UNIVERSIDAD INTERNACIONAL DE LA RIOJA

Universidad Internacional de La Rioja
Máster Universitario en Estudios sobre Terrorismo (MET)

PROTECCIÓN DE INFRAESTRUCTURAS CRITICAS FRENTE AL CIBERTERRORISMO.

Trabajo fin de Máster presentado por:
Titulación: Licenciado (ESO de la GC).
Master Universitario en Seguridad por la Facultad de Derecho de la UNED
Experto Universitario en Dirección de la Seguridad por la UNED.

Francisco Jesús Fernández Fernández.

Director/a:
Manuel Torres Soriano.

CATEGORÍA TESAURO: 3.1. DERECHO,
3.1.3 DERECHO INTERNACIONAL Y COMUNITARIO,
3.1.4 DERECHO PÚBLICO
4.5. TECNOLOGÍA,
4.5.4 INTEROPERATIBILIDAD
4.5.5 INTERCONECTIVIDAD

RESUMEN

El uso masivo del fenómeno de Internet y las Tecnologías de Información y Comunicaciones (TIC), en todos los ámbitos de la sociedad, ha creado un nuevo espacio, el ciberespacio, donde se producirán conflictos y agresiones, y donde existen ciberamenazas que atentarán contra la seguridad nacional, el estado de derecho, la prosperidad económica, el estado de bienestar y el normal funcionamiento de la sociedad y de las administraciones públicas.

El binomio Ciberamenaza&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 intereses particulares, y los sistemas informáticos empresariales (tanto públicos como privados), especialmente aquellos vinculados de alguna manera a Internet, son algo más que un riesgo y se han transformado en una amenaza emergente.

Estas acciones se realizan no sólo por grupos delincuenciales al uso (que se han adaptado y rápido a los nuevos tiempos), sino que también por otras formas de delincuencia grave tales como grupos y organizaciones terroristas, colectivos antisistema en general o que buscan la desestabilización de un Estado en particular, organizaciones clandestinas, e incluso las estructuras de inteligencia de algunos estados.

PALABRAS CLAVE

CIBERAMENAZA-CIBERSEGURIDAD–CIBERTERRORISMO-TIC-INFRAESTRUCTURAS

Í N D I C E

1.- INTRODUCCIÓN.

En los albores del siglo XXI, se dice que la humanidad está inmersa en la llamada "sociedad de la información"(Crespí, 2010)[1]. Esto se traduce en que cualquier tipo de dato, ya sea imagen, sonido, texto, voz y en general, todo lo que pueda ser digitalizado, se puede enviar telemáticamente. Un individuo, con el equipo adecuado y con el sistema de telecomunicación idóneo, puede disponer de todo tipo información, en cualquier parte del mundo, en la que exista cobertura de ese sistema de telecomunicación.

Para ello, hoy en día se cuenta con distintos tipos de soportes tecnológicos, como son, ordenadores personales (portátiles y de sobremesa) y terminales móviles de acceso que son capaces de comunicar con los anteriores. Si se combina un dispositivo capaz de comunicarse con una tecnología de telecomunicación como la telefonía para la voz, y además desarrolla capacidad para acceso a Internet de banda ancha, obtenemos esa capacidad de comunicación y de intercambio de datos.

En los últimos tiempos se ha producido un gran avance en cuanto al desarrollo de las nuevas tecnologías de comunicación se refiere. De hecho, resulta idóneo hablar de una auténtica revolución en todos los sentidos, pues ha cambiado no sólo la forma de comunicarse de las personas, sino también de las máquinas y servidores informáticos, ya no importan las distancias. Se han reducido los tiempos de las comunicaciones al mínimo, ha cambiado la forma de hacer la guerra(Clarke y Knake, 2001:14), la manera de trabajar de los personas, y lo que es más importante, hoy en día no se concibe empresa, institución o Estado alguno cuyo eje central para su correcto funcionamiento no sean las Tecnologías de la Información y las Comunicaciones (en adelante TIC,s).

Tal es la dependencia que los países desarrollados poseen de las nuevas tecnologías, que, como muestran recientes estudios sociológicos (Cisco Connected World Technology Report. 2012)[2], casi la mitad de los jóvenes equipara el acceso a Internet con el acceso al agua y la comida,

1 Se emplea el término cuando se hace referencia al hecho de que la sociedad actual, especialmente en los países desarrollados, es objeto de fenómenos y transformaciones que tienen su raíz en la información y su tratamiento y uso intensivo. El término sociedad de la información en el mundo occidental fue introducido oficialmente por el sociólogo estadounidense Daniel Bell. "Una sociedad post-industrial es básicamente una sociedad de la información. El intercambio de información en términos de varios tipos de procesamiento y almacenamiento de datos, investigación de mercado, etc., es la base de la mayoría de cambios económicos" (Bell, 1973). Además, la IBM Community Development Foundation, dio en 1997 la siguiente definición a la sociedad de la información: "una sociedad caracterizada por un alto nivel de intensidad de información en la vida cotidiana de la mayoría de ciudadanos, organizaciones y sitios de trabajo, por el uso de tecnología común o compatible para un amplio rango de actividades de negocio, educacionales, personales o sociales, y por la habilidad de transmitir, recibir e intercambiar datos digitales rápidamente entre sitios indistintamente de la distancia"

2 Estudio sociológico realizado por CISCO entre tres mil profesionales y estudiantes de entre 18 y 29 años procedentes de 14 países distintos. Este estudio confirma la realidad social de Internet, ya tipificada como Infraestructura Estratégica, pero además, esta situación abre la puerta a la tipificación de ciertas aplicaciones como "aplicaciones estratégicas" debido a la gran dependencia social y mercantil que su uso está generando.

o lo prefiere a tener un coche. Es decir, las nuevas tecnologías son percibidas por gran parte de la población como un bien de primera necesidad.

Resulta evidente que tal dependencia no la poseen únicamente los particulares, sino que el correcto funcionamiento de todo Estado y su seguridad dependen, en gran medida, de las TIC,s. Sin embargo, esta fortaleza de las sociedades de Occidente es al mismo tiempo su gran debilidad. Es decir, las sociedades desarrolladas y altamente tecnificadas dependen en extremo de una serie de servicios esenciales sin los cuales no hay capacidad de subsistencia. Esos servicios pueden ser el sistema de transportes, el abastecimiento de agua o de electricidad, las telecomunicaciones, etc. Por este motivo, se ha decidido acuñar el término Infraestructura Crítica (IC) definido en la propia Ley 8/2011 de protección de las IC, como ***"Las infraestructuras estratégicas (es decir, aquellas que proporcionan servicios esenciales) cuyo funcionamiento es indispensable y no permite soluciones alternativas, por lo que su perturbación o destrucción tendría un grave impacto sobre los servicios esenciales".***(www.cnpic-es.es, 2014)[3]para referirse a la prestación de estos servicios básicos e imprescindibles sin cuyo servicio, el normal funcionamiento del Estado se ve imposibilitado.

2.-PROTECCIÓN DE INFRAESTRUCURAS CRÍTICAS FRENTE AL CIBERTERRORISMO EN ESPAÑA. PREGUNTA DE INVESTIGACIÓN.

El uso masivo de las TIC, en todos los ámbitos de la sociedad, ha creado un nuevo espacio, el ciberespacio, donde se producirán conflictos y agresiones, y donde existen ciberamenazas que atentarán contra la seguridad nacional, el estado de derecho, la prosperidad económica, el estado de bienestar y el normal funcionamiento de la sociedad y de las administraciones públicas.

Las amenazas para la seguridad, tanto individual como colectiva son múltiples, diversas y cambiantes, e Internet y su tecnología asociada están contribuyendo, de una forma cada vez más determinante en ello; ya que está siendo utilizada con profusión como soporte para la ejecución de múltiples y diversas acciones ilícitas, no sólo por grupos delincuenciales al uso (que se han adaptado y rápido a los nuevos tiempos), sino que lo están siendo también por otras formas de delincuencia grave tales como grupos y organizaciones terroristas, colectivos antisistema en general

3 La relevancia no la tiene tanto la infraestructura en sí, sino la función que ésta desempeña o el servicio que presta. Es decir, son determinadas funciones las que, a juicio del Centro Nacional de protección de IC, merecen el calificativo de esenciales y a partir de ahí, mediante el estudio de las instalaciones, las redes y los procesos de trabajo por los que se desarrollan estas funciones, se puede determinar si alguna de las infraestructuras sobre las que operan reúne las características precisas para ser considerada de una manera especial.

o que buscan la desestabilización de un Estado en particular, organizaciones clandestinas, e incluso las estructuras de inteligencia de algunos estados.

De todo lo anterior deriva la necesidad de estudiar las amenazas que pueden constituir los ciberataques, entendiendo como tales, aquellas en las que se utilizarán las TIC, por parte de organizaciones terroristas, para lograr sus objetivos, utilizando Internet, entendido como una base de datos de información y los servicios de comunicación que proporciona, llegando a hacer uso de Internet para la realización de actividades terroristas, o Internet se toma como objeto de ataque o acción del delito (por ejemplo para el ataque a infraestructuras críticas y estratégicas).

Los responsables del mantenimiento de las infraestructuras críticas y/o estratégicas en España, deberían establecer los mecanismos de seguridad necesarios para preservarlas, en colaboración con los componentes de las Fuerzas y Cuerpos de Seguridad. Éstos últimos deben trabajar en estrecha relación junto con las autoridades judiciales y los entes públicos para prevenir el ciberterrorismo, y una vez que éste se produce, imputarlo al autor o autores del mismo

¿Qué ocurriría si de un momento a otro se paralizara el tráfico aéreo en los principales aeropuertos españoles? ¿Y si el sistema de abastecimiento de agua o electricidad fuese igualmente atacado? ¿Cómo se vería afectada la vida diaria si las líneas de telecomunicación dejasen de prestar sus servicios?

Por todo ello se plantea la siguiente pregunta:

-¿De acuerdo con la legislación nacional e internacional vigente, y los avances tecnológicos actuales, ha adaptado España de manera efectiva sus medidas de protección a los éstandares internacionales y a los compromisos adquiridos, para hacer frente al ciberterrorismoy su amenaza para las infraestructuras críticas?

Dado el límite de extensión del presente TFM, el estudio tiene que ceñirse a la situación presente en España, pudiendo ser objeto de otro estudio el marco comparado entre las legislaciones nacionales de diferentes países de la Unión Europea.

3.-MARCO TEÓRICO PREVIO. EL CIBERTERRORISMO Y SUS AMENAZAS.

En cuanto al concepto de *ciberterrorismo*, no existe una definición general y globalmente aceptada del término. Cabe destacar que el ciberterrorismo como concepto ha ido evolucionando a lo largo de los años, hasta llegar a lo que actualmente se entiende por este término.

Para definirlo se va a seguir el hilo argumental comentado por Luís Hernández, en la Ponencia V, "Internet y las Nuevas Tecnologías frente a la amenaza del Terrorismo", del XX Seminario Duque de Ahumada, celebrado por la UNED y la Dirección General de la Guardia Civil en 2012:

En los 80 se definió como *"la convergencia del ciberespacio con el terrorismo"*(B. Collin, Instituto de Inteligencia y seguridad. USA. 1984); en los 90, se comenzó a profundizar de forma que se consideraba que "e*l ciberterrorismo es el ataque premeditado y políticamente motivado contra información, sistemas, programas y datos informatizados no combatientes, por parte de grupos terroristas o agentes encubiertos de potencias extranjeras*" (M. Pollit, E.A.FBI Proccedingsof the 20th NationalInformationSystems Security Conference. 1997).

Sin embargo, en la actualidad el concepto que se maneja aparece más definido y abarca mucho más, de forma que se puede afirmar que *"es la ejecución de un ataque sorpresa por parte de un grupo (o persona) terrorista, con objetivo político, utilizando tecnología informática e Internet para paralizar o desactivar las infraestructuras electrónicas y físicas de una nación, provocando de este modo la pérdida de servicios críticos, como energía eléctrica, sistemas de emergencia telefónica, servicio telefónico, sistemas bancarios, Internet y otros muchos servicios esenciales. El objeto de un ataque ciberterrorista no es solo impactar sobre la economía de una región o país, sino amplificar los efectos de un ataque terrorista físico tradicional provocando confusión y pánico adicionales en la población en general. El ciberterrorismo existe porque es en el reino cibernético donde son más débiles la mayoría de las naciones industrializadas"*. (Dan Verton. Periodista especializado en seguridad informática y ex oficial de inteligencia Naval de los Estados Unidos. 2003).

Desde el punto de vista del autor del mencionado artículo, se considera que se debe entender por ciberterrorismo el *empleo generalizado de las TIC, por parte de grupos terroristas u organizaciones afines, para la consecución de sus objetivos; utilizando Internet (sistemas informáticos y contenidos) como instrumento de comisión del delito ó como acción del delito.*

En sentido amplio, se puede deducir que se puede denominar ciberterrorismo al uso de las TIC y en particular Internet, como instrumento o medio para la realización de actividades terroristas; si bien, considerándolo de un modo más estricto, se debe contextualizar a Internet y más concretamente a los sistemas informáticos y de telecomunicación que lo sustentan o que sirven de base tecnológica para el normal y correcto funcionamiento de las denominadas y catalogadas infraestructuras críticas o estratégicas, como objetivo directo de una acción terrorista.

Tal y como relata el Profesor Torres Soriano en el libro "El Eco del Terror", es obvio que terroristas, como los yihadistas, tratan de obtener una captación global, no sólo en los países musulmanes, sino también en occidente. Para ello, utilizan las páginas web, foros y chats de internet, se identifican canales de financiación, se fomenta la recluta, y la red sirve de base para todo su aparato de propaganda[4].Aunque sigue siendo cierto, que todas estas páginas y contenidos son una fuente muy importante de información contraterrorista, para los servicios de seguridad e inteligencia de occidente, y una obligada observación constante de las mismas puede ser vital para prever futuras acciones.

El mantenimiento y soporte de las infraestructuras críticas se fundamenta en la seguridad de sus sistemas de información, y en garantizar la continuidad de la explotación del Sistema, evitando los riesgos potenciales, tanto accidentales como intencionados.

El concepto de seguridad de las TIC (STIC) es mucho más amplio que la simple protección de los datos a nivel lógico. Para proporcionar una seguridad real se han de tener en cuenta múltiples factores, tanto internos como externos. En primer lugar, habrá que caracterizar el Sistema que va a manejar la información para poder identificar las amenazas y en este sentido se pueden encontrar:

-**Sistemas aislados**: son sistemas que no están conectados a ningún tipo de red.

-**Sistemas interconectados**: hoy en día, casi cualquier ordenador pertenece a alguna red, enviando y recibiendo información del exterior casi constantemente.

El concepto STIC no sólo abarca la protección de la confidencialidad de la información, en la mayoría de los casos es necesario también que los sistemas sólo permitan el acceso de los

4 Aún se pueden recordar las crudas imágenes de rehenes asesinados por decapitación, o acciones terroristas filmadas y posteriormente difundidas a través de la Red, que lógicamente se escapan de la racional concepción de las cosas y escala de valores. Los videos con mensajes propagandísticos del propio Osama Bin Laden, los nuevos aparecidos recientemente realizados por la nueva organización Estado Islámico, cuya acción se desarrolla en Siria e Irak, o comunicados de la organización terrorista ETA; estas nuevas técnicas 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, amedrentan la moral de sus objetivos y víctimas y enaltecen la sinrazón de sus adeptos.

usuarios autorizados, se encuentren disponibles en todo momento y garanticen que la información que manejan mantiene su integridad.

En consecuencia, la STIC hace referencia al conjunto de medidas de seguridad para proteger la información almacenada, procesada o transmitida por Sistemas de Información y Telecomunicaciones, de manera que se aseguren o garanticen la confidencialidad[5], integridad[6] y disponibilidad[7] de la información y la integridad y la disponibilidad de los propios sistemas (IX Curso Gestión STIC-Módulo ENS-INAP: 2014). Por tanto, se pueden identificar los siguientes problemas:

-Denegación del servicio *(disponibilidad)*: impedir el acceso a la información.
-Observación no permitida *(confidencialidad)*: acceso no autorizado a la información.
-Modificación no autorizada *(integridad)*: alteración no permitida de la información, ya sea borrando, cambiando o sustituyendo datos.

Para supervisar el normal funcionamiento de los servicios se utilizan los sistemas SCADA (Sistemas de Supervisión, control y Adquisición de Datos), que comprenden el conjunto de aplicaciones que recogen medidas y datos operativos de los equipos pertenecientes a un determinado sistema. Ello se hace con la intención de controlar si el funcionamiento del sistema es correcto o no y, en caso de no serlo, tratar de tomar las medidas oportunas.

Los sistemas SCADA[8] resultan vitales para múltiples servicios esenciales, tales como los sistemas de transportes (metro, trenes, puertos o aeropuertos), sistemas industriales (químicas, refinerías, etc.), distribución y control de electricidad, agua o gas, centrales eléctricas, térmicas, hidroeléctricas, nucleares, etc.

Los sistemas de control de procesos son, además, también fundamentales en muchas industrias. Toda la producción depende de unos pocos sistemas, y un fallo de estos puede ocasionar que no se detecten malos funcionamientos que produzcan graves pérdidas económicas, cuando no

5 Que la información sea revelada exclusivamente a los usuarios autorizados a tal efecto.

6 Que la información sea modificada sólo por personal autorizado. La integridad garantiza la exactitud de la información contra la alteración, pérdida o destrucción, ya sea de forma accidental o intencionada.

7 Que la información sea utilizable cuándo y cómo lo requieran los usuarios autorizados.

8 Los sistemas SCADA fueron diseñados antes del surgimiento de Internet. Fueron pensados para ser sistemas aislados y no conectados en red, por lo que tradicionalmente carecen de dispositivos de seguridad como cortafuegos, mecanismos de cifrado o software antivirus. Su diseño se centraba en la funcionalidad, la fiabilidad y la seguridad física, en limitar el acceso.

un peligro para la seguridad de los empleados o desastres medioambientales[9]. Por lo tanto, y como punto único de fallo, la seguridad de estos sistemas debe ser una materia de máxima prioridad.

Se puede hablar de dos términos generalistas que aglutinan los ataques informáticos más relevantes que pueden ocurrir:

- *Cibersabotaje:* según el diccionario de la RAE, el sabotaje es el daño o deterioro que en las instalaciones, productos, etc., se hace como procedimiento de lucha contra los patronos, contra el Estado o contra las fuerzas de ocupación en conflictos sociales o políticos, en el presente campo de estudio el cibersabotaje se puede entender como la *"acción deliberada dirigida a debilitar un elemento de las TIC mediante la subversión, la obstrucción, la interrupción o la destrucción de sus componentes o de la información que gestiona."*, según se cita en es.wikipedia.org. Se trata por tanto de un concepto muy amplio en el que se aglutinan muchos de conceptos: ciberguerra, ciberterrorismo, ciberespionaje o activismo.

- *Hacktivismo:* se ha encontrado una definición apropiada en es.wikipedia.org, ya que este término no se encuentra en el diccionario de la RAE, proveniente de hacker y activismo, se entiende por el movimiento cuyas acciones están dirigidas a *"obtener el control de elementos TIC para promover una causa determinada, defender un posicionamiento político, interrumpir*

9 El 27 de septiembre de 2010, los principales diarios nacionales (La Vanguardia: *"Irán sufre un masivo ataque informático")* e internacionales (Financial Times, *Online attackwas Ahmed at nuclear work, saysTeheran")* se hacen eco de la misma noticia: el que hasta la fecha se considera el mayor ataque informático de la historia.En él, los sistemas de control de la central nuclear de Bushehr, así como otras industrias, se vieron afectados por el virus Stuxnet*(programa de software dañino del tipo Troyano muy avanzado, que aprovecha la vulnerabilidad MS10-0466 de los sistemas operativos Windows CC, empleados en los sistemas SCADAfabricados por Siemens y que se utiliza en Infraestructuras Críticas tales como el control de oleoductos, plataformas petrolíferas, centrales eléctricas, nucleares y otras instalaciones industriales con el objetivo de sabotearlos. Se cree que una vez dentro de una planta podría reprogramar las centrifugadoras para hacerlas fallar sin que se detectara)*, de una potencia sin precedentes. Los expertos consultados entonces por el diario el País afirmaron entonces que podrían haberse visto afectados hasta el 60% de los ordenadores iraníes, el 20% de los indonesios y el 8% de los indios.

El modo de funcionamiento de este virus consiste en convertirse en agente durmiente de forma que se pueda accionar a distancia en el momento que el creador lo considere oportuno. Todo ello sin que el legítimo usuario del equipo infectado sea consciente de estar de algún modo formando parte de un ciberataque. Dada su complejidad sin precedentes, se cree que es imposible que dicho virus informático fuese diseñado por una única persona. Por el contrario, todo apunta a un grupo de profesionales que dispusieran de medios y dinero suficiente para realizarlo.

Eugene Karsperky, cuya compañía de seguridad informática fue la primera en detectar la amenaza, afirmó poco después: "*Stuxnet no puede haber sido creado por ningún grupo de hackers, solo algunos estados tienen recursos para montar una operación semejante"*. Es por este motivo por el que surge la idea de que todo un Estado podría estar detrás de este hecho. De ser esto cierto, podría constituir el primer acto de *ciberguerra* propiamente dicho, pues hasta el momento estos ataques llevados a cabo por estados siempre se habían realizado como complemento a ataques convencionales, para facilitar la libertad de acción de las fuerzas propias y dificultar la del enemigo. De no ser así, sí que se puede afirmar, en cualquier caso, que constituye un punto de inflexión en cuanto al ciberterrorismo se refiere; el mismo Karsperky afirmó: "*Durante décadas hemos visto ataques de cibervándalos y ciberdelincuentes; acabamos de entrar en la era del ciberterrorismo"*.

El Stuxnet constituye un salto cualitativo en el panorama mundial de la ciberguerra. Aún se sabe muy poco de él, pero lo que nadie discute es que provocó la parálisis del programa nuclear de Irán. Además, es el primer virus capaz de penetrar en los sistemas automáticos de control de infraestructuras públicas tales como centrales eléctricas, nucleares, presas e industrias químicas.

Se especula mucho sobre quién lo diseñó o quién lo distribuyó. Siempre se ha sospechado de Israel, pero hay quien apunta a Estados Unidos, o incluso a una operación conjunta entre ambos estados. Richard Clarke, encargado de la Oficina Antiterrorista de los Estados Unidos durante los atentados del 11 de Septiembre de 2001, así como el Coordinador para la Seguridad Nacional y de Protección de Infraestructuras *(National Coordinator for Security, Infraestructure Protection)*, afirmó sobre los ataques: *"El ataque de Estados Unidos contra las instalaciones nucleares de Irán fue un ataque muy sofisticado. Se diseñó para romper cosas, para que estallaran… y funcionó"* .No obstante, resulta casi imposible probar de dónde viene el ataque. Incluso aún sabiendo que viene de un determinado territorio, no hay forma de afirmar si el responsable último es el gobierno en cuestión o simplemente un grupo organizado de hackers.

servicios, impidiendo o dificultando el uso legítimo de los mismos." Esta amenaza podría perjudicar las relaciones en el ciberespacio entre el ciudadano y cualquier organismo público o privado. A menudo se entiende que se trata de promover una ideología política, teóricamente relacionadas con derechos como la libertad de expresión, los derechos humanos o la ética de la información. Las teorías más benevolentes con estos movimientos lo conciben como un término que describe acciones directas llevadas a cabo en favor de un teórico cambio social. Sin embargo, por parte de los organismos e instituciones públicas se utiliza el término como sinónimo de actos maliciosos y destructivos que vulneran la seguridad de Internet como una plataforma tecnológica, económica y política. Es, probablemente esta última, la visión más acertada del término. El máximo exponente del activismo en España y probablemente también en el mundo es Anonymous.

4.- FORMULACIÓN DE HIPÓTESIS.

España se encuentra expuesta a amenazas de distinta índole provenientes del ciberespacio, las cuales pueden afectar en mayor o menor medida al bienestar de la sociedad, a la gobernabilidad y estabilidad del país y al funcionamiento de las infraestructuras tecnológicas nacionales, y a las privadas que son de máxima prioridad, como los servicios de abastecimiento. **Por todo ello, se acotará como campo de estudio la Protección de las Infraestructuras Críticas a nivel nacional desde el punto de vista de la seguridad lógica.**

Para enfrentarse al ciberterrorismo, y los ataques contra las Infraestructuras Críticas, existe una legislación internacional, avalada por una serie de convenios internacionales, que se conforman como herramientas para la prevención y la persecución del ciberterrorismo.

Dados los límites de extensión requeridos para el presente estudio, se debe proceder al estudio de la situación focalizada en España, por lo que se formula la siguiente **hipótesis primera.**

Hipótesis: existe una legislación extensa referente a la Protección de Infraestructuras Críticas (en adelante PIC) o aplicable a ella, que puede dar lugar a organizar una respuesta ante el ciberterrorismo. España ha incorporado al ordenamiento interno toda la legislación internacional y convenios internacionales relativos a la lucha contra el ciberterrorismo, llegando a desarrollar una prolífica legislación nacional que regula la acción del Estado, para lograr los fines de prevención y persecución del mismo.

Pero la acción de prevención y persecución se debe traducir en herramientas operativas que lleven a la práctica un procedimiento eficaz de implementación de esas herramientas, lo que lleva a la formulación de la siguiente **hipótesis segunda:**

Hipótesis: la legislación nacional española se ha traducido en la implementación de herramientas operativas efectivas diseñadas para la lucha contra el ciberterrorismo, desarrolladas para la prevención, recuperación de los servicios y sistemas de las Infraestructuras Críticas, y la persecución de los ciberterroristas.

5.- METODOLOGÍA Y FUENTES DE INFORMACIÓN.

Para confirmar las dos hipótesis formuladas, primero se va a estudiar la legislación internacional y los convenios internacionales existentes sobre protección de infraestructuras críticas frente al terrorismo, existentes dentro de la Unión Europea, como marco organizativo común y armonizador.

A continuación, se estudiará el ordenamiento interno en España, enumerando los procedimientos y herramientas que se establecen para proteger las infraestructuras críticas.

Finalmente, se describirán los procesos de prevención y las medidas establecidas para minimizar el impacto de un ciberataque terrorista, y los procedimientos para asegurar la continuidad de los sistemas y servicios.

Después de este proceso, se estará en condiciones de demostrar las dos hipótesis enunciadas, o de aceptarlas con matices.

6.- LA PROTECCIÓN DE INFRAESTRUCTURAS CRÍTICAS COMO OBJETO DE REGULACIÓN.

En este apartado se va a abordar el estudio para dar respuesta a la pregunta formulada, con la primera hipótesis, para ello, es necesario estudiar toda la legislación a tener en cuenta a la hora de valorar la adopción de la misma por parte de España.

A mediados de 2004, el Consejo Europeo encomendó a la Comisión Europea la elaboración de una estrategia global sobre PIC. El 20 de octubre del mismo año, la Comisión adoptó una

Comunicación[10] sobre la PIC en la lucha contra el terrorismo, que contiene propuestas para mejorar la prevención, preparación y respuesta de Europa frente a atentados terroristas que les afecten. Con posterioridad, en diciembre de 2004, el Consejo aprobó el Programa Europeo de Protección de Infraestructuras Críticas (en adelante, PEPIC) y puso en marcha una Red de Información sobre Alertas en Infraestructuras Críticas (CIWIN)[11], o *Critical Infraestructure Warning Information Network.*

La entrada en vigor de la Directiva 2008/114/CE (en adelante, Directiva) sobre la identificación y designación de Infraestructuras Críticas Europeas (en adelante ICE) y la evaluación de la necesidad de mejorar su protección, constituye un importante paso en la cooperación en esta materia en el seno de la UE. En dicha Directiva se establece que la responsabilidad principal y última de proteger las ICE corresponde a sus operadores y a los Estados miembros en los que se encuentran. También se determina el desarrollo de una serie de obligaciones y de actuaciones que se han de llevar a cabo por dichos Estados.

No obstante, no fue hasta el año 2007 cuando, tras los ciberataques sufridos por Estonia[12], se tomó conciencia de la importancia de fortalecer la seguridad lógica de dichas infraestructuras. Se

---

10 Comunicación de la Comisión publicada en Consejo y al Parlamento europeo – Protección de las infraestructuras críticas en la lucha contra el terrorismo. COM (2004) 702 final – no publicada en diario Oficial.

11 Propuesta de decisión del Consejo de 27 de octubre de 2008 relativa a una Red de información sobre alertas en infraestructuras críticas (CIWIN)COM(2008) 676 final – no publicada en el Diario Oficial. Tal y como se preveía en la Comunicación, esta propuesta independiente tenía como objetivo establecer una red de información sobre alertas en infraestructuras críticas (CIWIN). La CIWIN proporcionaría a los Estados Miembros un sistema de información, comunicación y alertas seguro para intercambiar datos referentes a la PIC. El sistema facilitaría la cooperación entre los Estados Miembros., permitiendo intercambios sobre amenazas y vulnerabilidades, así como sobre estrategias para mejorar la protección de infraestructuras críticas. La participación de los Estados Miembros en esta Red sería de carácter voluntario. La CIWIN consistiría en un foro electrónico y un sistema de alerta rápida, el primero para el intercambio de información y el segundo para alertas sobre riesgos y amenazas. Se trataría de un sistema clasificado seguro, en el que el acceso a la información se regularía consecuentemente. El desarrollo de los aspectos técnicos de la CIWIN es responsabilidad de la Comisión.

12 Los acontecimientos que entre el 27 de abril y 11 de mayo del 2007 tuvieron lugar en *Estonia* han hecho que la percepción del problema cambie de una forma radical, al encontrarnos ante el primer ciberataque a gran escala dirigido contra infraestructuras TIC de un país, vía Internet.

Parece ser que el detonante fue la retirada de una Estatua al Soldado Desconocido, erigida en homenaje a los soviéticos que combatieron en la Segunda Guerra Mundial. Tras ello y durante dos semanas se suceden ciberataques, dirigidos, en su mayor parte, contra organismos públicos (Gobierno, Parlamento, etc.), entidades financieras (banca electrónica), medios de comunicación (ediciones digitales) y empresas de telecomunicaciones (ISP,s, servidores de correo, etc.).

Las acciones consistieron mayoritariamente en oleadas de ataques del tipo denegación de servicio distribuido (DDoS) desde numerosas botnets (redes de ordenadores comprometidos con software malicioso ó malware, también conocidos como "zombies") calculándose que se llegaron a convocar aproximadamente un millón de atacantes, coincidiendo como día de mayor intensidad el 9 de mayo en el que, de promedio, una Web gubernamental pasó de recibir 1.500 visitas al día a 1.000-1.500 por segundo. Estas acciones vinieron complementadas con accesos no autorizados a contenidos Web y cambios de apariencia *(defacements, término que hace referencia a la acción de cambiar, sin consentimiento de legítimo administrador, la apariencia de una determinada página Web)* con propaganda reivindicativa nacionalista rusa.

En la resolución del incidente se involucraron instituciones y organismos de vigilancia a nivel internacional como los principales Centros de Respuesta (en adelante, CERT,s) europeos, de Rusia, EE.UU. e incluso la OTAN, ya que Estonia invocó el artículo 5 del Tratado al entender inicialmente que estaba siendo objeto de una acción de ciberguerra, con las consiguientes tensiones diplomáticas.

Finalmente y tras múltiples intentos fallidos, resultó necesario "desconectar" el país de Internet, con el consiguiente y temporal "aislamiento" que ello conlleva, como única y última medida para controlar la situación, toda vez que cerca del 99% de tráfico Internet "atacante" procedía del exterior.

A raíz del incidente, la OTAN ha creado y constituido en Tallín su *Centro de Ciberdefensa* que refuerza a su *Centro de Excelencia* Antiterrorista ubicado en Turquía que coordinan la actividad de los *Centros Operativos de Seguridad* (SOC) y *Centros con Capacidad de Respuesta ante Incidentes Cibernéticos* (CIRC) de los diferentes países integrantes de la Alianza.

En cuanto a la autoría, parece claro que detrás se encuentra Rusia. Sin embargo, el portavoz estonio de Defensa, Maddis (*"Decir que vienen de Rusia, en el sentido político, no es correcto. Hay indicios claros, con páginas escritas en ruso, de que han venido directamente de Rusia, pero no podemos decir, ni hemos dicho, que vengan del Kremlin.")*, no fue tan contundente en sus declaraciones. En ellas aseguraba que los ataques venían de Rusia, pero que ello no significaba que el país vecino hubiese participado como nación.

daba por supuesto que un ataque cibernético causaría pocas víctimas o ninguna, pero que podría acarrear la pérdida de servicios de infraestructuras vitales.

A) LIBRO VERDE SOBRE EL PROGRAMA EUROPEO DE PROTECCIÓN DE INFRAESTRUCTURAS CRÍTICAS (PEPIC), DE 17 DE NOVIEMBRE DE 2005.

El principal objetivo del Libro Verde es recabar puntos de vista en torno a las posibles opciones para el PEPIC gracias a una amplia participación de los agentes interesados. Una protección eficaz de las IC,s requiere la comunicación, coordinación y cooperación, en el ámbito tanto nacional como de la UE, entre todas las partes interesadas[13].

El Libro introduce, una serie de definiciones vitales, una catalogación de los sectores de infraestructuras primordiales y unas nociones y requerimientos básicos para la confección de los planes de seguridad del operador. Todo ello sentó las bases de la actual Directiva y normativa nacional.

El objetivo del PEPIC sería asegurar niveles adecuados y equivalentes de seguridad en las infraestructuras críticas, minimizar los puntos de fallo y proponer mecanismos rápidos y probados de recuperación de infraestructuras para toda la Unión Europea. Dicho nivel de protección dependerá de las repercusiones que ocasione el cese de la prestación de sus servicios, la extensión geográfica que puede verse afectada, la gravedad y los efectos en el tiempo.

B) DIRECTIVA UE 2008/114/CE, DE 8 DE DICIEMBRE, SOBRE IDENTIFICACIÓN Y DESIGNACIÓN DE ICE.

La Directiva constituye el primer paso en el proceso de identificación, designación y protección de las Infraestructuras Críticas Europeas. El principal objetivo de la Directiva es definir una serie de medidas y acciones que los diferentes Estados miembros y de la Unión Europea (en adelante UE) deben poner en marcha. Para ello se establece qué es una ICE, cuáles son las medidas que los operadores deben cumplir, y qué acciones deben desarrollar los Estados miembros para garantizar la seguridad global, ya que resulta lógico que un fallo en la seguridad de una IC de un

13 Se consideran partes interesadas a los propietarios y operadores de las infraestructuras, reguladores, asociaciones profesionales y empresariales en cooperación con todos los niveles de la administración y el público en general.

determinado país, no sólo tendría repercusiones en el Estado concreto en el que se encuentra. En cuanto a los objetivos concretos que se mencionan en la Directiva, los más relevantes son:

- Orientar la PIC desde el punto de vista de los riesgos terroristas.
- Los Estados deben identificar sus ICE.
- Los Estados miembros deben, del mismo modo, realizar una clasificación de seguridad.
- La responsabilidad en materia de la PIC recae no únicamente sobre los Estados, sino también sobre los operadores. Resulta de vital importancia el hecho de que estos operadores, en la mayor parte de los casos, son de carácter privado.
- Los propietarios/operadores deben establecer un Plan de Seguridad de Operador.
- Los propietarios/operadores deben designar un Responsable de Enlace para Seguridad.
- Se da un plazo de 24 meses desde la aprobación de la Directiva para adoptar las medidas necesarias.

El documento se encuentra estructurado en dos partes. La primera de ellas consiste en una serie de definiciones, identificación y designación de ICE y en ella se acota el tipo de infraestructuras que hay que tener en cuenta y se establece un procedimiento de identificación y designación de las ICE. En la segunda de las partes, sin embargo, se establece un planteamiento común para evaluar la necesidad de mejorar la protección de dichas infraestructuras, pasando por los planes de seguridad de los operadores, los responsables de seguridad y los informes que se deben de llevar a cabo para presentarlos a la Comisión.

C) CONSTITUCIÓN ESPAÑOLA DE 1978.

Parece obvio que la Carta Magna no va a regular de forma directa la PIC, pero esta protección de infraestructuras críticas se encuentra encuadrada dentro de la Seguridad Pública, por lo que tanto la LPIC como el RDPIC han sido elaborados en base a la competencia que la Constitución Española reconoce al Estado[14]. Ello significa que es el Estado (sin perjuicio de lo regulado en los correspondientes Estatutos de Autonomía acerca de sus policías autonómicas) es competente y responsable de gestionar y regular la seguridad la seguridad de dichas instalaciones.

14 Art. 149.1.29ª de la Constitución Española de 1978, por el que el Estado tiene competencia exclusiva sobre la *"Seguridad Pública, sin perjuicio de la posibilidad de creación de policías por las Comunidades Autónomas en la forma que se establezca en los respectivos Estatutos en el marco de lo que disponga la ley orgánica."*

En cuanto a las Fuerzas y Cuerpos de Seguridad, la Carta Magna les encomienda la misión de *garantizar la seguridad ciudadana,*[15] por lo que, de forma indirecta, se atribuye competencia sobre esta materia a la Guardia Civil, y al Cuerpo Nacional de Policía entre otros.

D) LEY ORGÁNICA 10/1995, DEL CÓDIGO PENAL.

En el Código Penal son pocos los artículos en que se alude, de forma expresa, a posibles ciberataques dirigidos contra infraestructuras críticas. De hecho, se encuentran no pocos artículos relativos a delitos informáticos[16], pero sólo algunos relacionados con el ciberespionaje o el ciberterrorismo. Cuando se habla de ellos, se hace alusión a los ataques más graves que afectan indiscriminadamente a intereses generales de la población, con la intención de crear pánico y terror, para subvertir el sistema político o de convivencia generalmente aceptado (Velasco, Eloy. 2010*)*. Estos delitos apenas tienen incidencia estadística en nuestra sociedad. No obstante, algunas de sus modalidades presentes en nuestro Código Penal pueden ser la usurpación de funciones públicas o el descubrimiento y revelación de secretos relativos a la defensa nacional[17].

E) LEY ORGÁNICA 2/1986, DE 14 DE MARZO, DE FUERZAS Y CUERPOS DE SEGURIDAD.

La LO 2/86 regula, en su Título II, Capítulo II, las funciones y competencias territoriales y materiales de las Fuerzas y Cuerpos de Seguridad del Estado. En cuanto a las funciones comunes a Cuerpo Nacional de Policía y Guardia Civil, resulta de especial interés para el presente estudio el apartado "C" del artículo 11, según el cual las FCSE *vigilarán y protegerán los edificios e instalaciones públicos que lo requieran*[18].

---

15 Art. 104 de la Constitución Española, en el que se establece que *"las Fuerzas y Cuerpos de seguridad, bajo la dependencia del Gobierno, tendrán como misión proteger el libre ejercicio de los derechos y libertades y garantizar la seguridad ciudadana.*

16 Arts. 169 y 172 CP, *Amenazas y coacciones informáticas.*

Arts. 168-189 CP, *Distribución de material pornográfico y pornografía infantil.*

Arts. 197-200 CP, *Descubrimiento y revelación de secretos.*

Arts. 205-216 CP, *Injurias y calumnias informáticas.*

Arts. 417, 418 y 423 CP, *Cesión inconsentida de datos ajenos.*

17 Art. 402 CP. *Usurpación de funciones públicas* mediante correo electrónico.

Arts. 598 y 603 CP. Descubrimiento y revelación de secretos relativos a la defensa nacional.

18 Art. 11. apartado C) de la LO 2/1986, de 13 de marzo de Fuerzas y Cuerpos de Seguridad, según el cual *"las Fuerzas y Cuerpos de Seguridad del Estado tienen como misión proteger el libre ejercicio de los derechos y libertades y garantizar la seguridad ciudadana mediante el desempeño de las siguientes funciones: (…) vigilar y proteger los edificios e instalaciones públicos que lo requieran"* Resulta obvio que esta vigilancia y protección de edificios e instalaciones se refiere a todos los tipos de seguridad posibles. Es decir, comprende no sólo la seguridad física, sino también la seguridad lógica o ciberseguridad.

Conviene resaltar, sin embargo, que la mayor parte de las Infraestructuras Críticas en territorio nacional se encuentran en manos de empresas privadas, y que la presente Ley Orgánica encomienda al Cuerpo Nacional de Policía *"el control de las entidades y servicios privados de seguridad, vigilancia e investigación de su personal, medios y actuaciones."*[19]Al leer estas líneas el lector puede pensar que, consecuencia de ello, la Guardia Civil podría ver disminuidas sus capacidades operativas a la hora de colaborar con dichas entidades privadas[20]. Sin embargo, en la práctica, el control al que se refiere la referida LO se ciñe exclusivamente al ámbito administrativo y la Guardia Civil no ve en absoluto mermadas sus capacidades a la hora de relacionarse con las empresas privadas de seguridad.

F) PLAN NACIONAL DE PROTECCIÓN DE INFRAESTRUCTURAS CRÍTICAS (PNPIC), DE 7 DE MAYO DE 2007.

En Octubre de 2005, el Ministerio del Interior encomendó al Comité Ejecutivo para el Mando Unificado (CEMU, cuya denominación ha cambiado por la de CECO, Comisión Ejecutiva de Coordinación) la elaboración del PNPIC[21]. Para el desarrollo de los trabajos técnicos y operativos precisos para la elaboración del PNPIC, se dotó al CEMU de un grupo de trabajo del que formaban parte especialistas de la GC y del CNP.

El presente Plan tiene como objetivo general establecer los criterios y las directrices precisas para movilizar las capacidades operativas y para articular las medidas y las respuestas necesarias para asegurar la protección permanente, actualizada y homogénea del sistema de IC,s. Dicho objetivo general se pretende alcanzar a través de las siguientes líneas de actuación:

- Establecimiento de programas y articulación de medidas sectoriales y territoriales de prevención y protección para así dotar de unos niveles adecuados de seguridad a los sistemas de infraestructuras estratégicas, especialmente frente a ataques deliberados.
- Articulación de una serie de actuaciones dirigidas a minimizar los riesgos y los daños que se derivan de una situación de crisis.

19 Art. 12. A) g) de la LO 2/1986, de 13 de marzo, de Fuerzas y Cuerpos de Seguridad.

20 Según fuentes consultadas en la Dirección General de la Guardia Civil, existen un total de 1396 Infraestructuras Estratégicas en demarcación de Guardia Civil de las que aproximadamente el 80% se encuentran en manos de empresas de seguridad privada. El total de infraestructuras consideradas como estratégicas son unas 3700, tal y como afirma D. Fernando Sánchez Gómez, director del CNPIC en una entrevista conferida a la revista Seguritecnia en septiembre de 2011.

21 Tal decisión fue comunicada a la opinión pública con ocasión de su comparecencia ante la Comisión de Interior del Congreso de los Diputados, para informar sobre la implementación de las recomendaciones de la Comisión de investigación sobre los atentados del 11-M en Madrid.

- Establecimiento de mecanismos permanentes que se llevarán a cabo en coordinación con los gestores de las diferentes infraestructuras, y teniendo en cuenta sus respectivos planes de seguridad y de emergencia.

El PNPIC clasifica las infraestructuras del Catálogo según su mayor o menor criticidad, al tiempo que realiza una gradación en función de los diferentes niveles de seguridad a los que se debe someter cada una de ellas. Es en este segundo campo donde las FCS van a desempeñar un papel más relevante y, en función del nivel que se decrete, van a desempeñar uno u otro papel.

Además, establece que las IC se clasificarán en doce sectores estratégicos: administración, energía, espacio, sistema financiero y tributario, agua, industria nuclear, industria química, instalaciones de investigación, salud, tecnologías de la información y las comunicaciones, y transporte.

G) LEY 8/2011, DE 28 DE ABRIL, SOBRE PROTECCIÓN DE INFRAESTRUCTURAS CRÍTICAS (LPIC):

Con el fin de dar cumplimiento a la ya mencionada Directiva, se hizo preciso elaborar una norma cuyos objetos eran no sólo regular la PIC contra ataques deliberados de todo tipo, (tanto de carácter físico como cibernético), sino también la definición de un sistema organizativo de protección de dichas infraestructuras que aglutinara a todas las entidades afectadas. Se puede considerar que la medida de mayor calado llevada a cabo por esta Ley es la creación del CNPIC (Centro Nacional para la protección de las infraestructuras críticas), órgano encargado de la asistencia al Secretario de Estado de Seguridad.

Por tanto, las actuaciones necesarias para optimizar la seguridad de las infraestructuras críticas se enmarcan principalmente en el ámbito de la protección contra agresiones deliberadas y, muy especialmente, contra ataques terroristas, resultando por ello lideradas por el Ministerio del Interior.

En este ámbito se aprobó la Ley 8/2011, que tuvo su desarrollo reglamentario a través del Real Decreto 704/2011, de 20 de mayo, por el que se aprueba el Reglamento de Protección de las Infraestructuras Críticas (en adelante normativa PIC).

Entre las principales novedades en el seno de la normativa PIC destacan:

- Creación del sistema de Protección de Infraestructuras Críticas.
- Diseño de unos instrumentos de planificación del Sistema.
- La implantación del concepto de Asociación Público-Privada.

H) REAL DECRETO 704/2011, DE 20 DE MAYO, SOBRE PROTECCIÓN DE INFRAESTRUCTURAS CRÍTICAS (RDPIC).

El RDPIC se aprobó, en primer lugar, con la finalidad de desarrollar, concretar y ampliar los aspectos contemplados en la Ley 8/2011, máxime cuando de ella se desprende no sólo la articulación de un complejo sistema de carácter interdepartamental para la protección de infraestructuras críticas, compuesto por órganos y entidades tanto de las Administraciones Públicas como del sector privado, sino el diseño de todo un planeamiento ordenado a prevenir y proteger las denominadas infraestructuras críticas de las amenazas o actos intencionados de figuras delictivas como el terrorismo, potenciados a través de las Tecnologías de la Información y las Comunicaciones (TIC).

En segundo lugar, este texto normativo no sólo es coherente con el marco legal del que emana, sino que cumple además con la transposición obligatoria de la Directiva Europea. A ello obedecen las amplias previsiones que el texto contempla en el ámbito de los diferentes planes que deben elaborar tanto las Administraciones Públicas[22] como las empresas, organizaciones o instituciones clasificadas como operadores críticos, a quienes la LPIC asigna una serie de obligaciones, entre las que se encuentran la elaboración de sendos instrumentos de planificación[23].

En lo que a su contenido se refiere, el RDPIC consta de 36 artículos estructurados en cuatro Títulos. El Título I contiene las cuestiones generales relativas a su objeto y ámbito de aplicación, y dedica un capítulo a la figura del Catálogo. El Título II está plenamente dedicado al SPIC, y desarrolla, entre otras, las previsiones legales relativas a los órganos creados por la LPIC, esto es, el CNPIC, la Comisión Nacional para la Protección de las Infraestructuras Críticas (en adelante, Comisión)[24] y el Grupo de Trabajo Interdepartamental para la Protección de las Infraestructuras

22 El PNPIC, los Planes Estratégicos Sectoriales y los Planes de Apoyo Operativo.

23 Los Planes de Seguridad de Operador y los Planes de Protección Específicos.

24 Esta Comisión ha quedado finalmente constituida el 1 de julio de 2014, como órgano responsable de la aprobación de los Planes Estratégicos Sectoriales, para cada uno de los doce sectores críticos ya definidos.

Críticas (en adelante, Grupo de Trabajo), concretando la composición, competencias y funcionamiento de todos ellos. El Título III se encarga de la regulación de los instrumentos de planificación, centrándose en cada uno de los planes antes citados, cuyo proceso de elaboración, aprobación y registro, así como sus contenidos materiales, regula con mayor detalle. En este sentido, es de reseñar que el PNPIC permanecerá ligado y coordinado al Plan de Prevención y Protección Antiterrorista en vigor[25] y los Planes Sectoriales deberán ser compatibles con otros planes[26]. Finalmente, el Título IV trata de la seguridad de las comunicaciones y de las figuras del Responsable de Seguridad y Enlace y del Delegado de Seguridad de la IC.

I) **ESTRATEGIA ESPAÑOLA DE SEGURIDAD DE 2011 (EES):**

Al contrario que en el Código Penal, tanto las Infraestructuras Críticas como las ciberamenazas están presentes en gran parte del documento. En cuanto a las primeras, a éstas se les dedica, al igual que a las ciberamenazas, un apartado entero en el Capítulo 4, titulado "Amenazas, Riesgos y Respuestas". También se considera, en el Capítulo 3, a los peligros tecnológicos como potenciadores de riesgo.

Los ciberataques son potencialmente una de las amenazas más peligrosas y con mayores posibilidades de desarrollo a corto plazo contra las IC,s. De hecho, se afirma *que "la tecnología es una creciente fuente de progreso. Internet y los teléfonos móviles forman ya parte de nuestra vida cotidiana, nos abren al mundo y generan riqueza, pero nos hacen también más vulnerables. La tecnología puede potenciar o crear nuevas amenazas y riesgos para la seguridad."* Se trata, por tanto, de una amenaza en crecimiento con la que los posibles agresores (terroristas, crimen organizado, empresas, Estados o individuos aislados) podrían poner en peligro el correcto funcionamiento de las IC,s. Existen precedentes (Estonia en 2007 o Irán en 2010 ya citados en este estudio) de cómo la pérdida de disponibilidad de las mismas puede causar serios daños a un país. La ciberseguridad de las IC se ha convertido, así, en un ámbito clave para la seguridad de cualquier Estado.

Los ámbitos y riesgos se pueden materializar en los ámbitos clásicos: terrestre, marítimo, aéreo, espacial o informativo. Sin embargo, a estos ámbitos tradicionales, se les añade el ciberespacio, del que se destaca que se trata de un entorno singular, puesto que carece de fronteras

25 Art. 16.3 del RD 704/2011, de 20 de mayo, sobre protección de infraestructuras críticas.

26 Art. 29 del RD 704/2011, de 20 de mayo, sobre protección de infraestructuras críticas.

geográficas, es anónimo, asimétrico y puede ser utilizado de forma casi clandestina, sin necesidad de desplazamientos.

El CNPIC asume y se identifica totalmente con las diferentes líneas de acción planteadas: por un lado, la implantación de planes derivados de la LPIC, mejorar el marco regulador de los sectores estratégicos y establecer medidas que aumenten la fortaleza, resistencia y recuperación de las IC,s. Por otro lado, mantener un diálogo constante entre las Administraciones Públicas y los operadores de servicios que gestionan las IC,s. La denominada Asociación Público – Privada es un concepto clave que el CNPIC está impulsando desde sus inicios como base del Sistema de PIC.

J) ESTRATEGIA ESPAÑOLA DE CIBERSEGURIDAD DE 2013.

El 5 de diciembre de 2013, el Consejo de Seguridad Nacional aprobó la Estrategia de Ciberseguridad Nacional. Este documento se adopta al amparo y está alineado con la Estrategia de Seguridad Nacional de 2013, que contempla la ciberseguridad dentro de sus doce ámbitos de actuación.

Se organiza en 5 capítulos.El primero, *"El ciberespacio y su seguridad"*, define el ciberespacio y sus características como un nuevo dominio global y dinámico que está compuesto por las infraestructuras TIC. Identifica como riesgos y amenazas a la Ciberseguridad Nacional un amplio espectro proveniente de: individuos aislados, hacktivistas, amenazas internas, delincuentes, terroristas, estados extranjeros que se suman a los problemas causados por causas técnicas o fenómenos naturales.

El segundo capítulo, *"Propósito y principios rectores de la ciberseguridad en España"*, establece el propósito respetando el objetivo de ciberseguridad marcado en la ESN, así fija las directrices generales de un uso seguro del ciberespacio, con una visión integradora a través de la adecuada coordinación y cooperación de todas las Administraciones Públicas, contando además, con el sector privado y con los ciudadanos.

El tercer capítulo *"Objetivos de la ciberseguridad"*, define un objetivo global y seis objetivos específicos. Este objetivo global recoge el objetivo planteado en la ESN en el ámbito de la ciberseguridad "Garantizar un uso seguro de las redes y los sistemas de información a través del

fortalecimiento de nuestras capacidades de prevención, detección y respuesta a los ciberataques". Este fin será recogido en la futura Política de Ciberseguridad Nacional.

El capítulo 4, *"Líneas de acción de la ciberseguridad Nacional"*, se centra en detallar las líneas de acción que habrán de articularse para alcanzar los objetivos señalados en el capítulo anterior.

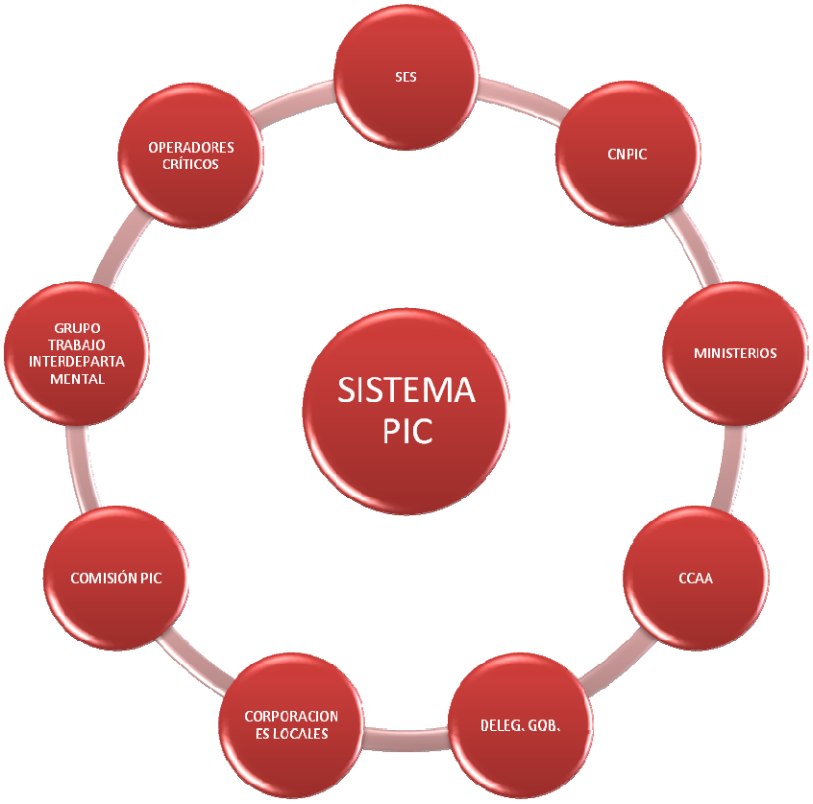
El quinto y último capítulo, "La ciberseguridad en el Sistema de Seguridad Nacional", establece la estructura orgánica al servicio de la ciberseguridad que responde a la visión integral del documento con objeto de dar una respuesta conjunta y adecuada para preservar la ciberseguridad. Esta estructura orgánica está formada por tres componentes, los dosúltimos de nueva creación, bajo la dirección del Presidente del Gobierno: a) el Consejo de Seguridad Nacional; b) el Comité Especializado de Ciberseguridad; c) el Comité Especializado de Situación, único para el conjunto del Sistema de Seguridad Nacional.

K) SISTEMA DE PROTECCIÓN DE INFRAESTRUCTURAS CRÍTICAS:

Este Sistema se compone de una serie de instituciones, órganos y empresas, procedentes tanto del sector público como del privado, con responsabilidades en el correcto funcionamiento de los servicios esenciales o en la seguridad de los ciudadanos.

Se establece la Secretaría de Estado de Seguridad como órgano superior del Ministerio del Interior responsable de este Sistema, siendo asistida por el Centro Nacional para la Protección de las Infraestructuras Críticas (CNPIC) para el desarrollo de todas aquellas actividades que tiene encomendadas dicha Secretaría de Estado en relación con la protección de Infraestructuras Críticas en el territorio nacional.

Dentro del Sistema, se instauran y se regulan las diferentes competencias y responsabilidades que tienen los agentes del mismo. Para comprender mejor el Sistema, a continuación se aporta un gráfico explicativo (www.cnpic-es.es).



F) OTROS.

Además, existe diversa legislación relacionada con la normativa existente sobre energía[27], transporte[28], centros propios de FCS y del Ministerio de Defensa, telecomunicaciones[29], o de protección de la información[30].

27 Ley 25/1964 de 29 de abril, sobre energía nuclear; Ley 15/1980, de 22 de abril, de creación del Consejo de Seguridad Nuclear; reformada por la Ley 33/2007, de 7 de noviembre.

28 Ley 21/2003, de 7 de julio, de Seguridad Aérea.

29 Ley 9/2014, de 9 de mayo, General de Telecomunicaciones; Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico.

30 Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, Ley 25/2007, de 18 de octubre, de Conservación de datos relativos a las comunicaciones.

7.- PROCEDIMIENTO DE RESPUESTA ESTATAL ANTE LAS AMENAZAS DE LAS INFRAESTRUCTURAS CRÍTICAS.

Una vez estudiada la legislación y las disposiciones nacionales e internacionales, se hace necesario desglosar los procedimientos prevención y de respuesta ante amenazas, para contrastar lo enunciado en la segunda hipótesis.

A) CENTRO NACIONAL DE PROTECCIÓN DE INFRAESTRUCTURAS CRÍTICAS (CNPIC)

La Secretaría de Estado de Seguridad (SES), es el órgano responsable de la dirección, coordinación y supervisión de la PIC nacional, de la creación del CNPIC como órgano director y coordinador de dichas actividades, y de la determinación, clasificación y actualización del Catálogo de Infraestructuras Críticas, de acuerdo con lo dispuesto en el Acuerdo de Consejo de Ministros de 2 de noviembre de 2007.

Las funciones principales del CNPIC son las de coordinar la información y la normativa; convertirse en el punto de contacto permanente con los administradores, tanto públicos como privados, de las IC; dirigir y coordinar los análisis de riesgos; establecer los contenidos mínimos de los planes de seguridad del operador y de los planes de protección específicos de las IC; establecer un sistema de mando y control y actuar como punto de contacto con centros similares en todo el mundo.

El CNPIC se erige así en un Punto de Contacto (en adelante, POC) que coordina lo que se podría considerar como los tres pilares fundamentales en la PIC:

-El primero de ellos está relacionado con la **cooperación interdepartamental**, que, coordinada por el CNPIC, está llegando a proveer un marco legal en el que desarrollar una estrategia nacional de ciberseguridad.

-El segundo de ellos también está relacionado con la cooperación, pero esta vez **con las agencias y organismos interesados**. Específicamente se debe establecer una correcta coordinación para dar una respuesta adecuada ante un ciberataque.

-Y por último, pero no menos importante, la **cooperación internacional,** entendiendo esta como un intercambio de información sobre experiencias reales.

Una herramienta esencial para esta cooperación es el sistema HERMES, del que se hablará más adelante. Por medio de esta herramienta informática y teniendo como base, entre otras, la información disponible por las Fuerzas y Cuerpos de Seguridad sobre desarrollos, tendencias y variaciones de los modus operandi de ciberataques, y el conocimiento existente en el CNPIC, los operadores críticos, con el asesoramiento de este Centro, podrán ajustar y poner en marcha sus medidas de seguridad.

B) CATÁLOGO DE INFRAESTRUCTURAS CRÍTICAS (CIC)

Este catálogo, clasificado de secreto, registra las infraestructuras consideradas como críticas y que, en su caso, requieren de especiales medidas de protección. Asociado a cada infraestructura, esta base de datos especifica las medidas de protección, los planes de reacción y la criticidad de la misma.

Del mismo modo, se clasifican las infraestructuras en los 12 sectores estratégicos ya mencionados[31], dividiéndose estos, a su vez, en subsectores[32].

Constituye la herramienta fundamental de trabajo de las FCSE y del CNPIC, pues, además de almacenar toda la información sobre la infraestructura, establece el punto de enlace con los operadores, las Fuerzas y Cuerpos de Seguridad del Estado y cualquier otro representante del SPIC. Permite la actualización continua y facilita el proceso de la evaluación de la criticidad y del nivel de seguridad de las infraestructuras evaluadas por el CNPIC.

Tal y como se afirma en la Web del CNPIC, el Catálogo deberá incorporar los datos relativos a la descripción de las IC, su ubicación, titularidad y administración, los servicios que prestan, medios de contacto con el administrador, el nivel de seguridad que precisan en función de los riesgos evaluados.

---

31 Según Ley 8/2011, de Protección de Infraestructuras Críticas, se define sector estratégico como "*cada una de las áreas diferenciadas dentro de la actividad laboral, económica y productiva, que proporciona un servicio dentro de la actividad laboral, económica y productiva, que proporciona un servicio esencial o que garantiza el ejercicio de la autoridad del Estado o de la seguridad del país.*"

32 Según Ley 8/2011, de Protección de Infraestructuras Críticas, se define subsector estratégico como "*cada uno de los ámbitos en los que se dividen los sectores estratégicos, conforme a la distribución que contenga, a propuesta de los Ministerios y organismos afectados, el documento técnico que se apruebe por el CNPIC*".

A través de HERMES, los operadores que finalmente sean designados críticos, podrán dar de alta, acceder y modificar la información relativa a aquellas infraestructuras que gestionen, configurándose de esta manera un sistema de intercambio de información continuo y fluido entre el CNPIC y los diferentes operadores.

C) SISTEMA HERMES

El Sistema HERMES (http://www.cnpic-es.es/) constituye el principal sistema de coordinación operativa. Se trata de un sistema pionero en Europa por la gran cantidad de datos que contiene, por la multitud de organismos que pueden acceder a él y por la alta seguridad de los procedimientos implantados para garantizar la confidencialidad de la información. Permite poner en contacto a todos y cada uno de los operadores críticos con el CNPIC y compartir así la información que se considere necesaria en cada circunstancia concreta. Se erige, de este modo, en puente que une a los operadores con las FCS, ya que la información de interés será accesible a éstos y al Centro Nacional de Coordinación Antiterrorista (en adelante, CNCA).

D) RED DE PROTECCIÓN SOBRE ALERTAS EN INFRAESTRUCTURAS CRÍTICAS (CIWIN)

La Red CIWIN es una iniciativa impulsada por la UE a través del PEPIC, aunque en realidad y a pesar de su nombre, no se trata de una red informática como tal, sino que consiste en la implementación de un catálogo de intercambio de información entre los Estados miembros de la UE. Su objetivo es ayudar a mejorar la PIC en los países que la forman, facilitando la coordinación y la cooperación entre los organismos competentes, que en la práctica no son los FCS de los diferentes países, sino que el uso que se da a esta Red se realiza a nivel CERT (Equipo de Respuesta ante Emergencias Informáticas, del inglés Computer Emergency Response Team). Se puede decir que los objetivos operativos son los siguientes:

- Proporcionar una herramienta que contribuya a la cooperación de los Estados miembros que lo deseen.
- Ofrecer un modo rápido y eficaz de obtención de información relativa a la PIC en la UE.
- Permitir a los Estados miembros comunicarse directamente e intercambiar la información que consideren pertinente.

En cuanto a la estructura de la Red CIWIN, ésta consiste en un documento que se va actualizando de forma continua y que ofrece principalmente información sobre los puntos de contacto de los Estados miembros (número de teléfono, dirección, correo electrónico…) así como sobre procedimientos de respuesta ante incidentes, siendo el punto de enlace nacional español el CNPIC.

E) INSTRUMENTOS DE PLANIFICACIÓN

Con el objeto de proteger aquellas infraestructuras críticas a nivel nacional frente a aquellas eventuales amenazas que puedan ponerlas en situación de riesgo, se diseñan unos planes de actuación. Estos planes se encuentran distribuidos de mayor a menor importancia según el siguiente gráfico (www.cnpic-es.es):

El Plan Nacional de Protección de Infraestructuras Críticas (PNPIC) es el instrumento de programación del estado elaborado por la Secretaría de Estado de Seguridad y dirigido a mantener seguras las infraestructuras españolas que proporcionan los servicios esenciales a la sociedad. A través de dicho Plan se establecen los criterios y las directrices precisas para movilizar las capacidades operativas de las Administraciones Públicas en coordinación con los operadores críticos, articulando las medidas preventivas necesarias para asegurar la protección permanente,

actualizada y homogénea de nuestro sistema de infraestructuras estratégicas frente a las amenazas provenientes de ataques deliberados contra ellas.

Los Planes Estratégicos Sectoriales (PES) son los instrumentos de estudio y planificación con alcance en todo el territorio nacional que permitirán conocer, en cada uno de los 12 sectores estratégicos en el ámbito PIC, entre los que se encuentra el sector de las Tecnologías de la Información y de las Comunicaciones (TIC), cuáles son los servicios esenciales proporcionados a la sociedad, el funcionamiento general de éstos, las vulnerabilidades del sistema, las consecuencias potenciales de su inactividad y las medidas estratégicas necesarias para su mantenimiento.

Dichos planes, que serán elaborados por el CNPIC con la colaboración de aquellos ministerios afectados por cada sector estratégico, se basarán en un análisis general de riesgos donde se contemplen las vulnerabilidades y amenazas potenciales, tanto de carácter físico como lógico, que afecten al sector o subsector en cuestión en el ámbito de la protección de las infraestructuras estratégicas.

Los Planes de Seguridad del Operador (PSO) son aquellos documentos estratégicos definidores de las políticas generales de los operadores críticos para garantizar la seguridad del conjunto de instalaciones o sistemas de su propiedad o gestión.

Los Planes de Protección Específica (PPE) son aquellos documentos operativos donde se deben definir las medidas concretas ya adoptadas y las que se vayan a adoptar por los operadores críticos para garantizar la seguridad integral (física y lógica) de cada una de sus infraestructuras críticas.

Por último, destacar que los Planes de Apoyo Operativo (PAO) son aquellos documentos operativos elaborados por las Fuerzas y Cuerpos de Seguridad con competencia en la demarcación territorial, donde se deben plasmar las medidas concretas a poner en marcha por las Administraciones Públicas en apoyo de los operadores críticos para la mejor protección de las infraestructuras críticas.

F) EQUIPOS DE RESPUESTA ANTE INCIDENTES (CERT)

Actualmente, los equipos de respuesta ante incidentes se consideran los organismos con mayor capacidad técnica y con la estructura más adecuada para luchar contra el mayor espectro de ciberamenazas. El modo de actuación se basa en la colaboración y sus relaciones son informales y flexibles pero guiadas por criterios de máxima eficiencia y rapidez en la actuación. Existen, en España y el mundo, gran cantidad de CERT que trabajan reaccionando ante ataques cibernéticos de diferentes clases.

El CCN-CERT es el centro de alerta nacional que coopera con todas las administraciones públicas para responder a los incidentes de seguridad en el ciberespacio y velar también por la seguridad de la información nacional clasificada. Tiene responsabilidades en ciberataques sobre sistemas clasificados, sistemas de la Administración General, Autonómica y Local y, en coordinación con el CNPIC, sobre sistemas que gestionen las IC. Se encarga de proporcionar a Presidencia del Gobierno, el estado de la amenaza en ciberseguridad.[33] Se trata por tanto de un CERT gubernamental de carácter nacional.

Durante el año 2008, el CCN-CERT inició el despliegue de un sistema de alerta temprana en la Red SARA[34] con el fin de detectar de manera proactiva las anomalías y ataques del tráfico que circula entre los diferentes ministerios y organismos interconectados.

No obstante el carácter nacional del mencionado CERT, algunas Comunidades Autónomas tienen también el suyo propio. Es el caso de la comunidad Valenciana, Cataluña y Andalucía, cuyos equipos de respuesta son CERT-CV[35], el CESICAT[36] y el Centro de Seguridad TIC de Andalucía respectivamente.

También destaca, por el importante papel que desempeña, el Instituto Nacional de Tecnologías de la Comunicación (en adelante, INTECO), dependiente del Ministerio de Industria, Turismo y Comercio. Es el responsable de gestionar, a través de su CERT, la defensa del ciberespacio relacionada con las Pequeñas y Medianas Empresas (en adelante, PYMES), así como con los ciudadanos en su ámbito doméstico. Resulta de gran importancia el encuentro anual que, desde el 2007 viene realizando: el Encuentro Internacional de la Seguridad de la Información (en

33 Art. 36 y 37 del RD 3/2012 de 8 de enero que desarrolla el Esquema Nacional de Seguridad.

34 Red de la que dependen aproximadamente el 90% de los sistemas de la Administración Pública.

35 CERT de la Comunidad Valenciana

36 Centro de Seguridad de la Información de Cataluña

adelante, ENISE) que pretende convertirse en un referencia entre los principales agentes en el campo de la seguridad, tanto en la UE como en Iberoamérica.

Otro equipo de respuesta es el IRIS-CERT, organismo también adscrito al Ministerio de Industria, Turismo y Comercio que con responsabilidad en la red IRIS que da servicio a múltiples universidades españolas y a diversos centros de investigación.

Del mismo modo existen también otros equipos de respuesta que ofrecen servicios a sectores más específicos, tales como La Caixa-CERT,[37] S21Sec-CERT[38], esCERT-UPC[39] o Hispasec[40].

G) PROCEDIMIENTO DE REACCIÓN ANTE ATAQUE INFORMÁTICO A UN SISTEMA CRÍTICO

En el modelo español se incorpora a las FSE como receptoras de Inteligencia. Se trabaja a través del Grupo de Trabajo Sectorial sobre las Tecnologías de la Información y Comunicaciones en el ámbito de las Infraestructuras Críticas (en adelante, GTS-TIC-IC) subordinado al Grupo de Trabajo para la Protección de las Infraestructuras Críticas (GT-PIC), en el marco de la Ley 8/2011, de 28 de abril, por la que se establecen medidas para la PIC, cuya representación permanente, para el Cuerpo Nacional de Policía y para la Guardia Civil recae en la Dirección Adjunta Operativa de cada uno de los cuerpos.

El procedimiento a seguir ante un incidente informático que, al menos a priori, ponga en entredicho la seguridad de una IC, se puede resumir en diez pasos que se explican a continuación.

1) El Operador crítico, con arreglo a los Manuales de Operación y Tipologías de Incidencias, ante la sospecha fundada (sin esperar a sufrir una acción hostil), inicia un procedimiento de incidencia.

2) Comunica ésta, mediante canal seguro, al CNPIC.

3) Expertos del Centro analizan la incidencia, determinando su nivel de criticidad.

37 Proporciona una respuesta ante incidentes de seguridad de este banco.

38 Proporciona servicios de gestión de incidentes para diferentes entidades del sector bancario.

39 Decano de los CERT nacionales. Fundado en 1994, proporciona servicios de seguridad informática a la Universidad Politécnica de Cataluña.

40 Empresa de seguridad que proporciona servicios de CERT.

4) Si la incidencia se cataloga de NO CRÍTICA, se activan mecanismos ordinarios de asesoramiento y apoyo.

5) Si por el contrario se cataloga como CRÍTICA, se comunica al CERT de referencia.

6) Se activan canales bidireccionales para intercambio fluido de información.

7) Igualmente se actúa cuando se considera que se puede prestar apoyo o asesoramiento para la resolución de la incidencia.

8) Con la información obtenida de incidentes, alertas de seguridad, se va alimentando la inteligencia básica de las FCSE[41].

9) Las FCSE comunican esta inteligencia obtenida al CNPIC, pudiendo también prestar apoyo a unidades especializadas de Policía Judicial.

10) El CNPIC, con toda la información y medios recopilados, auxilia al operador crítico para resolver la incidencia.

8.-CONCLUSIONES.

En cuanto a la primera hipótesis, se confirma que en España se han adoptado todas las disposiciones internacionales limitadas al ámbito de la UE, con respecto a la protección de las infraestructuras críticas. Se podría realizar un estudio más extenso, que tendría relación con el presente, sobre la distinta manera que han tenido otros países miembros de la UE de incluir en el ordenamiento interno las disposiciones europeas.

Se trata en todo caso de una regulación amplia y extensa impulsada en algo menos de una década. Sin embargo, se observa también que no se ha definido todavía una legislación específica y completa en materia de ciberseguridad. A este respecto, es de resaltar que la primera Estrategia Española de Ciberseguridad ha sido publicada en diciembre de 2013, y significará un antes y un después en todo lo relacionado con la ciberseguridad y la protección de las infraestructuras críticas.

41 En concreto, el grupo de Ciberterrorismo de la Guardia Civil, y el grupo de Ciberterrorismo del Cuerpo Nacional de Policía.

En cuanto al procedimiento para prevenir y para perseguir a los autores de los actos de ciberterrorismo, los ciberataques son una herramienta al alcance de cualquier grupo de individuos, ya sean terroristas, grupos radicales o hacktivistas con la intención de usarlas para producir grandes pérdidas económicas en empresas, organizaciones o naciones enteras.

Si a esta facilidad de acceso y uso de estas redes de ordenadores que, de forma coordinada, atacan a un determinado sistema, se le añade la vulnerabilidad de los sistemas SCADA, se obtiene un problema aún mayor y de difícil mitigación, pues un ataque con éxito dirigido hacia uno de ellos podría ocasionar inimaginables problemas no sólo en los servicios prestados por la infraestructura inicialmente atacada, sino que los sistemas SCADA acentúan la interconexión entre ellas de forma que la caída de la primera podría también afectar a las demás.

Cierto es que los antecedentes de ciberataques realizados contra empresas y organismos españoles, ya sean públicos o privados, no son de la entidad de los llevados a cabo en otras naciones. Sin embargo, resulta cuanto menos inquietante que aproximadamente el 90% de los organismos públicos españoles se conectan a la misma intranet, la red SARA. Ello hace de España un objetivo tan rentable como Estonia, pues un ataque llevado a cabo con éxito contra esta red podría llevar a una caída del Sistema, maximizada por el efecto en cascada anteriormente comentado, pudiendo llegar al cese total de la prestación de servicios esenciales tales como la luz, el agua o el sistema de transportes.

Para dar cumplimiento al mandato constitucional que encomienda a las FCS garantizar la seguridad ciudadana[42], así como a la LO 2/86 por la que se les encomienda la protección de edificios e instalaciones que así lo requieran[43], y a la Ley 11/2002, reguladora del CNI[44] por la que se le encomienda la coordinación de los organismos que intervengan en la protección de las TIC, se crean en su seno, el Centro Criptológico Nacional y el CCN-CERT. También se procede a la creación del CNPIC, erigiéndose en elementos indispensables para la prevención y la reacción ante incidentes cibernéticos en los sistemas críticos.

42Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el Ámbito de la Administración Electrónica.

43Art. 11. apartado C) de la LO 2/1986, de 13 de marzo de Fuerzas y Cuerpos de Seguridad, según el cual *"las Fuerzas y Cuerpos de Seguridad del Estado tienen como misión proteger el libre ejercicio de los derechos y libertades y garantizar la seguridad ciudadana mediante el desempeño de las siguientes funciones: (…) vigilar y proteger los edificios e instalaciones públicos que lo requieran"* Resulta obvio que esta vigilancia y protección de edificios e instalaciones se refiere a todos los tipos de seguridad posibles Es decir, comprende no sólo la seguridad física, sino también la seguridad lógica o ciberseguridad.

44Art. 4.e) de la Ley 11/2002, de 6 de mayo, reguladora del centro Nacional de Inteligencia, por el que se establece que, para el cumplimiento de sus objetivos, el Centro Nacional de Inteligencia se encargará, entre otras cosas, de: *"coordinar la acción de los diferentes organismos de la Administración que utilicen medios o procedimientos de cifra, garantizar la seguridad de las tecnologías de la información en ese ámbito, informar sobre la adquisición coordinada de material criptológico y formar al personal, propio o de otros servicios de la Administración, especialista en este campo para asegurar el adecuado cumplimiento de las misiones de Centro."*

A pesar de todo ello, España no dispone aún de una capacidad sólida que permita realizar una dirección y gestión eficaces y eficientes de la Ciberseguridad Nacional. Para definir y obtener dicha capacidad, se debe dotar a la Ley 8/2011, de Protección de Infraestructuras Críticas, de herramientas suficientes para obligar a su cumplimiento, pues se trata de una de las pocas leyes sin régimen sancionador. No existe, por tanto, un elemento coercitivo que obligue a su cumplimiento. Esta normas se crea bajo los principios y los ideales del común acuerdo y de la colaboración mutua entre organismos públicos y privados, pero el Estado dispondría, así, de elementos mediante los que obligar a cumplir las medidas que la citada Ley encomienda.

Como elementos críticos para mejorar la seguridad del ciberespacio en España, ayudados por la Estrategia de ciberseguridad Nacional, se pueden citar:

- Existencia de duplicidades y sistemas que pueden llegar a depender de diversos organismos, por lo que se debe establecer un elemento coordinador en ciberseguridad que integre a todos los actores y permita al gobierno conocer la situación nacional en este campo.

- Insuficiencia de recursos humanos, técnicos y económicos, en los diferentes organismos con competencias en ciberseguridad. Esto provoca un escaso despliegue de mecanismos de defensa en las Administraciones públicas, por lo que la plantilla dedicada en la ciberseguridad se debe potenciar, llegando a mejorar la gestión de las redes e infraestructuras públicas comunes.

- Existe una reducida comunicación entre organismos del sector público y privado. Hay una ausencia de procedimientos y sistemas que permitan un intercambio seguro de información útil y oportuna para implicar al sector privado, de un conjunto integrado de medidas de aplicación a los sectores afectados en materia de ciberseguridad que permita la aplicación de la normativa de Protección de Infraestructuras Criticas.

- Escasez de recursos destinados a las capacidades de prevención y respuesta a lasactividades del terrorismo y la delincuencia en el ciberespacio. Esto es un problema de concienciación, que compete sobre todo a los máximos responsables de los Ministerios de Interior, Defensa y Presidencia.

BIBLIOGRAFÍA

PUBLICACIONES:

CLARKE, R.A. y KNAKE, R.K. Guerra en la Red. Los nuevos campos de batalla. 2011

COLLIN, B.C. The Future of Cyberterrorism: Where the Physical and Virtual Worlds Converge. 1998

CRESPÍ, A. ¿Qué es la Sociedad de la Información? Cátedra Telefónica-UPC. Análisis de la Evolución y Tendencias Futuras de la Sociedad de la Información. 2010.

HERNÁNDEZ GARCÍA, L. F. Internet y las Nuevas Tecnologías frente a la amenaza del Terrorismo. Seminario Duque de Ahumada. UNED. 2012.

POLLIT, N.M. Proceedings of the 20th National Information Systems Security Conference. 1995.

TORRES SORIANO, M.R. El eco del terror. Ideología y propaganda en el terrorismo yihadista. 2009.

VELASCO NÚÑEZ, E. Delitos cometidos a través de Internet. Cuestiones procesales. 2010.

RECURSOS DIDÁCTICOS:

-Material de los cursos realizados en la Escuela de Formación de Telefónica:

- Seguridad en Redes. 2010.
- Comunicaciones móviles GSM-GPRS-EDGE-UMTS-HSPA-LTE. 2013.
- Comunicaciones de banda ancha en redes de telecomunicaciones cableadas. 2009
- Comunicaciones satelitales. 2011.

-Material del curso realizado en el Ericsson Education Iberia Center sobre las comunicaciones móviles, en conmutación de paquetes y conmutación de circuitos. 2008.

-IX Curso Gestión STIC-Módulo ENS-INAP: 2014. ww.ccn.cni.es

RECURSOS WEB:

http://www.cisco.com/en/US/solutions/ns341/ns525/ns537/ns705/ns1120/CCWTR-Chapter1-Report.pdf. Cisco Connected World Technology Report. Junio 2014.

http://www.cnpic-es.es. Centro nacional de protección de Infraestructuras críticas. Junio 2014.

http://europa.eu/legislation_summaries. Disposiciones de la Unión Europea. Junio 2014.

http://www.ccn.cni.es. Centro Criptológico Nacional. Procedimientos STIC. Septiembre 2014.

LEGISLACIÓN INTERNACIONAL:

- Libro verde sobre el programa europeo de protección de infraestructuras críticas (PEPIC), de 17 de noviembre de 2005.
- Directiva UE 2008/114/CE, de 8 de diciembre, sobre identificación y designación de Infraestructuras Críticas Europeas.

LEGISLACIÓN NACIONAL:

- Constitución española de 1978.
- Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal.
- Ley Orgánica 2/1986, de 14 de marzo, de Fuerzas y Cuerpos de Seguridad.
- Plan Nacional de Protección de Infraestructuras Críticas (PNIC), de 2 de mayo de 2007.
- Ley 8/2011, de 28 de abril, sobre protección de infraestructuras críticas.
- Real Decreto 704/2011, de 20 de mayo, sobre protección de infraestructuras críticas.
- Real Decreto 3/2012, de 8 de enero, que desarrolla el Esquema Nacional de Seguridad.
- Estrategia Española de Seguridad de 2011.
- Estrategia Española de Ciberseguridad de 2013
- Acuerdo Consejo de Ministros sobre Protección de Infraestructuras Críticas
- Estrategia de Seguridad Marítima Nacional
- Ley 5/2014, de 4 de abril, de Seguridad Privada
- Ley 2/1985 Protección Civil.
- R.D. 407/1992 Norma Básica de Protección Civil.
- R.D. 393/2007 Norma Básica de Autoprotección de Centros y Establecimientos
- R.D. 1468/2008 que modifica R.D. 393/2007
- R.D. 399/2007 Protocolo Intervención Unidad Militar Emergencia.