# La Ciberdefensa militar ante el reto de Internet de las Cosas

**La práctica totalidad de los elementos de soporte a la Ciberdefensa en las organizaciones y empresas con un alto grado de madurez a nivel internacional precisarán, a corto plazo, de diversos cambios de gran relevancia. Entre estos cambios a los que nos referimos incluimos, en primer lugar, una revisión de las estrategias, seguida de las políticas y los procedimientos y, finalmente, los procesos, los programas y proyectos, las tecnologías e incluso la propia gestión de los recursos humanos asociados a la Ciberdefensa. ¿Cuál es el disparador de estos cambios? Se trata del aspecto que está añadiendo una mayor complejidad en el entorno de la Ciberdefensa, si cabe, y es la consideración de la interconexión múltiple a la red de una gran variedad de dispositivos físicos. Este concepto, que los especialistas en Ciberdefensa comienzan a analizar bajo el paraguas de la arquitectura de sistemas, se conoce como Internet de las Cosas (Internet of the Things-IoT), y presenta una serie de nuevos retos que deben ser abordados con gran premura.**

Vicente José Pastor Pérez / José Ramón Coz Fernández

Los países, las organizaciones y las empresas que apuestan con claridad por una Ciberdefensa fuerte, y que cuentan con grandes presupuestos y programas que declaran de forma transparente, están llevando a cabo en la actualidad iniciativas para minimizar los riesgos asociados a IoT. Este artículo pretende exponer los principales riesgos y las ideas básicas que sustentan su aproximación desde la Ciberdefensa. Se trata, no obstante, de un primer artículo introductorio. En artículos posteriores iremos desgranando más las características del IoT y sus implicaciones técnicas.

El Internet de las Cosas ha evolucionado de forma exponencial en la última década. Ha pasado de una primera fase de despegue de la tecnología a comenzar a ser una realidad y una verdadera revolución tecnológica con un alcance global e imparable. Desde nuestro punto de vista, está aquí y ha llegado para quedarse. Los analistas predicen un gran crecimiento en la utilización de dispositivos que pueden conectarse a la red y las tecnologías asociadas a su despliegue, como son la computación en la nube, el *Big Data*, las técnicas analíticas de datos y los protocolos de comunicaciones entre máquinas (M2M).

IoT trae una mayor flexibilidad y automatización (y es innegable que muchas ventajas) aunque, al mismo tiempo, nos trae un gran potencial de empeoramiento en lo que se refiere a problemas relacionados con la seguridad de la información y, a la postre, con la Ciberdefensa. En este primer artículo sobre este complejo asunto, realizaremos una introducción a IoT en su vertiente relacionada con la Ciberdefensa, destacaremos en segundo lugar los riesgos de seguridad más comunes que vienen acompañando a estas tecnologías y veremos, por último, cómo se abordan estos riesgos en el campo de la Ciberdefensa.

### IoT y la Ciberdefensa. Definiendo conceptos.

El número de aparatos conectados a Internet está creciendo de forma exponencial y a una velocidad inconcebible hace unos años. Los dispositivos son cada vez más y más potentes y las capacidades de computación que hace no mucho tiempo eran costosas y sólo se podían encontrar en grandes computadores y centros de datos, están ahora al alcance de la mano de prácticamente todo el mundo y ocupan muy poco espacio físico. Todo ello lleva a que la agudeza de ingenio de los fabricantes les haga pensar en cómo incorporar esa capacidad de computación a prácticamente cualquier cosa y, por supuesto, a conectarlas a la red de redes de modo que sus datos se puedan explotar de manera conjunta.

La Ciberdefensa no es inmune a ello. Los dispositivos que forman parte de los sistemas de Mando y Control, de los sistemas aéreos, marítimos y terrestres y que se conectan a Internet u otra red de control con posibles conexiones externas son cada vez mayores. Además, el riesgo de que determinados dispositivos externos puedan capturar información de Ciberdefensa y comunicarla a través de Internet, sin ningún tipo de protección, es muy elevado.

Existen dos términos que son los más utilizados cuando se trata de describir este fenómeno: Internet de las Cosas (IoT – *Internet of the Things*) e Internet de Todo (IoE – *Internet of Everything*). Como con cualquier expresión que es aún relativamente nueva y no ha alcanzado un determinado nivel de madurez, existe cierto desacuerdo en cuanto a sus definiciones y la relación entre ellas. Para la Ciberdefensa, podemos definir *Internet of Things* como una red de dispositivos físicos interconectados, típicamente asociados a una función de sensor de su entorno, que recogen información para producir un beneficio al negocio o a funciones de control remoto que producen unos determinados ahorros en la gestión de alguna acción que, de otra manera, requeriría presencia física para poder ser ejecutada. Básicamente, hablamos de sensores, actuadores o una combinación de ambas funciones y estos elementos conectados a la red para su gestión a distancia.

Dentro del campo de la Ciberdefensa, podemos pensar en algunos ejemplos como componentes industriales del sector de la Defensa, automóviles para la Defensa y sistemas no tripulados, productos de automatización de grandes plataformas navales, terrestres y aéreas, aparatos de consumo personal o individual entre los que cabrían destacar los *wearables*, es decir, los que una persona llevaría encima durante prácticamente todo el día, pero también podríamos incluir los televisores, los refrigeradores y prácticamente cualquier electrodoméstico. Además, todos los dispositivos tecnológicos que dan soporte a sistemas en el entorno de la Ciberdefensa, pasando por dispositivos de comunicaciones como *routers*, *firewalls*, sónar, radares y hasta minicomputadores. Casi todos los dispositivos físicos a nuestro alcance se encontrarán permanente y ubicuamente conectados a la red y comunicándose entre ellos.

Para una mayor claridad, mencionaremos también el concepto de *Internet of Everything,* un término introducido por la empresa Cisco Systems y que, desde el punto de vista de la Ciberdefensa y la arquitectura de sistemas, no aporta nada añadido a la definición anterior. Al menos, no hemos encontrado en la literatura una definición que exponga claramente sus diferencias y éstas tengan

***Uno de los riesgos identificados en los grandes programas y en las organizaciones punteras de la Ciberdefensa indica que el incremento de dispositivos conectados a la red tiene un efecto multiplicador en las posibilidades de lanzar ataques DDoS, si se toma control sobre ellos. Estos ataques, lanzados sobre los dispositivos pueden suponer, en algunos casos del ámbito de la Defensa, amenazas a la vida humana.***

un impacto directo en la gestión de la Ciberdefensa, pese a que diversas entidades y organismos han intentado explicar ambos para promover su coexistencia. Sin embargo, y para nuestros propósitos, nos conformaremos con utilizar IoT como el término que explica esta explosión de aparatos conectados a la red y que, por lo tanto, provoca la aparición de los nuevos riesgos que queremos explicar en el entorno de la Ciberdefensa.

### Nuevos riesgos asociados a IoT y su impacto en la Ciberdefensa

La interconexión de millones de dispositivos entre ellos y con sistemas de información y sistemas operacionales conlleva todo un nuevo panorama de riesgos de seguridad para los gobiernos, los negocios y los consumidores. De acuerdo con un informe de la Comisión Europea sobre IoT en 2013, el desarrollo del Internet de las Cosas tiene muchas probabilidades de causar una mayor preocupación en temas y debates éticos en la sociedad, muchos de los cuales ya han surgido con las tecnologías de la información y las comunicaciones, e Internet en general. Algunos de estos problemas serían la pérdida de confianza, las violaciones de la privacidad, la mala utilización de los datos obtenidos para fines diferentes a los inicialmente previstos, la ambigüedad en los derechos de autor, la brecha digital, el robo de identidades, problemas de control y de acceso a la información y la libertad de discurso y de expresión. A pesar de ser problemas preexistentes, con IoT toman una nueva dimensión a causa del incremento en la complejidad.

En el caso de la Ciberdefensa, algunos de los riesgos ya identificados en los grandes programas y en las organizaciones más punteras son los siguientes:

• Un incremento en la dificultad de mantener los nuevos sistemas de Ciberdefensa y sus dispositivos asociados actualizados y parcheados correctamente, dada su heterogeneidad y el gran número de ellos.

• Una complejidad exponencial en el análisis de vulnerabilidades y las capas que permiten realizar una gestión federada de las vulnerabilidades en Ciberdefensa.

• Los dispositivos se pueden convertir en un nuevo vector de infección a través del cual pueden extenderse a otros componentes que formen parte de sistemas más complejos de soporte a la Defensa.

• El incremento de dispositivos conectados a la red tiene un efecto multiplicador en las posibilidades de lanzar ataques distribuidos de denegación de servicio, si se toma control sobre ellos. Los ataques de denegación de servicio lanzados sobre los dispositivos pueden suponer, en algunos casos del ámbito de la Defensa, amenazas a la vida humana que incluso podrían llegar a causar su pérdida.

• Los múltiples dispositivos se pueden convertir en un receptor de información clasificada o sensible.

• Los dispositivos pueden transmitir información clasificada irregularmente a través del uso de otros dispositivos no controlados o tomando el control de dispositivos supuestamente controlados.

• Los dispositivos se pueden convertir en bloqueadores de las comunicaciones entre los dispositivos o sistemas de información. De hecho, este posible ataque es uno de los más frecuentes en el campo de la Ciberdefensa, a través del bloqueo de las señales GPS.

• El desarrollo de nuevos dispositivos atacantes cuya única función es el control remoto de dispositivos o sistemas de soporte a la Defensa.

Hay muchos más, pero principalmente hemos expuesto los más habituales a los que nos enfrentamos en el campo de la Ciberdefensa.

Lo mismo que en la actualidad hay una explosión en el desarrollo de *malware* y herramientas de ataque, en el futuro se implementarán nuevas arquitecturas y componentes con el único objetivo de explotar las nuevas posibilidades que trae IoT. Estas arquitecturas permitirán llevar a cabo ataques con un mayor control, y la Ciberdefensa requerirá dotarse de un grado mayor de complejidad.

No debemos ignorar que las cifras de las previsiones de múltiples analistas para 2020 relacionadas con la evolución de IoT dan verdadero vértigo:

• Entre 25 y 50 mil millones de dispositivos conectados.

• Unos 6 objetos por persona (de media) conectados a la red.

• Un impacto económico de entre 2 y 5 billones de dólares.

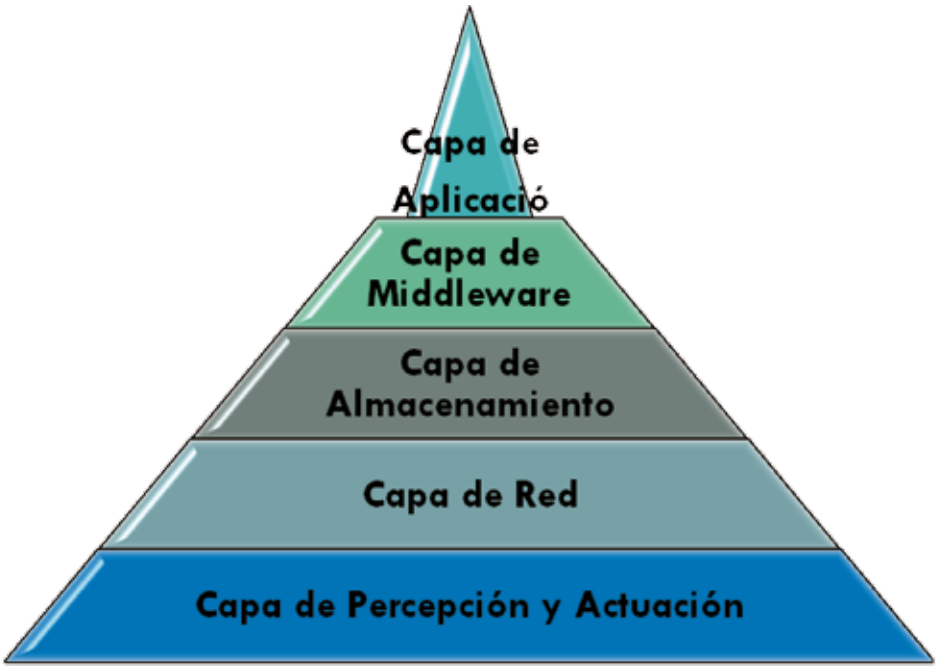


**Figura 1.- Arquitectura de un sistema IoT en Ciberdefensa.**

### Una aproximación a IoT desde la Ciberdefensa

Hewlett-Packard realizó un estudio el año pasado en el que analizó la seguridad de 10 de los dispositivos relacionados con las áreas de desarrollo en IoT más populares, y los hallazgos del mismo no pueden ser más preocupantes. Entre los aparatos analizados se encuentran televisores, cámaras web, termostatos domésticos, tomas de corriente con acceso remoto, controladores de rociadores anti-incendios, cerraduras de puertas y puertas automatizadas, alarmas e, incluso, básculas. Componentes, ellos mismos u otros similares, que también pueden ser utilizados dentro del ámbito de la Ciberdefensa, donde habitualmente las grandes plataformas tienden a un mayor grado de automatización.

Se descubrió un gran número de vulnerabilidades en todos los dispositivos y una mala praxis en su diseño en lo que se refiere a su seguridad. Algunos de los hallazgos más interesantes los exponemos a continuación:

• 6 de los 10 dispositivos tienen interfaces de usuario vulnerables a ataques conocidos que aprovechan debilidad en las credenciales y de *Cross-Site Scripting* persistente.

• El 70% de los dispositivos utiliza servicios de red no cifrados y envían las credenciales en texto plano.

• El 90% de los dispositivos recoge algún tipo de información personal a través del propio dispositivo, la nube o de la aplicación móvil asociada.

Desde el lado de la Ciberdefensa, nos gustaría pensar que se trata de casos aislados y que estas vulnerabilidades no se repiten sistemáticamente. También nos gustaría pensar que en sistemas industriales y empresariales los fabricantes

ponen muchísimo más cuidado en estos temas.

Sobre lo primero, la experiencia nos dice que no es así. La competitividad exige un rápido despliegue de los productos en el mercado y algunos fabricantes con menos escrúpulos dejan la seguridad para el final del desarrollo o no la tienen en cuenta en absoluto. Al fin y al cabo, el producto funciona y produce el resultado esperado incluso sin las medidas de seguridad. ¿O no? En este caso, está claro que su gestión de riesgos no incluye, por ejemplo, el impacto sobre el consumidor final de estos dispositivos, que es quien sufre las consecuencias de esa transferencia del riesgo.

No podemos olvidar que estamos en una industria a la que las leyes aún le permiten licencias del tipo "*this product is sold AS-IS*" (este producto se vende "tal cual") y en las que las garantías para el consumidor son mínimas en caso de que el producto no se comporte de la manera esperada o que incluso provoque daños materiales o personales. Eso, además, con la extensión generalizada de la idea entre los consumidores de que la tecnología falla "porque sí" e incluso una aceptación de esto como un hecho que no tiene solución.

Pero es que, incluso, en dispositivos creados específicamente para la Ciberdefensa donde las arquitecturas que se diseñan tratan la seguridad de la información de forma muy particular y específica, las pruebas que se realizan en este campo no son comparables a otros entornos y los controles son mucho más estrictos. A pesar de ello, muchas veces nos encontramos con estas claras deficiencias.

Desde nuestro punto de vista, tanto los consumidores como los propios clientes finales de estos servicios y sistemas han de ejercer una presión adecuada y constante para impedir la generalización de estos comportamientos y favorecer a aquellos fabricantes que sí tienen en cuenta estos aspectos. Si hablamos de sistemas específicos de soporte a la Defensa, si bien es cierto que para los elementos diseñados específicamente para este entorno los fabricantes ponen mucho más cuidado en cumplir con unos rigurosos requisitos de seguridad, también es cierto que es muy frecuente que se introduzcan en los diseños otros elementos no diseñados específicamente para estos entornos sino para el mercado de consumo. Los motivos son variados, siendo uno de los más utilizados el ahorro en costes, un ahorro que no justifica en muchas ocasiones el incremento del riesgo.

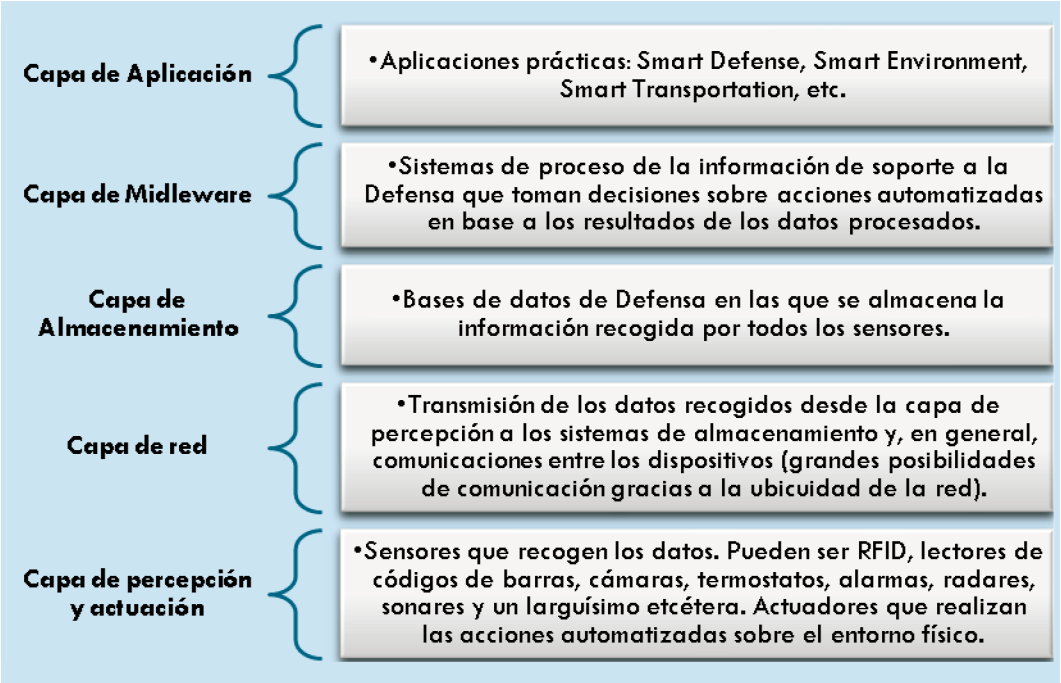


**Figura 2.- Visión detallada de la Arquitectura de un sistema IoT en Ciberdefensa.**

***IoT va a constituirse en uno de los principales motores de cambio de la Ciberdefensa en el futuro. Y no basta con afrontar iniciativas a largo plazo o programas de I+D+i ambiciosos, que también, sino que es totalmente necesario realizar desde ya y con premura cambios importantes.***

A modo simplificado y sin pretender profundizar más, por el momento, la **Figura 1** muestra las diferentes capas que son analizadas del concepto IoT en el campo de la Ciberdefensa.

La **Figura 2** muestra las principales características de cada una de ellas. Estas capas, además, están soportadas por una serie de tecnologías que destacaremos como parte del ecosistema, que junto con IoT, proporcionan las principales capacidades más demandadas en el entorno de la Defensa: la computación en la nube, el *Big Data*, las técnicas analíticas de datos, los protocolos de comunicaciones entre máquinas M2M y los sistemas Multiagente.

En posteriores artículos iremos desgranando, desde un punto de vista más técnico, todas estas implicaciones. No obstante, recomendamos al lector la revisión de un artículo parcialmente relacionado con estos temas, en su parte más tecnológica, publicado en la revista SIC de noviembre de 2014 (número 111) con el título "Entornos de Sistemas Multiagente y Ciber-Físicos en la Ciberdefensa".

## Conclusiones

En el artículo hemos expuesto el concepto de *Internet of the Things* y sus implicaciones en la Ciberdefensa a nivel de riesgos relacionados con la seguridad de la información. También hemos descrito desde la perspectiva de la arquitectura de sistemas cómo se afronta su análisis en el campo de la Ciberdefensa.

Desde nuestro punto de vista, y como ya se ha expuesto, este concepto va a constituirse en uno de los principales motores de cambio de la Ciberdefensa en el futuro. Pero no basta con afrontar iniciativas a largo plazo o programas de I+D+i ambiciosos, que también, sino que es totalmente necesario realizar desde ya y con premura cambios importantes en los elementos de soporte a la Ciberdefensa, incluyendo estrategias, políticas, procedimientos, programas, proyectos, tecnologías y gestión, para poder dar respuestas a los nuevos riesgos introducidos. ■

**Vicente José Pastor Pérez**
Jefe de Servicios de Seguridad Empresariales
Capacidad de Respuesta a Incidentes
de Seguridad Informática de la OTAN (NCIRC)
**OTAN**

**Dr. José Ramón Coz Fernández**
Auditor de Proyectos de Ciberseguridad
Service Security Manager en la BI_SC
Programme Management Integration Capability (PMIC)
NATO Communications and Information Agency
**ISDEFE**