Capítulo tercero

Análisis de las ciberamenazas

Aníbal Villalba Fernández
Doctor en Ciencias Políticas y Sociología, UNED
Asesor del Presidente del Consejo Nacional de Ciberseguridad

Juan Manuel Corchado Rodríguez
Doctor en Informática, Universidad de Salamanca
Doctor en Inteligencia Artificial, University of the West of Scotland
Catedrático Ciencias de la Computación e Inteligencia Artificial, Universidad de Salamanca
Vicerrector de Investigación y Transferencia, Universidad de Salamanca
Director del Parque Científico de la Universidad de Salamanca
Member of the Advisory Group on Online Terrorist Propaganda of the European Counter Terrorism Centre (ECTC)

Resumen

El ciberespacio ha introducido una nueva dimensión en las sociedades, favoreciendo el progreso gracias a las nuevas tecnologías y al uso extensivo de internet. No obstante, esta situación presenta nuevos retos a los que no se sustraen los diferentes actores políticos, principalmente los Estados. Entre estos desafíos se encuentran el ciberespionaje; las acciones de grupos terroristas y de corte yihadista; la ciberdelincuencia; y la protección y recuperación de los sistemas de infraestructuras críticas, entre otros.

España se ha dotado de un Consejo Nacional de Ciberseguridad, que preside el secretario de Estado director del Centro Nacional de Inteligencia; en cuya persona recae además la Autoridad Nacional para la protección de la información clasificada —que dispone de la Oficina Nacional de Seguridad—; la Autoridad Nacional de Inteligencia y Contrainteligencia; y la dirección del Centro Criptológico Nacional, que cuenta con el CERT Nacional Gubernamental CCN-CERT, con responsabilidad en la protección ante ciberataques sobre sistemas clasificados de las Administraciones públicas; y de empresas y organizaciones de interés estratégico.

Palabras clave

inteligencia, ciberespacio, ciberamenazas, riesgos, amenazas, ciberseguridad, ciberataques, CERT.

Abstract

Cyberspace has introduced a new dimension in societies, favoring progress thanks to new technologies and the extensive use of the Internet. However, this situation presents new challenges to which different political actors, especially States, do not escape. Among these challenges are cyber espionaje, the actions of terrorist and jihadist groups, cybercrime, and the protection and recovery of critical infrastructure, among others.

Spain has been endowed with a National Cybersecurity Council, chaired by the Secretary of State Director of the National Intelligence Center; in whose person also falls the National Authority for the protection of classified information —which has the National Security Office—; the National Intelligence and Counterintelligence Authority; and the direction of the National Cryptological Center, which has the National Government CERT CCN-CERT, with responsibility in the protection against cyber attacks on classified systems, Public Administrations; and of companies and organizations of strategic interest.

Keywords

intelligence, cyberspace, cyber threats, risks, threats, cybersecurity, cyber attacks, CERT.

Introducción

El ciberespacio ha introducido una nueva dimensión en las sociedades, y su uso se ha incorporado a las mismas de modo cotidiano y generalizado. Gracias a las nuevas tecnologías y al uso extensivo de internet, se están desarrollando proyectos que abarcan las áreas más diversas de las actividades humanas. Los adelantos en las comunicaciones y el abaratamiento de los costes están generando una red en la que pocos elementos escapan a estar conectados, incluso los objetos de uso cotidiano, en lo que se ha venido a llamar el Internet de las Cosas.

Los aspectos positivos de la utilización del ciberespacio son numerosos. La generación de nuevas capacidades en campos como las comunicaciones, la investigación científica, los procesos industriales o la gestión del conocimiento son evidentes. Además, el acceso de modo casi generalizado a las redes ha constituido un escenario rico en oportunidades para una gran parte de la población. Esta revolución tecnológica y su impacto social están conformando un escenario que impregna la vida de las sociedades. No obstante, esta situación presenta nuevos retos a los que no se sustraen los diferentes actores políticos, principalmente los Estados. Entre estos desafíos se encuentran la protección y recuperación de los sistemas de infraestructuras críticas ante agresiones que utilizan el ciberespacio como entorno y vehículo para interferir en las actividades de los ciudadanos y de las instituciones.

De esta forma, hoy en día los Estados deben hacer frente a ataques contra la seguridad de los sistemas de las Tecnologías de la Información y las Comunicaciones (TIC) de gobiernos, administraciones públicas y empresas con alto valor estratégico. Esta situación ha conformado un nuevo escenario, que precisa atención de los diferentes actores políticos para adaptarse adecuadamente.

Los riesgos y amenazas derivados de la utilización del ciberespacio han generado además discusiones relacionadas con la soberanía. La nueva dimensión que aporta el ciberespacio ha desdibujado las fronteras tradicionales, abriendo un debate acerca de las responsabilidades de los Estados. Aspectos como la deslocalización de los ciberataques y la dificultad de atribución de responsabilidades, dibujan un nuevo escenario relacionado con su interacción y con los intereses nacionales.

España no ha permanecido inmune a las agresiones que utilizan el ciberespacio para atentar contra los más variados aspectos de la seguridad, llegando a verse comprometidos servicios críticos y otros aspectos que afectan a la seguridad nacional.

En este escenario, se han desarrollado diferentes medidas de carácter político, de planeamiento estratégico de la ciberseguridad y de creación de estructuras organizativas y de carácter técnico, con el objetivo de hacer frente a los desafíos que el uso del ciberespacio presenta para la seguridad nacional.

En el ámbito del planeamiento de la seguridad nacional en España, cabe destacar la aprobación por el Consejo de Ministros, el 24 de junio de 2011, de la primera estrategia de seguridad nacional en España: «Estrategia Española de Seguridad. Una responsabilidad de todos», donde por vez primera se incorpora la ciberseguridad a los niveles superiores de planeamiento estratégico nacional.

Esta estrategia se actualizó con la aprobación por el Consejo de Ministros, el 31 de mayo de 2013, de la «Estrategia de Seguridad Nacional. Un proyecto compartido». Como señala la referencia del Consejo de Ministros: «la Estrategia de 2013 concibe la Seguridad Nacional de una forma amplia y global, por lo que incluye muy distintos ámbitos de actuación. Tradicionalmente, el concepto de Seguridad Nacional se ceñía a la defensa y la seguridad pública, pero hoy se extiende a nuevos actores y amenazas y, por ello, la Seguridad Nacional hace frente a nuevos riesgos como las ciberamenazas».

En este sentido, la Estrategia de Seguridad Nacional de 2013 contempla hasta doce riesgos para nuestra seguridad: conflictos armados, terrorismo, ciberamenazas, crimen organizado, inestabilidad económica y financiera, vulnerabilidad energética, flujos migratorios irregulares, armas de destrucción masiva, espionaje, emergencias y catástrofes naturales, vulnerabilidad del espacio marítimo y vulnerabilidad de las infraestructuras críticas y servicios esenciales.

Es interesante señalar que, aunque las ciberamenazas se contemplan como un riesgo en sí mismas, se encuentran presentes en prácticamente todo el resto de riesgos identificados, en mayor o menor medida, a excepción de los flujos migratorios irregulares y las emergencias y catástrofes naturales. Este carácter transversal de las ciberamenazas ha llevado al desarrollo de estrategias específicas en ámbitos que se consideran prioritarios. Además de la Estrategia de Ciberseguridad Nacional, es de destacar el componente de ciberseguridad de que se dotan las Estrategias Nacionales de Seguridad Marítima y de Seguridad Energética.

El Consejo de Seguridad Nacional ha creado también diferentes Comités especializados, ligados al desarrollo de las estrategias, entre ellos, el Consejo Nacional de Ciberseguridad. El Consejo Nacional de Ciberseguridad (CNCS) se constituyó formalmente el 24 de febrero de 2014, según decisión del Consejo de Seguridad Nacional de 5 de diciembre de 2013, que creó este comité especializado en ciberseguridad en la estela de la aprobación de la Estrategia Nacional de Ciberseguridad en esa misma fecha. El CNCS se encuentra compuesto por representantes de diferentes ministerios que tienen competencia en ciberseguridad en España, y su función principal consiste en desarrollar las líneas de acción y los cometidos especificados en la Estrategia Nacional de Ciberseguridad.

En este tiempo, el CNCS ha elaborado un Plan Nacional de Ciberseguridad, que desarrolla la Estrategia Nacional de Ciberseguridad, el cual fue aproba-

do por el Consejo de Seguridad Nacional el 14 de octubre de 2014. El Plan Nacional de Ciberseguridad, a su vez, establecía la necesidad de incorporar de modo integral los elementos relacionados con la ciberseguridad que son competencia, en diferentes ámbitos, de distintos organismos. De esta forma, el 14 de julio de 2015, el Consejo Nacional de Ciberseguridad aprobó los nueve Planes Derivados del Plan Nacional de Ciberseguridad,

El secretario de Estado director del Centro Nacional de Inteligencia (SED CNI) es, desde su creación, el presidente del Consejo Nacional de Ciberseguridad. Además, la Autoridad Nacional para la protección de la información clasificada recae en la persona del SED CNI, que es, asimismo, el director del Centro Criptológico Nacional (CCN). El SED CNI también es la Autoridad Nacional de Inteligencia y Contrainteligencia.

El CNI, como Servicio de Inteligencia de España, proporciona al Gobierno elementos de juicio para facilitar su toma de decisiones estratégicas, lo que incluye el ámbito de la ciberseguridad. Para llevar a cabo su misión utiliza los procesos, procedimientos y herramientas que distinguen a un Servicio de Inteligencia, de carácter técnico y humano, dentro y fuera del territorio nacional; así como el intercambio de información y análisis de inteligencia con otros Servicios de Inteligencia extranjeros. En el caso de las ciberamenazas, además de la obtención y análisis propios, cobra un especial valor la relación con otros Servicios, al tener las ciberamenazas un carácter global.

La Autoridad Nacional para la protección de la información clasificada, dispone de un órgano de trabajo, la Oficina Nacional de Seguridad (ONS). La ONS tiene por misión fundamental la de velar por el cumplimiento de la normativa relativa a la protección de la información clasificada tanto nacional como aquella que es entregada a la Administración o a las empresas en virtud de Tratados o Acuerdos internacionales suscritos por España. En el ámbito de la ciberseguridad, la ONS colabora para la protección de los sistemas y de la propia información clasificada ante las ciberamenazas.

El Centro Criptológico Nacional (CCN) es el organismo responsable de coordinar la acción de los diferentes organismos de la Administración para que utilicen medios o procedimientos de cifra, garantizar la seguridad de las Tecnologías de la Información en ese ámbito, informar sobre la adquisición coordinada del material criptológico y formar al personal de la Administración especialista en este campo.

En este escenario, en relación con las ciberamenazas, cobra un valor especial la labor del CCN-CERT, que constituye la capacidad de respuesta a incidentes de Seguridad de la Información del Centro Criptológico Nacional, CCN. Este servicio se creó en el año 2006 como CERT Gubernamental Nacional español y sus funciones quedan recogidas en la Ley 11/2002 reguladora del Centro Nacional de Inteligencia, el Real Decreto 421/2004 de regulación del CCN y en el Real Decreto 3/2010, de 8 de enero, regulador del Esquema Nacional de Seguridad, modificado por el Real Decreto 951/2015 de 23 de octubre.

De acuerdo a esta legislación, 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 para que coopere y ayude a responder de forma rápida y eficiente a los ciberataques y a afrontar de forma activa las ciberamenazas.

EL CCN-CERT viene desarrollando, desde el año 2008, un Sistema de Alerta Temprana (SAT) que busca actuar antes de que se produzca un incidente o, por lo menos, detectarlo en un primer momento para reducir su impacto y alcance. Este sistema para la detección rápida de incidentes y anomalías dentro de la Administración y de las empresas de interés estratégico, se enmarca dentro de las acciones preventivas, correctivas y de contención realizadas por el CERT Gubernamental Nacional. El SAT cuenta con dos vertientes con un denominador común: la detección temprana de intrusiones. En ambos casos existe un portal de informes al que los responsables de seguridad autorizados pueden acceder para la consulta en tiempo real de eventos de seguridad y para la generación de informes a medida[1].

El CCN-CERT da servicio también a la red SARA (Sistema de Aplicaciones y Redes para las Administraciones) que es un conjunto de infraestructuras de comunicaciones y servicios básicos que conecta las redes de las Administraciones públicas españolas e instituciones europeas facilitando el intercambio de información y el acceso a los servicios.

La información que se facilita en este capítulo, cuando no exista una referencia específica, proviene de la obtención y análisis propios del CNI, ONS, y –especialmente– del CCN-CERT.

Las ciberamenazas en el contexto de los riesgos globales

Es interesante situar los ciberataques en perspectiva con otros riesgos globales. El Foro Económico Mundial ha publicado el estudio «Riesgos Globales 2016»[2] en el que ofrece un análisis de la percepción del impacto y de la probabilidad de los riesgos globales.

En su 11.ª edición, el Informe Riesgos Globales 2016 destaca las formas en las que los riesgos globales podrían evolucionar e interactuar en la próxima década. El año 2016 marca un claro punto de quiebre con respecto a resultados anteriores, ya que los riesgos sobre los que el informe ha estado alertando durante la última década están empezando a manifestarse de

1 Véase la información facilitada por el CCN-CERT en https://www.ccn-cert.cni.es/gestion-de-incidentes/sistema-de-alerta-temprana-sat.html consulta: 31 de octubre de 2015.

2 World Economic Forum: *The Global Risks Report 2016; 11th Edition*. http://www3.weforum.org/docs/Media/TheGlobalRisksReport2016.pdf

formas nuevas y en ocasiones inesperadas y a afectar a las personas, las instituciones y las economías.

Señala el informe que los delitos cibernéticos cuestan a la economía mundial aproximadamente 445.000 millones de dólares, lo que supera los ingresos de Chile. En este contexto, el informe hace un llamamiento a la creación de resiliencia (el «imperativo de resiliencia») e identifica ejemplos prácticos sobre cómo podría lograrse.

Entre los riesgos globales que siguen siendo importantes debido a su impacto combinado y probabilidad se encuentran algunos riesgos económicos, como por ejemplo las crisis fiscales en economías clave y un alto desempleo estructural o subempleo. Estos se encuentran complementados por los ciberataques y una profunda inestabilidad social. El informe también analiza los riesgos y tendencias globales emergentes, señalando como el cambio climático, las desigualdades económicas y el aumento de la ciberdependencia.

En este estudio del Foro Económico Mundial se refleja la probabilidad y el impacto de los riesgos individuales. Los ciberataques se encuentran en cuarto lugar en la combinación entre su probabilidad e índice de impacto. Los riesgos asociados a los ciberataques son superados solo, en relación a la combinación de ambos parámetros, por la negativa adaptación al cambio climático, las crisis relacionadas con el agua y las migraciones involuntarias

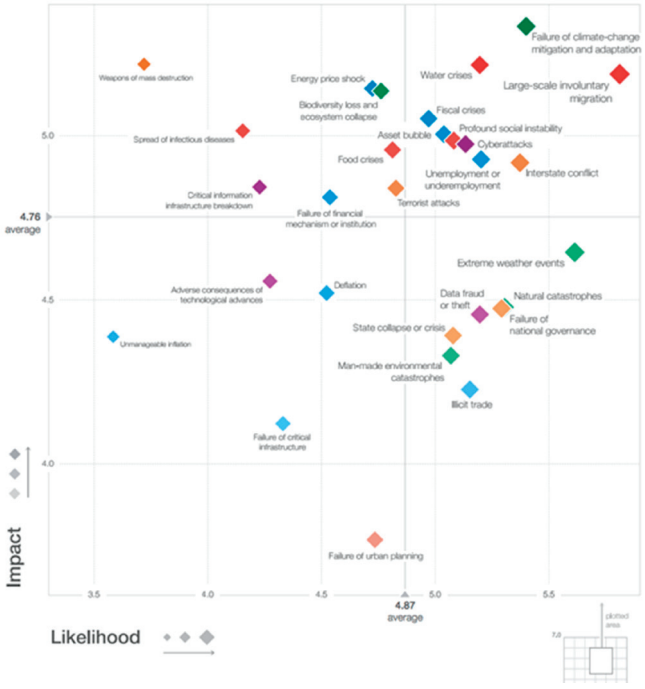

Figura 3.1. Mapa de riesgos globales 2016.
Fuente: World Economic Forum: The Global Risks Report 2016, p 3.

a gran escala. En relación con el anterior informe de 2015, los ciberataques han superado a dos riesgos que se encontraban por delante: el desempleo y los conflictos entre Estados. De este paisaje de riesgos globales se desprende la percepción de la alta probabilidad y el elevado impacto de los ciberataques en comparación con el resto de riesgos globales.

El mencionado *Informe de Riesgos Globales* 2016 ofrece también un mapa de interconexión de los riesgos, donde se puede observar que continúa, como en la edición anterior, la conexión directa de los ciberataques con otros riesgos tecnológicos como la ruptura de la infraestructura de información crítica, el mal uso de las tecnologías, el fraude y el robo de datos. También existe un enlace directo con un riesgo que en el informe se asocia a la economía, el fallo en las infraestructuras críticas. El resto de conexiones directas con otros riesgos caen en el ámbito de los riesgos denominados geopolíticos, ataques terroristas, fallo de la gobernanza nacional y conflictos entre Estados.

En el caso de los riesgos asociados al uso del ciberespacio, se observa en el gráfico que las conexiones de segundo nivel alcanzan a otros riesgos que tienen unos niveles elevados tanto de probabilidad como de peligrosidad, y que se incorporan a áreas económicas, sociales, ambientales y de riesgos geopolíticos.

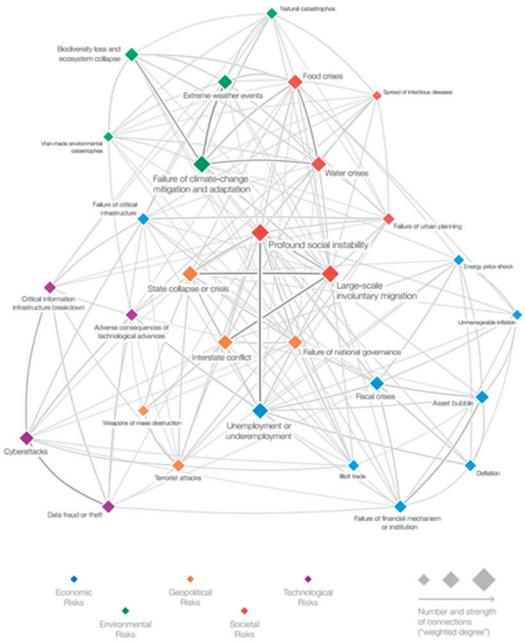

Figura 3.2. Mapa de interconexiones de riesgos globales 2016.Fuente: World Economic Forum: The Global Risks Report 2016, p 4.

Elementos esenciales en el análisis de las amenazas

La metodología empleada por el CCN-CERT, en el informe anual *Ciberamenazas 2015. Tendencias 2016*, señala como elementos esenciales a tener en cuenta para desarrollar un análisis coherente de las ciberamenazas los siguientes:

1. **Intereses.** Aquello que puede verse afectado por ciberataques contra las dimensiones de la seguridad: confidencialidad, disponibilidad, integridad, trazabilidad y autenticidad de la información tratada o los servicios prestados. ¿Qué intereses españoles, de sus socios o aliados, están viéndose afectados negativamente y en qué medida, por las restricciones de la disponibilidad de las tecnologías de la información y la comunicación (TIC), la pérdida de la confidencialidad de la información tratada o la agresión a la integridad de la información?
2. **Amenazas**. Agentes de la amenaza y objetivos: determinación de los eventos, circunstancias o actividades que, llevadas a cabo por los diferentes atacantes, pueden afectar a los intereses nacionales (o internacionales) considerados. ¿Qué tipo de actividades podrían llevar a cabo los atacantes o qué situaciones podrían darse, que pudieran afectar al normal desenvolvimiento de las TIC, en cualquier entorno? Esta cuestión incluye el examen de las herramientas usadas para todo ello, así como las tendencias observadas.
3. **Resiliencia.** Determinación de en qué medida los sistemas de información han sabido afrontar los ciberataques, así como las medidas que se han adoptado o están siendo adoptadas para mitigarlos. Obviamente,

Figura 3.3. Diagrama de elementos para análisis de ciberamenazas.
Fuente: CCN-CERT. Ciberamenazas 2015. Tendencias 2016, p. 14.

la resiliencia consiste tanto en la ausencia de vulnerabilidades, como en la adopción de medidas que incrementen la fortaleza de los sistemas frente a agresiones.

En el análisis de las ciberamenazas se aplican a estos elementos un esquema en el que se incluyen dos nuevas metacaracterísticas: la sociopolítica, que vincula al adversario con su víctima y la tecnológica, que vincula la infraestructura con la capacidad.

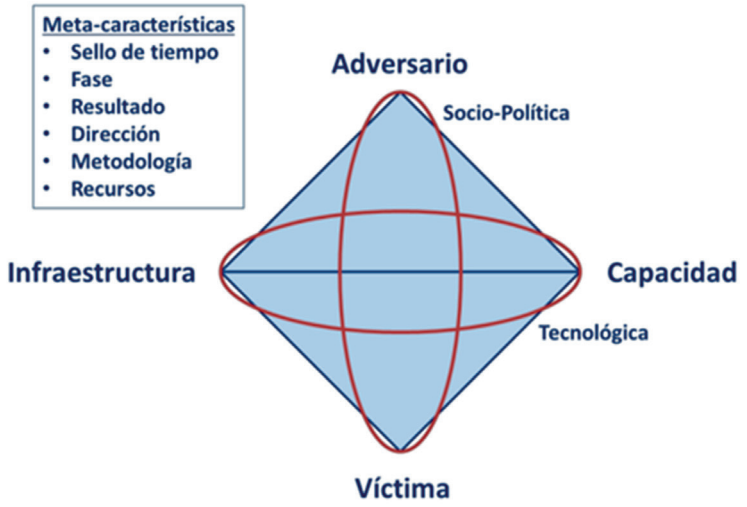

Figura 3.4. Metacaracterísticas aplicadas a los elementos en las ciberamenazas. Fuente: CCN-CERT. Guía CCN-STIC 425 Ciclo de Inteligencia y Análisis de Intrusiones.

Evolución tecnológica y ciberseguridad

Probablemente nos encontremos lejos del denominado punto de saturación de las TIC. Es de esperar todavía mayores tasas de crecimiento gracias a la miniaturización de los elementos tecnológicos y el desarrollo de redes y sistemas inteligentes.

La presencia de la tecnología en todo tipo de dispositivos (automóviles, equipos médicos, etcétera) los hacen igualmente vulnerables, provocando que la superficie de ataque esté en permanente crecimiento, y esta es una situación que, además, no tiene vuelta atrás: cada vez hay menos medios analógicos sustitutivos de los medios digitales.

La industria sabe muy bien que aquellos proveedores que descuidan innovación y competitividad corren el riesgo de ser expulsados del mercado. Esta realidad se traduce en un incremento de la presión para situarse por encima de la competencia, lo que no siempre permite conciliar adecuadamente las necesidades de seguridad de los usuarios finales con los intereses económicos.

La tendencia actual hacia la masiva utilización de los sistemas dirigidos por *software* (*software-driven systems*) escenifica el conflicto entre funcionalidad y seguridad. El término viene describiendo la tendencia hacia arquitecturas en las que los sistemas, redes, almacenamiento, etcétera no están estáticamente definidos y constreñidos por el *hardware* utilizado sino que se pueden configurar de forma dinámica mediante el *software* adecuado. Los beneficios de esta evolución son claros: los recursos se pueden mover rápidamente y a menor coste allí donde se necesitan. Sin embargo, esta tendencia puede entrar en clara confrontación con un concepto de seguridad sustentado en la separación de los procesos y sistemas clave. En un entorno dinámico *software-driven*, esta separación no puede efectuarse con la misma profundidad técnica que usando arquitecturas tradicionales, lo que hace imprescindible el uso de plataformas específicas que faciliten la separación virtual de entornos de manera segura.

De otra parte, la tendencia en el uso de los dispositivos móviles sigue en aumento. En el sector privado han venido comercializándose nuevos tipos de dispositivos que se van incorporando a la vida cotidiana y se suman al masivo despliegue de teléfonos inteligentes y *tablets*. Estos últimos, que ya forman parte del equipamiento estándar de los profesionales, se han incorporado a procesos corporativos tratando en ocasiones información sensible, lo que genera especiales medidas de seguridad para proteger aquella información corporativa especialmente valiosa.

En numerosas ocasiones la conciliación entre la utilización de productos modernos y seguros y la compatibilidad que deben poseer se torna una tarea difícil. Frecuentemente, la incorporación de medidas de seguridad a tecnologías tradicionales es un proceso lento que no permite siempre el desmantelamiento oportuno de aquella tecnología. Un ejemplo de esto es el protocolo TLS/SSL14, muy utilizado en internet para el cifrado del tráfico de datos. Muchos servidores *online* están configurados para permitir el uso de métodos criptográficos inseguros, al objeto de garantizar el acceso a una porción significativa de usuarios que pueden seguir usando navegadores con versiones sin actualizar. Otro ejemplo significativo es el uso de sistemas operativos para los que el fabricante ya no proporciona actualizaciones de seguridad.

De otra parte, se ha generado una cierta pérdida de confianza en los servicios electrónicos entre los usuarios, debido en buena parte a constantes y alarmantes informaciones sobre brechas de seguridad. Las razones más importantes esgrimidas por los usuarios han sido esencialmente las inadecuadas garantías de privacidad, lo que ha llevado a que determinados proveedores de servicios de mensajería hayan empezado a ofrecer a sus usuarios un cifrado extremo-a-extremo de forma que ni siquiera tales proveedores puedan tener acceso a los mensajes intercambiados.

La utilización de las TIC en nuevas áreas de aplicación y las vulnerabilidades de los sistemas utilizados, el denominado Internet de las Cosas, podría

tener un impacto importante en el normal desenvolvimiento de la vida cotidiana. Un buen ejemplo lo constituye el ataque del 21 de octubre de 2016, que dificultó el acceso a una serie de servicios en la red por causa de un importante ataque de denegación de servicio distribuido (*DDoS*) vertido contra la empresa de servicios de DNS Dyn, y que afectó a actores como Twitter, Spotify, Reddit, SoundCloud, Airbnb o Github, entre muchos otros. Este *DDoS* concentró un gran conjunto de peticiones de acceso a Dyn con el fin de colapsar el servicio. Para ello se utilizaron múltiples dispositivos –cámaras IP y otros– infectados con *malware* que permitía al atacante tener control del sistema, creando una red zombi o *botnet* (red de robots). Estos dispositivos suelen tener unas claves de seguridad generales y *el software* o el *firmware* no suele estar actualizado, lo que facilita el acceso a intrusos y su control de forma remota.

En lo relativo a los medios de transporte —automóviles, aeronaves y otros— se está incorporando a los mismos un amplio catálogo de componentes TIC, potencialmente sujetos a fallos, no es de extrañar, por tanto, que las tendencias en la instalación de tales tipos de dispositivos pase actualmente por separar adecuadamente las redes que conectan los sistemas de estos vehículos, que afectan a la seguridad, respecto a aquellos otros no directamente relacionados con la seguridad. No obstante, a pesar del establecimiento de redes separadas, no es descartable la explotación de vulnerabilidades. Obviamente, el desarrollo de los coches autónomos incrementará los problemas de seguridad en el futuro.

En el sector sanitario, la presencia de sistemas TIC vulnerables puede tener graves consecuencias, ya que cada vez son más los dispositivos médicos que pueden administrarse de forma remota, a través de conexiones *WiFi* o *Bluetooth*.

Como consecuencia de la penetración de las TIC en todos los sectores de la vida social, política, administrativa o económica de un país, la existencia de alternativas analógicas está desapareciendo de una manera rápida. Esta realidad hace a los sistemas TIC especialmente importantes, sistemas que, en muchos casos, son enormemente más complejos que sus antecesores analógicos y que suelen estar conectados a internet, lo que aumenta su riesgo.

Otro aspecto muy significativo es la dependencia tecnológica de las Infraestructuras Críticas respecto a la utilización de los medios electrónicos y la interconexión de sistemas. La prestación de sus servicios depende cada vez más de un correcto funcionamiento de las TIC. Un fallo o disfunción de cualquiera de sus componentes podría dar lugar, bajo determinadas circunstancias, a limitar o impedir tal prestación. Por otro lado, las interdependencias entre sectores o industrias individuales aumentan aún más los riesgos. Los fallos en un sector pueden propiciar fallos en otros sectores provocando un efecto dominó.

Los puntos siguientes tratan de esquematizar el nivel de amenazas específico contra las Infraestructuras Críticas.

1. En general puede afirmarse que no existe diferencia entre el nivel de amenaza que soportan las Infraestructuras Críticas u otro tipo de organizaciones, salvo en lo relativo al cibersabotaje o el terrorismo, que ofrecen características distintas toda vez que el objetivo de los atacantes sea provocar el mayor daño social posible.
2. La amenaza de la ciberdelincuencia es particularmente relevante para el sector financiero y el de seguros. Los delitos perpetrados van desde el robo de identidades a los ciberataques a las infraestructuras técnicas de las instituciones financieras pasando por la mera extorsión.
3. Es muy frecuente que los ataques realizados por grupos *hacktivistas* –grupos de *hackers* que utilizan el activismo político o social– se desarrollen contra empresas de medios de comunicación (desfiguraciones o emplazamiento de informaciones incorrectas en los sitios web de los medios secuestrados), energía y sector financiero.
4. El cibersabotaje es una amenaza permanente. Desde Stuxnet, se ha sabido que el sabotaje de las infraestructuras por medio de ciberataques no es solo posible sino real. El ataque contra el grupo audiovisual francés *TV5Monde* o las interrupciones de fluido eléctrico en Ucrania son ejemplos de este tipo de ataques.
5. La posibilidad de ciberataques con origen en otros Estados representa una amenaza real para la economía de cualquier país desarrollado.
6. No solo los ataques dirigidos representan una amenaza para las Infraestructuras Críticas. También los ataques no dirigidos con código dañino pueden interrumpir la operación de tales infraestructuras. Por ejemplo, los problemas detectados de *ransomware* en instituciones sanitarias.
7. El crecimiento de las redes que gestionan Infraestructuras Críticas supone el crecimiento correlativo de posibles vulnerabilidades.
8. Es muy difícil señalar qué sector en concreto está afectado por tal o cual amenaza. Un ataque dirigido contra un sector determinado también puede afectar inadvertidamente a otro sector, por ejemplo si ambos utilizaran los mismos protocolos o el mismo *software*.

Como ejemplo del impacto de un ciberataque contra una infraestructura crítica, el director general del Organismo Internacional de Energía Atómica (OIEA), Yukiya Amano, ha desvelado en octubre de 2016 que una central nuclear fue el objetivo de un ciberataque hace dos o tres años y que existe una seria amenaza de más ciberataques contra estas instalaciones nucleares. Señalaba Amano que «este tema de ataques cibernéticos a instalaciones o actividades relacionadas con el uso de la energía nuclear debe tomarse muy en serio. Nunca sabemos si lo sabemos todo o si es la punta del iceberg». Amano se negó a dar detalles de cualquiera de los incidentes, pero dijo que el ataque cibernético había causado «alguna interrupción» en la planta,

aunque no resultó ser muy grave ya que la planta no tuvo que cerrar sus operaciones[3].

Ciberamenazas, agentes y objetivos

El cuadro que muestra la siguiente figura muestra la relación entre los orígenes de las ciberamenazas, sus objetivos y el nivel de peligrosidad.

	Objetivos		
Origen de la amenaza	**Sector Público**	**Sector Privado**	**Ciudadanos**
Estados	Ciberespionaje político	Ciberespionaje económico	Ciberespionaje instrumental
	Cibercapacidades ofensivas	Cibercapacidades ofensivas	
Ciberdelincuentes	Sustracción, publicación o venta de información	Sustracción, publicación o venta de información	Sustracción, publicación o venta de información
	Manipulación de información	Manipulación de información	Manipulación de información
	Interrupción de sistemas	Interrupción de sistemas	Interrupción de sistemas
	Toma de control de sistemas	Toma de control de sistemas	Toma de control de sistemas
Grupos terroristas	Interrupción de Sistemas / Toma de control	Interrupción de Sistemas / Toma de control	
Grupos yihadistas	Interrupción de Sistemas / Toma de control	Interrupción de Sistemas / Toma de control	
	Desfiguraciones	Desfiguraciones	
			Propaganda y reclutamiento
Cibervándalos y script kiddies	Sustracción de información	Sustracción de información	Sustracción de información
	Interrupción de sistemas	Interrupción de sistemas	
Hacktivistas	Sustracción y publicación de la información sustraída	Sustracción y publicación de la información sustraída	
	Desfiguraciones	Desfiguraciones	
	Interrupción de sistemas	Interrupción de sistemas	
	Toma de control de sistemas	Toma de control de sistemas	

[3] *Reuters*, *IAEA chief: Nuclear power plant was disrupted by cyber attack*, 10 de octubre de 2016. http://www.reuters.com/article/us-nuclear-cyber-idUSKCN12A1OC

Actores internos	Sustracción, publicación o venta de información	Sustracción, publicación o venta de información	
	Interrupción de sistemas	Interrupción de sistemas	
Ciberinvestigadores	Recepción y publicación de información	Recepción y publicación de información	
Organizaciones privadas		Sustracción de información (espionaje industrial)	Uso/abuso o reventa de información de clientes

Nivel de peligrosidad:

Bajo:	**Medio:**	**Alto:**
• No se han observado nuevas amenazas o tendencias, o • Se dispone de medidas suficientes para neutralizar la amenaza, o • No ha habido incidentes especialmente significativos en el periodo analizado.	• Se han observado nuevas amenazas o tendencias, o • Se dispone de medidas (parciales) para neutralizar la amenaza, o • Los incidentes detectados no han sido especialmente significativos.	• Las amenazas o su tendencia se ha incrementado significativamente. • Las medidas adoptadas tienen un efecto muy limitado, por lo que la amenaza permanece. • Los incidentes detectados han sido especialmente significativos.

Figuras 3.5.1. y 3.5.2. Matriz de ciberamenazas. Fuente: Centro Nacional de Ciberseguridad de los Países Bajos: Cyber Security Assessment Netherlands 2016, 24 de octubre de 2016, p. 12. Con elaboración propia.

Los agentes de las ciberamenazas

Actores estatales

La posición de los Estados, como elementos activos o pasivos de los ciberataques, no es irrelevante para valorar el impacto de la ciberseguridad mundial. Sus actitudes, sus compromisos y sus respuestas pueden adoptar formas diferentes.

Todos los Estados occidentales, en mayor o menor medida, son objeto de ciberataques con origen en otros Estados, interesados en obtener información de relevancia económica, geoestratégica o militar.

Los ciberataques constituyen uno de los marcos de acción preferidos por su bajo coste si se compara con los importantísimos beneficios que pueden obtenerse, lo limitado de los riesgos asumidos y la dificultad de determinar sus autores. No se puede pasar por alto que este tipo de acciones permite que la infraestructura tecnológica de un tercer país pueda servir de base para la perpetración de un ataque, lo que dificulta aún más su atribución.

Los casos de ciberespionaje conocidos demuestran, sin lugar a dudas, que la mayor amenaza se encuentra en los Servicios de Inteligencia extranjeros, por sí mismos, o a requerimiento de empresas u organizaciones, vinculadas de alguna forma a tales Servicios.

Esta evidencia es especialmente peligrosa toda vez que los Servicios de Inteligencia suelen disponer de importantes recursos económicos, materiales y humanos, de la posibilidad de utilizar cualquier tipo de herramienta de ataque y de cualquier procedencia: grupos *hacktivistas*, organizaciones privadas, empresas tecnológicas o las propias universidades.

En muchas ocasiones se ha podido evidenciar que las infraestructuras técnicas de estas organizaciones han contribuido decisivamente en la perpetración de este tipo de ataques.

Además de lo anterior, los actores-estado con gobiernos totalitarios o formas de estado no democráticas gozan de ventajas añadidas a la hora de utilizar este tipo de mecanismos de ataque. A pesar del consenso internacional sobre la aplicación del Derecho Internacional también al ciberespacio, este tipo de Estados suelen prestar poca atención al cumplimiento de las normas jurídicas, permitiéndose usar sus capacidades de ataque sin control alguno, perpetrando, en consecuencia, acciones verdaderamente eficaces, toda vez que sus ataques no están limitadas por ninguna supervisión estatal o por la exigencia de transparencia.

En este tipo de países, además y con frecuencia, determinados intereses privados están en condiciones de desarrollar actividades de ataque sin interferencia gubernamental, pudiendo gozar, incluso, de protección oficial cuando no de cooperación soterrada. Obviamente, el número de actores implicados dificulta enormemente la atribución de tales ataques.

En general, del análisis realizado por el CNI y el CCN-CERT se desprenden los siguientes principios o elementos comunes de los ciberataques realizados por actores estatales:

- **Primer vector de ataque.** Obtención de información estratégica: pueden aprovecharse y analizarse todos los datos obtenidos de internet y de las comunicaciones entre sus nodos. En particular, el tráfico de datos de cualquier usuario. Siempre podrá monitorizarse aquella información que no esté cifrada. Todas estas acciones se desarrollan, generalmente, de forma automática siendo capaces de procesar enormes cantidades de datos.
- **Segundo vector de ataque.** Ataques individuales: ataques dirigidos a los sistemas pertenecientes a personas o instituciones que pueden revestir determinado interés. Los sistemas TIC identificados durante la recopilación de información son atacados mediante herramientas específicamente adaptadas, utilizando la información técnica y social que se dispone de la víctima.
- **Tercer vector de ataque.** Debilitar las implementaciones técnicas: durante este proceso se manipula la implementación de los estándares criptográficos para que sean vulnerables a ataques.

– **Cuarto vector de ataque.** Manipulación selectiva de equipos informáticos: durante este proceso se manipulan los sistemas o los servicios. Lo cual incluye, por ejemplo, la inserción de puertas traseras o el debilitamiento de la seguridad perimetral que podrán explotarse posteriormente durante la fase de recopilación de información o en ataques individualizados.

Conocedores de la potencialidad de tales acciones, mientras algunos estados han declarado públicamente que los ciberataques constituyen un elemento central de su estrategia militar, otros han sido acusados de perpetrar ciberataques dirigidos a magnificar los efectos de operaciones militares tradicionales. Estos programas de ciberataques, de naturaleza indirecta, suelen estar diseñados para inutilizar o dañar la infraestructura y las comunicaciones de los adversarios o dirigirse contra sistemas públicos de salud o de respuesta a emergencias, en cuyo caso los efectos sobre el adversario son directos.

En este sentido es ya significativo el número de países que están desarrollando capacidades para llevar a cabo operaciones militares ofensivas en el ciberespacio. Estas operaciones se denominan *CNE* (*Computer Network Explotation*) y/o *CNA* (*Computer Network Attack*). En ambos casos se trata de términos de origen militar. *CNE* es, en esencia, ciberespionaje. *CNA*, sin embargo, suele implicar acciones dirigidas a destruir o inutilizar las redes y sistemas del adversario o hacer inaccesible su información.

En el lado opuesto, se usa el término *CND* (*Computer Network Defense*), entendido como el conjunto de medidas dirigidas a proteger, monitorizar, analizar, detectar y responder a los ataques anteriores incluyendo intrusiones, interrupciones u otras acciones no autorizadas que puedan llegar a dañar o comprometer las redes o los sistemas de información.

La agrupación de estos tres términos (*CNE*, *CNA* y *CND*) es lo que se denomina *CNO* (*Computer Network Operation*).

Finalmente, no puede olvidarse tampoco que los Estados también pueden desarrollar sus ataques contratando servicios de otros actores (y operando, en consecuencia, bajo otra bandera) o haciéndose pasar por movimientos *hacktivistas*.

Terrorismo y ciberyihadismo

Como es sabido el objetivo de los grupos terroristas es provocar cambios políticos y/o ideológicos a través de acciones que provoquen pánico, generando terror en las sociedades.

Aunque la actividad terrorista en el ciberespacio está incrementándose en los últimos años todavía no debe considerarse una gran amenaza, especialmente debido a sus limitadas capacidades tecnológicas.

No obstante, la más importante amenaza proviene sin duda de los grupos yihadistas (pertenecientes o afines a Dáesh), que en repetidas ocasiones han

hecho llamamientos a la «ciber yihad» contra Occidente, lo que ha puesto en evidencia la necesidad de analizar hasta qué punto disponen de los elementos necesarios (capacidades y conocimientos) para desarrollar tales ataques.

Hasta el momento, los ataques atribuibles al yihadismo se han limitado a actividades que no exigen grandes conocimientos o infraestructura como 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 radicalización.

Quizás, una de las evidencias más significativas en 2015 de la actividad ciberyihadista fue el incipiente uso de código dañino. En Siria, por ejemplo, se detectaron ciberataques (atribuidos a Dáesh) con el propósito de obtener datos sobre posiciones de los objetivos locales.

Además de ello, grupos yihadistas han colgado en internet información y vídeos al objeto de difundir las capacidades tecnológicas digitales de sus partidarios. Estas instrucciones persiguen concienciar en materia de ciberseguridad a yihadistas potenciales. Además de esto, se localizaron en internet instrucciones para el uso de una herramienta de acceso remoto (*RAT*) utilizada para el control de equipos en remoto y que, al parecer, han sido usadas por diversos grupos enfrentados en Oriente Medio.

Para financiarse los ciberyihadistas recurren a las mismas tácticas que los ciberdelincuentes, mediante ataques de *phishing* para obtener los datos de tarjetas de crédito robadas. El dinero se utiliza, fundamentalmente, para sufragar los gastos derivados de operaciones de propaganda y reclutamiento o el pago de los proveedores de internet. Además de ello, lo utilizan para recaudar fondos directamente. Por ejemplo, la red mundial de recaudación de fondos de Al-Qaeda se sustenta en donaciones y en la utilización de ONG que se comunican con sus donantes a través de redes sociales y foros *online*.

Dáesh ha elevado su despliegue mediante el diseño de la aplicación móvil *Dawn of Glad Tidings*, que actualiza regularmente, y que enlaza con *tuits* a través de sus propias cuentas personales, ayudando al grupo a lograr más seguidores, incluidos potenciales donantes.

Los ciberyjihadistas también han ampliado su uso de internet para perpetrar ataques a los gobiernos e instituciones occidentales. Al-Qaeda, por ejemplo, alienta abiertamente a sus seguidores a atacar sitios web occidentales y páginas «moralmente corruptas». La «ciber yihad» también se menciona explícitamente como un deber sagrado para todos los musulmanes en una de sus documentos titulado *The 39 Principles of Jihad*.

Casos recientes demuestran que el ciberejército yihadista está creciendo en número y sofisticación. El grupo CyberCaliphate afiliado a Dáesh (supuestamente liderado por un ciudadano británico conocido como Abu Hussain Al Britani, quien dejó Birmingham para desplazarse a Siria) atacó y tomó el control de las cuentas de Twitter y Youtube del US Central Command.

Sea como fuere, todo lo anterior hace vaticinar que 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 Dáesh.

Profesionales del ciberdelito

Las capacidades de los profesionales de la ciberdelincuencia, cuyo objetivo es obtener beneficios económicos, han seguido creciendo. Las características más significativas de los ataques evidenciaron una magnifica organización, una ejecución inmejorable y una importante sofisticación técnica, con independencia de la ubicación geográfica mundial del atacante y sus víctimas.

Se está comprobando que las organizaciones cibercriminales están dispuestas a invertir grandes cantidades de dinero en la preparación de sus acciones, cada vez más creativas, como pudo demostrarse por ejemplo en la campaña «Carbanak», dirigida contra entidades financieras de Europa del Este.

Como decimos la creatividad de los ciberdelincuentes para convertir en dinero información sustraída, se ha incrementado notablemente. Algunos ejemplos:

En Estados Unidos, un grupo de ciberdelincuentes desarrolló una campaña utilizando una muestra de código dañino específico para obtener información relativa al comportamiento económico del sector farmacéutico, lo que les permitió predecir los precios de los medicamentos y obtener importantísimos beneficios.

Otro tipo de ataque especialmente significativo de los últimos años ha venido siendo el uso de código dañino dirigido a TPV (Terminales Punto de Venta). Ataques que cobran especial peligrosidad cuando se usan tarjetas bancarias de banda magnética, más inseguras que las basadas en chip.

Las acciones delictivas a fin de lograr datos o información médica de los pacientes de instituciones sanitarias o clientes de compañías de seguros de salud han cobrado especial importancia en los Estados Unidos. Además de todo lo anterior, el denominado Cibercrimen como Servicio (*CAAS Cybercrime-As-A-Service*) ha incrementado su penetración y profesionalización, habiéndose percibido una cierta «competencia» entre los propios ciberdelincuentes. Lo que obliga a sus autores a prestar a sus «clientes» un «servicio» cada vez más fiable.

El acceso a las herramientas de perpetración de este tipo de ataques es cada vez más fácil, lo que propiciará el incremento del número de ciberdelincuentes y, en consecuencia, de sus acciones. Hay que tomar en consideración, no obstante, que el nivel de conocimientos técnicos de los agentes de las amenazas puede ser muy variable.

Los métodos utilizados por los ciberdelincuentes se basan tanto en el progreso tecnológico como en las medidas de protección existentes. Cuando se trata de usuarios privados, las herramientas preferidas son el correo basura o *spam* y los correos electrónicos de *phishing*, el código dañino para robo de identidad y la utilización de *ransomware*. Las organizaciones, por su parte, se enfrentan, además, a otras formas de ataque, tales como la extorsión o la infección por código dañino para terminales de punto de venta, por ejemplo.

Asimismo, algunas organizaciones delictivas ofrecen sus capacidades y servicios a otras organizaciones (o Estados) que no tienen estas capacidades. Se trata del mercado de la ciberdelincuencia en el que se ofrecen las vulnerabilidades, los métodos de ataque y se garantiza el rendimiento de los mismos.

Cibervándalos y script kiddies

Se vienen denominando cibervándalos a aquellos individuos que, poseyendo significativos conocimientos técnicos, llevan a cabo sus acciones con el único motivo de demostrar públicamente que son capaces de hacerlo.

Por su parte, los denominados *script kiddies* son aquellos que, con conocimientos limitados y haciendo uso de herramientas construidas por terceros, perpetran sus acciones a modo de desafío, sin ser, en muchas ocasiones, plenamente conscientes de sus consecuencias.

Pese a la difusión mediática que han recibido en ocasiones las acciones de los cibervándalos, no constituyen una amenaza seria a los intereses de las organizaciones.

En algunas ocasiones, los cibervándalos o los *script kiddies* han utilizado la referencia al autodenominado Estado Islámico como un engaño para crear un efecto mediático mayor, tal y como pudo apreciarse en los ataques *DDoS* a plataformas de juegos *online* o la desfiguración de la página web de Malaysian Airlines.

Hacktivistas

Los *hacktivistas*, personas o grupos, más o menos organizados, que desarrollan sus acciones en el ciberespacio movidos generalmente por motivos ideológicos, se han mostrado activos en diferentes campañas políticas y sociales.

En los últimos años, sus ciberataques (desfiguración de páginas web, ataques *DDoS* o sustracción de datos confidenciales de sus objetivos) pretendieron ser la respuesta a determinadas medidas adoptadas por gobiernos y que consideraban perjudiciales para la libertad de internet.

Con frecuencia, las acciones de estos agentes pueden situarse dentro de un contexto geopolítico, es decir, allí dónde se han producido hechos que, a su entender, han sido injustos o desproporcionados, por lo que el riesgo

de ciberataques por grupos *hacktivistas* aumenta significativamente durante conflictos nacionales o internacionales.

La disparidad de intereses hace que, en ocasiones, se generen confrontaciones como la ocurrida entre grupos en la órbita de «Anonymous», por un lado, contra identidades *hacktivistas* con configuración islamista no afiliadas directamente pero sí apoyando o mostrando simpatía por el grupo yihadista Dáesh.

En Iberoamérica, por su parte, se ha mantenido prácticamente constante una ofensiva *hacktivista* reactiva contra el Gobierno de Nicolás Maduro en Venezuela, se han programado varias operaciones antigubernamentales en México y se han desarrollado algunas acciones en Colombia, Chile, Brasil y, en menor medida, Argentina, Guatemala o Nicaragua.

El ecosistema *hacktivista* en España está caracterizado por una baja densidad de identidades de propaganda adoptando la iconografía del colectivo «Anonymous», instaladas con vocación de permanencia a través de perfiles y canales de comunicación en redes sociales pero sin apenas capacidades operativas, con la excepción de «La 9.ª Compañía de Anonymous».

Actores internos

Los llamados actores internos (*insiders*) son personas que están o han estado trabajando para una organización tales como empleados o exempleados, trabajadores temporales, colaboradores y proveedores.

Son muchos los casos que han demostrado que el compromiso de un sistema de información (de naturaleza pública o privada) no se origina siempre por motivos económicos o políticos, sino que, en muchas ocasiones, la negligencia de los usuarios o el despecho de determinadas personas son causa directa de importantes brechas de seguridad.

En varios de los ciberincidentes se ha podido observar como algunos empleados colocaron información sensible en servidores privados sin adoptar las adecuadas medidas de seguridad, lo que provocó que fuera accesible por terceros a través de internet.

Análogamente, la disponibilidad de los sistemas de información también puede verse alterada debido a errores humanos. En todo caso, pese a su peligrosidad, los actores internos solo han venido representando un pequeño porcentaje de los agentes de las amenazas.

Ciberinvestigadores

Los llamados ciberinvestigadores buscan vulnerabilidades en entornos TIC al objeto de verificar la protección de los sistemas objeto de sus investigaciones. Con frecuencia, además de informar a las empresas, se publica en los medios de comunicación el resultado de sus investigaciones, con un doble efecto: positivo y negativo.

En el plano negativo es evidente que la publicidad de cualquier vulnerabilidad conlleva que los sistemas identificados sean más vulnerables a ataques exteriores, facilitando la acción de los atacantes, que pueden llegar a beneficiarse de los resultados de las investigaciones. Esto sucede con frecuencia cuando ciberinvestigadores (por sí mismos o a través de periodistas) deciden publicar determinadas vulnerabilidades de sistemas críticos o sensibles, pudiendo llegar a incurrir en responsabilidades administrativas, civiles o penales, según los casos.

Además, es preciso tener en cuenta que estos actores internos pueden ser empleados por otros actores agentes de la amenaza, especialmente por Estados y empresas dedicados al ciberespionaje, para la infección preliminar de la red objetivo o para la exfiltración de información de la misma. Este comportamiento no exige necesariamente amplios conocimientos técnicos, la conexión a un ordenador de la organización de una simple memoria USB conteniendo código dañino puede ser suficiente

Algunos países han publicado una guía para la revelación responsable de vulnerabilidades y fallos de seguridad. Tal es el caso de la *Policy for arriving at a practice for Responsible Disclosure*, publicación del Centro Nacional de Ciberseguridad de los Países Bajos. Desde la publicación de esta guía, en 2013, los ciberinvestigadores, junto con la comunidad de seguridad IT, han venido reportando vulnerabilidades de forma confidencial y responsable siguiendo un procedimiento que permite resolver rápidamente las vulnerabilidades detectadas. Siendo una práctica deseable, todavía no se ha extendido el uso internacional de este tipo de iniciativas.

Organizaciones privadas

Las motivaciones para perpetrar ciberataques también se encuentran en las organizaciones privadas cuando, movidas por el interés económico que supone poseer los conocimientos que tiene la competencia, desarrollan acciones de ciberespionaje industrial.

Por otro lado, también se han dado casos de empresas que, como consecuencia de las aplicaciones que venden o los servicios que prestan, recaban datos –en muchos casos de carácter personal– de sus clientes que pueden utilizar para propósitos comerciales no legítimos o que, incluso, pueden llegar a vender a terceros sin solicitar el consentimiento del cliente o bien le hayan sido requeridos de manera engañosa. Este problema adquiere especial relevancia cuando se trata de servicios en la nube, en los que el usuario depende totalmente del comportamiento del proveedor y de las medidas de seguridad que hayan sido adoptadas por las organizaciones para garantizar el adecuado tratamiento de sus datos.

Los analistas que tratan de determinar el origen de un ciberataque encuentran a menudo obstaculizada esta labor por el uso de *botnets* o redes de ordenadores infectados que son utilizados como robots. En primer lugar, los

ordenadores infectados a través de una *botnet* pueden estar ubicados en diferentes países de todo el mundo, limitando la capacidad de definir el país de origen del ciberataque.

En segundo lugar, la identidad del control de la *botnet* también puede ser ensombrecida por la utilización de *software peer-to-peer* o red entre pares (*P2P*, por sus siglas en inglés). Además, la dirección facilitada por un proveedor de internet (IP) que podría facilitar la ubicación de un equipo que lanzó un ataque puede ser falsificada (lo que se conoce como *spoofing*) e incluso con una dirección IP válida puede ser prácticamente imposible verificar el actor que se encontraba tras un sistema en el momento en que se produjo el ataque.

De otra parte, en las *botnet* se encuentran equipos que han sido infectados sin el conocimiento del usuario. En este escenario, a nivel de estado-nación, es plausible un cierto nivel de ausencia de responsabilidad, dada la proliferación de organizaciones de *hackers* y las herramientas cibernéticas a su disposición lo que facilita que los Estados puedan reclamar fácilmente la falta de responsabilidad ante ataques que parecen provenir del interior de sus fronteras estatales.

Criterios de determinación del nivel de peligrosidad de los ciberincidentes

Los incidentes de seguridad provocados por los diferentes actores se tipifican, atendiendo a su peligrosidad, en cinco niveles: bajo, medio, alto, muy alto y crítico. La tabla siguiente muestra el nivel de peligrosidad de los ciberincidentes, atendiendo a la repercusión que la materialización de la amenaza de que se trate podría tener en los sistemas de información de las entidades.

CRITERIOS DEL NIVEL DE PELIGROSIDAD DE LOS CIBERINCIDENTES			
NIVEL	**AMENAZAS SUBYACENTES MÁS HABITUALES**	**VECTOR DE ATAQUE**	**CARACTERÍSTICAS POTENCIALES DEL CIBERINCIDENTE**
CRÍTICO	Ciberespionaje	*APTs*, campañas de *malware*, interrupción de servicios, compromiso de sistemas de control industrial, incidentes especiales, etcétera.	- Capacidad para exfiltrar información muy valiosa, en cantidad y en poco tiempo. - Capacidad para tomar el control de los sistemas sensibles, en cantidad y en poco tiempo.

MUY ALTO	- Interrupción de los - Servicios IT. Exfiltración de datos. - Compromiso de los Servicios.	- Códigos dañinos confirmados de Alto Impacto (RAT, troyanos enviando datos, *rootkit*, etcétera). - Ataques externos con éxito.	- Capacidad para exfiltrar información valiosa, en cantidad apreciable. - Capacidad para tomar el control de los sistemas sensibles considerable.
ALTO	- Toma de control de los sistemas. - Robo y publicación o venta de información sustraída. - Ciberdelito. - Suplantación.	- Códigos dañinos medio impacto (virus, gusanos, troyanos). - Ataques externos compromiso de servicios no esenciales (*DoS*/*DDoS*). - Tráfico DNS con dominios APTs o campañas *malware*. Accesos no autorizados. - Suplantación. - Sabotaje. - *Cross-Site Scripting*. - Inyección *SQL*. - Spear *phising*/*pharming*.	- Capacidad para exfiltrar información valiosa. - Capacidad para tomar el control de ciertos sistemas.
MEDIO	- Logro o incremento de capacidades ofensivas. - Desfiguración de páginas web. - Manipulación de información.	- Descargas de archivos sospechosos - Contactos con dominios o direcciones IP sospechosas - Escáneres de vulnerabilidades. - Códigos dañinos de bajo impacto (*adware*, *spyware*, etcétera). - *Sniffing*. - Ingeniería social.	- Capacidad para exfiltrar un volumen apreciable de información. - Capacidad para tomar el control de algún sistema.
BAJO	- Ataques a la imagen. - Errores y fallos.	- Políticas. - *Spam* sin adjuntos. - *Software* desactualizado. - Acoso, coacción, comentarios ofensivos. - Error humano. - Fallo HW-SW.	- Escasa capacidad para exfiltrar volumen de información. - Nula o escasa capacidad para tomar el control de sistemas.

Tabla 3.1. CRITERIOS DEL NIVEL DE PELIGROSIDAD DE LOS CIBERINCIDENTES. CR
Fuente: CCN-CERT: *Guía de seguridad de las TIC, CCN-STIC-817, Esquema Nacional de Seguridad, Gestión de Ciberincidentes,* **p. 18.**

Herramientas de las amenazas

Herramientas construidas para otros fines.

Los atacantes están haciendo un uso masivo de herramientas desarrolladas para otros fines, tales como la monitorización de sistemas o la realización de pruebas de penetración. Algunos ejemplos de ello son los servicios *SaaS* (*Software as a Service* o *booter services*) que permiten a los atacantes perpetrar ataques de denegación de servicios distribuidos (*DDoS*) a través de un sitio web.

Como ejemplo, los responsables de las campañas de ataque denominadas Cleaver, Hurricane Panda y Anunak/Carbanak utilizaron la herramienta MimiKatz (diseñada originariamente para recuperar contraseñas, tickets Kerberos y funciones resumen —hashes15— de memoria de un sistema Windows) para obtener datos de registro (*log*) a una red Windows y lograr acceder a los sistemas de la red.

En otras ocasiones, los atacantes prefirieron seguir utilizando *exploits* ya construidos provenientes de Metasploit (una herramienta concebida para desarrollar pruebas de penetración) posibilitando a los atacantes explotar vulnerabilidades ya conocidas sin necesidad de poseer amplios conocimientos técnicos.

Exploits, Exploit-Kits y *Exploit Drive-By.*

Las herramientas más utilizadas para realizar los ataques, al igual que en los últimos años, son *exploits*, *exploit-kits* y *exploit* DriveBy (permiten infectar el sistema de la víctima con código dañino cuando accede a una determinada página web, distribuyéndose habitualmente mediante *banners* de publicidad).

Windows y las aplicaciones *PHP* (*plug-ins* para Wordpress y Joomla, sobre todo) siguen constituyendo el foco de los *exploits*, aunque es cierto que se ha reducido sustancialmente su publicación. Sin embargo, los *exploit-kits* más habituales se centran en Adobe Flash.

Estas herramientas no solo se utilizan en páginas web dudosas, sino también en aquellas otras absolutamente legítimas y fuera de sospecha. También son muy comunes los ataques por Watering Hole que constituyen un mecanismo habitual para iniciar ataques dirigidos, especialmente cuando las páginas web infectadas son de visita frecuente por parte de personas de la organización-víctima.

Los *exploits Drive-By* son mecanismos de ataque que permiten infectar el sistema de la víctima con código dañino cuando accede a una determinada página web previamente infectada, código que explota las vulnerabilidades de los navegadores web, sus complementos o el propio sistema operativo. Los llamados *exploits Drive-By* pueden usarse aisladamente o en conjunción con *exploits-kits* tradicionales, distribuyéndose habitualmente mediante *banners* de publicidad infectados o servidores web comprometidos. Obviamente, si una página web es muy popular, el número de infecciones será muy significativo y se logrará en muy corto período de tiempo.

Mientras que los *exploits-kits* suelen utilizarse principalmente para ataques masivos (no-dirigidos), los mecanismos *Drive-By* suelen utilizarse cuando se trata de ataques inmersos en campañas específicas de ataques dirigidos específicamente a un objetivo concreto (*APT* por ejemplo).

Código Dañino/*Ransomware*/*Cryptoware*.

El código dañino (en la bibliografía anglosajona suele denominarse también *malware*) tiene en la actualidad una tipificación muy compleja porque se compone de una multiplicidad de módulos con funciones diferentes (módulos adicionales que pueden descargarse de internet) en función de las características del ataque o de la víctima, etcétera.

Los mecanismos de infección suelen ser los archivos adjuntos a correos electrónicos o la visita a páginas web infectadas.

El código dañino representa una de las herramientas más utilizadas para realizar las infecciones que preceden a los ataques. El número total de versiones de código dañino para *personal computer* se estima actualmente en más de 439 millones (siendo Windows el sistema más afectado), al tiempo que el número de *malware* en plataformas móviles sigue aumentando de manera incesante (un 96 % de este código dañino afecta al sistema operativo Android).

La variedad de muestras de *ransomware* o *cryptoware* (Critroni, CryptoFortress, CTB-Locker, Cryptolocker y Cryptowall) no ha dejado de crecer y sus métodos de distribución van variando: *exploits Drive-By*, correos electrónicos con enlaces a programas dañinos, alojamiento en macros de los productos de Microsoft Office, etcétera.

Durante 2016 se han podido constatar infecciones por *cryptoware* en multitud de organizaciones, públicas y privadas, de todos los tamaños, incluyendo instituciones sanitarias y pymes.

A modo de ejemplo, podemos citar el caso Coinvault, una infección investigada conjuntamente por la Policía holandesa y Kaspersky Lab, en la que pudo determinarse que, aproximadamente, el 1,5 % de las victimas hicieron efectivo el pago del rescate. Es lógico que aparezcan nuevas variantes, dado que se calcula que un tanto por ciento de las víctimas satisfizo el rescate, lo que estimula a los delincuentes para mejorar continuamente sus herramientas y sus objetivos: grandes empresas, pymes y consumidores finales; nuevos sistemas operativos y nuevos dispositivos, incluyendo los dispositivos móviles.

Spam (correo basura) y *phishing*/*spearphishing*.

El término *spam* se puede subdividir en varios tipos: *spam* tradicional, *spam* de código dañino y mensajes de *phishing*. Tras un aumento en 2014 el *spam* tradicional disminuyó en 2015, aproximadamente el 30 % del volumen del año anterior, manteniéndose en la actualidad en esos niveles. Sin embargo, el *spam* que lleva incorporado *malware* y que utiliza direcciones de correo electrónico obtenidas en otros sistemas infectados, aumentó significativamente y constituye la principal la principal fuente de infecciones.

Se han encontrado numerosas muestras de código dañino de la familia Geodo. Se ha observado, además, que se distribuyen cada vez más profesionalmente. La utilización de técnicas de engaño y suplantación, el uso de versiones individuales del código dañino y el control horario de la descarga, son herramientas dirigidas a provocar la infección del sistema del usuario sin que el *software* antivirus sea capaz de detectarlo. En cuanto al *phishing* y *spearphishing* (correo dirigido de alguien conocido) son las herramientas más utilizadas para iniciar ataques personalizados y realizar ciberespionaje.

Botnets.

Las redes de robots, *botnets*, son utilizadas por los ciberdelincuentes de forma masiva al objeto de sustraer información, cometer fraude de banca *online*, atacar a la disponibilidad de los sistemas informáticos o enviar *spam*.

Debido a la profesionalización de los ciberdelitos operar una *botnet* es relativamente fácil y poco costoso para los no especialistas. Por ello, el nivel de peligrosidad actual continúa siendo crítico y la tendencia va en aumento.

Debido a su cuota de mercado, los sistemas comprometidos principalmente por *botnets* utilizan Windows, aunque los atacantes están aumentando sus esfuerzos para dirigirse contra sistemas Mac OS X y Android. Persiste la tendencia del uso dañino de servidores web comprometidos para operar servidores *C&C* (mando y control).

Ataques *DDoS*.

Aunque siguen produciéndose ataques *DDoS*, los perjuicios que han podido causar en los sistemas de información, especialmente del sector privado, han sido cuantitativamente menores que los ocurridos en 2014. Ello ha sido debido a la adopción de las medidas anti-*DDoS* que han podido tomar las organizaciones más vulnerables a este tipo de ataques, singularmente las entidades financieras. Estas medidas, que suelen ser significativamente onerosas, sin embargo, no eliminan los riesgos: los ataques siguen estando ahí y, para tener éxito, solo necesitan ser más sofisticados que las medidas adoptadas.

Otra consideración significativa que puede hacerse es que la duración media de un ataque *DDoS* disminuye. La mayoría de los ataques tienen una duración de entre treinta minutos y una hora. El 59 % de los ataques se detiene en quince minutos y más del 87 % lo hacen en la primera hora. En algunas ocasiones, los ataques solo duran cinco minutos, lo que podría estar indicando el uso de una prueba gratuita de los llamados servicios *booter*, que pueden utilizarse con facilidad para desarrollar ataques de denegación de servicio distribuida *DDoS*. Sea como fuere, la experiencia señala que, a menudo, cuanto más corto es un ataque más intenso es.

Por otro lado, y al objeto de asegurar que un ataque *DDoS* es efectivo, se emplean técnicas de amplificación: enviar una consulta pequeña que requiera

una respuesta de gran volumen. Se ha comprobado que, en ciertos casos, la respuesta puede llegar a ser casi 360 veces más grande que la consulta, lo que supone un alto grado de amplificación.

El motivo principal que inspira los ataques *DDoS* es la extorsión, aunque el *hacktivismo* también suele utilizar este mismo vector de ataque.

La modalidad denominada Ataque por Reflexión constituye también una amenaza significativa de este tipo de ataques. En esta modalidad, servidores de acceso público (por ejemplo, servidores *NTP*) se utilizan para reforzar el ataque. Esto hace que los operadores de este tipo de servidores se conviertan en coautores (involuntarios) de las acciones dañinas. Este tipo de ataque logra un efecto comparable al de un ataque mediante una *botnet* tradicional.

Ofuscación.

Se denomina ofuscación a cualquier actividad llevada a cabo por los atacantes para dejar el menor número posible de trazas de sus acciones con el objeto de dificultar su identificación, la metodología seguida, etcétera.

Rastrear el tráfico sospechoso dentro de una red es más difícil si se utilizan nombres de dominio, sitios web o servicios de comunicaciones que gocen de buena reputación. En muchos casos, la detección se centra en direcciones IP y nombres de dominio dañinos conocidos por su participación en ciberataques.

En general, los creadores de código dañino ofuscan el *software* tanto como es posible, al objeto de dificultar su análisis aunque, en ocasiones, no lo hacen como sucedió con los códigos dañinos Foxy148 y Babar. Esta situación hace que sea más fácil para los investigadores diseccionar el *malware*. La detección de este dentro de una red es, sin embargo, más difícil.

La utilización de técnicas de ofuscación y cifrado puede ser una señal para el *software* antivirus y otras herramientas de detección que conduzcan a desconfiar del programa.

Ingeniería social.

Constituye uno de los vectores de ataque preferidos por los agentes de las amenazas, que engañan a sus víctimas, para que permitan la instalación de programas dañinos y todo ello al objeto de acceder a la información del sistema atacado. En este caso, los atacantes tienen la posibilidad de obtener de forma rápida y anónima datos personales de sus víctimas a través de las redes sociales y suele constituir la primera fase de los ataques dirigidos (tratando de adivinar la contraseña de la víctima, generando confianza, correos electrónicos personalizados o *spearphishing*).

El ataque del «falso presidente» ha sido muy lucrativo en el entorno comercial (el atacante se hace pasar por un directivo de la organización, encargando a un empleado la transferencia urgente destinada a un proyecto secreto).

Watering Hole.

Suele ser la segunda opción para los atacantes cuando no tiene éxito un ataque mediante *spearphishing*. Los atacantes aprovechando una vulnerabilidad conocida infectan previamente con código dañino una página web que las víctimas visitan frecuentemente. También se ha incrementado el uso de mensajes publicitarios dañinos (lo que se ha denominado *malvertising*).

Librerías Javascript.

La inclusión de Javascript y otras librerías en una página web han propiciado en 2015 una importante serie de incidentes. Con frecuencia, los desarrolladores de sitios web invocan directamente una librería en lugar de copiarla a su propio sitio web. Si un atacante logra manipular una librería, está en condiciones de atacar a todos los sitios web que contengan una llamada dinámica a la misma.

Las macros como vector de ataque.

Varias familias recientes de *software* dañino, tales como Dridex, Vawtrak y Cryptodefense son claros ejemplos de código dañino que se instala en los sistemas de los usuarios finales a través de macros.

Routers inalámbricos.

Los *routers* de particulares y pymes comprometidos permiten, por ejemplo, ajustar la configuración del *DNS* (*Domain Name System*) para redirigir el tráfico a páginas web infectadas, formar parte de una *botnet*, propagar código dañino y penetrar en la red o manipular el tráfico sin ser detectado.

Robo de identidad.

Habitualmente el robo de identidad (usuario, contraseña u otros datos) se lleva a cabo mediante mecanismos de ingeniería social, instalación de código dañino en los sistemas de la víctima (incluso existen programas cuya función es precisamente este robo) o a través de ataques previos a sitios web. Así pues los atacantes pueden obtener un beneficio económico directo con la venta de identidades robadas y con un margen muy amplio, por lo que esta actividad se mantendrá como una amenaza permanente en los próximos años.

Tendencias de amenazas globales de ciberseguridad

En este escenario, se apuntan a continuación las tendencias de amenazas globales de ciberseguridad detectadas en los diferentes ámbitos.

Ciberespionaje. Muy probable.

El empleo del ciberespacio para la obtención de inteligencia se ha incrementado por todos los países de nuestro entorno por su eficacia y dificultad de

atribución. Debido a la publicación de campañas de ciberespionaje realizadas por compañías de seguridad, los países emplearán más recursos en la seguridad de sus operaciones aislando infraestructuras y diversificando las Técnicas, Tácticas y Procedimientos (TTP) de ataque.

Seguimos siendo testigos de acciones de ciberespionaje, consistentes en ciberataques originados o patrocinados por Estados y perpetrados por ellos mismos o por agentes a sueldo y siempre con la intención de apropiarse de información sensible o valiosa desde los puntos de vista político, estratégico, de seguridad o económico.

A modo de resumen, podemos decir que el ciberespionaje presenta las siguientes características generales: con origen en Estados, industrias o empresas. Utilizando, generalmente ataques dirigidos (APT, Amenazas Persistentes Avanzadas) contra los sectores público (información política o estratégica) y privado (información económicamente valiosa), con una enorme dificultad de atribución y persiguiendo obtener ventajas políticas, económicas, estratégicas o sociales.

Ante la peligrosidad de las campañas de ciberespionaje, especialmente las originadas por los propios Estados y la sofisticación de las técnicas y tácticas usadas, se realizan las siguientes recomendaciones:

- Es necesario aumentar la capacidad de vigilancia de las redes y los sistemas. Para ello, es indispensable contar con el adecuado equipo de seguridad interno o disponer de una consultoría externa, de eficacia debidamente contrastada.
- Es necesario disponer de herramientas de gestión centralizada de registros, incluyendo monitorización y correlación de eventos. Las herramientas utilizadas deberán ser capaces de monitorizar el tráfico de red, usuarios remotos, contraseñas de administración, etcétera.
- Es necesario disponer de la adecuada política de seguridad corporativa que contemple una restricción progresiva de los permisos de los usuarios, así como una aproximación práctica a los servicios en la nube o la utilización de dispositivos y equipos propiedad del usuario *Bring your own device* (*BYOD*).
- Es necesario aplicar configuraciones de seguridad a los distintos componentes de la red corporativa, incluyendo a los equipos móviles y portátiles.
- Es necesario emplear productos, sistemas y servicios confiables, certificados y redes y equipos acreditados para el manejo del nivel de clasificación que se determine.
- Es necesario automatizar e incrementar el intercambio de información con los Equipos de Respuesta ante Ciberincidentes (*CERT*) adecuados.
- Es necesario que la Dirección acepte la existencia de los riesgos y promueva las políticas de seguridad dentro de la organización.

- Es necesario formar y sensibilizar a todos los usuarios de la organización, incluyendo todos los niveles (dirección, gestión e implantación) para que tomen conciencia de los riesgos y actúen en consecuencia.
- Es necesario atenerse a la legislación y buenas prácticas vigentes, adecuándose a los diferentes estándares de seguridad (en el caso de las Administraciones públicas al Esquema Nacional de Seguridad).
- La organización debe trabajar como si los sistemas estuvieran comprometidos o lo vayan a estar pronto.

Los ataques como servicio. Muy probable.

A través de grupos con conocimiento y capacidad técnica sería posible contratar sus servicios y planificar un ataque «a medida» con garantías de éxito. Requerirá ampliar el conocimiento de las redes *Deep Web*, incrementar la cooperación público privada y armonizar la legislación internacional.

Fusión de tácticas, técnicas y procedimientos (TTP) utilizadas por el ciberespionaje y la ciberdelincuencia. Muy probable.

Evolución de la actividad cibercriminal a TTP empleados en el ciberespionaje usando herramientas del tipo Amenazas Persistentes Avanzadas (*APT*) y dirigidas especialmente contra el sector financiero persiguiendo la sustracción de dinero. Durante el último año se ha apreciado un aumento de los ataques, sustentados en la acción de código dañino y métodos propios de las *APT*, cuyo objetivo han sido entidades financieras, persiguiendo la sustracción de dinero, de varias formas:

- Control remoto de cajeros automáticos.
- Realización de transferencias *SWIFT* de las cuentas de ciertos clientes.
- Manipulación de los sistemas informáticos *online* para ordenar transferencias ilícitas.

Estabilización de los ataques *hacktivistas*. Muy probable.

Es de esperar una continuación de la actividad de grupos como «Anonymous» y una proliferación de células *hacktivistas* que operen con distintas narrativas en diversos países con una marcada orientación hacia la producción de ciberataques por desfiguración de páginas web, con incorporación de elaboradas composiciones gráficas en los sitios web de los objetivos atacados.

Herramientas de ataque para dispositivos móviles. Probable.

Además del crecimiento del número de las actuales amenazas de Android, se prevé que el crecimiento de vulnerabilidades en los dispositivos móviles, plataformas y aplicaciones presentará ciertos riesgos de seguridad especialmente graves: los datos almacenados en los dispositivos móviles podrán ser usados por los ciberdelincuentes para perpetrar otros ataques o para su venta en el mercado negro. Por otro lado, las vulnerabilidades no solo residen en los dispositivos sino también en las plataformas y aplicaciones.

El «secuestro» de organizaciones por *ransomware*. Muy Probable.

Durante 2016 se ha estado asistiendo a la expansión de los ataques por *ransomware*, especialmente de su variante más agresiva: el *cryptoware*. De esta forma, los atacantes solicitan un rescate por descifrar la información que ellos han encriptado al tomar el control del dispositivo.

Una nueva tendencia que está resultando exitosa en 2016 es el cambio de paradigma respecto a la liberación de la información y la disminución de la cuantía del pago del rescate. A diferencia de los comienzos del *ransomware*, en el que tras solicitar a los atacados una elevada cantidad de dinero por descifrar la información, en el caso de que estos hicieran efectivo el pago del rescate no se liberaban los sistemas, en la actualidad se han disminuido las cantidades solicitadas a la vez que si se pagaba se liberaba la información, lo que ha generado un mayor volumen de ingresos a los atacantes.

El uso de este tipo de código dañino y el consiguiente lucro obtenido con él han podido dar argumentos a los atacantes para diseñar ataques a mayor escala, todavía más lucrativos: los ataques a grandes empresas o instituciones. Perpetrando un ataque de este tipo, en caso de tener éxito, los agentes de las amenazas lograrían un nivel de compromiso tan grande de los sistemas atacados que podrían detener la normal actividad de la organización. Esta situación obligaría a las víctimas, presumiblemente, a satisfacer el rescate exigido. Obviamente, la publicidad del éxito de un ataque de este tipo alentaría a nuevos atacantes.

Incremento de los ataques contra cajeros automáticos y procedimientos de pago. Probable.

Los ataques contra cajeros automáticos han evidenciado la vulnerabilidad de tales dispositivos. Es presumible, por tanto, que se produzca un incremento y evolución tecnológica de los ataques contra estos dispositivos. No es desdeñable, tampoco, la utilización de técnicas *APT* para, a través de tales equipos, penetrar en la red de la entidad financiera y explotar acciones que persigan mayores objetivos. Este problema puede hacerse extensivo a los ataques dirigidos contra máquinas expendedoras de *tickets* y que, en muchas ocasiones, también aceptan tarjetas de crédito. Presumiblemente, asistiremos a nuevas y más sofisticadas acciones tendentes, por ejemplo, a obtener los datos de las tarjetas de crédito utilizadas por los clientes de las máquinas de *ticketing*. Además, es de esperar que en los próximos años los agentes de las amenazas desarrollen acciones contra sistemas virtuales de pago, atacando los puntos finales (teléfonos móviles, en la mayoría de casos). Este temor puede extenderse a Apple Pay, que utiliza la tecnología *NFC* (*Near Field Communications*) para manejar transacciones de forma inalámbrica.

Nuevas amenazas a los dispositivos móviles. Muy Probable.

Debido a la consolidación y a la comercialización de nuevos accesorios para los dispositivos móviles se incrementarán especialmente los incidentes de seguridad

sobre estos complementos o *wearables* (relojes, pulseras, etcétera) y sobre los nuevos (y ya existentes) métodos de pago basados en tecnologías inalámbricas, como *NFC* (*Near Field Communications*) o monedas virtuales. Pese a que la seguridad de los dispositivos móviles se fortalece con el paso del tiempo, las nuevas funcionalidades que son incorporadas cada año no están exentas de debilidades.

La tendencia parece evolucionar hacia escenarios más complejos, avanzados y profesionalizados de ataque, tanto en la investigación y descubrimiento de nuevas vulnerabilidades, como en la explotación de las debilidades existentes en las principales plataformas móviles. Por otro lado, no debe ignorarse la existencia de vulnerabilidades más sencillas de explotar, incluso ya conocidas en otras tecnologías y que a lo largo del tiempo vuelven a afectar a tecnologías más modernas o de última generación.

Asimismo, será importante permanecer alerta ante nuevas revelaciones asociadas a la privacidad y seguridad del usuario y a esquemas de espionaje globales por parte de agencias gubernamentales. Desde el punto de vista corporativo la integración de forma segura de los dispositivos móviles tanto corporativos como personales en las infraestructuras de información de las organizaciones a través de soluciones *MDM* (*Mobile Device Management*) sigue siendo un reto complejo que hay que afrontar.

Nuevas vulnerabilidades en *software* y protocolos habituales. Probable.

Las especialmente peligrosas vulnerabilidades reveladas el pasado año en *software* habitual, (tales como Shellshock, Heartbleed y OpenSSL), han sumido a la comunidad tecnológica en importantes dudas acerca de la fiabilidad de un *software* muy común que, a la fecha, permanece sin auditar debidamente. Pese a los esfuerzos de muchas organizaciones dedicando recursos para analizar tal tipo de *software* —incluso contratando a grupos de expertos para descubrir nuevas vulnerabilidades—, es muy posible que todavía sean muchas las que permanecen ocultas.

Ataques contra Infraestructuras Críticas. Posible.

La especialmente peligrosa combinación de tecnologías antiguas —sin mantenimiento, en muchos casos— y una superficie de ataque cada vez mayor, hacen a ciertas Infraestructuras Críticas especialmente vulnerables a los ataques. Es sabido que son muchos los Estados que están desarrollando capacidades para atacar de forma remota los sistemas SCADA (Supervisión, Control y Adquisición de Datos) –que permiten controlar y supervisar procesos industriales a distancia– y otros sistemas críticos. Los analistas coinciden en señalar que las grandes cadenas de fabricación y las redes de energía eléctrica constituyen los objetivos más probables para este tipo de ataques.

Ataques contra Linux y OS-X. Posible.

Hasta el momento, tanto Linux160 como OS-X no han sido objeto de grandes ataques, aunque esto puede cambiar en los próximos años. La adopción

masiva de Linux en muchas organizaciones ha provocado un repunte del número de muestras de código dañino para este sistema operativo, tales como Cdorker.

La ampliación de la superficie de ataque supondrá previsiblemente para los agentes de las amenazas un estímulo para perpetrar acciones contra esta plataforma. Por su parte, a pesar de los esfuerzos de Apple para fortalecer el sistema operativo de los Mac, se sigue constatando la presencia de código dañino, introducido a través de paquetes de *software* pirateado. La creciente popularidad de los dispositivos Mac OS-X en todos los ámbitos —junto con la aparición de *exploits* día cero específicos— está despertando la atención de los ciberdelincuentes por desarrollar *malware* específicamente dirigido a este tipo de dispositivos. Dada la dificultad que supone penetrar en esta plataforma, y a la vista de que son muchos los usuarios de Mac que están desactivando determinadas medidas de seguridad por defecto —al objeto, generalmente, de permitir la instalación de software pirata—, los agentes de las amenazas están incorporando código dañino camuflado dentro de programas al objeto de infectar las máquinas.

Quizás, como así se ha considerado por muchos analistas, el mayor motivo de preocupación para los usuarios radica en que, gracias a la imagen de seguridad de la que hasta ahora han gozado estos equipos, no se han desarrollado significativamente herramientas de seguridad para ellos, lo que puede convertirlos en dispositivos vulnerables.

Los ataques contra el Internet de las Cosas (*IoT*). Probable.

Aunque, hasta el momento, los ataques contra el Internet de las Cosas no han ido más allá de unos pocos intentos o algunas amenazas sobre la posibilidad de utilizar *botnet*s para desplegar ataques masivos contra televisores o frigoríficos inteligentes. Sin embargo, a medida que un mayor número de estos dispositivos se conecten, asistiremos a un mayor debate sobre los problemas de seguridad y, especialmente, de privacidad derivados de su conexión. En todo caso, es presumible que se produzcan ataques contra dispositivos de red, que pueden facilitar a un atacante mantener la persistencia en la organización y desarrollar movimientos laterales dentro de una red corporativa, como parte de una acción *APT* a mayor escala.

En el nivel de los usuarios domésticos, es presumible que las primeras acciones de compromiso de la *IoT* se traduzcan en la manifestación de ciertas vulnerabilidades de los dispositivos y la posibilidad de incrustar publicidad (*adware*/*spyware*) en, por ejemplo, la programación del receptor de televisión inteligente.

En cambio, si se han mostrado especialmente vulnerables algunos de estos dispositivos a ser infectados por *malware* que permitía incorporarlos a una *botnet* que los ha utilizado para realizar ataques de denegación de servicio distribuido. El ataque *DDoS* a la empresa de servicios de DNS Dyn del 21 de

octubre de 2016, con impacto en importantes plataformas y redes sociales, ha marcado un punto de inflexión en este ámbito. La modificación de las claves de seguridad por parte de los usuarios y la actualización del *software* o *firmware* de estos dispositivos limitarían este impacto.

Ciberincidentes en España

Un documento que se estima relevante, para situar a España en el contexto de la comunidad internacional en el ámbito de las Tecnologías de la Información y Comunicaciones (TIC), es el *Informe Global de Tecnología 2016*. Desde 2001, este informe publicado por el Foro Económico Mundial, en colaboración con la Universidad de Cornell y el INSEAD, ha medido diferentes parámetros de ciento cuarenta y tres países[4]. En este informe se realiza un estudio comparativo de diferentes factores, elaborando una clasificación que en 2015 coloca a España en el puesto número treinta y cinco de este estudio, el cual valora la penetración en la sociedad de las tecnologías de la información y comunicaciones, como se refleja en el gráfico:

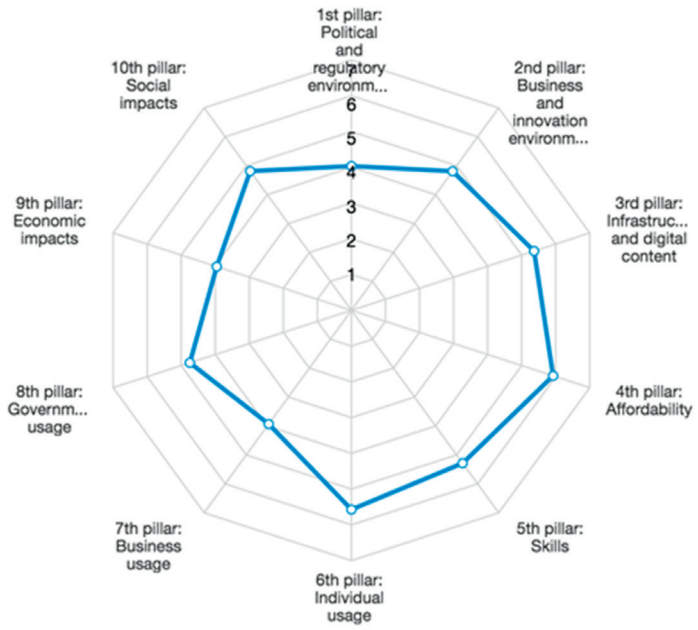

Figura 3.6. Informe sobre España TIC 2016.
Fuente: Foro Económico Mundial. Global Information Technology Report 2016.

[4] DUTTA Soumitra, GEIGER Thierry y LANVIN Bruno, Eds.: *The Global Information Technology Report 2016,* World Economic Forum & INSEAD, Ginebra, 2016. http://reports.weforum.org/global-information-technology-report-2016/

El grado del cumplimiento de España de los diez pilares que analiza el informe en relación con las TIC se refleja en la siguiente figura.

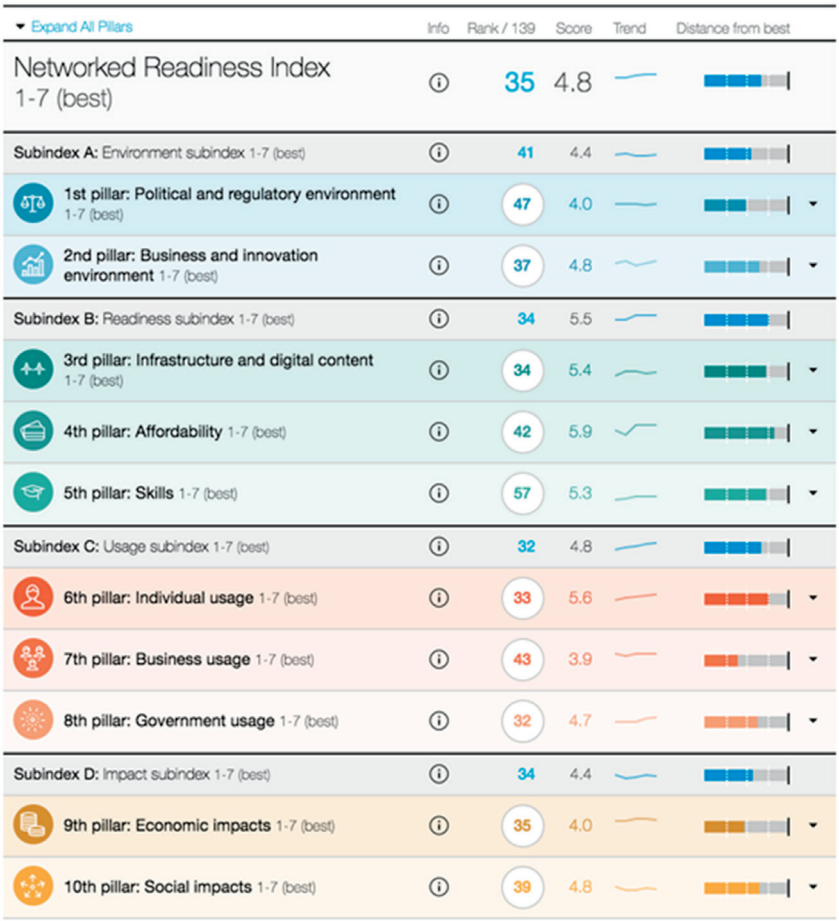

Figura 3.7. Grado de cumplimiento de España en el sector TIC.
Fuente: Foro Económico Mundial. Global Information Technology Report 2016.

Microsoft en su informe de inteligencia de seguridad global más reciente[5] ofrece datos sobre la situación en España[6]. En relación a las tendencias de las tasas de encuentro[7] y de infección, Microsoft señala que en el cuarto

[5] Microsoft Corporation: *Microsoft Security Intelligence Report, Volume 20, julio a diciembre de 2015, España*, Redmond, WA, 2016.

[6] Ibídem, p. 3. Microsoft Corporation señala que las estadísticas son generadas por los programas de seguridad de Microsoft y servicios que se ejecutan en los ordenadores en España. Se utiliza la geolocalización utilizando la dirección IP para determinar el país o la región.

[7] Tasa de encuentro es el porcentaje de equipos que ejecutan productos de seguridad de Microsoft en tiempo real que reportan un encuentro con *malware*, independientemente de si produce o no la infección en el equipo.

trimestre de 2015 el 23,3 % por ciento de los ordenadores en España tuvo un encuentro con *malware*, en comparación a la tasa de encuentro de todo el mundo en este periodo, que fue del 20,8 %. Además, la herramienta de eliminación de *software* malicioso de Microsoft detectó y eliminó el *malware* de treinta y cuatro de cada mil ordenadores escaneados en España en el cuarto trimestre de 2105 (una puntuación CCM[8] de 34, comparada con la medición CCM mundial de 16,9).

La siguiente figura muestra las tendencias de las tasas de encuentro y de infección para España en 2015, en comparación con el mundo en su conjunto.

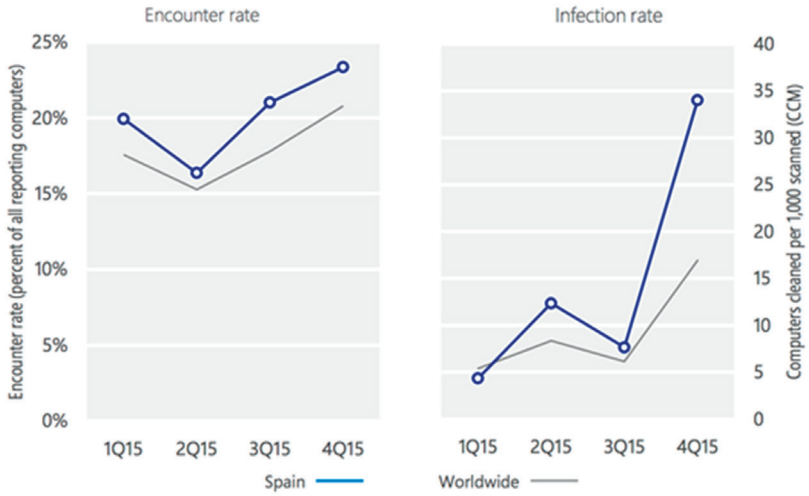

Figura 3.8. Tasas de encuentro y de infección para España en comparación global. Fuente: Microsoft Corporation: Microsoft Security Intelligence Report, Volume 20, julio a diciembre de 2015, p. 840

La categoría de *malware* más común en España, detectada por Microsoft en el cuarto trimestre de 2015, corresponde a los troyanos, que fueron encontrados en un 5,8 % de todos los ordenadores, por debajo del 7,4 % contabilizado en el tercer trimestre de 2015. La segunda categoría de *malware* más común en España durante el cuarto trimestre de 2015 fue la de los gusanos, que se encontraron en un 2,3 % de los ordenadores, frente al 2,6 % del anterior trimestre. La tercera categoría de *malware* más común en España en el cuarto trimestre de 2015 fue la correspondiente a los «descargadores» y «cuentagotas» (*downloaders* & *droppers*) con un 2,2 % de los ordenadores, frente al 1,6 % en el anterior trimestre.

[8] *CCM* (*Computers cleaned per mille*) o número de equipos limpiados por cada mil, es una medición de la tasa de infección de ordenadores únicos que ejecutan la herramienta de eliminación de *software* malintencionado (*MSRT*).

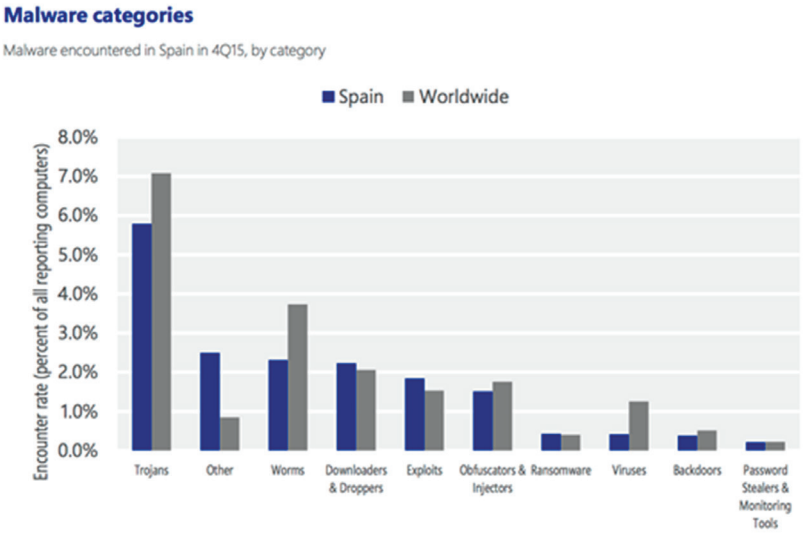

Figura 3.9. Categorías de malware en España detectadas el cuarto trimestre de 2015. Fuente: Microsoft Corporation: Microsoft Security Intelligence Report, Volume 20, julio a diciembre de 2015, p. 841.

En cuanto al *malware* que infectó los equipos en España durante el cuarto trimestre de 2015, Microsoft ofrece los datos reflejados en los gráficos que se muestran a continuación.

Top malware families by encounter rate

The most common malware families encountered in Spain in 4Q15

	Family	Most significant category	% of reporting computers
1	JS/Axpergle	Exploits	1.1%
2	Win32/Dynamer	Trojans	0.9%
3	Win32/Obfuscator	Obfuscators & Injectors	0.9%
4	Win32/Peals	Trojans	0.9%
5	Win32/Sventore	Downloaders & Droppers	0.8%
6	Win32/Skeeyah	Trojans	0.8%
7	INF/Autorun	Obfuscators & Injectors	0.7%
8	Win32/Dorv	Trojans	0.6%
9	Win32/Conficker	Worms	0.5%
10	HTML/Meadgive	Exploits	0.5%

Figura 3.10. Familias de malware encontradas en España en el cuarto trimestre de 2015. Fuente: Microsoft Corporation: Microsoft Security Intelligence Report, Volume 20, julio a diciembre de 2015, p. 843.

El CCN-CERT ha proporcionado la siguiente información actualizada a 4 de noviembre de 2016.

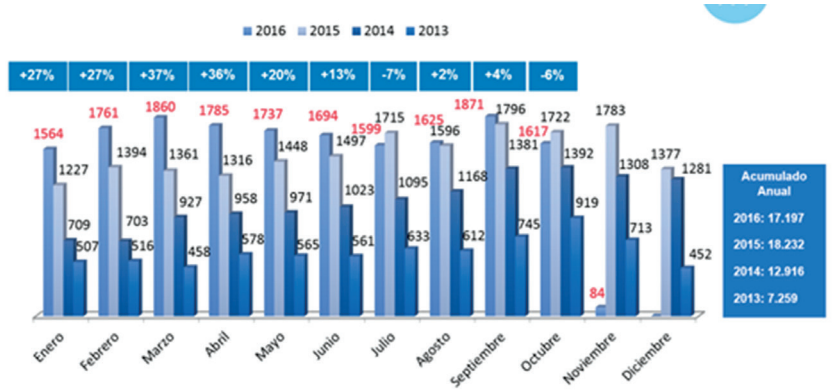

Figura 3.11. Número de incidentes de ciberseguridad gestionados por el CCN-CERT 2013-2016.Fuente: CCN-CERT. 4 de noviembre de 2016.

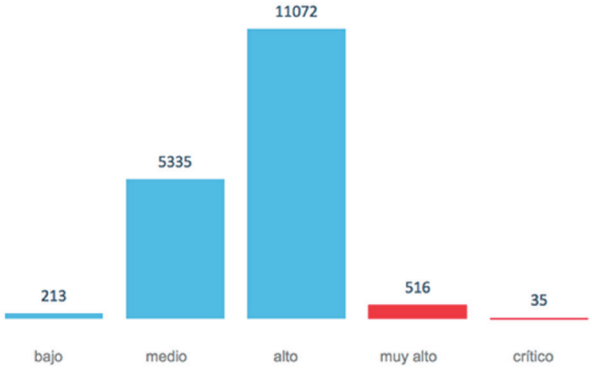

Figura 3.12. Peligrosidad de los ciberincidentes gestionados por el CCN-CERT en 2016. Fuente: CCN-CERT. 4 de noviembre de 2016.

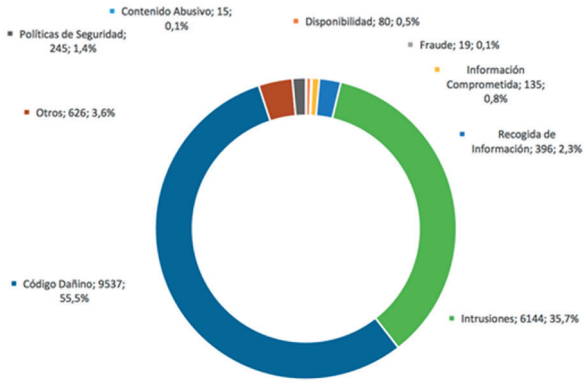

Figura 3.13. Tipología de los incidentes gestionados por el CCN-CERT en 2016.Fuente: CCN-CERT. 4 de noviembre de 2016.

Es significativo resaltar que aunque el CCN-CERT, como CERT Gubernamental Nacional, sirve a las Administraciones públicas (en sus tres niveles, nacional, autonómico y local), a los sistemas clasificados y a las empresas de interés estratégico para el país, buena parte de sus servicios (formación, informes, guías, herramientas, etcétera) están publicados en su portal web y son de libre disposición para cualquier persona.

Conclusiones

El ciberespacio ha introducido una nueva dimensión en las sociedades y su uso se ha incorporado a las mismas de modo cotidiano y generalizado. Los aspectos positivos de la utilización del ciberespacio son numerosos, especialmente en campos como las comunicaciones, la investigación científica, los procesos industriales o la gestión del conocimiento.

Esta revolución tecnológica tiene un elevado impacto social. Los adelantos en las comunicaciones y el abaratamiento de los costes están generando una red en la que pocos elementos escapan a estar conectados, incluso los objetos de uso cotidiano, en lo que se ha venido a llamar el Internet de las Cosas.

Gracias a las nuevas tecnologías y al uso extensivo de internet se están desarrollando proyectos que abarcan las áreas más diversas de las actividades humanas.

Este escenario presenta también nuevos retos a los que no se sustraen los diferentes actores políticos, principalmente los Estados. Entre estos desafíos se encuentran la protección y recuperación de los sistemas de infraestructuras críticas ante agresiones que utilizan el ciberespacio como entorno y vehículo para interferir en las actividades de los ciudadanos y de las instituciones.

De esta forma, hoy en día los Estados deben hacer frente a ataques contra la seguridad de los sistemas de las Tecnologías de la Información y las Comunicaciones de gobiernos, administraciones públicas y empresas con alto valor estratégico.

En este capítulo se han analizado las ciberamenazas en el contexto de los riesgos globales, así como su interconexión con el resto de riesgos. De igual forma se han estudiado los criterios de clasificación de las ciberamenazas, los actores, ámbitos, objetivos, los niveles de peligrosidad de las ciberamenazas y las principales herramientas utilizadas.

Posteriormente se ha presentado la situación en España y los ciberincidentes gestionados por el CERT Gubernamental Nacional, CCN-CERT. España no ha permanecido inmune a las agresiones que utilizan el ciberespacio para atentar contra los más variados aspectos de la seguridad, llegando a verse comprometidos servicios críticos y otros aspectos que afectan a la seguridad nacional.

Desde el Centro Nacional de Inteligencia, la Oficina Nacional de Seguridad y el Centro Criptológico Nacional ––destacando su capacidad CERT—, se generan los elementos de prevención y recuperación de los sistemas de las Tecnologías de la Información y las Comunicaciones para que España y los españoles puedan desarrollarse en el entorno digital de forma segura.