversarios.

El primer comandante en jefe del ciberejército es el general Keith B. Alexander, del Ejército de Estados Unidos, que compatibilizará su cargo con el que ya ostentaba de director de la Agencia Nacional para la Seguridad (NSA) (50). La Capacidad Operativa Inicial (IOC) (51) fue lograda el 21 de mayo de 2010, convirtiéndose en plenamente operativo (FOC) (52) el 3 de noviembre de 2010 [49].

El USCYBERCOM será el medio por el que se consiga centralizar el mando de las operaciones en el ciberespacio, fortaleciendo e integrando las capacidades del Departamento de Defensa en el ciberespacio, ya que reunirá todas las cibercapacidades existentes, creando una sinergia que no existía hasta ese momento.

De esta forma, el USCYBERCOM se compondrá de las ciberunidades de los diferentes servicios (53) que componen las Fuerzas Armadas estadounidenses, en concreto [50]:

---

(49) *U.S. Cyber Command.*

(50) *National Security Agency.* La ANS se define a sí misma como el hogar de los criptólogos y criptoanalístas estadounidenses. Durante sus más de 50 años de vida, ha sido la fuente que ha proporcionado información oportuna y a tiempo a los mandos militares y a los altos responsables del Gobierno de Estados Unidos. Por su naturaleza, como miembro clave de la comunidad de inteligencia americana, la NSA se enfrenta al doble reto de evitar, por una lado, que adversarios extranjeros puedan tener acceso a la información clasificada nacional y, por otro, a recopilar, procesar y difundir información de inteligencia de señales extranjeras, para propósitos de inteligencia y contrainteligencia, así como para apoyar las operaciones militares estadounidenses, en: *http://www.nsa.gov/*

(51) *Initial Operational Capability.*

(52) *Full Operational Capability.*

(53) Consisten en el Ejército, la Armada, la Infantería de Marina y la Fuerza Aérea.

1. *Cibermando del Ejército (ARCYBER)* (54): aportando la componente cibernética del Ejército de Tierra, denominada segundo Ejército. Incluirá las siguientes unidades subordinadas [51]:
   – IX Mando de Señales del Ejército, o el Mando de Tecnología Global de Red del Ejército (NETCOM) (55).
   – I Mando de Operaciones de Información (del componente terrestre).
   – Mando de Inteligencia y Seguridad del Ejército, que estará bajo el control operacional del cibermando del Ejército para las acciones en el ciberespacio.
2. *Cibermando de la Fuerza Aérea (AFCYBER)* (56): aportando la componente cibernética del Ejército del Aire, denominada XXIV Fuerza Aérea. Incluirá las siguientes unidades subordinadas [52]:
   – Ala 67 de Guerra en Red.
   – Ala 688 de Operaciones de Información.
   – Ala 689 de Comunicaciones de Combate.
3. *Cibermando de la Flota (FLTCYBERCOM)* (57): aportando la componente cibernética de la Armada, denominada X Flota. Incluirá entre otras las siguientes unidades subordinadas [53]:
   – Mando Naval de Guerra en Red.
   – Mando Naval de Operaciones de Ciberdefensa.
   – Mando Naval de Operaciones de Información.
4. *Cibermando de la Infantería de Marina (MARFORCYBER)* (58): aportando la componente cibernética de la Infantería de Marina:
   – Por otro lado, desde hace tiempo se viene revisando la Doctrina Militar estadounidense, en sus diferentes componentes, para adecuarla a los nuevos retos que suponen las operaciones militares en el ciberespacio, intentado definir las capacidades que deben preparase para afrontarlas.
   – Así, el Ejército de Estados Unidos establece, en su Plan de Capacidad de los años 2016-2028 [54] para el concepto de Operaciones en el Ciberespacio (CyberOps) (59), que éstas se componen de:

---

(54) *Army Cyber Command.*
(55) *Network Enterprise Technology Command.*
(56) *Air Force Cyber Command.*
(57) *Fleet Cyber Command.*
(58) *Marine Forces Cyber Command.*
(59) *Cyberspace Operation.*

Comprensión de la Cibersituación (CyberSA) (60), Operaciones de la Red Cibernética (CyNetOps) (61), Ciberguerra (CyberWar) y, finalmente, Soporte Cibernético (CyberSpt) (62).

- No vamos a entrar a analizar en detalle las capacidades de CyNetOps y de CyberSpt, que están muy relacionadas con los aspectos defensivos de las capacidades de ciberdefensa, ya vistos en los apartados anteriores del presente capítulo, abordando con más detenimiento las capacidades que se deben incluir en CyberSA, directamente relacionadas con las capacidades de explotación, y en la CyberWar, que conformarían fundamentalmente las capacidades de respuesta.

5. *Comprensión de la cibersituación*: se compondría del conocimiento inmediato, tanto del adversario cómo del aliado, así como de toda información pertinente sobre las actividades en el ciberespacio o en el espectro electromagnético. Se obtiene a partir de una combinación de actividades de inteligencia y operativas en el ciberespacio, así como en el resto de dominios, llevadas a cabo tanto de manera unilateral como a través de la colaboración con socios de los sectores público o privado. La discriminación entre las amenazas naturales y artificiales es una pieza clave de este análisis.
   - Una apropiada comprensión de la cibersituación permitirá la toma de decisiones adecuadas, en todos los niveles de decisión, a través de productos a medida de cada audiencia, que pueden ir desde los boletines de sensibilización con una amplia difusión dirigida a los usuarios en general, hasta informes de cuestiones específicas, extremadamente sensibles y de naturaleza clasificada. Una buena comprensión de la cibersituación debe incluir también las capacidades para:
     - La comprensión del adversario y del aliado, así como de otras actividades relevantes en el ciberespacio.
     - La evaluación de las capacidades cibernéticas amigas.
     - La evaluación de las capacidades cibernéticas e intenciones del adversario.
     - El análisis de las vulnerabilidades cibernéticas del adversario y del aliado.

(60) *Cyber Situational Awareness.*
(61) *Cyber Network Operations.*
(62) *Cyber Support.*

   – La comprensión de la información que fluye a través de las redes para deducir su propósito y criticidad.
   – La comprensión de los efectos y el impacto en la misión, resultante de las degradaciones en el ciberespacio amigo y también adversario.
6. CyberWar: es el componente de las CyberOps que extiende el poder cibernético más allá de los límites de la Defensa del ámbito cibernético propio, para detectar, detener, denegar y derrotar a los adversarios. Las capacidades de la CyberWar tienen como objetivos las redes de telecomunicaciones y los ordenadores, así como los procesadores y controladores integrados en equipos, sistemas e infraestructuras.

La CyberWar incluirá acciones de ataque en las que se combinarán ataques a redes informáticas, con otras capacidades de apoyo (por ejemplo, ataque electrónico o ataque físico) para negar o manipular la información o la infraestructura.

En la CyberWar, se combinarán medios políticos, de inteligencia, sensores y procesos altamente automatizados para identificar y analizar la actividad maliciosa, al tiempo que se ejecutarán acciones de respuesta con autorización previa para eliminar ataques hostiles antes de que puedan causar impacto. Además, se usarán principios tradicionales de seguridad de los ejércitos como la defensa en profundidad. Se incluirá la vigilancia y el reconocimiento para emitir alertas tempranas de las acciones enemigas.

En un desglose detallado de las capacidades para la CyberWar se incluirán también:

– Acceder, tanto por medios directos como a distancia, a redes, sistemas o nodos marcados como objetivos, con el fin de garantizar el acceso que requieren las acciones de CyberWar contra objetivos fugaces.
– Permitir el acceso recurrente, tanto por medios directos como a distancia, a redes, sistemas o nodos marcados como objetivos, para garantizar el acceso requerido por las CyberOps.
– Acceder al *hardware* y al *software* del adversario, por medios directos o a distancia, con el fin de garantizar las acciones de CyberWar.
– Acceder, recopilar y explotar la información del adversario marcada como objetivo, por medios directos o a distancia, con el fin de detectar, disuadir, denegar y derrotar a las acciones y la libertad de acción del adversario.

– Habilitar la capacidad de agregar, administrar, descifrar, traducir lingüísticamente, analizar e informar sobre todos los datos recogidos en los sistemas de gestión del conocimiento, con el fin de apoyar las CyberOps y a los mandos críticos de batalla.
– Proporcionar capacidades de CyberWar, tanto a distancia como de forma expedicionaria, con el fin de detectar, disuadir, denegar y derrotar a las acciones y la libertad de acción del adversario.
– Proporcionar capacidades, basadas en sensores, para la detección automatizada de ataques de red y de intrusiones con el fin de detectar, disuadir, denegar y derrotar a las acciones del adversario, integrar la defensa en profundidad, garantizar la libertad de acción propia y de los aliados, así como negar la libertad de acción del adversario en el momento y lugar de nuestra elección.
– Atacar (negar, degradar, interrumpir, engañar o destruir) las redes del adversario y su infraestructura crítica con el fin de detectar, disuadir, denegar y derrotar a las acciones y la libertad de acción del adversario.
– Proporcionar capacidades, basadas en sensores, de respuesta a la intrusión o el ataque a la Red, con el fin de detectar, disuadir, denegar y derrotar las acciones del adversario, integrando la defensa en profundidad y garantizando la libertad de acción amistosa, así como negando la libertad de acción del adversario, en el momento y el lugar de nuestra elección.
– Atacar las redes del adversario con el fin de detectar, disuadir, denegar, y derrotar a sus acciones y su libertad de acción.
– Atacar (negar, degradar, interrumpir, engañar o destruir) los procesadores y controladores integrados en los equipos y sistemas del adversario, con el fin de detectar, disuadir, denegar y derrotar sus acciones, integrando la defensa en profundidad y garantizando la libertad de acción propia y aliada, así como negando la libertad de acción del adversario en el momento y el lugar de nuestra elección.
– Proporcionar conocimiento de la situación del adversario y de otras redes específicas, con el fin de aumentar el conocimiento general de la situación del comandante, permitiendo las CyberOps, así como las acciones integradas del comandante.
– Mapear y entender al adversario y otras estructuras específicas de la Red, a fin de garantizar todos los aspectos de las CyberOps.
– Rastrear, localizar y predecir las actividades del adversario en el ciberespacio, a fin de garantizar nuestras acciones de CyberWar y del conocimiento de la cibersituación.

– Atacar la información del adversario con el fin de disuadir, socavar o engañar a los adversarios, apoyando los objetivos generales del comandante de la misión.
– Mitigar o evitar las medidas de ciberdefensa del adversario, con el fin de ejecutar las capacidades propias de CyberWar.
– Impactar en la infraestructura cibernética del adversario, con el fin de apoyar la efectividad de las acciones en el ciberespacio, así como los objetivos generales del comandante de la misión.

Aunque la lista anterior parece larga y ambiciosa, hay que considerar que las citadas capacidades para las CyberOps no serán implementadas todas en todos los escalones (63) de la estructura militar, sino que a cada nivel estratégico le corresponderán unas u otras cibercapacidades. Así, por ejemplo, sin entrar en un análisis detallado que queda fuera del alcance del presente estudio, podemos decir que las capacidades para la ciberguerra no serán desarrolladas a nivel de compañía, comenzándose a implementar a nivel de batallón. O que la capacidad para acceder al *hardware* y al *software* del adversario, por medios directos o a distancia, con el fin de garantizar las acciones de ciberguerra, sólo se comienza a implementar a nivel del mando del componente terrestre del teatro de operaciones.

Finalmente, conviene indicar que la doctrina militar estadounidense establece que para un adecuado desarrollo de las capacidades citadas anteriormente hay contemplar los aspectos de la doctrina, la organización, el entrenamiento, el material, el liderazgo y la educación, el personal y las instalaciones (64). Lo que nos devuelve casi al principio del presente documento, cuando al revisar el «Concepto de Ciberdefensa Militar» del JEMAD, ya observamos que las capacidades de ciberdefensa deberían ser desarrolladas considerando los mismos aspectos o dimensiones.

## Conclusiones

Tras el análisis realizado sobre la ciberdefensa y sus capacidades, podemos extraer las siguientes conclusiones:

(63) Para el Ejército de Tierra estadounidense estos escalones militares son: compañía, batallón, brigada, división, cuerpo de ejército, mando del componente terrestre del teatro de operaciones, cibermando del Ejército y mando conjunto de combate.
(64) Se utiliza el acrónimo DOTMLPF para referirse a ellos, y se corresponde con: *Doctrine, Organizations, Training, Materiel, Leadership and education, Personnel and Facilities.*

– La ciberdefensa sería el subconjunto más operativo de las capacidades de ciberseguridad [55], lo que parece lógico y coherente si pensamos que en el mundo físico la defensa es la parte más operativa de las capacidades que desarrollan las naciones para garantizar la Seguridad Nacional.
– La mayoría de los cuerpos de doctrina militar clasifican las capacidades de ciberdefensa en tres tipos: las de defensa, centradas en la prevención, detección, reacción y recuperación frente a ataques; las de *explotación*, que permiten la recopilación de información sobre potenciales adversarios; y las de *respuesta*, que incluyen las medidas y acciones a tomar ante amenazas o ataques.
– Una capacidad de respuesta a incidentes informáticos implementa fundamentalmente capacidades de defensa, dentro de la estrategia de ciberdefensa de una nación u organismo internacional, buscando garantizar la prevención, detección, reacción y recuperación frente a ataques, intrusiones, interrupciones u otras acciones hostiles deliberadas.
– Un «Ciberequipo Rojo» también implementa la capacidad de defensa, dentro de la ciberdefensa, puesto que al centrar su actividad únicamente en los sistemas propios, se excluyen por definición las actividades de explotación y respuesta. De todas formas, no debemos confundirlo con una CIRC, ya que es una capacidad complementaria y potenciadora de ésta, y cuyo adiestramiento y forma de operar está más próximo al de un ciberejército, diferenciándose de éste fundamentalmente en su doctrina y en los objetivos de su misión.
– Debido a la creciente sofisticación de la ciberamenaza, cada vez en más países se está imponiendo la opinión de que es necesario hacerle frente con medidas más activas, que busquen no sólo prevenir, detectar, reaccionar y recuperarse ante un ataque, sino neutralizar la ciberamenaza desde su origen, desarrollando las capacidades de un ciberejército, así como las reglas de enfrentamiento que permitan a éstos pasar al ataque.
– Tras analizar los diferentes modelos, compromisos y alcances, no excluyentes unos de otros, a la hora de implementar una adecuada capacidad de ciberdefensa, podemos deducir que en general ésta busca dar respuesta a dos aspectos o misiones diferenciados:
– Por un lado, la protección de las TIC de la Defensa, sobre las que se apoya la capacidad operativa militar en el mundo físico tradicional. Estas capacidades suelen ser las primeras en implementarse en forma de CIRC-CERT-CSIRT.

– Por otro, implementar una capacidad militar en el ciberespacio, para garantizar la defensa de los intereses nacionales en ese nuevo ámbito. Que se suele implementar partiendo de las anteriores y cuya máxima expresión serían los ciberejércitos.

**Bibliografía**


[1] Gobierno de España: *Estrategia Española de Seguridad: «Una responsabilidad de todos»,* 2011.

[2] House, White: *Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure,* 2011.

[3] House, White: *International Strategy For Cyberspace: Prosperity, Security, and Openness in a Networked World,* 2011.

[4] Ganuza, Néstor; Hernández, Alberto and Benavente, Daniel «NECCS-1: An Introductory Study to Cyber Security in NEC», *NATO CCD COE Publications,* junio de 2011.

[5] Real Academia Española: *Diccionario de la Lengua Española,* vigésima segunda edición, Madrid, 2010.

[6] Candau Romero, Javier: «Estrategias nacionales de ciberseguridad. Ciberterrorismo», en *Ciberseguridad: retos y amenazas a la Seguridad Nacional en el ciberespacio,* volumen 149, pp. 257-322, edición de 2010, Ministerio de Defensa, Madrid.

[7] Díaz del Río Durán, Juan José: «La ciberseguridad en el ámbito militar», en *Ciberseguridad: retos y amenazas a la Seguridad Nacional en el ciberespacio,* volumen 149, pp. 217-256, edición de 2010, Instituto Español de Estudios Estratégicos (IEEE), Madrid.

[8] Tiirmaa-Klaar, Heli «NATO Policy on Cyber Defence», in *2011 3rd International Conference on Cyber Conflict,* Tallin (Estonia), 2011.

[9] Centro Criptológico Nacional y Mañas, José A.: *Guía de Seguridad de las TIC (CCN-STIC-401) glosario y abreviaturas,* diciembre de 2006.

[10] García Sieiro, José Manuel: «Planeamiento por Capacidades», *Revista Española de Defensa,* pp. 38-43, junio de 2006.

[11] Joint Chiefs of Staff: *Joint Publication 3-13 Information Operations,* Departamento de Defensa, 13 de febrero de 2006.

[12] European Network and Information Security Agency: *Good Practice Guide-Cooperative Models for Effective Public Private Partnerships,* Publications Office of the European Union, Luxemburgo, 2011.

[13] Laborie Iglesias, Mario A.: «La Alianza tras la cumbre de Lisboa», *Revista Española de Defensa,* pp. 62-65, noviembre de 2010.

[14] Caro Bejarano, María José: «Documento Informativo del IEEE 9/2011-Nuevo Concepto de Ciberdefensa de la OTAN», IEEE, marzo de 2011.

[15] NATO C3 Agency: «Multinational Cyber Defence Capability Development (MN CD2) Initiative-Info Sheet», NC3A, 5 de mayo de 2011.

[16] Spafford, E. H.: «The Internet worm program: an analysis», *ACM SIGCOMM Computer Communication Review,* volumen 19, número 1, pp. 17–57, 1989.

[17] Bronk, Henk; Thorbruegge, Marco y Hakkaja, Mehis: *Cómo crear un CSIRT paso a paso,* ENISA *(European Network and Information Security Agency)*, 22 de diciembre de 2006.

[18] Centro Criptológico Nacional: *Guía de Seguridad de las TIC (CCN-STIC-810) Guía de Creación de un CERT/CSIRT,* septiembre de 2011.

[19] West-Brown, Moira J.; Stikvoort, Don; Kossakowski, Klaus-Peter; Killcrece, Georgia; Ruefle, Robin and Zajicek, Mark: *Handbook for Computer SecurityIncident ResponseTeams (CSIRTs)*, Carnegie Mellon University, abril de 2003.

[20] Carnegie Mellon University: «CERT®/CC: Computer Security Incident Response Team FAQ», 1 de abril de 2008, (on-line), en: *http://www.cert.org/csirts/csirt_faq.html,* acceso: 6 de noviembre de 2011.

[21] Carnegie Mellon University: Stelvio bv, y Presecure Consulting GmbH, «CSIRT Services», Carnegie Mellon University, 26 de noviembre de 2002.

[22] Lord Jopling: «Information and National Security», NATO Parliamentary Assembly, Committee Report 171 CDS 11 E, Bucharest, 2011.

[23] Anil, Suleyman: «NCIRC (NATO Computer Incident Response Capability)», in *11th TF-CSIRT Meeting,* Madrid, 2004.

[24] Milburn, John: «Red Team U. creates critical thinkers», *InfoSec News,* Fort Leavenworth, 18 de mayo de 2007.

[25] Mejia, Robin: «Red Team Versus Blue Team: How to Run an Effective Simulation», *CSO Security and Risk,* California, 25 de marzo de 2008.

[26] Defense Science Board: «The Role and Status of DoD Red Teaming Activities», Departamento de Defensa, Washington, D.C., septiembre de 2003.

[27] Assistant Chief of the Defence Staff: «A Guide to Red Teaming-DCDC Guidance Note, Ministerio de Defensa, Reino Unido, febrero de 2010.

[28] Spad, Marcus: «Army approves plan to create school for Red Teaming», *U.S. Army Tradoc News Service,* Fort Monroe, Va., 13 de julio de 2005.

[29] Craig, Susan: «Reflections from a Red Team Leader», *Military Review,* volumen 2007, número de marzo-abril, pp. 57-60, 6 de marzo de 2007.

[30] Mateski, Mark Dr.: «A Short Introduction to Red Teaming (1.0)», *Red Team Journal,* de 2009.

[31] «NATO plans force to respond to cyber attacks», *Physorg News,* 8 de junio de 2011.

[32] Dandurand, L.: «Rationale and blueprint for a Cyber Red Team within NATO: An essential component of the Alliance's Cyber Forces», in *2011 3rd International Conference on Cyber Conflict Proceedings,* volumen 1, pp. 71-86. Tallin (Estonia), 2011.

[33] Peake, Chris: *Red Teaming: The Art of Ethical Hacking*, SANS Institute, 16-de julio de 2003.

[34] McAfee® Foundstone® Professional Services: «Global Energy Cyberattacks: "Night Dragon"», White Paper, McAfee Labs™, Santa Clara, C. A., febrero de 2011.

[35] Clayton, Mark: «Stuxnet malware is "weapon" out to destroy... Iran's Bushehr nuclear plant?», *The Christian Science Monitor,* 21 de septiembre de 2010.

[36] Clarke, Richard A. and Knake, Robert: *Cyber War: The Next Threat to National Security and What to Do About It,* Harper Collins, 2010.

[37] Miles, Donna: «Doctrine to Establish Rules of Engagement Against Cyber Attacks», *American Forces Press Service,* Baltimore, 20 de octubre de 2011.

[38] U.S. Department of Defense: *Department of Defense Strategy for Operating in Cyberspace*, Estados Unidos, julio de 2011.

[39] Espiner, Tom: «MoD cyber-command will combine with intelligence», *ZDNet UK,* 27 de junio de 2011.

[40] Fernández de Lara, Carlos: «China confirma existencia de escuadrón de ciberguerra: "Ejército Azul"», *BSecure Magazine,* 30 de mayo de 2011.

[41] Giles, K.: «"Information Troops"-A Russian Cyber Command?», in *Cyber Conflict (ICCC), 2011 3rd International Conference on*, pp. 1-16*,* 2011.

[42] Agencia EFE: «Irán establece su primer cibercomando para luchar contra ataques informáticos», *El Nacional*, Caracas, 31 de octubre de 2011.

[43] Gupta, Harish: «As cyber attacks rise, India sets up central command to fight back», *Daily News & Analysis,* Nueva Delhi, 15 de mayo de 2011.

[44] Pakistan News Service: «New war between India and Pakistan: Cyber Warfare», *Pak Tribune,* 8 de febrero de 2011.

[45] Yoon, Sangwon: «North Korea recruits hackers at school», *Al Jazeera* (en inglés), 20 de junio de 2011.

[46] Channel NewsAsia: «South Korea to set up cyber command against North Korea», *MediaCorp,* Seul, 9 de julio de 2009.

[47] Reuters: «Israel lanza un "cibercomando" contra ataques informáticos», *El Mundo,* 18 de mayo de 2011.

[48] U.S. Department of Defense: *U.S. Cyber Command Fact Sheet*, US Department of Defense Office of Public Affairs, 13 de octubre de 2010.

[49] Office of the Assistant Secretary of Defense (Public Affairs): «Cyber Command Achieves Full Operational Capability», *Defense.gov News Release,* 3 de noviembre de 2010.

[50] U.S. Cyber Command: *U.S. Cybercom Tri-fold*, 19 de octubre de 2010.

[51] U.S. Army Cyber Command: «Army Cyber Command Organization», *(on-line),* en: *http://www.arcyber.army.mil/org-arcyber.html* acceso: 13 de noviembre de 2011.

[52] U.S. Air Force: «24th Air Force - Fact Sheet», abril de 2010, *(on-line),* en: *http://www.24af.af.mil/library/factsheets/factsheet_print.asp?fsID=15663&page=1* acceso: 11 de noviembre de 2011.

[53] United States Navy: «U.S. Fleet Cyber Command/U.S. Tenth Fleet», *(on-line),* en: *http://www.fcc.navy.mil/* acceso: 13 de noviembre de 2011.

[54] U.S. Army: *Cyberspace Operations Concept Capability Plan 2016-2028*, U.S. Army Capabilities Integration Center, 22 de febrero de 2010.

[55] Haller, John; Merrell, Samuel A.; Butkovic, Matthew J. and Willke, Bradford J.: *Best Practices for National Cyber Security: Building a National Computer Security Incident Management Capability, version 2.0*, Software Engineering Institute-Carnegie Mellon University, Pittsburgh, PA 15213, Technical CMU/SEI-2011-TR-015, abril de 2011.

## CAPÍTULO SEXTO

# TECNOLOGÍAS PARA LA DEFENSA EN EL CIBERESPACIO

# TECNOLOGÍAS PARA LA DEFENSA EN EL CIBERESPACIO

Por Manuel Pérez Cortés

> «Es imposible que los viejos prejuicios y hostilidades sigan existiendo, cuando se ha creado tan formidable instrumento para el intercambio de ideas entre todas las naciones de la Tierra» (1).
>
> Comentario sobre el primer cable telegráfico transatlántico, 1858.

## Introducción

La cita que encabeza este capítulo, que tiene más de 150 años, hace referencia a lo que sin duda podríamos llamar primer soporte tecnológico «mundial» del ciberespacio, el primer cable telegráfico transatlántico. Refleja una visión, si se quiere un tanto ingenua, pero en todo caso optimista de las ventajas que, se pensaba, proporcionaría a la humanidad, «todas las naciones de la Tierra» en expresión grandilocuente y solemne, el «ciberespacio».

A pesar de que las cosas no han ido exactamente según los deseos de los autores anónimos de la cita, y una visión más realista o pesimista del

(1) «What the Internet cannot do», *Economist*, 19 de agosto de 2000, citado por Cornish, Paul; Livingstone, David; Clemente, Dave and Yorke, Claire: *On Cyber Warfare, A Chatham House Report,* noviembre de 2010.

ciberespacio lo puede identificar como un escenario más para el desarrollo de conflictos, como se analiza en profundidad en capítulos previos, no es menos cierto que las ventajas y avances positivos que plantea en numerosos aspectos, que es innecesario enumerar, hacen que esa concepción optimista y esperanzadora de elemento esencial de cohesión mundial, como medio que permita superar los «viejos prejuicios y hostilidades», deba mantenerse y retenerse.

La tecnología es la base del ciberespacio, y también sobre la que se apoyan las principales amenazas de éste y en éste. Un enfoque aséptico tecnológico del ciberespacio da cabida a las dos visiones previas, tanto la pesimista como la optimista. Tan cierto es que las amenazas crecen, se especializan y sofistican sus métodos de manera continua, como que las ventajas que aporta el ciberespacio, y las herramientas de defensa de las que se dispone, y no sólo tecnológicas, permiten asegurar que este es un medio irrenunciable que establece un nuevo paradigma de cohesión mundial.

Así pues, este capítulo presenta una visión, necesariamente parcial por lo extenso e impreciso de sus límites y porque éstos avanzan de manera continua e imparable, de cuáles son los elementos tecnológicos principales que intervienen en la arquitectura del ciberespacio, cómo muchas amenazas se apoyan en dichos elementos para organizar los ataques y también cómo la tecnología y las buenas prácticas permiten luchar contra esas amenazas. Se estructura en los siguientes apartados:

– Concepción tecnológica del ciberespacio, enfatizando en la perspectiva militar de dicha concepción tecnológica, y cómo la infraestructura tecnológica que se ha desarrollado para el ciberespacio es la misma que se utiliza para las operaciones militares en red, todo ello asociado al concepto de interoperabilidad de los sistemas.
– Cómo se estructura un ataque en el ciberespacio y cuáles son las amenazas desde un punto de vista técnico, asociado a las vulnerabilidades de los sistemas, con una breve descripción de algunas de las más conocidas.
– Cuáles son las tecnologías que se utilizan para la prevención de las amenazas.
– Cuáles son las tecnologías que se utilizan para la detección de las amenazas, la respuesta y la recuperación.
– Cuáles son algunas de las herramientas, metodologías y normas disponibles relacionadas con el ámbito de la seguridad en el ciberespacio.

## Concepción tecnológica del ciberespacio

Frente a otras concepciones más conceptuales, organizativas, filosóficas, legales, sociológicas, psicológicas, de relaciones internacionales, etc., algunas de las cuales se abordan en detalle en otros capítulos de la presente *Monografía*, desde un punto de vista estrictamente tecnológico el ciberespacio serían las infraestructuras técnicas de un conjunto interconectado de redes de información, tanto públicas como privadas, incluyendo Internet. Ello incluye los enlaces físicos y protocolos y controladores de *comunicaciones*, los sistemas de *ordenadores*, entendidos éstos en un sentido amplio tanto de propósito general como de usos específicos y empotrados, el *software* instalado y los datos con *información* depositada (2). La complejidad de esta infraestructura global va aumentando desde distintos puntos de vista con el paso del tiempo, al menos por los siguientes aspectos (3):

– Por su extrapolación a nuevas redes en la que se incluyen otros tipos de dispositivos distintos de los «ordenadores», como teléfonos inteligentes (4), televisores, electrodomésticos, etc.
– Por la interconexión con las redes de propósito general del ciberespacio de otras redes de propósito específico. Entre ellas conviene mencionar, por ejemplo, los Sistemas de Control Remoto para la supervisión y el mantenimiento de sistemas industriales (Sistemas de Control SCADA, etc.), en algunos casos asociados a infraestructuras críticas (5) de distribución de energía, de telecomunicaciones, etc.
– Por la tendencia creciente a la descentralización de los recursos propios de cálculo y almacenamiento, de manera que también estos residan de manera compartida en la red *(Cloud Computing)* (6).
– Por la tendencia creciente a que no sólo las personas, sino también las cosas interactúen a través de red (Internet de las cosas, IoT) (7), por

(2) Winterfeld, Steve (dir.): *Understanding Today's Cyber Challenges:* Technology TASC, mayo de 2011.
(3) Jabbour, Kamal ST Senior Scientist: *The Science and Technology of Cyber Operations,* Information Assurance Air Force Research Laboratory, Information Directorate Rome, Nueva York, 2011.
(4) NTECO: Informe de vulnerabilidades y amenazas en dispositivos Iphone, Ipad, enero de 2011.
(5) Saadawi, Tarek and Jordan, Louis jr. (edit.): *Cyber infrastructure protection,* SSI *(Strategic Studies Institute),* 2011.
(6) ENISA*: Cloud Computing-Benefits, risks and recommendations for information security,* 2009.
(7) Saalbach, K. doctor: *Cyber War- Methods and Practice,* versión 3.0, 2011.

ejemplo, mediante distintos tipos de dispositivos RFID, con su propia dirección Protocolo de Internet (IP), etc.

Sobre todas o alguna de las distintas partes de esta infraestructura técnica que, en resumen, incluye comunicaciones de largo o corto alcance, ordenadores junto con el concepto más genérico de dispositivos inteligentes en sentido amplio, *software* y datos se pueden realizar acciones, entre otras cosas, para defenderla, atacarla o explotarla. Responden dichas acciones al concepto militar de las llamadas Operaciones sobre Redes de Ordenadores, CNO *(Computer Network Operations),* entendidos dichos «ordenadores» en el sentido amplio previamente esbozado, que incluye:

– Explotación de redes de ordenadores, CNE *(Computer Network Exploitation)*, que es la habilidad para acceder a la información guardada en un sistema de información, y la capacidad de hacer uso del propio sistema.
– Ataque a redes de ordenadores, CNA *(Computer Network Attacks),* que es el uso de técnicas novedosas para entrar en las redes de ordenadores y atacar los datos, los procesos o el *hardware*.
– Defensa de redes de ordenadores, CND *(Computer Network Defence)*, que es la protección frente a enemigos de la explotación o ataque a nuestras redes de ordenadores CNE y CNA.

Aunque es fácil separar, a efectos de discusión y análisis, los tres conceptos anteriores, por supuesto no son excluyentes entre sí y lo normal es que se solapen (8). En la mayor parte de las ocasiones es necesario combinar el ataque (CNA) para ejercer una mejor defensa (CND), junto con la disponibilidad de datos de inteligencia (CNE), y ello tanto en el mundo real como en el ciberespacio.

Si tanto en el campo civil como en la vida cotidiana la presencia del ciberespacio y las operaciones en red es cada vez más habitual, también lo es en el ámbito militar, tanto para los Sistemas de Mando y Control como Sistemas de Armas que se manejan, concebidos éstos en general como sistemas de sistemas (9). Un aspecto de particular relevancia para los

(8) Bernier, Melanie and Treurniet, Joanne: *Understanding Cyber Operations in a Canadian strategic context: more than C4ISR, more than CNO,* 2010.

(9) En otro capítulo de esta *Monografí*a se detallan las actividades en este campo de distintas organizaciones internacionales del ámbito de la defensa. Como información adicional indicar que el año 2010 la Agencia Europea de Defensa (EDA) sacó a concurso un estudio sobre operaciones militares en red, que adjudicó a la empresa GMV.

sistemas militares, sobre todo por el tipo de operaciones colaborativas entre ejércitos de distintos países y organizaciones que se abordan cada vez más habitualmente, es el de interoperabilidad, que incide de manera directa en la seguridad de las redes militares. La interoperabilidad no es una característica que se le exija de manera creciente exclusivamente a los sistemas militares, que permita que técnicamente puedan operar de manera conjunta, sino que, simplificando mucho el concepto, respondería a la visión militar de la idea de normalización de otros ámbitos tecnológicos.

A pesar de que es un elemento crítico para las operaciones militares y los sistemas de información militares, la interoperabilidad debe ser entendida como uno de los varios atributos técnicos de cualquier sistema de sistemas. Pero no es el único. De hecho debe buscarse un adecuado equilibrio con otros atributos, que a veces entran en competencia, si no en conflicto, con la interoperabilidad. Por ejemplo, debe encontrarse el equilibrio entre la seguridad y la interoperabilidad. La necesidad de interoperabilidad puede simplificar el acceso de un atacante a diversos sistemas, lo que facilita la rápida propagación de los ataques. Otro aspecto tener en cuenta es el problema que puede plantear a la interoperabilidad la introducción de nuevas características de seguridad, en el marco de un sistema de sistemas. Así, centrándose en la funcionalidad general del sistema y su rendimiento, los requisitos clásicos de seguridad tales como la confidencialidad, autenticación, no repudio, integridad y disponibilidad del sistema, deben considerarse conjuntamente con la interoperabilidad.

El hecho de aumentar la confianza en las tecnologías de la información para las operaciones militares, aumenta también el valor de las infraestructuras de información militar y, con ello, los Sistemas de Información y el ciberespacio se convierte cada vez más en un objetivo militar. Por tanto, para que cualquier organización militar obtenga los beneficios que proporciona un mayor uso de los Sistemas de Armas en Red y los Sistemas de Información Militar (C4I), debe asegurar que esos Sistemas están suficientemente bien protegidos contra los ataques de posibles intrusos.

Como se ha indicado previamente, el máximo beneficio de los Sistemas C4I se deriva de su capacidad de interoperabilidad y la integración entre ellos. Es decir, para actuar con eficacia, los Sistemas C4I deben estar interconectados para que puedan funcionar como parte de un sistema más grande de sistemas. Estas interconexiones electrónicas

multiplican muchas veces las posibilidades técnicas de un adversario para atacarlas.

El mantenimiento de la seguridad de los Sistemas C4I es un problema de dos dimensiones. La primera dimensión es física (10). Consiste en la protección física de los ordenadores y enlaces de comunicaciones, así como de las instalaciones de mando y control, para evitar el que sean atacadas o destruidas. Para esta tarea, en el ámbito militar se tiene una gran experiencia, que se aplica tanto a las instalaciones fijas como a los sistemas desplegados en campo. El militar sabe en qué lugares clave debe desplegar los nodos del Sistema C4I para que estén bien protegidos, añade además vigilancia y otros mecanismos de control de acceso para impedir el sabotaje. En el entorno militar también se sabe muy bien cómo desplegar y utilizar los enlaces de comunicaciones inalámbricas para que el posible *jamming* del enemigo sea una amenaza menor.

Por el contrario, la segunda dimensión, que es preservar la seguridad de la información de los sistemas, es una tarea con muchas más aristas (11). La protección de la seguridad de la información de de los sistemas –la tarea de proteger los Sistemas C4I conectados a la red de comunicaciones contra el ataque a la información de un adversario– es un área mucho peor entendida que la seguridad física. Dentro de la industria de las tecnologías de la información, el término «seguridad de la información» incluye las medidas técnicas y de procedimiento que preservan la confidencialidad, la autenticación, la integridad de datos, el no repudio, así como aquellas medidas que incrementan la resistencia a los ataques de denegación de servicio.

El problema general de la protección de los Sistemas de Información, y en particular los Sistemas C4I militares, contra ese tipo de ataques es enormemente complicado por el hecho de que, muy a menudo, los sistemas y las redes a las que están conectados no son independientes de las infraestructuras nacionales de información. De hecho, la línea de separación entre ambos es bastante borrosa debido a que, cada vez más a menudo, muchos sistemas militares hacen uso de las infraestructuras

(10) La dimensión física no es objeto de este capítulo, aunque ambas están íntimamente interrelacionadas. *Véase,* por ejemplo, Frontier, High: *Journal for Space & Missile Professionals,* volumen 5, número 3, mayo de 2009.

(11) El problema presenta más complejidad que el de protección de infraestructuras críticas. *Véase,* por ejemplo, Saadawi, Tarek and Jordan, Louis Jr. (edits.): *Cyber infrastructure protection,* SSI, 2011.

de información civil, y además los sistemas militares y civiles están en muchas ocasiones interconectados, intercambiando información.

Un problema que cada vez con más frecuencia van a tener las redes militares es el de depender de los componentes de una infraestructura sobre la cual en parte no tienen el control. Por último, los Sistemas C4I están cada vez más desarrollados sobre tecnologías comerciales y Sistemas COTS y, por lo tanto, sufren el mismo conjunto básico de vulnerabilidades que se observan en el sector comercial.

En relación con los dos aspectos mencionados previamente, al ser el mercado de los componentes de las infraestructuras cada vez más global, se plantea un complejo problema: garantizar que la cadena de suministros de componentes no incluye ninguno ya dotado de vulnerabilidades intencionadas (puertas traseras, etc.) para ser explotadas por organizaciones gubernamentales u otro tipo de organizaciones en un futuro (12). Esto es especialmente crítico para redes en las que se manejen datos muy sensibles o críticos, como pueden ser algunas redes militares o gubernamentales.

## Los ataques y las amenazas

En julio de 2011 Willian Lynn, *deputy* del secretario de Defensa de Estados Unidos, reveló que un «gobierno extranjero no especificado» había sido el responsable del robo de 24.000 archivos de una red de ordenadores relacionada con defensa (13). Hacía esta afirmación para anunciar un plan del Pentágono para protegerse activamente ante esta clase de ataques. En el plan se afirma que cada año se roba en redes gubernamentales y del sector privado un volumen de propiedad intelectual mayor que la Biblioteca del Congreso. En paralelo Michael Mullen, *parallel US Joint Chiefs of Staff Chairman Adm*., ha declarado que:

> «*The single biggest existential threat that's out there, I think, is cyber*» (14).

(12) Winterfeld, Steve (dir.): *Understanding Today's Cyber Challenges,* Technology TASC, mayo de 2011.

(13) En: *http://www.c-span.org/Events/Pentagon-Reveals-Computer-Attack-by-Unspecified-Foreign-Government/10737422869-1/*

(14) En: *http://www.dailytech.com*

En el ámbito militar, los ataques se dirigen tanto a las redes gubernamentales como a los contratistas de defensa. Por ejemplo, el sistema de armas más costoso de la historia, el JSF *(Joint Strike Fighter)*, ha sido recientemente objeto de un ataque a las instalaciones del contratista principal. Un grupo ciberterrorista, llamado *AntiSec*, ha anunciado que ha entrado en las redes del contratista y robado 90.000 direcciones de *e-mail* militares y contraseñas.

También se pueden describir ataques durante operaciones militares. En septiembre de 2007, durante una operación realizada por la Fuerza Aérea de Israel, parte del Sistema de Defensa Aérea de Siria fue neutralizado mediante el uso de cibertácticas. Se cree que había *malware* embebido en el *software* de los rádares sirios (15).

Estos ejemplos, y otros muchos, muestran que las amenazas en el ciberespacio y la necesidad de una ciberdefensa militar son una realidad. Algunos aspectos a considerar respecto a las ciberamenazas son los siguientes:

– La ubicuidad de Internet y su facilidad de uso la hacen muy vulnerable a la infiltración, la explotación y el sabotaje.
– Los ataques en el ciberespacio pueden requerir muy poco equipamiento y esfuerzo, proporcionando a países pequeños o con pocos recursos, a grupos terroristas e incluso individuos aislados la capacidad de provocar conflictos con unos daños y unas consecuencias que hasta ahora estaban reservados sólo para las grandes potencias.
– Los ciberataques pueden amenazar a cualquier sistema de ordenadores que esté conectado a una red exterior.
– El origen de los ciberataques puede ser muy dificultoso de trazar, lo que dificulta la atribución definitiva. Por ello, un elemento esencial en el paradigma de la defensa, el establecimiento de medidas de disuasión (16), todavía no funciona adecuadamente en el ciberespacio.
– El número de amenazas aumenta diariamente, y la ventana de tiempo para luchar contra ellas se contrae de manera continua.
– Las herramientas de los *hackers* son cada vez más sofisticadas y poderosas.
– Los métodos de ataque tanto para obtener beneficios económicos como para acceder a secretos militares se han desarrollado en para-

(15) Marke, John: *Operation «Orchard We Have Crossed Into Syrian Airspace»,* 2010.
(16) Libicki, Martin C.: *Cyberdeterrence and cyberwar,* Rand Corporation, 2009.

lelo, al ser las tecnologías implicadas las mismas. Es sólo el propósito del atacante el que diferencia unos ataques de los otros.
– Es cierto que en este momento, en cierto modo, la situación es de ventaja del ataque sobre la Defensa. Los atacantes sólo necesitan encontrar una vulnerabilidad en la Red para acceder a su interior, mientras que la defensa implica asegurar todas las vulnerabilidades. No obstante se está avanzando mucho en el campo de la protección de redes como se irá viendo a lo largo de este capítulo.
– Los expertos indican que el 80-85% de los ciberataques pueden ser neutralizados si se aplican buenas prácticas de manera efectiva. Amenazas más avanzadas APT *(Advanced Persistent Threat)*, representan el otro 15-20%. La mayor parte de los ataques APT se considera que sólo pueden venir de una lista corta de países.

Siguiendo el enfoque técnico de este capítulo, los ataques a las infraestructuras del ciberespacio y, por tanto, las amenazas de las que deben ser protegidas, se pueden agrupar en dos grandes categorías (17):

– Por una parte, está la propia anulación física de las infraestructuras (redes de comunicaciones, ordenadores, etc.). Dentro de esta categoría se incluye tanto la destrucción real (o el robo) de los elementos hardware, como también su inutilización física mediante, por ejemplo, pulsos electromagnéticos de gran potencia que imposibiliten el funcionamiento de componentes electrónicos como transistores, etc. Este es un riesgo en el que no se profundiza en lo que sigue en el presente capítulo. La forma de afrontarlo es con medidas de protección física o perimetral de las instalaciones donde se encuentra los elementos susceptibles de ser saboteados, la instalación de éstos en el interior de jaulas de Faraday, etc.
– Por otra, está la manipulación de los ordenadores o redes, bien insertando y activando software con un propósito malicioso en los primeros, o perturbando o anulando las capacidades de comunicación de las segundas. Este tipo de amenazas y los ataques asociados son los que abordamos a continuación.

Las distintas etapas que suelen presentarse durante la ejecución de un ataque en el ciberespacio, son las que se plantean a continuación (18). Por supuesto, en función del tipo de ataque la importancia

(17) Convertino II, Sebastian M. *et alt.: Flying and Fighting in Cyberspace,* julio de 2007.
(18) Saalbach, K. doctor: *Cyber War- Methods and Practice,* versión 3.0, 2011.

o relevancia de alguna de estas etapas es muy distinta, y algunas de ellas pueden ni llevarse a cabo, bien porque no son necesarias en función de la naturaleza del ataque, o porque el atacante puede que no se atreva o no tenga capacidad y conocimientos para atravesar ciertas «líneas rojas»:

1. *Recoger datos en la Red de los objetivos a ser atacados:* el origen de los datos y la forma de obtención de los mismos puede ser muy variada: localizaciones, números de teléfono, trazas de búsquedas en buscadores, noticias e informaciones en las redes sociales y foros, ingeniería social con empleados, etc.
2. *Escanear sistemáticamente los sistemas*: durante esta fase se hace una búsqueda sistemática de posibles vías de acceso en el sistema a ser atacado: puertos, sistemas operativos. Parte de estos procesos se pueden realizar de manera automatizada con probetas, *software* de escaneado de puertos, etc.
3. *Ganar el acceso:* el escaneado sistemático de la etapa anterior puede permitir, una vez identificadas las potenciales vulnerabilidades, el acceso al sistema objeto de ataque. Entre los posibles métodos para ganar el acceso estarían:
   - La utilización de las brechas de seguridad, oficialmente conocidas o no, en los sistemas operativos *(Windows)*, en los dispositivos de red (cortafuegos, routers, etc.) y en los programas de *software* (navegadores, etc.).
   - El empleo de ingeniería social para obtención de determinados datos como contraseñas de acceso basándose en prácticas poco seguras de la organización.
   - La obtención de contraseñas de acceso, por ejemplo mediante prueba y error sistemático (fuerza bruta).
   - El empleo de código malicioso (*malware*) recibido, por ejemplo, como adjunto de un correo electrónico o en la visita a un portal *web*.
4. *Aumentar los privilegios:* cuando se dispone de privilegios de usuario, ello permite leer y escribir datos para ese usuario, además de poder ejecutar determinadas aplicaciones; pero si se obtiene, aumentando los privilegios, una cuenta de administrador, se puede leer y escribir sobre cualquier dato, además de poder ejecutar todas las aplicaciones del sistema. Además, el aumento de privilegios puede permitir la instalación de puertas traseras, que serán explotadas posteriormente, o la obtención de ficheros de contraseñas y su craqueado en una fase posterior.

5. *Explotar los sistemas:* una vez obtenidos los privilegios necesarios el sistema de puede explotar con el propósito malicioso de interés: desde manipular de alguna forma la información (espiarla, alterarla, borrarla, etc.), hasta utilizarlo para lanzar ataques a otros sistemas.
6. *Ciberguerra* (19)*:* respondería al concepto de un ataque sistemático al más alto nivel, incluyendo ataques de denegación de servicios críticos con el empleo de *botnets*, la mutilación de sitios *web*, el daño a los sistemas, la intrusión en infraestructuras críticas, etc.
7. *Denegar el servicio:* la denegación de servicio, que se describe posteriormente con algo más de detalle, es un tipo de ataque que puede no exigir el acceso al sistema a ser atacado y, por tanto, no es necesario cubrir las etapas anteriores, sino que simplemente éste se satura con peticiones espurias para ralentizar o impedir el uso de los usuarios legítimos.

En un ataque en el ciberespacio, se pueden presentar algunas o todas las fases anteriores dependiendo de cuál sea la fuente de la amenaza, su intencionalidad, las motivaciones que le mueven a realizar el ataque, la capacidad técnica y el nivel de información del que dispone, etc. Tradicionalmente las distintas fuentes de amenaza, sus motivaciones y las acciones que típicamente realizan se han clasificado en los grupos principales que se recogen en el cuadro 1, pp. 266-267.

Sin, ni con mucho, pretender ser exhaustivo algunos de los tipos de amenazas que, desde un punto de vista tecnológico, se presentan en el ciberespacio son las siguientes (20):

1. *Abuso de los privilegios de acceso:* dentro de la Red, cada usuario cuenta con un nivel de privilegios para un propósito específico. Cuando los usuarios abusan de alguna manera de este nivel de privilegios que se les han fijado, y llevan a cabo tareas que no son de su responsabilidad puede producirse un problema de confidencialidad. Normalmente, el acceso a las distintas partes de los sistemas está protegido mediante claves de acceso u otros sistemas de identificación (tarjetas, biometría, etc.) y métodos que facilitan las aplicaciones, y que se configuran en función de las prácticas de la organización.

---

(19) Cornish, Paul; Livingstone, David; Clemente, Dave and Yorke, Claire: *On Cyber Warfare, A Chatham House Report,* 2010.

(20) OCDE: Software *malicioso* (malware) *una amenaza de seguridad para la economía de Internet,* 2008.

**Cuadro 1.—** *Fases de un ataque en el ciberespacio.*

| Fuente de la amenaza | Motivación | Acciones |
|---|---|---|
| *Hacker, cracker* | – Desafío<br>– Ego<br>– Rebelión | – *Hacking*<br>– Ingeniería social<br>– Intrusión en los sistemas, robos<br>– Acceso no autorizado al sistema |
| *Delincuente informático* | – Destrucción de información<br>– Divulgación de información<br>– Ganancias económicas<br>– Alteración no autorizada de datos | – Delitos informático<br>– Acciones fraudulentas<br>– Soborno<br>– *Spoofing*<br>– Intrusión en los sistemas |
| *Terrorista* | – Chantaje terrorista<br>– Destrucción<br>– Explotación<br>– Venganza | – Bomba-terrorismo<br>– Guerra de la información<br>– Ataque a los sistemas (por ejemplo, la denegación de servicio distribuido)<br>– Penetración en los sistemas<br>– Manipulación de los sistemas |
| *Espionaje industrial* (empresas, gobiernos extranjeros, otros intereses del gobierno) | – Ventaja competitiva<br>– Espionaje económico | – Explotación económica<br>– Robo de información<br>– Intrusión en la intimidad personal<br>– Ingeniería social<br>– Penetración en los sistemas<br>– Acceso no autorizado a los sistemas (acceso a información clasificada, propietaria, y/o relacionadas con la tecnología) |

**Cuadro 1.—** *(Continuación).*

| Fuente de la amenaza | Motivación | Acciones |
|---|---|---|
| *Insiders* (personal con mala formación, descontento, malicioso, negligente, deshonesto, o empleados despedidos) | – Curiosidad<br>– Ego<br>– Inteligencia<br>– Ganancia económica<br>– Venganza<br>– Errores y omisiones no intencionadas (por ejemplo, error en la entrada de datos, errores de programación) | – Asalto a un empleado<br>– Chantaje<br>– Exploración de información propietaria<br>– Abuso en el uso de los ordenadores<br>– Fraude y robo<br>– Información para soborno<br>– Entrada de datos falsos o dañados<br>– Intercepción<br>– Código malicioso (por ejemplo, virus, bombas lógicas, «caballos de Troya»)<br>– Venta de información personal<br>– Errores del sistema<br>– Intrusión al sistema<br>– Sabotaje del sistema<br>– Acceso no autorizado al sistema |
| | | |

2. *Mal uso de los recursos de los sistemas*: consiste en el uso de los recursos del sistema para fines no establecidos, generalmente de interés particular: juegos, búsquedas personales en Internet, bases de datos particulares, programas particulares, etc.
3. *Ordenadores infectados por* botnet: una *botnet* es una colección de agentes de *software*, o robots, que funcionan de forma autónoma y automática. Las *botnets* son explotados con fines diversos, incluidos los ataques de denegación de servicio, la creación o el mal uso de transmisiones de correo SMTP no deseado, fraude; el robo, entre otros, de números de serie de aplicaciones, los Sistemas de Detección de Intrusos (IDS) de inicio de sesión e información financiera como números de tarjetas de crédito, etc. Dos amenazas que han tenido gran impacto en los últimos meses han sido Zeus y Koobface. ENISA (21) indica que en los años 2009 y 2010, dos redes de *bots* de espionaje se exploraron en profundidad, GhostNet y Shadow Network. Las investigaciones de GhostNet llevaron al descubrimiento de 1.295 máquinas infectadas en 103 países, con alrededor del 30% de las máquinas infectadas consideradas como de alto valor, ya que se encontraban en instituciones gubernamentales, incluyendo equipos informáticos de varias embajadas y ministerios. McAfee Labs predice que la reciente fusión de Zeus con SpyEye producirá bots más sofisticados gracias a las mejoras en burlar mecanismos de seguridad. Además, los laboratorios de McAfee esperan ver un incremento significativo en la actividad de *botnet* para recogida y borrado de datos, más que para el uso que tradicionalmente se le ha dado, que es el envío de *spam*. El predominio de *botnets* para ciberataques se basa en que:
   – Normalmente los *botnets* no están localizados en el país del atacante, lo que dificulta enormemente el proceso de atribución del ataque.
   – Proporcionan unas grandes capacidades de computación, lo que garantiza la efectividad del ataque.
   – Permiten ataques a objetivos especificados, al contrario que virus o gusanos que se expanden sin control.
   – El *software botnet* puede implementarse en cada ordenador específico, por lo que no es posible proteger un sistema excluyendo sólo algunos grupos de ordenadores.

(21) En: *http://www.enisa.europa.eu/*

4. Troyano-*sypware*: un troyano o «caballo de Troya», es un *software* que parece desempeñar una función deseada por el usuario antes de ser ejecutado o instalado, pero cuyo propósito final es robar información o causar daños en el sistema. Una vez que el troyano ha sido instalado en un equipo, un *hacker* pueda tener acceso al ordenador de forma remota y realizar diversas operaciones, limitadas por los privilegios de acceso que obtenga en el equipo de destino y por el propio diseño del troyano. Por la popularidad de los *botnets* entre los *hackers* y la publicidad, los troyanos son cada vez más accesibles. En general, el *spyware* es un tipo de *malware* que se instala en los ordenadores, normalmente de forma inadvertida para el usuario, y que recoge pequeños fragmentos de información sobre los usuarios sin su conocimiento. La presencia de *spyware* no es conocida por el usuario, y puede ser difícil de detectar.
5. *Gusanos y virus:* un gusano informático es un programa de *malware* para ordenador, autoreplicante, que utiliza una red de ordenadores para enviar copias de sí mismo a otros nodos de la red. Esto puede hacerlo sin la intervención del usuario. Los gusanos siempre causan daños en la red, aunque sólo sea por el consumo de ancho de banda, además los virus casi siempre corrompen o modifican los archivos en el equipo en el que se aposentan. La diferencia entre troyanos, gusanos y virus es la siguiente, partiendo siempre de la base de que es un código con un propósito malicioso:
   – Si el código no se replica se entiende que es un troyano.
   – Si se replica, pero no infecta o causa daños importantes en los ordenadores portadores, se dice que es un gusano.
   – Si además de replicarse infecta los ordenadores portadores es un virus.
6. *URL (Uniform Resource Locator) malicioso*: la manipulación de URL, también llamado reescritura de direcciones URL, es el proceso de alterar (a menudo de forma automática mediante un programa escrito para tal fin) los parámetros en una dirección URL. La modificación de URL se puede emplear, de manera adecuada por el administrador de un servidor *web*, o para propósitos maliciosos por un *hacker*. Sophos destaca que durante el año 2010 han aparecido cada día 30.000 nuevas URL maliciosas. Eso significa aproximadamente una cada dos o tres segundos. Los 10 principales países anfitriones de URL maliciosas en el año 2010 fueron Estados Unidos 39,39%; Francia 10,00%; Rusia 8,72%; Alemania 5,87%; China 5,04%; 2,68% del Reino Uni-

do; Polonia 2,43%; Canadá 2,03%; Ucrania 1,97%; Hungría 1,84%; otros 20,03%.

7. *Reenrutamiento de mensajes*: esta amenaza se refiere al envío de determinada información a un destino incorrecto a través de un sistema o red. Pueden ser mensajes entre personas, entre procesos o entre ambos. Un atacante puede forzar que un mensaje viaje a través de un nodo específico en la red donde puede ser interceptado y de ahí transmitido al lugar que desea el atacante. Especialmente importante es el caso en que el ataque de enrutamiento provoca una entrega fraudulenta y, por ejemplo, información clasificada llega a las manos de una persona no autorizada.
8. *Alteración de secuencia*: consiste en la alteración del orden de los mensajes enviados. La idea es que el nuevo orden cambia el significado del grupo de mensajes y perjudica la integridad de los datos afectados.
9. *Acceso no autorizado*: el atacante logra acceso a los recursos del sistema sin autorización. Para hacerlo normalmente aprovecha un fallo en el sistema de identificación y/o autorización, ya sea un fallo de tipo técnico o mediante ingeniería social. El acceso no autorizado a información confidencial causa la mayor parte de las brechas graves en seguridad, como la pérdida de información confidencial, el fraude financiero y los ataques de denegación de servicio.
10. *Espionaje*: los atacantes tienen acceso a información que no es de ellos, sin que se modifique dicha información. El espionaje es el acto de escuchar en secreto la conversación privada de otras personas sin su consentimiento o la consulta de datos y mensajes. Se puede hacer a través de líneas telefónicas (escuchas telefónicas), correo electrónico, mensajería instantánea, y otros métodos de comunicación considerados privados.
11. *Alteración de la información*: se refiere a la alteración intencionada de la información para obtener un beneficio o causar daños.
12. *Entrada de información falsa*: se refiere a la entrada deliberada de información falsa, en un sistema o en el ciberespacio, para obtener un beneficio o causar daños.
13. *Destrucción de la información*: esta amenaza consiste en la supresión deliberada de la información, para obtener un beneficio o también causar daños.
14. *Divulgación de información*: esta amenaza de revelación de información implica la exposición de información a personas que se supo-

ne que no tienen acceso a ella, ni derecho a conocerla. Uno de los acontecimientos más notables y recientes en este ámbito ha sido *Wikileaks*, que siguió adelante con su promesa de revelar más de 250.000 comunicados diplomáticos clasificados, que abarca cuestiones como el programa nuclear de Irán, o las relaciones entre Estados Unidos y sus aliados europeos

15. *Detección de posición*: esta amenaza se refiere al proceso de detección de la ubicación física de un dispositivo remoto y, por añadidura, de otros elementos asociados al mismo: personas, vehículos, instalaciones, etc. Geolocalización es la identificación de la ubicación geográfica en el mundo real de un objeto con sistemas como el radar, Sistema de Posicionamiento Global (GPS), el teléfono móvil o un terminal de ordenador conectado a Internet. ENISA indica en un estudio reciente que la mayoría de las personas no son conscientes del hecho de que las fotos y videos tomados con sus teléfonos inteligentes o cámaras contienen información de geolocalización. Esta información puede ser utilizada para localizarles mientras están de viaje, o incluso revelar su dirección. Esto puede ser considerado como una fuente potencial de fuga de información y puede dar lugar a una violación de la privacidad si se utiliza para hacer seguimientos, o se obtiene con datos online recogidos de redes sociales. Además, ENISA señala que un número creciente de sitios proveen API *(Appliation Programming Interface)* públicas para realizar geolocalización. Por ejemplo, *Flickr*, *YouTube*, *Twitter* incluyen este tipo de API para poder realizar consultas de los resultados que se originan en un determinado lugar. *PicFog* utiliza una de estas API para facilitar la búsqueda basada en la localización en tiempo real de imágenes publicadas en *Twitter*. McAfee Labs predice que los cibercriminales harán cada vez más uso de estas técnicas a través de los sitios de las redes sociales más populares.
16. *Hacktivismo*: es el acto de piratería informática, o el acceso a un sistema informático en general motivado por una finalidad política o social. El *hacktivista* utiliza las mismas herramientas y técnicas que un *hacker*, pero lo hace con el fin de interrumpir los servicios y llamar la atención sobre una causa política o social.
17. *SQL (Ataque de inyección)*: es una técnica de inyección de código que explota una vulnerabilidad de seguridad que se presente en la capa de base de datos de alguna aplicación. Se trata de un caso particular de una clase más general de vulnerabilidades que puede ocurrir cuando un fragmento de programación está incrustado den-

tro de otro, por ejemplo para crear una puerta trasera que permita en el futuro el acceso al sistema, o la activación de una bomba lógica. McAfee indica que: China, Estados Unidos, Irán, Alemania, Vietnam, República Checa, Ucrania, Rusia, Brasil e Indonesia se encuentran en el top 10 en la manipulación del *software*.

18. *Inyección del Protocolo Compacto de Acceso a Directorio, LDAP (Lightweight Directory Access Protocol)*: la inyección LDAP es un ataque para aprovechar las aplicaciones basadas en *web* que construyen sentencias LDAP a partir de las entradas del usuario. Cuando una aplicación falla al limpiar de forma adecuada la entrada del usuario, es posible modificar las declaraciones LDAP usando un *proxy* local. Esto puede permitir la ejecución de comandos arbitrarios, como la concesión de permisos a consultas no autorizadas y la modificación de contenidos dentro del árbol LDAP.
19. *Ataques de virtualización*: la virtualización (también conocida como *Cloud Computing)*, consiste en el acceso a las aplicaciones y/o a los datos y/o a los recursos de computación a través de internet, lo que facilita la rápida disponibilidad y movimiento virtual de máquinas en las organizaciones. Por supuesto, este enfoque en red abre un abanico todavía no totalmente explorado de potenciales amenazas. Existen, básicamente, tres modelos de virtualización:
    - *Software* como un servicio (SaaS): el usuario accede a las aplicaciones que están en la Red.
    - Plataforma como un Servicio (PaaS): el usuario usa la nube como un entorno para ejecutar aplicaciones. En este caso el usuario controla las aplicaciones, pero no el sistema operativo, o el *hardware* en el que éstas se ejecutan.
    - Infraestructura como un Servicio (IaaS): es el más alto nivel de abstracción. El usuario, en lugar de disponer de servidores, memoria, medios de almacenamiento, equipos de red, *software*, etc. propios, accede, cuando lo necesita, a los recursos que le proporciona un tercero a través de la Red.

Es evidente que la virtualización plantea grandes ventajas, sin embargo, debe asegurarse de que se han implementado y puesto en práctica los controles de seguridad adecuados para las Máquinas Virtuales (VM), y se cumplen los requisitos y las políticas de seguridad de la organización. Los avances en la tecnología de virtualización también han dado lugar a nuevos métodos para atacar y penetrar en las redes. Uno de los más comunes entre este tipo de ataques en los entornos virtuales es la

tecnología *Hyper-Jacking*. Otro tipo de ataque es escapar de la VM, lo que puede causar grave amenaza a la seguridad. El código del atacante rompe el sistema operativo de la máquina virtual e interactúa directamente con el hipervisor. Con este tipo de ataque se pueden descubrir otras VM y, finalmente, hacerse con el control de todo el entorno virtual. La caza furtiva de VM es un proceso similar a un ataque de denegación de servicio. El objetivo del atacante es sobrecargar el hipervisor y saturar todos sus recursos.

1. *Bypass de la autenticación*: el *bypass* de la autenticación consiste en el acceso al sistema evitando la autenticación estándar. Esto permite al atacante realizar alguna acción que quien diseñó la aplicación restringió sólo para los usuarios autenticados. Con el uso de estas técnicas, un atacante puede, por ejemplo, controlar una aplicación *web* específica en remoto sin perder el tiempo también en el craqueo de contraseñas.
2. *Denegación de servicio*: en muchas ocasiones un sistema puede fallar cuando la carga de trabajo es demasiado alta, por falta de recursos. Un ataque de denegación de servicio o ataque distribuido de denegación de servicio es un intento de hacer que un recurso del ordenador no esté disponible para sus usuarios legítimos. Aunque los medios para llevarlo a cabo, los motivos, y los objetivos de un ataque de denegación de servicio pueden variar, por lo general consiste en impedir que un sitio de Internet o un servicio dejen de funciona de manera eficiente, o no funcionen en absoluto, temporal o indefinidamente. Un método común de ataque consiste en saturar el equipo de destino con solicitudes de comunicación externa, de tal manera que no puede responder al tráfico legítimo, o responde tan lentamente que a todos los efectos se considere no disponible. Una nueva forma de ciberataque es el ataque distribuido reflejado de denegación de servicio, en el que se envían preguntas a una gran cantidad de ordenadores de Internet (por ejemplo, mediante botnets), que responden a la pregunta, pero a una dirección IP errónea, que es a la que se quiere denegar el servicio.
3. *Infección de unidades, USB (Universal Serial Bus):* el *malware* puede propagarse e infectar nuevas máquinas mediante la infección de cualquier unidad USB que se conecta a un sistema comprometido. Se aprovecha de los archivos vulnerables que se colocan en la unidad USB infectada. Uno de los casos más conocidos en este campo es el del gusano *stuxnet*, que se cree se propagó mediante USB. Está dirigi-

do contra los Controladores Lógicos Programables (PLC) (se cree que sólo los de la marca Siemens), y con el que se ha atacado algunos de los equipos sensibles del programa nuclear iraní. Hay distintas teorías sobre cuál ha sido el origen de este ataque, algunas de las cuales asociadas a los servicios secretos de determinados países.

4. *Ingeniería social:* la ingeniería social se define como el proceso de engañar a la gente para que den claves de acceso o información confidencial, de manera «voluntaria». La ingeniería social es el acto de manipular a la gente a realizar acciones de divulgación de información confidencial, en lugar de hacer un acceso directo ilícito a los ordenadores. Es un tipo de amenaza que se aprovecha de la buena voluntad o la ingenuidad de las personas.
5. *Phishing:* el *phishing* es una técnica fraudulenta de obtención de información privada. Normalmente el phiser envía un *e-mail* que parece venir de un origen legítimo (un banco, una compañía de tarjetas de crédito) indicando la necesidad de alguna «verificación», y las consecuencias graves que tendría el no proporcionar la información solicitada. El correo electrónico suele contener un enlace a una página web fraudulenta que parece legítima, con logotipos de la compañía y un formulario de solicitud de los datos requeridos, como el domicilio o el PIN de una tarjeta.
6. *Motores de búsqueda*: los motores de búsqueda simplifican el proceso de localización de información en el ciberespacio. El mismo mecanismo que ofrece esta capacidad también puede representar una amenaza para muchas organizaciones. McAfee espera un incremento significativo de los ataques, utilizando técnicas basadas en el uso indebido de los motores de búsqueda. Shopos recuerda que una de las amenazas más persistentes del año 2010 fue un falso antivirus. De hecho, se han encontrado más de medio millón de variantes de *software* falso antivirus. Por otra parte, McAfee señala que determinadas utilidades de sistema y utilidades de disco están reemplazando a los antivirus falsos como una de las principales fuentes de ganancias de los ciberdelincuentes.

Un punto objeto de debate es la potencial existencia de puertas traseras, instaladas intencionadamente en los sistemas operativos y/o en el hardware, para permitir el acceso de determinados servicios secretos a los sistemas. Un aspecto importante a tener en cuenta en este punto es la cadena de suministro de los componentes *hardware*. En un mundo globalizado, donde muchos componentes que integran los ordenado-

res proceden de distintos lugares del mundo como: China o Taiwan, la autenticación del *hardware* y *firmware* asociado, y la verificación de que no incluye puertas traseras o bombas lógicas que se puedan activar en determinadas condiciones, no es una tarea fácil.

## La prevención de las amenazas

Una vez asumidas las ventajas de la utilización del ciberespacio, es necesario aceptar que debe convivirse con las amenazas previamente identificadas, y otras más complejas y sofisticadas que irán apareciendo de manera continua con el paso del tiempo. Como se ha explicado previamente, muchas de estas amenazas se basan en la utilización perniciosa de las herramientas y componentes que posibilitan la arquitectura tecnológica del ciberespacio. Para luchar de una manera eficaz contra ellas, deben realizarse determinadas acciones en todas las fases de un potencial ataque, incluyendo también, como elemento primordial, las etapas anteriores a que éste se produzca. Es por ello preciso el establecimiento de medidas de prevención que anulen o minimicen los efectos debidos a los potenciales ataques de esas amenazas. Por lo tanto, la prevención debe considerarse como una prioridad en el proceso de gestión de riesgos para una infraestructura imbricada de alguna manera en el ciberespacio. Tres de las acciones preventivas más eficaces, que se analizan con algo de detalle a continuación, son las siguientes:

1. Análisis y evaluación de los riesgos.
2. Realización de pruebas de penetración.
3. Sensibilización y educación.

### *Análisis y evaluación de los riesgos*

De entrada, el riesgo es una función compleja del valor de los activos que se quiere proteger, de las vulnerabilidades existentes y de la probabilidad de ataques potenciales. En todo caso, siempre es necesario el despliegue de controles de seguridad, con mayor o menor complejidad y sistematicidad, para reducir la probabilidad de éxito de los potenciales ataques, erradicar vulnerabilidades y minimizar la frecuencia de ocurrencia o el impacto de los incidentes. Debe tenerse en cuenta que el propio proceso de gestión de riesgos para la gestión de los Sistemas de Información, la infraestructura técnica del ciberespacio, está siendo estandarizado como parte de la Norma ISO/IEC 27001.

El contexto, el alcance y los límites de este proceso se definen mediante la política de gestión de la seguridad. En el ámbito de evaluación y análisis de riesgos se suelen diferenciar conceptos como *identificación*, *estimación*, *evaluación* o *tratamiento* de los riesgos.

*La identificación del riesgo* permite analizar dónde, por qué y cómo pueden surgir los problemas, sirviendo esto como base para su posterior análisis. La identificación consiste en establecer el listado de los activos a proteger, las amenazas y las vulnerabilidades, todo ello con su probabilidad y consecuencias, esto es, su impacto. En este paso se identifican los riesgos que deben gestionarse. Es fundamental la identificación completa mediante un proceso sistemático bien estructurado, porque un riesgo potencial no identificado durante esta fase se excluye del análisis posterior. La identificación debe incluir todos los riesgos, estén o no bajo nuestro control. La identificación del riesgo implica además la formulación de qué consecuencias son inaceptables. Hay muchos métodos de identificación de riesgos tales como listas de control, auditorías e inspecciones, juicios basados en la experiencia y registros, diagramas de flujo, intercambio de ideas, entrevistas, análisis de los sistemas, análisis de escenarios, técnicas de ingeniería de sistemas, etc.

*La estimación del riesgo* determina la efectividad de los controles existentes, y analiza los riesgos en términos de las consecuencias y la probabilidad de ocurrencia en el marco de estos controles. Este análisis debe considerar todo el rango de las posibles consecuencias y la probabilidad de que se produzcan dichas consecuencias. Las consecuencias y sus probabilidades se combinan para proporcionar una estimación del riesgo, que deben ser evaluadas en términos del daño que sería causado, por ejemplo, por una violación de la confidencialidad, integridad, disponibilidad, no repudio, autenticidad, fiabilidad, etc., u otro tipo de consecuencias que se deriven de la materialización efectiva de la amenaza.

*En la evaluación del riesgo* se comparan los niveles estimados de riesgo con respecto a los criterios preestablecidos, como la duración de la interrupción, el impacto económico (en términos de pérdida), etc. Este paso permite la clasificación de los riesgos, con el fin de identificar las prioridades en la gestión de los mismos. Hay varias metodologías para llevar a cabo las actividades de evaluación de riesgos, que se pueden dividir en dos grupos:

1. *Métodos cualitativos*: los métodos cualitativos analizan diferentes escenarios con sus posibilidades de riesgo y clasifican la gravedad de

las amenazas y la validez de las contramedidas previstas. Las técnicas cualitativas de análisis incluyen el juicio, las mejores prácticas, la intuición y la experiencia.

2. *Métodos cuantitativos*: implican la asignación de valores y métricas significativas para todos los elementos del proceso de análisis de riesgos. Pueden incluir los costes de protección, el valor de los activos, el impacto en el negocio, la frecuencia de la amenaza, la eficacia de las protecciones, etc. Cuando todos estos elementos se cuantifican, se dice que la evaluación es cuantitativa. El análisis cuantitativo de riesgos ofrece valores porcentuales concretos para determinar la probabilidad de las amenazas. Cada elemento en el análisis (valor de los activos, la frecuencia de la amenaza, la gravedad de la vulnerabilidad, los costes de proteger el sistema, etc.) se cuantifica y se entra en las ecuaciones para determinar los riesgos totales y residuales.

Por otra parte, mediante el *tratamiento de los riesgos* se desarrolla e implementa un plan específico para el tratamiento de de cada uno de ellos, que incluye, por supuesto, los criterios de evaluación de riesgos previamente desarrollados. Cada alternativa de tratamiento de riesgos contempla:

1. *Análisis de requisitos de seguridad funcional y objetivos de control.* En las estrategias de tratamiento de los riesgos se tienen en cuenta varios factores:
   - Tipo de control: administrativo, organización, técnico, personal.
   - Tipo de protección: disuasión, detección, reducción, recuperación, corrección, seguimiento, sensibilización.
   - Limitaciones: tiempo, financieras, técnicas y tecnológicas, culturales, éticas, legales, medioambientales, facilidad de uso.

   Las limitaciones técnicas tales como requisitos de prestaciones, facilidad de uso, interoperabilidad, etc. pueden dificultar el uso de ciertos controles. En estos casos, los responsables de los sistemas y de seguridad deben trabajar juntos para identificar soluciones óptimas.

2. *Requisitos de aseguramiento de la seguridad*. El uso correcto y eficaz de los controles de seguridad de la información es un elemento fundamental para garantizar dicha seguridad. El aseguramiento de la seguridad es la razón para confiar en que una entidad cumplirá con sus objetivos de seguridad, y proporciona la confianza de que los controles de seguridad en curso funcionarán correctamente y serán efectivos en el entorno operativo.

Algunos métodos de uso generalizado para obtener información sobre la calidad de la seguridad de un sistema mediante pruebas y evaluación pueden incluir los siguientes:

– Criterios Comunes, CC (Common Criteria) (22): el CC utiliza los requisitos de seguridad, como por ejemplo la evaluación de los niveles de aseguramiento implementados, para ofrecer garantías basadas en una evaluación (investigación activa) de que se puede confiar en el sistema de información.
– Las evaluaciones de terceros: las agencias gubernamentales evalúan productos para su uso en sus propios entornos. También determinadas organizaciones profesionales realizan evaluaciones independientes. Al utilizar evaluaciones de terceros debe tenerse muy en cuenta la independencia y la objetividad de la evaluación.
– Acreditación del sistema: para operar en un determinado entorno. Estas acreditaciones, que a veces no se publican, son específicas para el entorno y el sistema.
– Pruebas basadas en un protocolo formal: se trata de una evaluación técnica del proveedor de un sistema para demostrar que cumple con los requisitos de seguridad internos establecidos. Aunque este método no proporciona una revisión imparcial de las características del sistema, si puede ser válido en muchas ocasiones. Estos informes de certificación pueden ser analizados para determinar si, al menos, los requisitos de seguridad se han definido y si se ha llevado a cabo una significativa revisión de los mismos.
– Pruebas y evaluaciones realizadas por organización independiente: este método puede permitir combinar unos costes no excesivos con la imparcialidad de una revisión independiente. El examen, sin embargo, puede no ser tan a fondo como una evaluación formal y completa o un proceso global de pruebas.

3. *Consideraciones de coste*. Es importante sopesar el coste de adquisición, implementación y mantenimiento de los controles de seguridad frente al valor de los activos a ser protegidos, y el retorno de la inversión en términos de reducción de riesgos. El coste de implementación y mantenimiento de un determinado control puede ser mucho mayor que el coste del propio control, por lo tanto, dichos costes deben ser tenidos en cuenta durante la selección. Además, se debe también te-

(22) En: *http://www.commoncriteriaportal.org/*

ner en cuenta la necesidad de personal especializado para realizar los controles.

*Pruebas de penetración*

El propósito de realizar pruebas de intrusión o penetración (también conocidas como métodos de *hacking* ético) es poner a prueba, de una forma sistemática, los controles que se ha implementado en la Red para proteger el acceso no autorizado. Hay varios tipos de pruebas de intrusión o pruebas de penetración que, dependiendo de las circunstancias, afectan al alcance de la evaluación, a la metodología adoptada y los niveles de seguridad de la auditoría que se está llevando a cabo:

– Pruebas desde el exterior de penetración a la Red.
– Pruebas de penetración desde el interior.
– Controles de acceso físico a los centros de datos y otros sitios de trabajo.
– Pruebas de ingeniería social.
– Tecnologías de acceso inalámbrico (si procede).
– Pruebas de intrusión a aplicaciones.

El objetivo de las pruebas de penetración desde el exterior es poner en peligro la red objetivo. La metodología necesaria para realizar estas pruebas permite una comprobación sistemática de las vulnerabilidades conocidas y la búsqueda de posibles riesgos de seguridad. La metodología empleada habitualmente incluye algunos de los procesos típicos de un ataque a una red, junto con otros:

– Obtención de información (reconocimiento).
– Enumeración de red: la enumeración de red se efectúa a partir de la información obtenida: los recursos de red, los inicios de sesión de usuario, identificación del *hardware* instalado y los identificadores de los proveedores de software de usuario, los identificadores de grupos, las aplicaciones, etc.
– Análisis de vulnerabilidades: permite evaluar los posibles métodos de ataque basados en la identificación de las vulnerabilidades. Para ello, las máquinas identificadas dentro de la red de destino se examinan para identificar todos los puertos abiertos, los Sistemas Operativos (OS), las aplicaciones y lo servidores (incluyendo número de versión, el nivel de revisión y/o de *Service Pack*). Además, esta información se compara con las bases de datos de vulnerabilidades disponibles en Internet para conocer cuáles pueden ser las vulnerabilidades y *exploits*

aplicables a la red objetivo. Esto suele hacerse mediante la ejecución de herramientas de evaluación de vulnerabilidades, disponibles tanto como software comercial como de código abierto. Algunas de las herramientas más populares son *Nessus*, *ISS Internet Scanner*, *Foundstone's FoundScan*, *eEye's Retina Scanner* y *GFI's LANguard*.

– Explotación: el objetivo es explotar las vulnerabilidades identificadas en el análisis previo para intentar obtener el acceso de nivel de administrador de los sistemas objetivo, o de otro tipo de acceso en cuentas de usuario, para a continuación, lanzar ataques contra otros sistemas de la Red desde el *host* que se ha visto comprometido. Si es posible, se instala un conjunto de herramientas en los hosts bajo control para acceder a otras máquinas y conocer sus vulnerabilidades. Este conjunto de herramienta puede incluir *Netcat*, *crackeadores* de contraseñas, *software* de control remoto, *sniffers* y herramientas de análisis, que pueden ser ejecutadas desde línea de comandos. En este punto, el método desde Internet (externo) se fusiona con los métodos de penetración internos.
– Análisis de resultados y presentación de informes: es un documento con toda la información pertinente sobre el control y acceso a la línea de comandos del sistema objetivo, con la descripción de los puntos de acceso identificados en el análisis de la vulnerabilidad, incluyendo el anfitrión y el directorio o el nombre del recurso compartido al que se accedía, el nivel de acceso obtenido con la fecha y la hora y, finalmente, el agujero o agujeros de seguridad que se explotaron para obtener acceso.

Hoy en día, el 85% de las intrusiones que se realizan son a través de aplicaciones *web*. Por lo tanto las pruebas sobre este tipo de aplicaciones resulta cada vez más y más relevante. Las pruebas sobre aplicaciones incluye la realización de pruebas tanto manuales como automatizadas, sin la información de acceso. Estas pruebas complementan a otras pruebas de penetración externa. El objetivo de las mismas es obtener una comprensión de cómo las personas interactúan con el sistema de acceso a datos sensibles.

Como pruebas adicionales se pueden incluir pruebas de aplicación desde el interior de la Red, a través de una cuenta de entrada estándar. El objetivo de estas pruebas es determinar la facilidad de acceso a la información sensible por quien no está autorizado según su cuenta de inicio de sesión (es decir, determinar cómo de fácil es conseguir una escalada de privilegios).

*Sensibilización, educación y formación de usuarios*

Las organizaciones no pueden proteger la confidencialidad, integridad y disponibilidad de información en el actual entorno de sistemas en red en el ciberespacio sin asegurarse de que todas las personas involucradas en el uso y la gestión de las Tecnologías de la Información (TI):

– Entienden sus funciones y responsabilidades relacionadas con la misión de la organización.
– Comprenden cómo es la organización de la política de seguridad de las TI, así como los procedimientos y prácticas aplicables.
– Tienen un conocimiento adecuado de la gestión de diversos operativos y controles técnicos necesarios y disponibles para proteger los recursos de las TI de los que son responsables.

Según se destaca en numerosos informes de auditoría, en las revistas especializadas y en presentaciones en conferencias, las personas son uno de los eslabones más débiles en los intentos de asegurar los sistemas y las redes. Muchas veces, el «factor humano» –y no la tecnología– es clave para proporcionar un nivel adecuado y apropiado de seguridad. En efecto, las personas son la clave, pero también son uno de los eslabones más débiles, por lo que debe prestarse a este «activo» cada vez mayor y mejor atención. Es fundamental un programa robusto de sensibilización y de formación en toda la organización, que garantice que la gente entiende sus responsabilidades de seguridad, las políticas de la organización en ese campo, y cómo usar correctamente y proteger los recursos de las TI que se les encomienden.

Los programas de sensibilización y de formación deben ser diseñados con la misión de la organización en mente. Es importante que el programa de sensibilización y formación sea compatible con las necesidades empresariales de la organización y sea relevante para la cultura de la organización y su arquitectura de las TI. Hay en general tres pasos principales en el desarrollo de una conciencia de seguridad y un programa de formación:

– El diseño del programa (incluido el desarrollo de la conciencia de la seguridad informática y el plan del programa de formación).
– El material de formación.
– La ejecución del programa.

Además, es necesario mantener el esfuerzo después de la ejecución del programa, para garantizar el seguimiento de los resultados y, sobre

todo, con el fin de mantener al personal al día. Esto, por lo tanto, podría considerarse como un cuarto paso, hacer que de manera recurrente se actualice y ejecute de nuevo el programa.

Desarrollado con algo más de detalle, las etapas son las siguientes:

1. *Planificación*: en la etapa de diseño del programa se identifica tanto la sensibilización de la organización en los aspectos de seguridad, como las necesidades de formación; se desarrolla una conciencia efectiva de toda la organización y el plan de formación; se solicita y asegura la involucración de toda la organización desde los niveles inferiores hasta la dirección, y se establecen las prioridades.
2. *Desarrollo:* una vez que el programa de sensibilización y formación ha sido diseñado, se puede desarrollar el material de apoyo. Este material debe ser desarrollado con los siguientes criterios en mente:
   - ¿Qué comportamiento es el que queremos reforzar? (concienciación).
   - ¿Qué habilidades o destrezas queremos que la audiencia aprenda y aplique? (formación).

   Un programa de sensibilización y de formación sólo puede ser efectivo si el material que se emplea es interesante, actual y relevante.
3. *Implementación:* una vez que la evaluación de necesidades se ha llevado a cabo, se ha desarrollado una estrategia, se ha completado un plan de sensibilización y formación para la aplicación de esa estrategia y el material de capacitación se ha desarrollado, se puede aplicar el programa de formación. Es esencial que todos los involucrados en la ejecución del programa comprendan sus funciones y responsabilidades.

Hay una serie de alternativas para la aplicación del programa de sensibilización y de seguridad:

1. *Concienciación sobre la seguridad:*
   - Salvapantallas y pancartas de advertencia y mensajes, carteles, boletines, mensajes a toda la organización por *e-mail*.
   - Presentaciones y talleres presenciales dirigidas por instructores.
2. *Formación en seguridad:*
   - Formación dirigida por un instructor, incluyendo presentaciones y cursos de capacitación.

El número final de los talleres, presentaciones y cursos, así como el calendario correspondiente dependerá de los resultados de las fases del

diseño y la planificación y la existencia de otras actividades programadas para el personal involucrado.

Cuando todos los cursos y actividades previstas se han realizado, queda la cuestión abierta de si han sido suficientemente eficaces. Evaluar la eficacia de la formación es un paso vital para garantizar que la formación impartida es útil. La formación es «útil» sólo cuando responde a las necesidades tanto de los alumnos (los empleados) como de la organización. Gastar tiempo y recursos en una formación que no logra los efectos deseados pueden reforzar, en lugar de disipar, la percepción de la seguridad como un obstáculo frente a la productividad.

**La detección, la respuesta y la recuperación**

La prevención, analizada en el punto anterior, es necesaria, pero no suficiente. Desgraciadamente, las amenazas del ciberespacio están presentes y, antes o después, la infraestructura tecnológica de una determinada organización puede ser atacada, por lo que es también necesario disponer de elementos de detección de intrusos, así como de herramientas para la respuesta y la recuperación, una vez que el sistema está siendo o ha sido atacado.

El disponer de una capacidad adecuada para vigilar las redes y así detectar precozmente los ataques de red reduce considerablemente el tiempo de respuesta y la capacidad para recuperar los servicios afectados. Por lo tanto, es fundamental disponer de la correspondiente plataforma de supervisión de la seguridad, entendida ésta como una plataforma especializada que se centra en la gestión de la seguridad de los Sistemas de Información y de las redes bajo la responsabilidad de una determinada organización. Un aspecto relevante de estas plataformas es la amplia gama de servicios que pueden ofrecer, como la detección de intrusiones, control y monitorizado de los servicios, gestión inteligente de registros, etc. En ellas se registran y evalúan los fallos del sistema (en relación con la disponibilidad de la infraestructura), así como los incidentes de seguridad (en relación con la integridad y confidencialidad de la información). Cada uno de este tipo de análisis tiene connotaciones, aproximaciones y procedimientos diferentes y por lo tanto cada uno requiere un método de procesamiento diferente, con distinto tipo de herramientas.

A continuación se describe con algo más de detalle el contenido de los servicios antes mencionados y la forma de proporcionarlos.

*Detección de intrusos*

Por lo general, a fin de seleccionar la mejor aproximación tecnológica para la detección de intrusos es necesario analizar y comprender las características siguientes:

– *Eficacia:* relativa tanto a la tasa de falsos negativos como a la posibilidad de pasar por alto actividades sospechosas. Este parámetro se puede medir de manera objetiva, teniendo en cuenta el número de patrones (o protocolos) que la herramienta puede administrar y la periodicidad en las actualizaciones de la base de datos de patrones.
– *Eficiencia*: relativa tanto a la tasa de falsos positivos como a la posibilidad de notificar como sospechosas actividades que en realidad son correctas. También este parámetro se puede medir de manera objetiva, teniendo en cuenta la flexibilidad de la configuración de los sistemas con el fin de adaptarlo al contexto de la organización (políticas de seguridad, niveles de gravedad, integración con la evaluación de vulnerabilidades de los sistemas, gestión de redes, etc.).
– *Gestión*: la gran cantidad de información que suele haber disponible y que se genera dentro de los sistemas es uno de los problemas más importantes a la hora de la detección de intrusos. La herramienta o tecnología seleccionada debe ofrecer el apoyo necesario para convertir datos en información fácil de usar. Además es muy importante la disponibilidad y uso de medios de notificación de alertas (correo electrónico, SMS, etc.) y su integración con los sistemas de gestión de la red.

Algunas características importantes que suelen pedirse a este tipo de herramientas y soluciones son las siguientes:

1. IDS de sus siglas en inglés *(Intrusion Detection System)* basado en *red*, con patrones de ataques conocidos, y preconfigurados (firmas) y análisis de protocolos de alto rendimiento. Son funcionalidades de gran interés para el IDS las siguientes:
   – Capacidad de definición de políticas de acuerdo con la arquitectura y notificación de vulnerabilidades específicas del sistema objetivo.
   – Análisis de tráfico en relación con el origen y el destino.
   – Reglas personalizadas para procesar ataques específicos.
   – Disponibilidad muchos formatos simultáneos para ahorrar alertas.
   – Disponibilidad de muchos preprocesadores para el análisis de protocolos.
   – Relación completa de eventos y acciones recomendadas.

2. *Arquitectura de la Red y del sistema oculta*, y sin perjuicio de rendimiento de los servicios (si un componente falla, el servicio permanece disponible).
3. *Interfaz* web *para el análisis de eventos:*
   – Filtros y búsquedas avanzadas teniendo en cuenta muchos parámetros: IP de origen, IP de destino, agentes, protocolo, categoría de ataque, etc.
   – Análisis en tiempo real.
   – Repositorio de información analizada.
   – Generación de gráficos.
   – Integración con bases de datos públicas (*who-is* y similar y repositorios específicos basados en *web*).
   – Fácil de usar y de navegar, basado en estructura de árbol.
   – Lista de enlaces IP.
   – Repositorio con el almacenamiento de actividades anteriores.
4. *Interfaz* web *para otras actividades:*
   – Gestión de agentes (parada, cambios de inicio y configuración).
   – Gestión de firmas.
   – Definición fácil de reglas personalizadas.
   – Gestión de políticas específicas para la mejora de la implementación de agentes nuevos.

En el ámbito de la detección de intrusión y de ciberataques, uno de los procesos más complejos es el de la *atribución* (23), esto es, la determinación precisa de quién está realizando una determinada actividad. Se pueden distinguir tres tipos principales de atribución:

– Geolocalización (lugar desde donde se está realizando la actividad de intrusión).
– Ciberidentidad de la persona o grupo que realiza la actividad (facilita la identificación real de la personal específica o grupo que realiza la actividad).
– Identificación física de la persona que realiza la actividad desde un teclado concreto.

La solución completa al problema global de la atribución en el ciberespacio no es fácil tecnológicamente, además de un muchos casos plantear problemas de restricciones legales y de protección de la intimidad. No

(23) Hunker, Jeffrey, doctor; Hutchinson, Bob and Margulies, Jonathan: *Role and Challenges for Sufficient Cyber-Attack Attribution Authors,* 2008.

obstante, es necesaria en muchas situaciones establecer una identidad con pocas dudas para poder dar una respuesta efectiva y, sobretodo, legal. La recolección de evidencias forenses, la gestión de *logs* que se describen posteriormente, etc. en muchos casos no permiten alcanzar una evidencia completa de quién ha lanzado el ciberataque. Un ejemplo clásico fue el ataque a Georgia desde Rusia. Aunque pudo establecerse que el ataque se realizó desde servidores instalados en el territorio ruso, no se ha podido determinar con certeza si los servidores fueron controlados por grupos de crimen organizado u organizaciones paraestatales. Todavía es tecnológicamente muy difícil, en muchos casos, fijar la geolocalización o el sistema original desde el que se lanza un ciberataque, y más la identidad o grupo que lo ha iniciado.

La complejidad en la atribución lleva asociado que sea también complejo establecer mecanismos de *disuasión* de ataques. Una disuasión efectiva implica el disponer de unos sistemas de detección y atribución eficaces (24), o unos desincentivos que penalicen el coste de realizar un ataque, así como la disminución en la percepción de los beneficios. Por ejemplo, para evitar el *spam* masivo de correos electrónicos se ha propuesto cobrar una cantidad nimia por el envío de un correo, que para un usuario normal sería un coste despreciable, pero para quien envía millones de correos puede suponer un coste inaceptable. No obstante, este enfoque asume un atacante racional al que se le pueden trasladar las percepciones de coste y beneficio. Sin embargo, el conflicto en el ciberespacio es en general de naturaleza asimétrica, y con escalas de valores que en muchos casos no pueden enmarcarse dentro del ámbito de lo «racional».

*Plataformas de seguridad, controles y servicios de vigilancia*

Una manera rápida de saber que algo va mal es detectar que un servicio ha reducido sus prestaciones o se ha caído. Así pues, otro aspecto a tener en cuenta es la disponibilidad de herramientas específicas para analizar el estado de las infraestructuras y los servicios.

Mediante este tipo de servicios de monitorizado será posible conocer en todo momento y desde cualquier lugar el estado operacional de la plataforma, junto con el estado de cada componente. Además, permite

(24) Mowbray, Thomas J.: *Solution Architecture for Cyber Deterrence,* SANS Institute, GIAC (GPEN) Gold Certification, 2010.

de manera fácil encontrar los elementos y servicios que están operando próximos a su saturación, para detectar cuellos de botella y para verificar la actividad por unidad, departamento, gerente, etc.

Con el fin de seleccionar las mejores soluciones tecnológicas es fundamental entender las características básicas de las que deben disponer:

1. *Flexibilidad y capacidad*: no puede ser una herramienta con funcionalidad limitada y rígida, sino con una arquitectura que haga posible una configuración fácil y rápida para adaptarse a unos requisitos específicos.
2. *Gráficos y generación de informes*: el formato y el contenido de la información reportada se debe poder personalizar.
3. *Notificaciones personalizadas*: debe ser posible configurar la generación de notificaciones y alertas para distintas situaciones, y su integración en varios canales (por ejemplo: SMS, correo electrónico, voz, *WAP-Push*, etc.).
4. *Estabilidad y baja carga*: debe funcionar con pocos recursos de *hardware* y tener tasas de disponibilidad muy altas.
5. *Madurez*: la herramienta-tecnología debiera estar suficientemente desplegada en el mercado.
6. *Fácil de usar*: en general debiera disponer de interfaz *web* que proporcione una vista rápida del estado del sistema con varias opciones o niveles de detalle:
   - Vista táctica: resumen del estado de todo el sistema para implementar acciones inmediatas, de acuerdo con su situación real. Se debe poder ver el estado de las distintas aplicaciones y obtener información adicional (por ejemplo, los fallos, la falta o pérdida de datos, etc.).
   - Mapa de estado: mapa de configuración de la red, las dependencias entre los componentes, la disponibilidad y otras características.
   - Detalles de los servidores: información sobre si los servidores están funcionando, caídos o sin acceso. Suele ser interesante disponer de esta información por grupos de servidores.
   - Detalle del estado de las plataformas: información sobre el estado de las plataformas y sus servicios asociados, recursos, etc.
   - Detalle de los servicios: información sobre si los servicios están funcionado y el resultado de la última comprobación. Suele ser interesante disponer también de esta información por el grupo al que pertenecen.

– Problemas: se debe poder ver la lista de servidores o servicios con algún tipo de problema y una breve descripción del mismo.
– Alertas y notificaciones: información sobre el número de alertas y notificaciones que ha enviado el sistema.
– Visualización rápida del estado (por ejemplo, con códigos de colores) y generación de informes detallados: debe mostrar una gran cantidad de informes por grupos de servidores, servicios, etc.; el porcentaje de tiempo que cada servidor ha estado funcionando o caído; saber si no una plataforma falla con frecuencia, etc.
– Configuración y operación a través de navegador *web*: se deben poder programar los controles de los servidores y los servicios, notificaciones, etc.

Un concepto importante es la capacidad de definir jerarquías en la red, lo que permite detectar y distinguir entre servidores que están caídos y los que son inaccesibles, así como la capacidad de escalar las notificaciones sobre servidores y servicios a diferentes grupos.

*Gestión de LOGs*

Como viene detallándose a lo largo de este capítulo, la detección y prevención de problemas de seguridad en el ciberespacio es una misión compleja. El uso de herramientas potentes de gestión de *LOGs* permite monitorizar los incidentes de seguridad sin interrupción (operación 7 por 24), y hace posible un modelo de gestión de la seguridad de alta calidad y a un coste razonable.

Para la gestión de logs deben, por supuesto, tenerse en cuenta:
– Las políticas de seguridad de la organización.
– La infraestructura tecnológica específica de la que se dispone.
– El conocimiento que aporte a la gestión de los mismos un experto en seguridad.

Una gestión adecuada de *LOGs* debe estar orientada a proporcionar un conocimiento adecuado y, sobre todo, debe reducir el esfuerzo necesario para la gestión de incidentes de seguridad, al realizarse un filtro previo eficaz de dichos incidentes. Cuando está debidamente implementada esta gestión de *LOGs*, sólo los incidentes que son notables se presentan al experto en seguridad. Esta selección previa evita la saturación del especialista, porque una gran cantidad de información, que no es relevante, es analizada previamente por la herramienta.

Estas herramientas de supervisión se definen como herramientas de monitorización basadas principalmente en la correlación de registros (pero no sólo), que proporcionan indicadores de seguridad y envían alertas cuando se superan los umbrales predefinidos, y dan apoyo al equipo de expertos en seguridad que debe reaccionar de manera inmediata cuando surgen incidentes de seguridad. También deben disponer de una consola que muestre al usuario información integrada respecto a indicadores de amenazas para los diferentes sistemas. Hoy día, nuevas técnicas de representación ofrecen una visión global e intuitiva de la seguridad.

La información se obtiene a través de un sistema no intrusivo de análisis de registros con capacidades de aprendizaje. Una vez recibidos los registros se clasifican y se procesan de acuerdo con algunos patrones lógicos. El sistema debe poder detectar nuevos patrones y añadirlos al repositorio. Además, este proceso de aprendizaje debe poder ser supervisado por el administrador, que deberá poder ajustar los distintos parámetros y reglas que se utilizan en la generación de indicadores de amenazas y alertas de seguridad.

La personalización se puede basar en los siguientes tres pasos:

1. *Definición de modelos sospechosos de comportamiento*: que se esperan, de acuerdo con las políticas de seguridad. Los comportamientos se pueden clasificar en dos grupos:
   - Comportamientos sospechosos, son los que desea supervisar porque se cree que su presencia podría poner en peligro la seguridad con alta probabilidad.
   - Comportamientos esperados, son los que ocurren por lo general, pero un cambio no habitual, por ejemplo en su frecuencia, podría implicar un riesgo de seguridad con alta probabilidad (por ejemplo, un ataque de denegación de servicio).
   - Finalmente, después de la definición de las conductas se seleccionan los sistemas de monitorizado de acuerdo con la existencia de registros con información útil acerca de la ocurrencia de estos comportamientos.
2. *Asimilación de registros y eventos*: el proceso de asimilación de los registros permite establecer el canal a través del que un sistema final (con registros) se conectará al sistema. Este proceso funciona de la siguiente manera: se proporciona un número significativo de registros para analizar, un generador automático de expresiones de definición

de eventos y, finalmente, el experto en seguridad válida las definiciones de eventos y las modifica si es necesario.

3. *Plantillas para la generación de modelos identificados de comportamiento:* la generación de plantillas es un proceso que permite asociar un comportamiento específico con la aparición simultánea de ciertos eventos en los registros durante una ventana de tiempo. Una plantilla se puede definir como una colección de reglas (cálculo y correlación) que hacen posible combinar eventos primarios con el fin de generar uno o más eventos secundarios y, finalmente, decidir si un cierto tipo de comportamiento (esperado o sospechosos) se está llevando a cabo.

Por último, algunas características más específicas serían las siguientes:

- La información que debe centralizarse puede obtenerse de los archivos con registro y de soluciones comerciales de gestión y monitorizado.
- Debe ser capaz de utilizar agentes intrusivos y no intrusivos (predefinidos o genéricos).
- El análisis automático de los registros por medio de expresiones regulares para incluir todo tipo de registros (incluyendo registros de aplicación).
- Base de datos genérica de eventos (para poder definir nuevos tipos de eventos).
- Correlación de registros con reglas personalizadas para buscar patrones específicos.
- Asociación de eventos en distintos niveles jerárquicos.
- Información detallada de eventos con la capacidad de filtrado por gravedad.
- Heurística personalizada para obtener índices de seguridad en relación con el tipo de eventos, los atributos de los registros, la frecuencia, la periodicidad, la fiabilidad y la gravedad.
- Árbol de mapas y gráficos de históricos.
- Funciones de filtrado para ayudar a una detección temprana de problemas de seguridad.
- Notificaciones por correo electrónico u otro método definido por el usuario (SMS, MMS, voz).
- Informes personalizados sobre los datos históricos.

*Desarrollo continuo*

El análisis y la evaluación de riesgos, las pruebas de penetración, las auditorías, el desarrollo e implementación de contramedidas, etc. son,

como se indicó previamente, actividades necesarias, pero no suficientes para lograr plenamente los objetivos de protección. Por supuesto, con el fin de conseguir una mayor efectividad es altamente recomendable llevar a cabo todas estas actividades tras la definición previa y detallada de unos objetivos de seguridad bien definidos. Es también esencial la programación y coordinación de todas las tareas, la medición de los resultados de las acciones realizadas, la mejora de la eficacia a través de la innovación y el aprendizaje y, si es necesario, la redefinición de los objetivos o la estrategia, y todo ello mediante un proceso de desarrollo continuo, basado no sólo en la tecnología, que es el objeto del presente capítulo, pero fundamentalmente en ésta.

La mejor manera de afrontar el reto descrito anteriormente es incluir todas las actividades relacionadas con la seguridad y aspectos asociados en un proceso denominado Gestión de Seguridad de la Información (GSI). La Norma Internacional ISO/IEC 27001 (25) es un buen modelo, con un enfoque basado en procesos, para la gestión de seguridad y también de la información.

El enfoque basado en procesos para la GSI que se presenta en esta Norma Internacional anima también a los usuarios a hacer hincapié en la importancia de:

– Comprender los requisitos de seguridad de la información de una organización, y la necesidad de establecer políticas y objetivos para la seguridad de la información.
– Implementar y operar los controles necesarios para gestionar los riesgos de seguridad de la información de la organización, en el contexto de los riesgos de la organización en general.
– Supervisar y revisar el rendimiento y la eficacia del Sistema de Gestión de la Seguridad de la Información (SGSI).
– La mejora continua basada en mediciones objetivas.

Esta Norma adopta el modelo PDCA *(Plan-Do-Check-Act)*, que se aplica a la estructura de todos los procesos del SGSI. La Norma proporciona un modelo sólido para la aplicación de los principios que rigen la evaluación de riesgos, diseño e implementación de la seguridad, gestión de la seguridad y la reevaluación.

(25) En: *www.iso27000.es*

El proceso de GSI tal como se define en la Norma ISO/IEC 27001 e ISO/IEC 27002 cumple los requisitos más importantes y establece las mejores prácticas para garantizar la mejora de la seguridad mediante el aprendizaje continuo, una mayor protección de los sistemas, el análisis de riesgos, etc. En efecto, estos requisitos y controles son esenciales para la familia de Normas ISO/IEC 27000:

– Análisis y evaluación de riesgos.
– Tratamiento de riesgos.
– Mantener y mejorar el SGSI.
– Formación, sensibilización y competencia.
– Auditorías internas del SGSI.
– Gestión de la información de incidentes de seguridad.
– Control de vulnerabilidades técnicas.
– Comprobación de cumplimientos técnicos.

El proceso GSI debe ser un proceso continuo. Las amenazas a la seguridad, los objetivos, las tecnologías (y el uso que se hace de ellas) y los usuarios pueden variar con el tiempo, haciendo obsoletos los resultados del análisis anterior y los controles implementados. Por lo tanto, resulta claro que el análisis y valoración del riesgo, la realización de pruebas de penetración, las auditorías y la formación son actividades que deben ejecutarse periódicamente a fin de mantener los niveles adecuados de protección de la información, y la seguridad, desde un punto de vista tecnológico, en el ciberespacio.

## Las herramientas, las metodologías y las normas en el ámbito de la seguridad en el ciberespacio

Siguiendo con la visión tecnológica del ciberespacio que se está abordando en este capítulo, en esta sección se enumeran las principales herramientas, metodologías y normas que se aplican para el ámbito de la seguridad en el ciberespacio.

A veces, cuando se mencionan conceptos como normas, o normalización, o estandarización en el ciberespacio se piensa, por parte de muchos, que se va a plantear el establecimiento de limitaciones a la concepción de libertad sin límites que algunos plantean para su funcionamiento. Independientemente de que es muy interesante el debate que se aborda en otro capítulo de esta *Monografía* sobre los aspectos regulatorios, muchas veces asociados a cómo minimizar el mal uso del ciberespacio y

cómo poder establecer responsabilidades legales ante ese mal uso; la normalización que aquí se describe, siguiendo el hilo argumental de este capítulo, está asociada a la infraestructura tecnológica. Los protocolos de comunicaciones tienen que estar normalizados y también la forma en la que las aplicaciones acceden a la Red. Cuestión aparte, que, por supuesto, no es éste el lugar para abordarla, es establecer quién puede o debe estandarizar la red. ¿La red debe autoregularse? ¿Debe dejarse a las industrias y a los fabricantes que organicen entre ellos los aspectos de infraestructura tecnológica y estandaricen, o deben intervenir los gobiernos? (26). Cuestiones de este tipo son puntos de debate abierto.

*Las herramientas*

Para el campo de la seguridad y la prevención de riesgos en el ciberespacio hay una pléyade enorme de tipos de herramientas disponibles, basadas en tecnologías muy variadas. Se escapa del alcance del presente capítulo hacer una identificación exhaustiva de las mismas, ni detallar el estado del arte de cada una de ellas, tanto en el ámbito comercial como militar. Aspectos que habría que tener en cuenta en ese análisis riguroso son, por ejemplo, cuales son las soluciones disponibles y, entre éstas, cuales son las más extendidas (principales proveedores); las funcionalidades y las amenazas tratadas por cada una de ellas; la reducción del nivel de riesgo que aportan; el coste de adquisición; el esfuerzo que lleva asociado su despliegue, así como los costes y esfuerzos necesarios para el soporte y mantenimiento; las posibles restricciones legales y reglamentarias en función del ámbito en el que se apliquen, etc. Una enumeración de los principales ámbitos tecnológicos a considerar es la que se incluye a continuación. Es, por tanto, un mero listado introductorio y que, entre otras cosas por limitaciones de espacio y por el alcance que se le pretende dar al presente capítulo, no se desarrollan cada uno de los puntos enumerados.

TÉCNICAS Y TECNOLOGÍAS DE AISLAMIENTO DE REDES

Como tecnologías, dispositivos o normas que facilitan el aislamiento de las redes y, por tanto, dificultan su vulnerabilidad conviene mencionar los siguientes:

(26) Benoliel, Daniel: *Cyberespace technological standardization: an institutional theory retrospective,* 2003.

– *Cortafuegos*: permiten el filtrado de tráfico sobre redes TCP/IP, de manera que se bloquea el acceso no autorizado y a la vez se permite el autorizado. Los cortafuegos más extendidos son los cortafuegos de capa tercera, que básicamente permiten el filtrado de paquetes según el tipo de protocolo y el estado, equipo de origen y de destino y puerto.
– *Routers*: conmutadores, concentradores y cualquier otro dispositivo de comunicación y de interconexión con capacidades de segmentación y/o de filtrado.
– *Servidor proxy*: que es un ordenador o aplicación que recibe las peticiones y conexiones de red que los clientes hacen a un servidor de destino.
– *VLAN (Virtual Local Area Network)*: red de área local virtual, que permite la creación de redes lógicas independientes, dentro de una única red física.
– *NAT (Network Address Translations)*: traducción de direcciones de red, que es un mecanismo que usan los *routers* para permitir el intercambio de paquetes entre redes, asignándose entre ellas direcciones incompatibles. De esta manera se puede acceder a internet con direcciones privadas.
– *NAC (Network Access Control)*: control de acceso a red, que es un concepto emergente y en evolución sobre productos de seguridad y que está relacionado con el hecho de que al disponer de un ordenador en red es preciso también disponer de un conjunto de protocolos para definir como asegurar los nodos de la Red, incluso antes de que estos accedan a la Red.
– 802.1.x-Norma del IEEE para el control de acceso a la red mediante puertos.

CRIPTOGRAFÍA

La criptografía no es una tecnología específica del ciberespacio, pues el cifrado de mensajes existe desde tiempos inmemoriales, pero sí es cierto que está teniendo un auge muy significativo por la necesidad de disponer de unas comunicaciones seguras y privadas. En el ámbito del ciberespacio, relacionado con la criptografía se manejan, entre otros, los siguientes conceptos y tecnologías:

1. *Cifrado de comunicaciones:*
   – Dispositivos de cifrado de comunicaciones: cortafuegos con capacidades de Red Privada Virtual, VPN *(Virtual Private Network),*

dispositivos de cifrado dedicados, *routers* y conmutadores que permiten VLAN y VPN.
   - Protocolos de transmisión segura: SSL *(Secure Sockets Layer)*, protocolo de capa de conexión segura, SSH *(Secure Shell)*, intérprete de órdenes segura, IPSec *(Internet Protocol security)*, como conjunto de protocolos cuya función es asegurar las comunicaciones IP, autenticando y cifrando cada paquete IP, etc.
   - VPN redes privadas virtuales, que es una tecnología que permite la extensión de una red local privada sobre una red pública o no controlada.
2. *Algoritmos de cifrado simétricos y asimétricos*.
3. *PKI (Public Key Infrastructure)*, infraestructura de clave pública para la autenticación de usuarios para poder realizar con garantías operaciones como el no repudio de transacciones electrónicas.
4. Almacenamiento y gestión de claves.
5. *HSM (Hardware Security Module)* módulo de seguridad *hardware*, que normalmente es un dispositivo *hardware* para almacenar y proteger claves criptográficas, además de en muchos casos realizar otras operaciones criptográficas.
6. *Aseguramiento de la integridad*, mediante el cálculo *hash* y herramientas de verificación.

DETECCIÓN DE INTRUSIÓN

Para la detección de potenciales intrusiones en una red del ciberespacio se dispone de diversas herramientas y tecnologías entre las que se pueden mencionar las siguientes:

- Herramientas de evaluación y de detección de vulnerabilidades, como son los llamados escáneres de vulnerabilidad o analizadores de red, los escáneres de puerto (detecta para cada puerto de una máquina si está abierto, cerrado o protegido por un cortafuegos), los escáneres de sistema operativo, etc.
- IDS-IPS, esto es, Sistemas de Detección de Intrusión-Sistemas de Prevención de Intrusión. Como se ha indicado antes, el funcionamiento de los IDS se basa en el análisis detallado del tráfico que se está llevando a cabo en la Red, que se compara con firmas de ataques ya conocidos, o con comportamientos que se pueden clasificar como sospechosos (por ejemplo, detección de que se están llevando a cabo un escaneo de puertos, etc.). Aunque parecidos a los IDS, los IPS

permiten además establece políticas de seguridad para proteger un determinado equipo o la red completa de un ataque. El IPS protege de forma proactiva, mientras que el IDS lo hace de manera reactiva.
– *Honeypot*, que es un *software* o a un grupo de ordenadores cuyo objetivo es atraer a potenciales atacantes, simulando ser sistemas vulnerables o débiles a los ataques. Es una herramienta de seguridad informática utilizada para recoger información sobre los atacantes y sus técnicas.
– Centralizado de registros, correlación de eventos y gestión y respuesta de alertas

DETECCIÓN Y PROTECCIÓN DE VIRUS Y *MALWARE*

En el ámbito de la detección y protección contra virus y *malware* se dispone de los siguientes tipos de soluciones:
– Antivirus y soluciones para *software* malicioso para equipos de sobremesa y portátiles
– Antivirus y soluciones de *software* malicioso para los servidores (*gateways* HTTP, servidores de correo, servidores de archivos, etc.).
– Soluciones *antispam.*
– Herramientas de verificación de integridad de archivos críticos.

OFUSCACIÓN DE LA INFORMACIÓN

En general, la ofuscación se refiere al proceso de encubrir la información haciéndola más confusa de leer e interpretar. Es distinto de la criptografía, en la cual los mensajes y la información se cifran. Como tecnologías en el campo de la ofuscación se pueden distinguir, entre otras, las siguientes:
– *Esteganografía*, que es el hecho de ocultar mensajes o información dentro de otros objetos, que actúan como portadores, de manera que para alguien no avisado no es capaz de detectar su presencia. A su vez estos mensajes pueden ir además encriptados. Se utiliza sobre todo en archivos multimedia.
– *Ofuscación de código*, que es el hecho deliberado de realizar un cambio no destructivo, ya sea en el código fuente de un programa con el propósito de que no sea fácil de entender o leer. Un código ofuscado es un código que aunque se disponga del código fuente este es muy enrevesado de interpretar, lo que dificulta el entender la funcionalidad implementada.

### AUDITORÍAS DE LAS POLÍTICAS DE SEGURIDAD

Para realizar estas auditorías existen distintos tipos de herramientas orientadas a los siguientes propósitos:

- Auditado y cumplimiento de las directivas de seguridad (*software* local e instalado en los servidores).
- Distribución de *software* y soluciones de instalación remota.
- Revisores de código.
- Herramientas para auditar la seguridad de las aplicaciones *web.*
- *Proxys Man in the middle*, herramientas de inyección automática SQL, escáneres URL, etc.
- Depuradores.

### *BACKUP* DE INFORMACIÓN

La realización de *backups* y copias de respaldo de toda la información depositada en los ordenadores es un principio básico dentro de las políticas de seguridad. Para ello se dispone de:

- Utilidades de copia de seguridad.
- Dispositivos y herramientas de generación de imágenes.

### ELIMINACIÓN DE DISPOSITIVOS EXTRAÍBLES Y DOCUMENTOS

En este campo es preciso destacar los siguientes aspectos:

- Máquina de triturado de papel y de soportes ópticos.
- Sistema de borrado de discos ópticos.
- Soluciones *software* para eliminar información.

### DISPOSITIVOS DE ANÁLISIS FORENSE

Para la realización de análisis forense se utilizan los siguientes tipos de dispositivos y tecnologías:

- *Sniffers* de red.
- Esteganografía.
- Volcadores de memoria.
- Analizadores de disco.
- En general, distintos tipos de herramientas forenses también de propósito específico.
- Analizadores y depuradores de código.
- Herramientas de verificación la integridad de archivos críticos.
- Centralizado de registros y correlación de eventos.

ALTA DISPONIBILIDAD (HA), MECANISMOS DE BALANCEO (LB) DE CARGA Y REDUNDANCIA

Para los sistemas en alta disponibilidad (son aquellos sistemas cuyo modo de implementación garantiza un alto grado de continuidad operacional durante un período de tiempo, normalmente 7 por 24) se utilizan distintas tecnologías y conceptos, entre los que cabe mencionar los siguientes:

– *Clustering* de servidores.
– Discos en espejo.
– Sistemas RAID.
– Virtualización.
– Balanceo de carga.
– Monitorizado del estado de los sistemas.

CONFIGURACIÓN DE TRÁFICO

La configuración de tráfico (o la configuración de paquetes) es una práctica de gestión de tráfico en Internet, orientada al control del tráfico de redes informáticas con el fin de optimizar las prestaciones o la garantía de servicio, mejorar la latencia y/o aumentar el ancho de banda utilizable, retrasando los paquetes que cumplen con ciertos criterios.

Esto es útil para dar prioridad a algunos protocolos o paquetes cuando se dispone de un ancho de banda limitado. La capacidad mencionada permite garantizar la rápida transmisión de comandos críticos, incluso en redes con ancho de banda muy reducido. La configuración de tráfico se realiza por los administradores de ancho de banda, que son aplicaciones de gestión de comunicaciones y un software de gestión de consola para el operador de red. La configuración de tráfico es comúnmente aplicada en los extremos de la red para controlar el tráfico que entra en la Red, pero también puede ser aplicado a un elemento particular de la Red.

AISLAMIENTO ELECTROMAGNÉTICO (EM)

Desde el punto de vista de aislamiento electromagnético conviene destacar los siguientes conceptos:

– Jaula de *Faraday*, para evitar interferencias electromagnéticas. La jaula de *Faraday* es un recinto formado por material conductor o por una malla de dicho material. Este tipo de jaula bloquea la entrada de campos eléctricos estáticos externos. Los sistemas de información

alojados en este tipo de salas están protegidos contra los campos eléctricos estáticos externos, sin importar el origen de dichos campos, ya sea creados por la naturaleza (por ejemplo, rayos) o de forma intencionada (ataque). La protección electromagnética proporcionada por las jaulas de *Faraday* no sólo es una forma de aislamiento. Estas jaulas también disipan las emanaciones electromagnéticas desde el interior hacia el exterior. Esta capacidad hace que la zona protegida con una jaula de *Faraday* disponga de una medida de protección eficaz contra los ataques TEMPEST *(Transient Electromagnetic Pulse Surveillance Technology)*.
– Reducción al mínimo de nivel de señal. El diseño y operación de los circuitos cada vez a niveles más bajos de potencia permite minimizar la potencia de las emisiones no intencionales.

CABLEADO DE SEGURIDAD

También en cableado de seguridad hay tecnologías específicas como son las relativas a cable blindado, cable termo acoplado, cable coaxial, etc.

DEFENSA DEL PERÍMETRO DE SEGURIDAD FÍSICA,
CONTROLES FÍSICOS DE ENTRADA Y SISTEMAS DE APOYO

También es preciso protegerlos lugares e instalaciones donde está depositada la información, ello implica el disponer en dichas instalaciones de sistemas que permitan realizar las siguientes funciones:
– Detección de intrusos, detectores de movimiento, video vigilancia IP, CCTV, sensores para detección de intrusos y activación de alarmas con distintas tecnologías, sistemas de control de alarmas, etc.
– Escáneres de rayos X.
– Control de acceso electrónicos y mecánicos, puertas, cerraduras electrónicas, controles de acceso para la administración y supervisión de los sistemas, sistemas biométricos (huellas dactilares, escaneado del iris), tarjetas de banda magnética, tarjetas de proximidad, etc.
– Sistemas de detección de incendios y equipos de extinción.
– Instalaciones de apoyo: UPS, generadores, ventilación.

Independientemente de las técnicas, tecnologías y soluciones enumeradas y otras no mencionadas, todas ellas deben orientarse a garantizar las propiedades de seguridad de la información: confidencialidad, integridad, disponibilidad y responsabilidad.

*Las metodologías y las normas*

Hay una gran cantidad de herramientas, normas y metodologías para realizar análisis de riesgos en la seguridad en los medios tecnológicos del ciberespacio. Algunas de las más significativas son las que se describen continuación.

METODOLOGÍAS DE ANÁLISIS DE RIESGOS

MARION *(Méthodologie d'Analyse des Risques Informatiques et d'Optimisation par Niveau)* (27) es un producto francés, que se utiliza para el análisis de riesgos en las organizaciones comerciales. Este paquete se basa en una librería de incidentes detectados, además de incluir muchas encuestas y cuestionarios aplicados para la evaluación de soluciones en el ámbito de la seguridad. En el caso de análisis de riesgos este método contiene elementos para realizar tanto análisis cualitativos como cuantitativos. El *software* proporciona los resultados de los análisis para hasta 27 categorías distintas de recursos y amenazas. La presentación de los resultados es posible tanto en formato numérico como gráfico.

CORA (*COst-of-Risk-Analysis System*) (28) es un sistema elaborado hace más de 30 años por International Security Technology, Inc. Los especialistas que tratan con el riesgo definen y almacenan los parámetros de riesgo en ficheros como normas de riesgo. Estas normas constituyen más tarde la base de trabajo para el personal operativo. CORA proporciona la estructura que permite el almacenamiento de la información. La estimación de las pérdidas potenciales en caso de un determinado incidente de seguridad, es preparada por separado para todos los elementos de organización y CORA se utiliza para llevar a cabo la evaluación. Los expertos usan CORA para la detección y almacenamiento de datos sobre la susceptibilidad de todas las amenazas.

COBRA *(Consultative, Objective and Bifunctional Risk Analysis)* (29) se utiliza para el análisis cualitativo y cuantitativo de riesgos, y para la evaluación de la compatibilidad de las soluciones aplicadas a la Norma Internacional en el ámbito de de gestión de seguridad de la información ISO/IEC 17996. Este *software* está dirigido a expertos en este campo y

(27) En: *http://www.clusif.asso.fr/*
(28) En: *http://www.softscout.com/software/Project-and-Business-Management/Risk-Management/CORA-Cost-of-Risk-Analysis.html*
(29) En: *http://www.security-risk-analysis.com*

su elemento principal es un conjunto de modelos de formularios generados automáticamente, así como su base de conocimiento. Los módulos básicos de COBRA son el módulo de creación de cuestionarios, el módulo de revisión de riesgo-compatibilidad es informes del análisis llevado a cabo. Este sistema se compone de cinco herramientas básicas:

– Herramienta de Análisis de Riesgo *(Risk Consultant)*.
– Programa de Evaluación de Riesgos de TI *(PC Security Consultant)*.
– Módulo para la evaluación de la compatibilidad de las soluciones aplicadas a la norma británica BS 7799 *(BS 7799 Security Consultant)*.
– Herramienta para el análisis de la compatibilidad de las funcionalidades de la organización con la política de seguridad aceptadas en la misma *(Policy Compliance Analyst)*.
– Módulo de apoyo a la creación y evaluación del plan de continuidad *(Continuity Consultant).*

MEHARI *(Methode Harmonisée d'Analyse de RIsques)* (30). Este método se deriva de los métodos MARION y MELISA, y es compatible con las Normas ISO 13335 e ISO 17799:2000 y BS7799-2: 2002. MEHARI se basa en el análisis de riesgos con el fin de medir el nivel de impacto. Para la aplicación del método, el producto de *software* RISICARE ofrece una serie de funciones: auditoría de vulnerabilidades, gestión de escenarios, planificación de la acción y la medición de los niveles de riesgo. El método evalúa:

– Las causas de los incidentes y la probabilidad de su ocurrencia.
– Las consecuencias y los impactos.
– Los escenarios de incidentes relacionados con aspectos comerciales y técnicos

MELISA *(Methode d'Evaluation de la Vulnerabilite Residuelle des Systèmes d'Informa)*. Este es un método de análisis de riesgos desarrollado por la Dirección General de Armamento francesa. El método ha sido adquirido por la empresa CF6, que lo ha promovido durante muchos años y ha desarrollado las bases de conocimiento para una gran cantidad de sistemas. Desde la adquisición de Telindus por CF6, MELISA ha sido abandonada por sus propietarios, a pesar de que era ampliamente utilizado en Francia.

(30) En: *http://www.clusif.asso.fr/fr/production/mehari/*

OCTAVE *(Operationally Critical Threat, Asset and Vulnerability Evaluation)* (31) es una colección de herramientas, técnicas y métodos para el desarrollo de análisis de riesgos basado en la gestión y organización de la planificación estratégica. Son todas las acciones que deben realizarse dentro de la organización para llevar a cabo la gestión de activos, para afrontar las amenazas potenciales y evaluar las vulnerabilidades. Ha sido desarrollado por SEI *(Software Engineering Institute)*.

CRAMM (32). Es la metodología aceptada por la CCTA *(Central Computer and Telecommunications Agency)* del Reino Unido, como norma gubernamental de análisis y gestión de riesgos. El proceso de gestión de riesgos, de acuerdo con esta metodología, consta de las tres etapas siguientes:

1. Identificación y evaluación de los recursos.
2. Evaluación de amenazas y vulnerabilidades.
3. Selección y recomendación de mecanismos de control y protección.

Para el análisis del riesgo el principal objetivo es la determinación de la probabilidad de ocurrencia de incidentes interfiriendo el funcionamiento normal de los recursos. Los recursos identificados son asignados a grupos de activos. A continuación se generan las listas de amenazas que pudieran afectar a un grupo determinado, y se determina nivel de riesgo de cada grupo (en una escala de cinco grados). Esta metodología utiliza software dedicado, que es su elemento integral de apoyo para determinadas etapas del método.

La versión actual del Sistema de CRAMM ha sido desarrollada y es comercializada por Insight. Es un paquete para la gestión y análisis de riesgo que consta de tres componentes, y que cuenta además con el apoyo de una gran biblioteca de encuestas, cuestionarios y recomendaciones. Hay dos versiones básicas de este sistema: simplificado *(Express)* y avanzado para profesionales *(Expert)*.

MAGERIT *(Metodología de Análisis y GEstión de Riesgos de IT)* (33). Es una metodología para el análisis de riesgos elaborada por el Ministerio de Administraciones Públicas, siendo la metodología más utilizada en España. MAGERIT persigue los siguientes objetivos:

---

(31) En: *http://www.cert.org/octave/*

(32) En: *http://www.cramm.com/*

(33) En: *http://administracionelectronica.gob.es/?_nfpb=true&_pageLabel=PAE_PG_CTT_General&langPae=es&iniciativa=184*

1. Objetivos directos:
   – Hacer que los responsables de los sistemas de información tomen conciencia tanto de la existencia de riesgos como de la necesidad de tratarlos a tiempo.
   – Ofrecer un método sistemático para el análisis de estos riesgos.
   – Ayudar en la descripción y la planificación de las medidas adecuadas para mantener los riesgos bajo control.
2. Objetivos indirectos:
   – Preparar a la organización para la evaluación de los procesos, la auditoría, y la certificación o acreditación, según proceda en cada caso.

También tiene como objetivo lograr la uniformidad en los informes que contienen los resultados y las conclusiones de un análisis de riesgos y gestión de proyectos.

*RiskPAC*. Es un paquete elaborado en Estados Unidos por la compañía CSCI *(Computer Security Consultants Inc.)*, y está orientado a la realización de análisis de riesgos y la definición de la influencia de este riesgo en los procesos de negocio. Se aplica tanto para el análisis cuantitativo como cualitativo de los riesgos. El *software RiskPAC* contiene: herramienta para el diseño de cuestionarios *(Designer Module)*, herramienta para la gestión de la evaluación de riesgos con el uso de los cuestionarios *(Survey Manager)*.

### OTRAS NORMAS Y METODOLOGÍAS

Otras normas de seguridad y metodologías de interés en el ámbito del presente capítulo son las que se listan a continuación:

1. Documentación de referencia TEMPEST (34):
   – NACSIM 5000. TEMPEST *Fundamentals*.
   – NSA 94-106. *NSA Specification for RF-Shielded Enclosure for Communications Equipment.*
   – NSA 73-2A. *NSA Specification for Foil RF-Shielded Enclosure.*
2. Controles de Seguridad y Guías de Implementación:
   – ISO/IEC 27002. *Information technology-Security techniques-Code of practice for information security management* (35).

(34) En: *http://cryptome.org/nsa-tempest.htm*
(35) En: *http://www.iso27001security.com/html/27002.html*

- NIST SP 800-53. *Recommended Security Controls for Federal Information Systems* (36).
- DoD 8500.2. *Department of Defense Instruction 8500.2. Security controls implementation guide* (37).

3. Acreditación y certificación en seguridad:
   - *Common Criteria* (38).
   - Es un marco en el que los usuarios pueden especificar sus requisitos funcionales y de aseguramiento de la seguridad, los vendedores aplicar y/o certificar determinados aspectos sobre los atributos de seguridad de sus productos, y los laboratorios de ensayo evaluar los productos para determinar si, efectivamente, cumplen los requisitos establecidos:
     - ISO/IEC 15408-1. *Information technology-Security Techniques-Evaluation Criteria for IT Security-Part 1: Introduction and general model.*
     - ISO/IEC 15408-2. *Information technology-Security Techniques-Evaluation Criteria for IT Security-Part 2: Security functional requirements.*
     - ISO/IEC 15408-3. *Information technology-Security Techniques-Evaluation Criteria for IT Security-Part 3: Security assurance requirements.*
     - ISO/IEC 18045. *Information Technology-Security Techniques-Methodology for IT Security evaluation.*
     - DoD 8000.1. DIACAP *(DoD Information Assurance Certification and Accreditation Process)* (39).
4. Gestión de la continuidad:
   - BS 25999. *BSI standard for Business Continuity Management Systems (System Requirements)* (40).

(36) En: *http://csrc.nist.gov/publications/nistpubs/800-53A*
(37) En: *http://www.cac.mil/assets/pdfs/DoDD_8500.2.pdf*
(38) En: *http://www.commoncriteriaportal.org/*
(39) En: *http://www.diacap.net/*
(40) En: *http://www.bsigroup.com/en/Assessment-and-certification-services/management-systems/Standards-and-Schemes/BS-25999/*

## Conclusiones

En un reciente informe (41) en el que se revisan las principales implicaciones, retos y desafíos que supone la introducción sistemática del uso del ciberespacio a nivel mundial, tanto en la economía como en el ámbito militar, etc., se identifican 21 aspectos que en este momento son todavía un desafío. Éstos se agrupan en tres grandes categorías: el primer grupo está fundamentalmente condicionado por aspectos sicológicos y de naturaleza humana, el segundo por aspectos organizativos y el tercero por aspectos tecnológicos. De los 21 grandes desafíos que plantea el ámbito del ciberespacio, al menos ocho de ellos debe abordarse y solucionarse esencialmente con propuestas tecnológicas:

– El problema de la atribución de las acciones y los ataques en el ciberespacio, que ya ha sido esbozado en secciones previas y que está en la base para poder disponer de un ciberespacio seguro.
– La necesidad de una monitorización y auditoría continua de los sistemas, esto es, la necesidad de implementar buenas prácticas de manera sistemática, que ha sido el hilo conductor de este capítulo.
– La necesidad de protección de los datos desde el punto de vista de su confidencialidad, integridad, y disponibilidad, frente al concepto más tradicional de protección de las redes y los sistemas operativos, la protección de ciberperímetro.
– La detección de intrusión de manera rápida y eficaz.
– La capacidad de adaptación y recuperación de los sistemas cuando se ven sometidos a ataques.
– El problema del control sobre la cadena de suministro de sistemas y componentes de manera que siempre se disponga de un *software* y *hardware* autenticado.
– La integración de sistemas de protección basados en tecnologías diferentes, con conceptos y niveles de protección diferentes y muchas veces con enfoques de soluciones multipunto.
– Todo el abanico de posibilidades, pero también de riesgos, que se abren con la virtualización y el *Cloud Computing*.

De los anteriores posiblemente los dos aspectos más críticos que todavía tienen que resolverse mediante un enfoque tecnológico son el pro-

(41) Winterfeld, Steve (dir.): *Understanding Today's Cyber Challenges,* Technology TASC, mayo de 2011.

blema de la atribución y el de la garantía en la seguridad de la cadena de suministro.

Así pues, a la vista de todos los aspectos desarrollados en las secciones previas, es necesario concluir este capítulo resaltando la importancia intrínseca que tiene la tecnología en el nuevo paradigma relacional representado por el ciberespacio. Sin la infraestructura tecnológica en la que se apoya, sencillamente el ciberespacio no existe.

## COMPOSICIÓN DEL GRUPO DE TRABAJO

*Presidente:* D. JOSÉ RAMÓN CASAR CORREDERA
*Catedrático de Universidad de la Escuela Técnica Superior de Ingenieros de Telecomunicaiones de la Universidad Politécnica de Madrid*

*Secretario-coordinador:* D. ÁNGEL GÓMEZ DE ÁGREDA
*Teniente coronel del Ejército del Aire.*

*Vocales:* D. LUIS FELIU ORTEGA
*Teniente general del Ejército de Tierra (R).*

D. CARLOS ENRÍQUEZ GONZÁLEZ
*Comandante del Ejército de Tierra.*

D. JAVIER LÓPEZ DE TURISO Y SÁNCHEZ
*Teniente coronel del Ejécito del Aire.*

D. ÓSCAR PASTOR ACOSTA
*Gerente de Seguridad de Ingeniería de Sistemas para la Defensa de España, S. A.*

D. MANUEL PÉREZ CORTÉS
Security & Defense.

# ÍNDICE

## RELACIÓN DE MONOGRAFÍAS DEL CESEDEN

***1.** Clausewitz y su entorno intelectual. (Kant, Kutz, Guibert, Ficht, Moltke, Sehlieffen y Lenia)

***2.** Las Conversaciones de Desarme Convencional (CFE)

***3.** Disuasión convencional y conducción de conflictos: el caso de Israel y Siria en el Líbano

***4.** Cinco sociólogos de interés militar

***5.** Primeras Jornadas de Defensa Nacional

***6.** Prospectiva sobre cambios políticos en la antigua URSS. (Escuela de Estados Mayores Conjuntos. XXIV Curso 91/92)

***7.** Cuatro aspectos de la Defensa Nacional. (Una visión universitaria)

**8.** Segundas Jornadas de Defensa Nacional

**9.** IX y X Jornadas CESEDEN-IDN de Lisboa

**10.** XI y XII Jornadas CESEDEN-IDN de Lisboa

**11.** *Anthology of the essays* (Antología de textos en inglés)

***12.** XIII Jornadas CESEDEN-IDN de Portugal. La seguridad de la Europa Central y la Alianza Atlántica

**13.** Terceras Jornadas de Defensa Nacional

***14.** II Jornadas de Historia Militar. La presencia militar española en Cuba (1868-1895)

***15.** La crisis de los Balcanes

***16.** La Política Europea de Seguridad Común (PESC) y la Defensa

**17.** *Second anthology of the essays* (Antología de textos en inglés)

***18.** Las misiones de paz de la ONU

***19.** III Jornadas de Historia Militar. Melilla en la historia militar española

**20.** Cuartas Jornadas de Defensa Nacional

**21.** La Conferencia Intergubernamental y de la Seguridad Común Europea

***22.** IV Jornadas de Historia Militar. El Ejército y la Armada de Felipe II, ante el IV centenario de su muerte

**23.** Quinta Jornadas de Defensa Nacional

**24.** Altos estudios militares ante las nuevas misiones para las Fuerzas Armadas

**25.** Utilización de la estructura del transporte para facilitar el cumplimiento de las misiones de las Fuerzas Armadas

**26.** Valoración estratégica del estrecho de Gibraltar

**27.** La convergencia de intereses de seguridad y defensa entre las Comunidades Europeas y Atlánticas

**28.** Europa y el Mediterráneo en el umbral del siglo XXI

**29.** I Congreso Internacional de Historia Militar. El Ejército y la Armada en 1898: Cuba, Puerto Rico y Filipinas

**30.** Un estudio sobre el futuro de la no-proliferación

**31.** El islam: presente y futuro

**32.** Comunidad Iberoamericana en el ámbito de la defensa

**33.** La Unión Europea Occidental tras Ámsterdam y Madrid

**34.** Iberoamérica, un reto para España y la Unión Europea en la próxima década

**35.** La seguridad en el Mediterráneo. (Coloquios C-4/1999)

**36.** Marco normativo en que se desarrollan las operaciones militares

**37.** Aproximación estratégica española a la última frontera: la Antártida

**38.** Modelo de seguridad y defensa en Europa en el próximo siglo

***39.** V Jornadas de Historia Militar. La Aviación en la guerra española

**40.** Retos a la seguridad en el cambio de siglo. (Armas, migraciones y comunicaciones)

**41.** La convivencia en el Mediterráneo Occidental en el siglo XXI

**42.** La seguridad en el Mediterráneo. (Coloquios C-4/2000)

**43.** Rusia: conflictos y perspectivas

**44.** Medidas de confianza para la convivencia en el Mediterráneo Occidental

**45.** La cooperación Fuerzas de Seguridad-Fuerzas Armadas

**46.** La ética en las nuevas misiones de las Fuerzas Armadas

**47.** VI Jornadas de Historia Militar. Operaciones anfibias de Gallípolis a las Malvinas

**48.** La Unión Europea: logros y desafíos

**49.** La seguridad en el Mediterráneo. (Coloquios C-4/2001)

**50.** Un nuevo concepto de la defensa para el siglo XXI

**51.** Influencia rusa en su entorno geopolítico

**52.** Inmigración y seguridad en el Mediterráneo: el caso español

**53.** Cooperación con Iberoamérica en el ámbito militar

**54.** Retos a la consolidación de la Unión Europea

**55.** Revisión de la Defensa Nacional

**56.** Investigación, Desarrollo e innovación (I+D+i) en la defensa y la seguridad

**57.** VII Jornadas de Historia Militar. De la Paz de París a Trafalgar (1763-1805). Génesis de la España Contemporánea

**58.** La seguridad en el Mediterráneo. (Coloquios C-4/2002)

**59.** El Mediterráneo: Proceso de Barcelona y su entorno después del 11 de septiembre

**60.** La industria de defensa: el desfase tecnológico entre la Unión Europea y Estados Unidos de América

**61.** La seguridad europea y las incertidumbres del 11 de septiembre

**62.** Medio Ambiente y Defensa

**63.** Pensamiento y pensadores militares iberoamericanos del siglo xx y su influencia a la Comunidad Iberoamericana

**64.** Estudio preliminar de la operación: *Libertad para Irak*

**65.** Adecuación de la defensa a los últimos retos

**66.** VIII Jornadas de Historia Militar. De la Paz de París a Trafalgar (1763-1805). La organización de la defensa de la Monarquía

**67.** Fundamentos de la Estrategia para el siglo XXI

**68.** Las fronteras del mundo iberoamericano

**69.** Occidente y el Mediterráneo: una visión para una nueva época

**70.** IX Jornadas de Historia Militar. De la Paz de París a Trafalgar (1763-1805). Las bases de la potencia hispana

**71.** Un concepto estratégico para la Unión Europea

**72.** El vínculo trasatlántico

**73.** Aproximación a las cuestiones de seguridad en el continente americano

**74.** Defensa y Sociedad Civil

**75.** Las organizaciones internacionales y la lucha contra el terrorismo

**76.** El esfuerzo de Defensa. Racionalización y optimización

**77.** El vínculo trasatlántico en la guerra de Irak

**78.** Mujer, Fuerzas Armadas y conflictos bélicos. Una visión panorámica

**79.** Terrorismo internacional: enfoques y percepciones

**80.** X Jornadas de Historia Militar. De la Paz de París a Trafalgar (1763-1805). El acontecer bélico y sus protagonistas

**81.** Opinión pública y Defensa Nacional en Iberoamérica

**82.** Consecuencias de la guerra de Irak sobre el Mediterráneo Occidental

**83.** La seguridad en el Mediterráneo. (Coloquio C-4/2004-2005)

**84.** Hacia una Política de Cooperación en Seguridad y Defensa con Iberoamérica

**85.** Futuro de la Política Europea de Seguridad y Defensa

**86.** Una década del Proceso de Barcelona: evolución y futuro

**87.** El conflicto árabe-israelí: nuevas expectativas

**88.** Avances en Tecnologías de la Información y de la Comunicación para la Seguridad y la Defensa

**89.** La seguridad en el Mediterráneo (Coloquio C-4/2006)

**90.** La externalización en las Fuerzas Armadas. Equilibrio entre apoyo logístico propio y el externalizado

**91.** La entrada de Turquía en la Unión Europea

**92.** La seguridad en el Mediterráneo: complejidad y multidimensionalidad

**93.** La situación de seguridad en Irán: repercusión en el escenario regional y en el entorno mundial

**94.** Tecnología y Fuerzas Armadas

**95.** Integración de extranjeros en las Fuerzas Armadas españolas

**96.** El mundo iberoamericano ante las actuales retroestratégicas

**97.** XI Jornadas de Historia Militar. La enseñanza de la Historia Militar en las Fuerzas Armadas

**98.** La energía y su relación con la Seguridad y Defensa

**99.** Prospectiva de Seguridad y Defensa: viabilidad de una Unidad de Prospectiva en el CESEDEN

**100.** Repercusión del actual reto energético en la situación de seguridad mundial

**101.** La evolución de la Seguridad y Defensa en la Comunidad Iberoamericana

**102.** El Oriente Próximo tras la crisis de El Líbano

**103.** Los estudios de posgrado en las Fuerzas Armadas

**104.** Las fronteras exteriores de la Unión Europea

**105.** La industria y la tecnología en la Política Europea de Seguridad y Defensa

**106.** De la milicia concejil al reservista. Una historia de generosidad

**107.** La Agencia Europea de Defensa: pasado, presente y futuro

**108.** China en el sistema de seguridad global del siglo XXI

**109.** Naciones Unidas como principal elemento del multilateralismo del siglo XXI

**110.** Las relaciones de poder entre las grandes potencias y las organizaciones internacionales

**111.** Las nuevas guerras y la Polemología

**112.** La violencia en el siglo XXI. Nuevas dimensiones de la guerra

**113.** Influencia de la nueva Rusia en el actual sistema de seguridad

**114.** La nueva geopolítica de la energía

**115.** Evolución del concepto de interés nacional

**116.** Sesenta años de la OTAN ¿Hacia una nueva estrategia?

**117.** La importancia geostratégica de África Subsahariana

**118.** El Mediterráneo: cruce de intereses estratégicos

**119.** Seguridad nacional y estrategias energéticas de España y Portugal

**120.** Las armas NBQ-R como armas de terror

**121.** El futuro de las relaciones Latinoamérica-Estados Unidos

**122.** La influencia social del islam en la Unión Europea

**123.** África ¿nuevo escenario de confrontación?

**124.** Las nuevas guerras: globalización y sociedad

**125.** El impacto de la crisis económica en el área de la seguridad y la defensa

---

* Agotado. Disponible en las blibliotecas especializadas y en el Centro de Documentación del Ministerio de Defensa.