LAS NUEVAS AMENAZAS CIBERNETICAS DEL S.XXI CIBERTERRORISMO: NUEVA FORMA DE SUBVERSIÓN Y DESESTABILIZACIÓN

ÁLVARO ORTIGOSA

PROFESOR DE LA ESCUELA POLITÉCNICA SUPERIOR DE LA UNIVERSIDAD AUTÓNOMA DE MADRID (UAM). DIRECTOR DEL MÁSTER EN ANÁLISIS DE EVIDENCIAS DIGITALES Y LUCHA CONTRA EL CIBERCRIMEN. MIEMBRO DE CNEC –ICFS

LUIS FERNANDO HERNANDEZ GARCIA

UNIDAD DE CIBERSEGURIDAD - JEFATURA DE INFORMACIÓN DE LA GUARDIA CIVIL

RESUMEN

La sociedad, soporte del individuo como ser social, es un ecosistema en constante mutación y evolución, y esta a lo largo del último cuarto de siglo ha experimentado cambios sin precedentes; la generalización en el uso de las Tecnologías de la Información y las Comunicaciones ha propiciado un fenómeno sin precedentes y con profunda influencia en lo político, social y económico. El fenómeno de *Internet* ha traído consigo la mayor revolución tecnológica que ha vivido la humanidad; más allá de los aspectos meramente técnicos y productivos, ha tenido y sigue teniendo una significada repercusión en la forma de moldear nuevos hábitos y comportamientos sociales. Resulta incuestionable que esta revolución tecnológico-social ha aportado aspectos muy positivos, como lo es la globalización del conocimiento y su acceso universal, pero como ocurre con demasiada frecuencia, esta creación humana también está siendo utilizada para satisfacer los ilícitos intereses de individuos y grupos faltos de escrúpulos, que han visto una oportunidad para saciar sus oscuros e ilegítimos intereses. De esta forma, términos tales como *ciberterrorismo, hacktivismo, ciberdelito, ciberespionaje o ciberguerra* se están haciendo un hueco en lo cotidiano; de igual manera, las relaciones entre Estados se están viendo profundamente distorsionadas y en algunos casos gravemente alteradas.

Palabras Clave: ciberterrorismo, ciberamenazas, ciberseguridad, ciberyihadismo, cibercalifato.

ABSTRACT

Society, individual support as a social being, is an ecosystem constantly mutating and envolving, and has suffered a unmatched change along the last quarter century; the spread of using Information and Communication Technologies has led to an unprecedented phenomenon and with a deep influence political, social and economic. The Internet phenomenon has brought the greatest technologic revolt that Hummanity have seen; beyond technical and production issues, have had and still having a signified impact on they way of develop new social habbits and behaviors. It is unquestionable that this social-technologic revolution has provided very positive aspects, as the knowledge

globalization and universal access, but as happens too often, this human creation is also being used for satisfy the illicit interests of unscrupulous groups and indivuduals that have seen the chance for accomplish their dark and illegal interests. Thereby terms like *cyberterrorism*, *hacktivism*, cybercrime, *cyberspying* or *cyberwar* are finding a niche in everyday life; same form, relationships between States are beeing deeply distorted and sometimes severely upset.

Keywords: Cyberterrorism, cyberthreats, cybersecurity, cyberyihad, cyberkahilafah.

La sociedad, soporte del individuo como ser social, es un ecosistema en constante mutación y evolución, que a lo largo del último cuarto de siglo ha experimentado cambios sin precedentes; la generalización en el uso de las *Tecnologías de la Información y las Comunicaciones (*TIC) ha propiciado un fenómeno sin precedentes y con profunda influencia en lo político, social y económico. El fenómeno de *Internet* ha traído consigo la mayor revolución tecnológica que ha vivido la humanidad; más allá de los aspectos meramente técnicos y productivos, ha tenido y sigue teniendo una significada repercusión en la forma de moldear nuevos hábitos y comportamientos sociales. La denominada "globalización" representa un marco de grandes oportunidades, pero lleva pareja riesgos, la mayoría a priori intangibles y por lo tanto de difícil percepción, que en una imparable escalada están llegando a tener trascendentales repercusiones. Internet ha pasado de ser un sueño de visionarios, allá por los años 70, un valioso instrumento de investigación, en los 80, o un insustituible elemento en el crecimiento económico, en los 90, a irrumpir con fuerza de la mano del nuevo siglo, para convertirse en el mayor fenómeno social conocido, con marcada influencia en lo cotidiano.

Resulta incuestionable que esta revolución tecnológico-social ha aportado aspectos muy positivos, como lo es la globalización del conocimiento y su acceso universal. Con la extensión de la Red se ha proporcionado interoperabilidad a millones de usuarios de todo el mundo con un abanico de servicios hasta ahora impensables -navegación y acceso a contenidos web tanto abiertos como restringidos, correo electrónico, trasmisión de audio y video en tiempo real, redes sociales, mensajería instantánea, información compartida, transferencia y salvaguarda de datos, tanto personales como profesionales, etc. y todo en tiempo real; así pues, a través de la Red de redes, estamos siendo testigos de excepción de una total transformación de las relaciones humanas. Pero como ocurre con demasiada frecuencia, esta creación humana también ha sido y está siendo utilizado para satisfacer los ilícitos intereses de individuos y grupos faltos de escrúpulos que han visto en *Internet* una oportunidad para saciar sus oscuros e ilegítimos intereses. De esta forma términos tales como *ciberdelito*, *ciberterrorismo*, *hacktivismo*, *ciberespionaje* o *ciberguerra* se están haciendo un hueco en lo cotidiano, hasta tal punto que los ciudadanos están aprendiendo a convivir con esta nueva realidad, ya que cada vez está siendo más frecuente hallar noticias sobre algún hecho ilícito que se ha producido a través de la red. De igual manera, las relaciones entre Estados se están viendo profundamente distorsionadas y en algunos casos gravemente alteradas.

Estos nuevos marcos de relación en lo social, cultural, económico, político y militar dependen cada vez en mayor medida de lo que acontece en el denominado *ciberespacio*, y han hecho más que convenientemente necesario articular un *Sistema de Seguridad*

Nacional[1], que gestione los riesgos que amenazan su funcionamiento. Su más clara aproximación hasta la fecha es la aprobación por parte del Gobierno de España de la Estrategia de Seguridad Nacional (ESN) -de 31 de mayo del 2013-, ahondando y concretando a través de la Estrategia de Ciberseguridad Nacional (ECSN), de la Estrategia de Seguridad Marítima Nacional (ESMN)-ambas de 5 de diciembre del 2013- y de la Estrategia de Seguridad Energética Nacional (ESEN) –de 20 de julio del 2015-. En estos documentos las *ciberamenazas* se presentan como una amenaza trasversal que afecta a todas las estrategias hasta la fecha aprobadas y que previsiblemente también estarán presentes en las que sean aprobadas en el futuro.

Para el profesor Manel Medina «*el ciberespacio es una red etérea e intangible de infraestructuras tecnológicas, entre las que se encuentra Internet, las redes de telecomunicaciones, redes sociales y plataformas de mensajería, nubes de ordenadores y ordenadores incrustados en controladores de infraestructuras críticas*»[2].

El presente documento se estructura en seis bloques temáticos que, aunque se presenten relativamente diferenciados, no dejan de ser partes de un todo, con niveles de interrelación (imbricación) tales que resultaría difícil y sesgado tratar cada uno de ellos de forma autónoma; Iniciando la exposición con un bloque introductorio de lo que hoy en día engloba el término *seguridad*, seguido por un segundo en el que se pretende evidenciar los problemas y retos que una "sociedad digital" como la actual tiene que afrontar desde la perspectiva de la *ciberseguridad*; el tercero comprenderá una sucinta exposición sobre las nuevas *ciberamenazas*, para enlazar con una visión descriptiva de capacitación y respuesta coordinadas desde el Gobierno de España en lo que podríamos bautizar como *ciberrespuestas*, resultando obligado recoger en el texto un breve estudio de las diferentes *estrategias de seguridad nacional y ciberseguridad*, nacionales y europeas que nos son de aplicación. Por último se relatarán las principales *iniciativas* de la Jefatura de Información de la Guardia Civil en materia de ciberseguridad.

La pretensión del documento no es otra que la de esbozar una visión actualizada, con una perspectiva amplia -nacional e internacional- y desde diferentes enfoques de cómo, desde las diferentes organizaciones de investigación e inteligencia, se afrontan los nuevos retos de combatir a la delincuencia especializada, el terrorismo y otras

1 *El año 2013 trajo consigo aportaciones fundamentales a la política de Seguridad Nacional en forma de nuevos documentos estratégicos y de una estructura integral orientada a la mejor organización del Sistema de Seguridad Nacional. En cuestión de meses se aprobaron tres estrategias y se constituyeron órganos interministeriales con poder de decisión, coordinación y apoyo en materia de Seguridad Nacional. La aprobación de dichos instrumentos vino precedida de cambios en la estructura de la Presidencia del Gobierno. Al comienzo de la presente Legislatura se detectó la necesidad de dotar al Gabinete de la Presidencia del Gobierno de un órgano eficaz que sucediera al Departamento de Infraestructura y Seguimiento de Situaciones de Crisis (DISSC) en la función de prestar asesoramiento y apoyo técnico en materia de Seguridad Nacional a la Presidencia del Gobierno. Ello se materializó en la creación del Departamento de Seguridad Nacional del Gabinete de la Presidencia del Gobierno (DSN) mediante el Real Decreto 1119/2012, de 20 de julio, de modificación del Real Decreto 83/2012, de 13 de enero, por el que se reestructura la Presidencia del Gobierno...* [Resulta recomendable la lectura del capítulo "El Sistema de Seguridad Nacional" del Informe Anual de Seguridad Nacional 2013].

2 *El profesor Manel Medina es Catedrático de la Universidad Politécnica de Cataluña (UPC) y hasta 2014 subdirector de Programas de la Agencia Europea de Seguridad de la Información (ENISA); su definición del Ciberespacio está recogida en el libro Cibercrimen - Aprende de víctimas, expertos y cibervigilantes.*

amenazas; concretando aún más en aquellas unidades de Investigación Tecnológica del Cuerpo de la Guardia Civil, integradas en las Jefaturas de Información y Policía Judicial, y enfatizando aquellos que afectan al ámbito de responsabilidad del *SIGC* (acrónimo histórico del Servicio de Información de la Guardia Civil).

La dualidad *"Ciberamenaza Vs Ciberseguridad"* es una realidad en permanente metamorfosis. A pesar de los constantes esfuerzos, tanto gubernamentales como del sector privado, cada día resulta más evidente que las acciones hostiles dirigidas contra los sistemas informáticos, especialmente aquellos vinculados de alguna manera a Internet, son algo más que una amenaza y se han transformado en una *riesgo emergente*. Esto es más evidente cuando se vinculan al concepto de infraestructuras críticas (IC,s) en general e infraestructuras críticas de la información (ICI,s) en particular.

1. SEGURIDAD, TÉRMINO ANTIGUO, CONCEPTO NUEVO

El nuevo concepto de *seguridad* surge en la década de los ochenta del pasado siglo XX. Una vez que se hace realidad la distensión Este-Oeste, donde el empleo de la fuerza, incluida la nuclear, era el eje principal del concepto tradicional de la seguridad, emerge la realidad de considerar a la seguridad bajo un prisma más amplio que incardine, entre otros, a los riesgos económicos, medioambientales, delincuencia transnacional o que surgen de cuestiones de identidad social. Se ha pasado de un periodo de bipolaridad de la guerra fría a una multipolaridad. La globalización provocada por la revolución de la tecnologías de la información ha invadido exponencialmente los espacios de todas las actividades humanas, conformando un concepto de seguridad más heterogéneo de multipolaridad que contrasta con la unipolaridad que ejerció Estados Unidos desde la distensión de la guerra fría hasta los atentados del 11 de septiembre de 2001 (11-S). Desde esa fecha tan fatídica se ha evidenciado que el poder militar por sí solo, aunque siendo de un gran potencial, no es determinante para conseguir combatir adecuadamente los conflictos asimétricos. Los problemas globales de seguridad afectan a toda la comunidad internacional; el terrorismo yihadista, el tráfico encubierto de armas de destrucción masiva, la delincuencia internacional organizada –narcotráfico, tráfico clandestino de seres humanos o de armas, blanqueo de capitales y financiación del terrorismo, etc.− crecientes problemas medioambientales, pandemias, hambrunas, guerras y sus consecuentes éxodos de refugiados. Estos problemas, configuran un escenario de seguridad con un enfoque novedoso, donde el motivo no solo es el Estado, sino que el individuo es también un elemento fundamental en cuanto sujeto a proteger y como actor imprescindible para colaborar en la prevención y respuesta -concienciación-.

2. CIBERSEGURIDAD, LA SEGURIDAD EN EL CIBERESPACIO

Y es precisamente a raíz de los atentados del 11-S, cuando en los diferentes entes gubernamentales, tanto de los Estados Unidos como de los países occidentales, se generalizó la *percepción de la amenaza desde el ciberespacio*; inicialmente orientada hacia la potencial actuación de organizaciones terroristas, de ahí que tomara fuerza el concepto de ciberterrorismo como una amenaza global. Transcurrida ya más de una década, la realidad se ha mostrado muy diferente, ya que el concepto de ciberterrorismo se ha visto desplazado del todo a una parte de un nuevo

concepto globalizador, el de *ciberamenaza*, y frente a esta, como antagonista, el ya mencionado de la *ciberseguridad*.

Para entender este nuevo escenario y estar en condiciones de interactuar en él resulta fundamental adquirir una *conciencia de ciberseguridad*, tanto en lo profesional como en lo personal, faceta esta que se convierte en vertebral, ya que la seguridad es una percepción que permite al ser humano y a las organizaciones desarrollar de una forma armónica sus relaciones. Y es que las relaciones sociales se desarrollan en marcos conceptuales definidos, en los que la seguridad jurídica y el cumplimiento de la ley y de las normas establecidas permiten una ordenación estable, definida. Pero los espacios donde esas relaciones se desarrollan no están aún regulados, porque la velocidad de los cambios son significativamente superiores al de su marco regulatorio de referencia racionalmente establecido.

Para la ESN España, al igual que el resto de países de nuestro entorno sociocultural, está expuesta a los ciberataques, que no solo generan elevados costes económicos sino también, y lo que es más importante, la pérdida de confianza de los ciudadanos en unos sistemas que, en la actualidad, resultan críticos para el normal funcionamiento de la sociedad.

3. CIBERAMENAZAS, LAS NUEVAS AMENAZAS TRANSNACIONALES DEL S.XXI

Y es que las nuevas amenazas para nuestra seguridad, tanto individual como colectiva, son múltiples, diversas y cambiantes, e *Internet y su tecnología asociada* están contribuyendo a ello de una forma cada vez más determinante -*ciberamenazas*-, ya que están siendo utilizados con profusión como *soporte* para la ejecución de tradicionales acciones ilícitas, pero con novedosos *modus operandi*; y no solo empleados por los grupos delincuenciales al uso -que se han adaptado y rápido a los nuevos tiempos- sino también por otras formas de delincuencia grave y organizada, tales como *grupos y organizaciones terroristas*, colectivos antiglobalización y antisistema -preferentemente a través del denominado *hacktivismo*- o que tienen como fin último la desestabilización de un Estado en particular, atacando su estructura social, económica y política, sin olvidar organizaciones clandestinas, e incluso acciones encubiertas de las estructuras de inteligencia de algunos Estados.

Al hablar de delincuencia vinculada a organizaciones terroristas o afines, debemos contemplar Internet y las TIC desde una óptica amplia; verlo como parte de su “negocio”, su forma de obtener ilícitos beneficios o saciar sus más depravados instintos; para ellos representa una oportunidad, sin precedentes, de organizarse, comunicarse y coordinarse, de compartir, de proclamar, intoxicar y difamar, de reclutar y financiarse, etc… y todo ello con unas condiciones de seguridad y anonimato inusuales.

Quizás antes de continuar con la exposición; resulte oportuno adelantar una de las posibles conclusiones, y es el hecho de considerar algunas de las ideas que a lo largo de este documento se exponen como parte de una visión fatalista y alejada de la realidad; es por ello que se debe *desmitificar pero no subestimar* el riesgo creciente que supone Internet como medio e instrumento del denominado “Ciberterrorismo”.

3.1. CIBERDELITO

El *ciberdelito*[3] conforma naturalmente uno de los cinco grandes bloques de las ciberamenazas del siglo XXI, pero no será tratado con profundidad en el presente monográfico. Esto es así porque, como se adelantó en la introducción, este trabajo se orienta hacia las responsabilidades que recaen en el ámbito competencial de la Jefatura de Información y, como es lógico, el ciberdelito, entendido como tal, incurre plenamente en el marco de actuación de la Jefatura de Policía Judicial. No obstante, sí se considera oportuno realizar ciertos apuntes sobre la materia para entender la magnitud del problema y porque la aplicación "transversal" de ciertas tecnologías es común a todas las ciberamenazas. La globalización de la delincuencia y la indeterminación del ámbito geográfico en el que viene actuando la delincuencia organizada trasnacional en las últimas dos décadas, donde el lucro obtenido por el ciberdelito se estima supera ya el del tráfico de drogas, armas y seres humanos juntos -cifrado por las autoridades de EE.UU en 2012 en 1'3 billones de US $, el 1'7% del PIB mundial- genera constantes conflictos de jurisdicción entre estados o en el peor de los casos impunidad. Pero en este sombrío panorama se llegó a un acuerdo histórico, el conocido como Convenio de Budapest, promovido por el Consejo de Europa y aprobado el 23 de noviembre del 2001 en la ciudad de Budapest, de ahí su nombre. El Convenio de Budapest es, sin lugar a dudas, un acuerdo nacido con vocación universal, que supuso y sigue siendo el máximo referente para la lucha contra la ciberdelinciencia y el único tratado que tiene por objeto la armonización normativa del derecho penal de las naciones o estados que lo ratifican. Nuestro país lo ratificó en 2010 y se unió así a los Estados miembros de la UE que lo han ratificado -23 países-. Y a través de la Estrategia de Ciberseguridad de la UE se ha solicitado a los cinco Estados que aún no lo han ratificado que así lo hagan y lo incorporen a su ordenamiento jurídico -Grecia, Irlanda, Luxemburgo, Polonia y Suecia- buscando con ello la homogeneización normativa, o su universalización cuando menos, en el espacio común europeo.

3.2. CIBERTERRORISMO

Retomando el concepto de *ciberterrorismo* y haciendo una interpretación extensiva del término, se vincula al uso que de las TIC en general, y de Internet en particular, vienen haciendo las organizaciones terroristas y grupos afines, para la consecución de sus objetivos, siempre enmarcados en el uso de estas TIC como *medio o instrumento*, más que como *objetivo* de la acción ilícita -momento en que en realidad sí nos encontraríamos ante una acción pura del denominado ciberterrorismo-. Por lo tanto, en su concepción estricta, estaría orientado a la realización de acciones ofensivas contra los sistemas de información y comunicaciones que sustentan el normal funcionamiento de las denominadas Infraestructuras Críticas (IC,s) y Estratégicas, así como cualquier otro servicio esencial para la ciudadanía.

3 *Quizás, de entre todas las definiciones de delito informático o Cibercrimen la que goza de mayor aceptación, por el consenso alcanzado, ha sido la realizada por el Consejo de Europa a través de su Convenio de Ciberdelincuencia. Éste, fue promulgado a la firma, el 23 de noviembre del 2001 en Budapest, y ratificado por España en el año 2010. Posteriormente, en enero de 2003, se añadió al Convenio un Protocolo Adicional para criminalizar los actos de racismo y xenofobia cometidos a través de sistemas informáticos.*

En el seno de la Unión Europea ya en el año 2002, y a través de la DM 173/2002[4], al analizar la amenaza de ataques terroristas contra los sistemas de información vitales de la UE ya se vislumbró la naturaleza del riesgo de ciberataques para emplear expresamente el término ciberterrorismo.

El año 2015 nos ha traído un nuevo término asociado al ciberterrorismo, el *ciberyihadismo*[5], "*que usando métodos, procedimientos y herramientas del terrorismo, el hacktivismo y la ciberguerra constituye una realidad incipiente y supone una de las mayores amenazas con las que se enfrentarán las sociedades occidentales en los próximos años. Las importantes vías de financiación de estos grupos, al socaire de Daesh, hacen posible que puedan llegar a adquirir los conocimientos y las herramientas precisas para el desarrollo de ciberataques o la contratación de los mismos. Hasta el momento sus ciberataques se han limitado a la desfiguración de páginas web, ataques DDoS a pequeña escala o, más comúnmente, al uso de Internet y de las redes sociales para la diseminación de propaganda o el reclutamiento y la radicalización, actividades que no exigen grandes conocimientos o infraestructuras.*

En julio del 2015 se constituyó una nueva estructura en Europol, esta vez focalizada en la prevención y respuesta del fenómeno del ciberterrorismo y bautizada como *Unidad de Referencia de Internet* – IRU– (Internet Referral Unit).

Pero, como ya se ha dicho, los tiempos y los conceptos cambian. Volviendo a la reflexión sobre el dualismo *"ciberamenazas Vs ciberseguridad"*, un factor fundamental es que las primeras pueden tener su origen no solo en organizaciones terroristas, sino en países o estados -tanto hostiles como "aliados"-, redes de delincuencia organizada, movimientos y colectivos reivindicativos de toda índole, hackers, etc. De hecho, los incidentes más serios que han acontecido en los últimos años se han centrado en acciones de *espionaje (económico, militar y político), sabotaje*, *desobediencia civil e incluso guerra*.

Concretando aún más el concepto, se pueda hablar del:

- *Uso con fines terroristas*: las diferentes organizaciones terroristas, vienen utilizando las TIC e Internet como instrumento[6] para la consecución de sus objetivos y, en este sentido, utilizan en su beneficio las posibilidades que las nuevas tecnologías les ofrecen para ocultar sus comunicaciones o blindar la información contenida en los ordenadores que les son incautados. De hecho, en los últimos años se ha realizado un gran esfuerzo para dotar, humana y materialmente a los departamentos de Informática Forense, a fin de poder dar respuesta al aumento, casi exponencial, tanto del número de dispositivos incautados como de la de complejidad de su análisis. Así mismo, destacar el uso de Internet y las

4 *Decisión Marco del Consejo, Bruselas 19.04.2002 COM(2002)173 final 2002/0086 (CNS).*

5 *Ciberyihadismo, terminología y reflexiones acuñadas por el Centro Criptológico Nacional. Véase CCN-CERT IA-09/16 CIBERAMENAZAS 2015 / TENDENCIAS 2016 [RESUMEN EJECUTIVO].*

6 *Es una realidad que ya no existen operaciones contra cédulas, taldes o grupos terroristas en las que no se intervengan medios informáticos, es más, la presencia de estos ha experimentado un crecimiento exponencial, no tanto en el número sino en su capacidad de almacenamiento, lo que ha obligado a afrontar nuevos retos en todo lo relativo a la informática forense; tanto por su complejidad como por los cada vez más sofisticados procedimientos y sistemas informáticos que dan soporte a las necesidades de las unidades de lucha antiterrorista. En este sentido destacar el éxito obtenido con el modelo de informática forense-operativa, haciendo salir a los analistas forenses de sus laboratorios, transformar estos en elementos móviles y fusionar la actividad técnica con la operativa de obtención sobre el terreno, con más que notables resultados.*

TIC como medio[7] para el reclutamiento, financiación, difusión de ideas, comunicados o reivindicaciones y localización de información esencial para la planificación de acciones contra potenciales objetivos; este uso resulta más evidente en la actividad de la *Ciberyihad*.

Conscientes de la importancia de mantener una presencia activa en Internet, y especialmente en las redes sociales, para la consecución de sus objetivos (en particular la captación, adoctrinamiento y el reclutamiento, la financiación y el proselitismo), las organizaciones terroristas como Al Qaeda y Daesh han multiplicado su presencia en la Red. Para ello, *Al Qaeda* creó *As Sahab*, dedicado a *desarrollar y ejecutar la estrategia de comunicación, propaganda y captación* de esta organización terrorista, apoyado por el **"***Global Islamic Media Front***"** como medio de difusión; y Daesh emplea con gran sofisticación los m.c.s y las nuevas tecnologías para la consecución de sus objetivos, a través de "*ALHAYAT Media Center*".

El 26 de febrero de 2016 ha tenido lugar un incidente que no pasaría de ser una pura anécdota en un mar de relevantes incidentes si no fuera por dos motivos, la víctima y el alcance mediático. La cuenta de Twitter del conocido cantante *Justin Bieber* fue hackeada por seguidores de Daesh para publicar un vídeo titulado "*Un mensaje al Islam de Occidente*" de unos quince minutos, en el que se podía ver a los terroristas haciendo un llamamiento a sus fieles para que se unieran a la causa islámica, también se podía ver la ejecución de cuatro hombres. Además, usaron el hashtag #JustinBieber, para mandar mensajes. Más allá del hecho de que este cantante mostrara una actitud pública "beligerante" contra Daesh, a raíz de que uno de sus managers falleciera en la sala de conciertos Bataclán de París, es de destacar que esta acción le reportó a sus autores generosos titulares en los diferentes m.c.s. y lo que sin duda fue más atractivo para sus fines, un acceso "directo" a los *más de 76 millones de jóvenes* seguidores del cantante a través de la cuenta de Twitter hackeada.

La "presencia" de Daesh, en Internet en general y en las redes sociales en particular, donde su campaña de propaganda, financiación y en especial de captación y reclutamiento están alcanzando niveles nunca vistos, está obligando a los gobiernos occidentales a reaccionar, y no solo con campañas de contrapropaganda y sensibilización ante la problemática de la radicalización de algunos de sus nacionales, sino con medidas más directas contra la fuente del problema. En este sentido, EE.UU anunció el 29 de febrero de 2016, a través de su secretario de Defensa, que "*utilizamos herramientas informáticas para debilitar la capacidad del grupo terrorista Daesh de operar y comunicarse en el campo de batalla virtual (…) se trata de hacerles perder confianza en sus redes, de sobrecargarlas para que no puedan funcionar, y hacer todo aquello que perturbe su capacidad para comandar sus fuerzas, y controlar su población y economía*", apostillando el jefe

7 *Como medio reseñar que el empleo de las TIC les está reportando claros beneficios a la hora de facilitar las relaciones y colaboraciones entre diferentes organizaciones, grupos o células, favorece sus objetivos de guerra psicológica al posibilitar la desinformación y difusión de amenazas, posibilita e identifica canales de financiación, fomenta la recluta, sirve de base para todo su aparato de propaganda. Nuevas técnicas que mejoran y optimizan la consecución de sus objetivos, ya que impiden la "censura y/o valoración" a que mayoritariamente son sometidos por los medios de comunicación en el momento de su difusión. Finalmente constituye una inestimable fuente de información de todo tipo sobre potenciales objetivos tanto personales como de infraestructuras.*

del Estado Mayor de las Fuerzas Conjuntas que "*estamos tratando a la vez físicamente y virtualmente de aislar al grupo Daesh (…) pero no queremos que los terroristas sean capaces de notar la diferencia entre las perturbaciones vinculadas a las ciber-armas estadounidenses y otras perturbaciones*".

- *Internet como medio para llegar a objetivos tecnológicos u objeto directo de acciones hostiles*: el grave incidente acaecido en Estonia en la primavera de 2007 supuso el punto de inflexión *entre la especulación a la constatación* de una realidad, por primera vez se producía un ciberataque "a gran escala" y con éxito contra un Estado, inutilizando o colapsando una parte más que considerable de sus infraestructuras TIC. Internet había sido algo más que el medio, había sido el objetivo de las acciones ilícitas. Este incidente obligó a la OTAN a replantear toda su estrategia de Ciberseguridad y Ciberrespuesta, o más bien a definirla, concretándose en dos hechos de evidente relevancia: por un lado la Creación del Centro de Excelencia de Ciberdefensa Cooperativa (CCD CoE) en Tallín, capital de Estonia, y por otro la nueva Estructura de la Alianza surgida de la Cumbre de Lisboa en octubre de 2010.

  Igualmente resulta muy significativa la constitución, por parte del DoD, del denominado *Mando de Defensa Cibernética* (CYBERCOM o USCMBERCOM) en 2010. En analogía al anterior y clara inspiración en este el día 26 de febrero de 2013, y mediante la *Orden Ministerial 10/2013,* vio la luz en el seno de las Fuerzas Armadas Españolas el *Mando Conjunto en Ciberdefensa* (MCCD).

Aunque el *caso Estonia*, por ser considerado el primer ciberataque de grandes dimensiones, es tomado como referente, sucedió otro caso aún más grave si cabe entre julio y agosto de 2008. Fue el denominado *caso Georgia,* ya que un enquistado conflicto en el Cáucaso, entre Rusia y Georgia por el control del enclave estratégico de Osetia del Sur, llevó a que el 21 de julio se iniciaran una serie de oleadas de ataques DDoS procedentes de suelo ruso, y que precedieron a una incursión militar sobre el territorio de Georgia. Para la mayoría de analistas no cabe duda de que se trató de un escenario de *Ciberguerra*[8], dando entrada a otros actores en este complejo escenario (hablamos de los denominados *hackers patrióticos* o *cibermilicianos)*.

Finalmente *Internet como objetivo* es la razón última del *ciberterrorismo*; y a la pregunta de cuáles serían los objetivos propios del terrorismo a través de Internet la respuesta resulta obvia, los mismos que ya lo son en la actualidad: *telecomunicaciones*, *infraestructuras*, *economía y empresa*, *servicios públicos* en general y *Administración y Estado*. En suma, aquellos que se encuadran en el concepto de Infraestructura Crítica (IC,s), entendiendo como tal:

«instalaciones, redes, servicios, equipos físicos y de tecnología de la información cuya interrupción o destrucción tendría un impacto mayor en la salud, la seguridad o el bienestar económico de los ciudadanos o en el eficaz funcionamiento de los gobiernos» (COM (2004) 702 final, 20 octubre).

La debilidad de las IC,s, además de su naturaleza intrínseca, viene amplificada por el hecho de la interconexión e interdependencia que existe entre ellas, propiciando

8 *El concepto y casos reales son quirúrgicamente diseccionados y analizados por el Richard A. Clarke -responsable de seguridad con cuatros presidentes de EE.UU- prestó servicio durante 30 años en la Casa Blanca, el Departamento de Estado y el Pentagono. [GUERRA En la RED - Los nuevos campos de batalla, Editorial Ariel].*

efectos encadenados, también conocidos como “en cascada” o “dominó”, que posibilitarían que la pérdida directa de uno de ellos conlleve a su vez la merma, inoperatividad o inaccesibilidad de otras. Esto provocaría no solo los consiguientes perjuicios y daños en servicios esenciales, sino también, y muy especialmente, efectos psicológicos en la población. *No perdamos de vista que nuestra cada vez mayor dependencia tecnológica nos hace más débiles y vulnerables*[9].

Realmente existen elementos tangibles de la amenaza. Aunque a nivel nacional aún no se podría hablar de proyección real de una amenaza concreta, a nivel internacional, y más concretamente de EE.UU., sí, toda vez que han obtenido evidencias reales de que algunos sistemas informáticos de administración remota de infraestructuras críticas están comprometidos, concretamente los denominados *sistemas SCADA*[10] *o Sistemas de Control Industrial (SCI)*.

El supuesto que se está planteando es *perfectamente viable,* ya que en la actualidad las TIC están diariamente comprometidas por la acción anónima de hackers, organizaciones delictivas, corporaciones empresariales y acciones clandestinas de los servicios de inteligencia de los estados, algunas con bastante éxito por la relevancia de los sistemas comprometidos, el número de ordenadores afectados o incluso por los daños económicos causados. Pues bien, lo único que le faltaría a cualquiera de estas acciones para convertirse en una *acción ciberterrorista* es la *motivación o reivindicación* por parte de una organización terrorista.

Sin lugar a dudas, un nuevo hito en la evolución o materialización de la amenaza ciberterrorista lo encontramos en el ciberataque sufrido, en la madrugada del 8 al 9 de abril de 2015, por la cadena francesa TV5 Monde. El ataque, a manos del autodenominado *Cyber Kahilafah* (CiberCalifato), vinculado a Daesh, bloqueó la emisión de la señal de televisión satélite de la cadena, su página web y perfiles en redes sociales. Esta acción supone un cambio cualitativo sin precedentes en la percepción de la amenaza y en la constatación de que la amenaza ya no es tal, sino más bien una inquietante realidad. Este mismo grupo de hackers protagonizó un ciberataque contra la cuenta de Twitter del Mando Central de Estados Unidos (CENTCOM), el 13 de enero de ese mismo año.

Ya en enero de 2015 se tuvo conocimiento de un incidente de ciberseguridad cualitativamente relevante y muy sintomático de que realmente las ICs cada vez están más cerca de la mano hostil de terroristas y saboteadores (individuos, grupos, organizaciones o incluso estados). Según el informe oficial ‘Seguridad TIC en Alemania 2014′, publicado el 26 de diciembre de 2014 y elaborado por la Oficina Federal para la Seguridad de la Información (BSI), una planta siderúrgica no identificada en el país germano fue atacada por hackers que manipularon los sistemas de control, de tal manera que un alto horno no pudo ser correctamente apagado, generando de este modo daños “masivos” (aunque no especificados). Los atacantes tuvieron acceso a

9 *La población mundial en general, y en particular los más jóvenes, cada vez es más dependiente del uso de la tecnología y consecuentemente vulnerable a su carencia. Psiquiatras surcoreanos ya han desarrollado el concepto de “demencia digital” y han identificado la sintomatología de este cuadro clínico de trastorno mental. Dr. Manfred Spitzer [Demencia Digit@l - El peligro de las nuevas tecnologías - editorial B grupo Zeta].*

10 «*los ataques con éxito sobre los sistemas SCADA podrían producir terror a gran escala. En las cuevas de Afganistán, las tropas de EE.UU. encontraron planes de Al Qaeda para atacar esos sistemas*». C*ita de Mark Rasch – antiguo jefe de la Unidad de delitos informáticos del Departamento de justicia de EE.UU.*

la planta a través de la red corporativa, desde la que se abrieron paso hasta las redes de producción y los equipos de control. El método usado para infiltrarse en la red corporativa fue mediante un ataque phishing, enviando un *e-mail* diseñado para que aparentara proceder de una fuente fiable. Este incidente resucitó los "fantasmas" surgidos tras el incidente acaecido en 2010 en la Central Nuclear iraní de Bushehr y el Complejo Nuclear de Natanz, que sufrieron un ciberataque protagonizado por el malware tipo gusano bautizado como Stuxnet, que se replicaba, mutaba y adaptaba de forma desasistida (sin la presencia de un panel de mando y control), infectando solo en Irán 63.000 ordenadores (significar que lo fueron 88.000 a nivel mundial, lo que da idea de lo "dirigido" que fue el ataque) sin causar daños en ninguno de ellos, hasta encontrar ese ordenador objetivo para el que había sido programado y sobre el que sí causo daños.

Pero el temor a las implicaciones de un ciberataque exitoso contra una IC es la esencia de toda amenaza ciberterrorista, pues garantizaría una rápida e inevitable degradación de servicios esenciales para el normal desarrollo de la actividad de nuestra sociedad, tal y como esta se concibe. Y es que *la tecnología es el "talón de Aquiles" de las sociedades modernas*, como tantas y tantas veces se ha constatado con ocasión de accidentes, sabotajes o desastres naturales. La dependencia de la tecnología cada vez es mayor y su pérdida o disrupción acarrea cada vez mayores problemas.

Sirva de ejemplo la problemática en torno a las infraestructuras de generación, transporte y distribución de energía eléctrica, que tan sensibles y críticas resultan. Lo que en el mundo anglosajón denominan el "blackout", o gran apagón, supondría la rápida degradación o pérdida de servicios esenciales hasta alcanzar niveles "apocalípticos". Pues bien, lo que hasta ahora no ha sido más que un ejercicio de informática ficción o un recurrente guión del cine más catastrofista, parece estar más próximo a la vista de los inquietantes acontecimientos que han sucedido en los primeros meses de 2016. Por un lado Ucrania: si ha sufrido o no un ciberataque a gran escala es una de las cuestiones que las agencias de inteligencia de la OTAN están estudiando. Lo que sí es cierto es que miles de familias pasaron unos días muy duros después de que la compañía energética Prykarpattyaoblenergo**,** prestadora del servicio de abastecimiento eléctrico a la región de Ivano-Frankisvk, al oeste del país, interrumpiera el suministro eléctrico el 23 de diciembre a cerca de 600.000 hogares tras sufrir una 'interferencia' en sus sistemas de control. Pero aún el 20 de enero de 2016 la situación se repitió en otras regiones de Ucrania. Los ataques parecen tener una clara motivación política y materializarse desde la vecina Rusia. Pues bien, el pasado 27 de enero de 2016 Israel sufrió un grave ciberataque contra su red energética que afectó a varios de sus sistemas, en uno de los momentos de mayor demanda eléctrica por las bajas temperaturas. No han trascendido muchos de los detalles del incidente, si bien el ministro de energía israelí aseguró que tuvieron que parar algunos sistemas para poder solucionar el problema sobre su *Nation's Electrical Power Grid Authority's Network,* confirmando durante la celebración de la conferencia CyberTech 2016 que habían sufrido *uno de los ciberataques más graves que han experimentado hasta el momento.*

El año 2015 nos ha traído un nuevo término asociado al ciberterrorismo, el *ciberyihadismo*[11], "*que usando métodos, procedimientos y herramientas del terrorismo, el*

11 *Ciberyihadismo, terminología y reflexiones acuñadas por el Centro Criptológico Nacional. Véase CCN-CERT IA-09/16 CIBERAMENAZAS 2015 / TENDENCIAS 2016 [RESUMEN EJECUTIVO].*

hacktivismo y la ciberguerra constituye una realidad incipiente y supone una de las mayores amenazas con las que se enfrentarán las sociedades occidentales en los próximos años. Las importantes vías de financiación de estos grupos, al socaire de Daesh, hacen posible que puedan llegar a adquirir los conocimientos y las herramientas precisas para el desarrollo de ciberataques o la contratación de los mismos. Hasta el momento sus ciberataques se han limitado a la desfiguración de páginas web, ataques DDoS a pequeña escala o, más comúnmente, al uso de Internet y de las redes sociales para la diseminación de propaganda o el reclutamiento y la radicalización, actividades que no exigen grandes conocimientos o infraestructuras. Las capacidades del ciberyihadismo no han hecho sino empezar a mostrarse. Es de esperar ciberataques más numerosos, más sofisticados y más destructivos en los próximos años, en tanto persista la actual situación en torno a Daesh.

En julio del 2015, se constituyó una nueva estructura en Europol, está vez focalizada en la prevención y respuesta del fenómeno del ciberterrorismo, y bautizada Unidad de Referencia de Internet – IRU– (Internet Referral Unit).

4. CIBERRESPUESTA, LAS CAPACIDADES NACIONALES

Alcanzado este punto, ha llegado el momento de identificar y realizar una somera descripción de los mecanismos de *ciberrespuesta* que han sido articulados en los últimos años, tanto a nivel nacional como europeo e internacional.

En los últimos años los esfuerzos para la protección, prevención y respuesta, en torno a las catalogadas como IC,s, tanto nacionales como europeas, ha sido constante y creciente. El máximo exponente es la creación del *Centro Nacional de Protección de Infraestructuras Críticas* (CNPIC), Órgano Ministerial encuadrado en la Secretaría de Estado para la Seguridad del Ministerio del Interior. Es responsable de *impulsar, coordinar y supervisar* los esfuerzos nacionales de adecuación al Plan Europeo de Protección de Infraestructuras Críticas (PEPIC), a través de su traslación a la normativa nacional. Así, a través del Plan Nacional de Protección de Infraestructuras Críticas (PNPIC), ha puesto en marcha importantes iniciativas para alcanzar los objetivos para los que ha sido creado. Estos planes preventivos y medidas de protección se han ido transponiendo de su concepción teórica a su plasmación real a través del *Catálogo de Infraestructuras Críticas* (CIC); en la actualidad se encuentran incluidos en el citado CIC *la Red Energética, Instalaciones Nucleares, las grandes operadoras y gestoras TIC, Transportes, Agua y Alcantarillado, Alimentación, Salud, Sector Financiero y Bancario, Industria Química, Industria Espacial, Centros de Investigación y Desarrollo y por último la Administración General del Estado.* El CNPIC fue creado en el año 2007, mediante Acuerdo de Consejo de Ministros de 2 de noviembre, siendo sus competencias reguladas por la Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas y por el Real Decreto 704/2011, de 20 de mayo, por el que se aprueba el Reglamento de protección de las infraestructuras críticas.

La actividad desarrollada desde el CNPIC se vio reforzada con la firma, el pasado 5 de marzo de 2013, de un *convenio de colaboración entre las Secretarías de Estado de Seguridad* (SES-Ministerio del Interior) *y la Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información* (SETSI-Ministerio de Industria) , acuerdo que ha permitido que el Instituto para las Tecnologías de la Comunicación (INTECO)

–INTECO ha pasado a denominarse INCIBE Instituto Nacional en Ciberseguridad- se convierta en el Centro de Respuesta ante Incidentes Cibernéticos (o CERT según su acrónimo en inglés) de las Infraestructuras Críticas nacionales y por extensión del Ministerio del Interior, rebautizado como *CERT de Seguridad e Industria* (CERTSI_).

Asimismo, y con el objetivo de reforzar las capacidades en ciberseguridad y mejorar la coordinación de las acciones de las Fuerzas y Cuerpos de Seguridad del Estado en este ámbito, el 25 de octubre del 2013 fue creada la *Oficina de Coordinación Cibernética* (OCC), que es el órgano técnico de coordinación del Ministerio del Interior en materia de ciberseguridad, creado mediante Instrucción del secretario de Estado de Seguridad 15/2014, de 19 de noviembre. Depende funcionalmente de la Secretaría de Estado de Seguridad y orgánicamente del CNPIC. La OCC proporciona las capacidades de coordinación técnica entre el CERTSI_ y los órganos subordinados de la Secretaría de Estado de Seguridad y las Fuerzas y Cuerpos de Seguridad del Estado en lo que respecta a las competencias propias del Ministerio del Interior en el campo de la ciberseguridad. La OCC mantiene personal técnico permanentemente integrado en la estructura del CERTSI_.

Con respecto a las medidas y planes de protección puestos en marcha, se debe destacar la constitución del Centro de Respuesta ante Incidentes de Seguridad Informática de ámbito gubernamental, también conocido como CCN-CERT, dependiente del Centro Criptológico Nacional – Centro Nacional de Inteligencia – Ministerio de la Presidencia. Constituido en el año 2006 como CERT (acrónimo en inglés de Centro de Respuesta ante Incidentes de Seguridad Informática) al amparo de la *Ley 11/2002* reguladora del Centro Nacional de Inteligencia, el *RD 421/2004* de regulación del CCN y en el *RD 3/2010,* de 8 de enero, regulador del Esquema Nacional de Seguridad. De acuerdo a todas ellas, el CCN-CERT tiene responsabilidad en ciberataques sobre sistemas clasificados y sobre sistemas de las Administraciones Públicas y de empresas y organizaciones de interés estratégico para el país. Su misión, por tanto, es contribuir a la mejora de la ciberseguridad española, siendo el centro de alerta y respuesta nacional que coopere y ayude a responder de forma rápida y eficiente a los ciberataques y a afrontar de forma activa las ciberamenazas.

Toda esta actuación se ve reforzada con la activa y directa participación en foros y grupos de trabajo de instituciones de vigilancia como son la *Agencia Europea de Seguridad de las Redes y de la Información* (ENISA), la *Red de Centros de Emergencia europeos* (CERTs y CSIRTs) y de EE.UU. (US-CERT) o el *Centro de Ciberdefensa de la OTAN* (CCD-CoE), entre otros.

5. ESTRATEGIAS DE SEGURIDAD Y CIBERSEGURIDAD

En este sentido la *Estrategia de Ciberseguridad de la Unión Europea* (ECUE), de 7 de febrero de 2013, «un ciberespacio abierto, protegido y seguro», representa la visión de conjunto de la UE sobre cómo prevenir y resolver mejor las perturbaciones de la red y los ciberataques. El objetivo consiste en *impulsar los valores europeos de libertad y democracia* y velar por un crecimiento seguro de la *economía digital*. Evidencia una *creciente preocupación por el más que notable incremento de la delincuencia económica*; y es que el tradicional espionaje industrial/económico dirigido contra grandes corporaciones industriales (preferentemente del ámbito de la Defensa), de corte

más bien artesanal, ha cedido el testigo a ciberataques indiscriminados que afectan a todo el tejido industrial básico, formado por las PYMES y los autónomos.

«Cuanta más gente dependa de Internet, más gente dependerá de que la red sea segura. Una red segura protege nuestros derechos y libertades y nuestra capacidad de ejercer actividades económicas. Ha llegado el momento de coordinar nuestra acción: el coste de la inacción es mucho más elevado que el de la acción»[12].

Todo Estado moderno necesita disponer de capacidad de reacción para evitar los colapsos financieros tanto públicos como privados, y en ello la integridad económica es un pilar fundamental en la gestión de lo que se denomina ***resiliencia*** *-entendiendo como tal la capacidad de afrontar una situación crítica con flexibilidad y fortaleza tales que permitan minimizar daños y recuperar estructuras y capacidades* -.

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

La *Estrategia de Seguridad Nacional* (ESN2013) , aprobada en Consejo de Ministros el 30 de mayo de 2013, es un instrumento que refleja los riesgos y amenazas que son necesarios afrontar, siempre bajo sus principios informadores: *Unidad de Acción, Anticipación y Prevención, Eficiencia y Sostenibilidad* en el uso de los recursos y *Resiliencia* o capacidad de resistencia y recuperación[13].

Resulta crucial conseguir el objetivo marcado en el ámbito de la ciberseguridad pues es prioritario por la repercusión que tiene en el resto de los ámbitos, como es la seguridad económica y financiera.

Sirvan de ejemplo de lo anterior dos datos relacionados con dos países de la Europa Occidental y con economías saneadas, como son Alemania y Holanda. Las autoridades de la RFA publicaron un cálculo del "valor intelectual" aportado por sus PYMES en 2013, próximo a los 55.000 millones de euros anuales, estimando a su vez que las pérdidas por ataques cibernéticos de diversa índole supusieron un 40% del total; se está hablando de unas pérdidas anuales de unos 22.000 millones de euros. Mientras que Holanda vino a considerar materialmente imposible hacer frente a todas las amenazas procedentes del ciberespacio, por lo que decidió focalizar sus esfuerzos en ese

12 *Cita de Neelie Kroes, vicepresidenta de la Comisión Europea responsable de la Agenda Digital con ocasión de la presentación de la Estrategia de Ciberseguridad de la UE, rueda de prensa en Bruselas el 7 de febrero del 2013.*

13 «*La seguridad es un fundamento esencial para el desarrollo y el progreso de una sociedad libre. Por eso, resulta imprescindible un entendimiento básico y generalizado de la importancia de la seguridad como garantía de bienestar de los ciudadanos y de la estabilidad del propio Estado. Esta visión solo se puede articular a través de una Estrategia que defina un marco de referencia global y omnicomprensivo en materia de seguridad, contemplando las singularidades de los riesgos y amenazas a los que nos enfrentamos en un mundo que experimenta cambios tan profundos como constantes. Y orientando la acción del Estado de cara a dar respuesta a los desafíos actuales utilizando los recursos disponibles de forma flexible y eficaz. (…) Con esta Estrategia de Seguridad Nacional 2013 avanzamos todos en la dirección adecuada*».fragmentos del preámbulo de la Estrategia de Seguridad Nacional 2013, firmado por el presidente del Gobierno de España D. Mariano Rajoy Brey.

año tan solo en dos de ellas, centrándose fundamentalmente en la amenaza económica y la amenaza yihadista.

La ESN2013 se articula en torno a cinco capítulos, en los que se ofrece un concepto de Seguridad Nacional, se sitúa la seguridad de España en el mundo, se identifican los riesgos y amenazas actuales, se trazan a partir de esta base los objetivos y las líneas de acción estratégicas en los ámbitos de actuación prioritarios para España y se configura un nuevo *Sistema de Seguridad Nacional*.

Los *riesgos y amenazas* para la Seguridad Nacional, describe los riesgos y amenazas que afectan singularmente a la Seguridad Nacional: los conflictos armados, el terrorismo, las *ciberamenazas*, el crimen organizado, la inestabilidad económica y financiera, la vulnerabilidad energética, la proliferación de armas de destrucción masiva, los flujos migratorios irregulares, el espionaje, las emergencias y catástrofes, la vulnerabilidad del espacio marítimo y la vulnerabilidad de las *infraestructuras críticas* y los servicios esenciales. También se contemplan los factores potenciadores como el cambio climático, la pobreza, la desigualdad, los extremismos ideológicos, los desequilibrios demográficos o la generalización del uso nocivo de las nuevas tecnologías, que, sin ser en sí mismos un riesgo o una amenaza, pueden desencadenarlos o agravarlos.

Como líneas de acción para alcanzar los objetivos descritos en la ESN destacan: la implantación de una adecuada *Cultura de Ciberseguridad*, "*las sociedades que se hacen responsables de su seguridad son sociedades más libres*".

Con la ESN2013 nos encontramos ante lo que se denomina estrategia de primer nivel, el 5 de diciembre de ese mismo año, el *Consejo de Seguridad Nacional* (CSN) aprobó dos nuevas estrategias, estas de segundo nivel, focalizadas a dos de los riesgos identificados en la primera, la Ciberseguridad y la Seguridad Marítima, y más recientemente la de Seguridad Energética. Estas estrategias tienen muchos aspectos comunes, pero sin duda uno de los más destacados es la coincidencia de contemplar las ciberamenazas como una de las principales amenazas, ya que si bien el ciberespacio es un nuevo ámbito de relación que ha proporcionado el desarrollo de las TIC, también ha diluido las fronteras, permitiendo una globalización sin precedentes que propicia nuevas oportunidades, pero que a su vez conlleva nuevos y preocupantes riesgos y amenazas. Resulta evidente que las *ciberamenazas deben ser consideradas como amenaza trasversal* y sin duda estarán presentes en las estrategias que pudieran ser aprobadas en el futuro, en analogía al tratamiento que ya recibe en las dos precitadas.

La última iniciativa, a nivel nacional, que por su relevancia se estima importante reseñar en este documento, es la constitución, en septiembre de 2012, del *Centro Nacional de Excelencia en Ciberseguridad* (CNEC), que bajo los auspicios de la UE y de su programa ECTEG (European Cybercrime Training and Education Group) e integrado en la Red Europea de Centros de Excelencia -2CENTRE- coordinados por el EC3 de EUROPOL, pretende facilitar la más alta *capacitación en ciberseguridad e informática forense* a los miembros de las Fuerzas y Cuerpos de Seguridad del Estado, a través del desarrollo de cursos específicos que posibiliten la ampliación y mejora de las capacidades de prevención, localización y análisis de ciberamenazas, detección y respuesta ante ciberataques, lucha contra el ciberdelito, creación de programas de certificación y acreditación -desarrollado a través de la *Agencia de Certificación de Seguridad* (ACS)- y apoyar la potenciación de las capacidades de I+D+i de las PyMEs.

Ambos -el CNEC y la ACS- operan bajo el manto del *Instituto de Ciencias Forenses y de la Seguridad* (ICFS) de la Universidad Autónoma de Madrid. En diciembre de 2010 el ICFS y la SES firmaron un convenio de colaboración para la investigación y cooperación educativa, reportando evidentes beneficios a ambos.

Una muestra palpable de la creciente preocupación y alta sensibilización con la que se vive la problemática de la ciberseguridad desde el Gobierno de España y en lo que a Fuerzas de Seguridad del Estado concierne, se vivió en las jornadas previas y durante los actos de Proclamación de SAR Don Felipe de Borbón y Grecia como Rey de España, pues por primera vez en nuestra historia se contempló y activó un *dispositivo específico y concreto de ciberseguridad*. La Instrucción núm. 11/2014 de la SES así lo contempló, ordenando cometidos concretos al CNPIC y la OCC, así como a las Unidades especializadas de los Cuerpos.

Y desde los atentados de París del 7 de enero del 2015, como una de las iniciativas tomadas, el Ministerio del Interior, a través de la Secretaría de Estado de Seguridad, elevó la alerta antiterrorista al nivel 4 de 5, y se activó, entre otras medidas, un *dispositivo extraordinario de ciberseguridad*, coordinado desde la OCC, que al día de la fecha sigue operativo.

6. INICIATIVAS DESDE LA JEFATURA DE INFORMACION DE LA GUARDIA CIVIL

La amenaza del *uso de Internet y de las tecnologías de la Información y Comunicaciones* por parte de organizaciones terroristas o afines, y la adecuación de los procedimientos de actuación y respuesta por parte de la Guardia Civil, *se convirtieron en una de sus prioridades desde el año 2000*, como así lo atestiguan informes y estudios del entonces Servicio de Información.

Estos estudios y planes iniciaron su materialización en *noviembre de 2002*, con la incorporación al Servicio del primer personal expresamente seleccionado para conformar el embrión del entonces *Subgrupo de Ciberterrorismo*; desarrollando su primera actuación de apoyo especializado, en beneficio de una Unidad de Investigación de la Jefatura de Información, en febrero de 2003.

Una constante desde entonces y hasta la actualidad ha sido la firme apuesta por este proyecto, y el decidido empeño de los sucesivos mandos del entonces Servicio y actual Jefatura de Información, con la lógica “complicidad” de las más altas instancias de mando y dirección del Cuerpo.

De esta forma en 2007 se conformó como *Grupo de Ciberterrorismo*; pero sin duda la fecha más emblemática la encontramos en el *31 de marzo de 2011*, cuando el entonces Grupo de Ciberterrorismo se incorporó, junto con otras unidades de claro perfil tecnológico como son los *Grupos Técnico Informático, de Interceptación de las Telecomunicaciones y de Informática Forense*, al nuevo y ambicioso proyecto de integrar capacidades y esfuerzos bajo el manto del, con esa fecha creada, Área Técnica de la Jefatura de Información, al mando de un coronel.

Paralelamente, en diciembre de 2012, se constituyó la *Unidad de Ciberseguridad*, como otra ambiciosa apuesta del mando ante la creciente preocupación por esta amenaza.

En la actualidad lo integra un equipo humano polivalente y multidisciplinar de muy alta cualificación, dotado de novedosos sistemas tecnológicos y herramientas informáticas; todo ello con muy significativas inversiones económicas y evidentes esfuerzos y sacrificios de otras unidades de la Jefatura para atender la constante demanda de incremento de recursos humanos.

BIBLIOGRAFÍA

Ley Orgánica 5/2005, de 17 de noviembre, de la Defensa Nacional [BOE 276 de 18 de noviembre del 2005].

Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas. [BOE 102 de 29 de abril 2011].

Real Decreto 704/2011, de 20 de mayo, por el que se aprueba el Reglamento de protección de las infraestructuras críticas. [BOE 121 de 21 de mayo 2011].

Convenio sobre la ciberdelincuencia del Consejo de Europa – Budapest 23 de noviembre del 2001.

Estrategia de Ciberseguridad de la Unión Europea - Comisión Europea - (7 de febrero 2013).

Estrategia de Seguridad Nacional - Departamento de seguridad Nacional - Presidencia del Gobierno - (31 de mayo 2013).

Estrategia de Ciberseguridad Nacional - Departamento de seguridad Nacional - Presidencia del Gobierno - (5 de diciembre 2013).

Estrategia de Seguridad Marítima Nacional - Departamento de seguridad Nacional - Presidencia del Gobierno - (5 de diciembre 2013).

Acuerdo para afianzar la unidad en defensa de las libertades y en la lucha contra el terrorismo – Presidencia del Gobierno – (2 de febrero del 2015).

Estrategia de Seguridad Energética Nacional - Departamento de seguridad Nacional - Presidencia del Gobierno - (20 de julio del 2015).

Informe Anual de Seguridad Nacional 2013 - Departamento de seguridad Nacional - Presidencia del Gobierno - (julio 2014).

Informe Mensual de Ciberseguridad junio 2014 - CCN-CERT IS-06/14.

Informe de amenazas – medidas de seguridad contra ransomware abril 2015 – IA-21/14.

Ciberamenazas 2014 Tendencias 2015 – CCN-CERT IA-09/15.

Amenazas y análisis de riesgos en Sistemas de Control Industrial (ICS) enero 2016 – CCN-CERT IA-04/16.

Ciberamenazas 2015 Tendencias 2016 [Resumen Ejecutivo] abril 2016 – CCN-CERT IA-09/16.

Monografía del CESEDEN nº126 - El Ciberespacio. Nuevo escenario de confrontación - (febrero 2012).

Monografía del CESEDEN nº137 - Necesidad de una conciencia nacional de ciberseguridad. La ciberdefensa: un reto prioritario - (abril 2013).

Cuaderno de Estrategia nº149 del IEEE - Ciberseguridad. Retos y amenazas a la Seguridad Nacional - (diciembre 2010).

Cuaderno de Estrategia nº159 del IEEE - Los Potenciadores del riesgo - (febrero 2013).

Cuaderno de Estrategia nº162 del IEEE - La inteligencia económica en el mundo globalizado - (mayo 2013).

Cuaderno de Estrategia nº166 del IEEE - Energía y Geoestrategia 2014 - (mayo 2014).

Cuaderno de Estrategia nº167 del IEEE – Prespectivas de evolución futura de la política de seguridad y defensa de la UE. Escenarios de Crisis 2014 - (agosto 2014).

Cuaderno de Estrategia nº168 del IEEE – Evolución del mundo árabe: tendencias 2014 - (octubre 2014).

Cuaderno de Estrategia nº173 del IEEE – La Internacional Yihadista 2015 - (septiembre 2015).

Boletín SCEPS nº5 mayo / agosto 2015 – Sociedad Científico Española de Psicología Social.

Convención de las Naciones Unidas contra la delincuencia organizada transnacional y sus protocolos - Oficina de las Naciones Unidas contra la Droga y el Delito (2004).

Manual de respuestas de la justicia penal al terrorismo – Oficina de las Naciones Unidas contra la Droga y el Delito (2009).

Compendio de casos relativos a la lucha contra el terrorismo – Oficina de las Naciones Unidas contra la Droga y el Delito (2010).

Compendio de casos de delincuencia organizada - Oficina de las Naciones Unidas contra la Droga y el Delito (2012).

Uso de Internet con fines terroristas - Oficina de las Naciones Unidas contra la Droga y el Delito (2013).

Los riesgos globales para el 2016 – Foro Económico Mundial.

Recomendación UIT-T X.12/05 (04/2008) – Seguridad en el Ciberespacio – Ciberseguridad – Aspectos generales de la ciberseguridad.

Kevin D. Mitnick y William L. Simon (2006) – El Arte de la Intrusión – Editorial Ra-Ma.

Eloy Velasco Núñez (2010) – Delitos cometidos a través de Internet. Cuestiones Procesales –Editorial La Ley.

Richard A. Clarke y Robert K. Knake (2011) – Guerra en la Red. Los nuevos campos de batalla. Editorial Ariel.

Tom Chatfield (2012) – 50 cosas que hay que saber sobre el Mundo Digital –Editorial Ariel.

Jorge Alberto Lizarra Mendoza (2012) – Hackers. Software libre y hacktivismo en la sociedad de la información –Editorial Académica Española.

Dr. Manfred Spitzer (2013) – Demencia digit@l . El peligro de las nuevas tecnologías – Editorial B grupo Zeta.

Román Cendoya (2013) – Revolución . Del homo sapiens al homo digital –Editorial SEKOTIA.

José Luis González Cussac y Mª Luisa Cuerda Arnau (2013) – Nuevas amenazas a la Seguridad Nacional . Terrorismo, criminalidad organizada y tecnologías de la información y las comunicaciones –Editorial TIRANT LO BLANCH.

Adrianna Llongueras Vicente (2013) – La guerra inexistente, la ciberguerra .Ciberdefensa –Editorial Académica Española.

Luciano Salellas (2013) – Delitos informáticos. Ciberterrorismo. Aanálisis del origen y evolución del ciberterrorismo como nuevo escenario de conflicto mundial – Editorial Académica Española.

Mª Ángeles Caballero, Diego Cilleros y Abtin Shamsaifar (2014) – El libro del hacker –Anaya Multimedia.

Eric Schmidt y Jared Cohen (2014) – El futuro digital –Anaya Multimedia.

Julio Gómez López y otros (2014) – Hackers. Aprende a atacar y a defenderte – Editorial RaMa.

Jaron Lanier (2014) – Contra el rebaño digital . Un manifiesto –Editorial Debate.

Marta Peirano (2015) –El pequeño libro rojo del activista en la Red –Editorial eldiario.es libros.

Manel Medina y Mercé Molist (2015) – Cibercrimen / Aprende de víctimas, expertos y cibervigilantes –Tibidabo ediciones.

Eduardo Martín de Pozuelo, Jordi Bordas y Eduard Yitzutak (2015) – Objetivo: Califato Universal. Claves para entender el yihadismo –La Vanguardia Ediciones.

Romain Rissoan (2015) – Redes sociales. Comprender y dominar las nuevas herramientas de comunicación –Ediciones ENI.

Pere Cervantes y Oliver Tauste (2015) – Internet negro . El lado oscuro de la Red – Editorial Planeta.

Marc Goodman (2015) – Los delitos del futuro – Editorial Ariel.

Daniel Echeverri Montoya (2016) – Deep Web: TOR, FreeNET & I2P. Privacidad y Anonimato –Edición Zeroxworld Computing.

Gabriella Coleman (2016) – Las mil caras de Anonymous. Hackers, activistas, espías y bromistas – Arpa Editores.

Andrew Keen (2016) – Internetno no es la respuesta – Editorial Catedral.

César Álvarez Fernández y equipo Fundación Borrerá (2016) – El modelo de protección de las Infraestructuras Críticas en España. Guía PIC –Edición de la Fundación Borrerá.

Fecha de recepción: 01/05/2016. Fecha de aceptación: 01/06/2016