derecom

ISSN: 1988-2629. No. 11. Nueva Época. Septiembre-Noviembre, 2012

La ciberguerra: los casos de Stuxnet y Anonymous

Gema Sánchez Medero[1]

Resumen

En un mundo tan hiperconectado, el ciberespacio ofrece medios para realizar ataques organizados a distancia. Además, permite a los agresores esconder sus identidades, localizaciones y rutas de entrada. Solamente es necesario disponer de la tecnología y conocimientos necesarios. Por tanto, es un medio más barato, difícil de contratacar y con menor riesgo que muchos otros, y además, prácticamente, puede ocasionar los mismos daños que cualquier acción bélica tradicional. De ahí que, a lo largo de este artículo, nos hayamos dedicado a estudiar que es la ciberguerra y la ciberseguridad, para determinar si los casos Stuxnet y Anonymous son actos de ciberguerra, y qué tipo de medidas deben adoptarse para evitar, en la medida que sea posible, este tipo de acciones.

Palabras clave

Ciberguerra, ciberseguridad, stuxnet y anonymous

Abastract

In a world so hyperconnected, cyberspace provides organized facilities for remote attacks also allows attackers to hide their identities, locations and routes of entry. It is only necessary to have the technology and knowledge. Therefore, it is a cheaper way, hard to fight back, and with lower risk than many others, and also, and practically, can cause the same damage as any traditional military action. Hence, throughout this article we have been studying it cyberwarfare and cybersecurity, to determine whether cases such as Stuxnet and Anonymous, are acts of cyberwar, and what sort of measures should be taken to avoid, as far possible, this type of action.

Keywords

Cyberwar, cybersecurity, stuxnet y anonymous.

1. Introducción

En la última película de Bruce Willis, la "Jungla de Cristal 4", un *hacker* lanza un ataque masivo a los sistemas informáticos de Estados Unidos para controlar Internet, el tráfico, los móviles, los sistemas de seguridad, etc, dejando al país a su merced, y generando un enorme pánico entre la población. Esto es mera ficción, pero cada vez son más lo que hablan de un posible ataque ciberterrorista. Aunque todavía ningún país ha registrado uno

[1] Prof. de Ciencia Política y de la Administración en la Universidad Complutense de Madrid. Doctora en Ciencias Políticas y de la Administración por la Universidad Complutense de Madrid. gsmedero@cps.ucm.es

que haya afectado a sus instalaciones críticas. Es cierto que diariamente se producen ataques a sistemas operativos de diferentes organismos o instituciones, pero no pueden ser considerados propiamente como ciberguerra o ciberterrorismo, sino más bien como acciones realizadas por *hackers* (Sánchez Medero, 2008: 15).

En cualquier caso, ya son muchos los que se aventuran a pronosticar que la guerra del siglo XXI se librará en el ciberespacio. Eso no significa que la guerra tradicional desaparezca, pero sí que la ciberguerra irá ganando espacio en los conflictos internacionales. Dada cuenta que como señala John Arquilla es "una guerra mejor, más barata y menos sangrienta", y que puede ser tan efectiva como una guerra convencional. Y para ello, solamente es necesario disponer de la tecnología y los conocimientos precisos para perpetuarlos. Por tanto, los ciberataques pueden originarse desde cualquier parte del mundo, e incluso simultáneamente desde diferentes lugares unos de otros. De tal manera, que cualquier cibersolado puede dejar, por ejemplo, sin comunicación, electricidad o transporte a una ciudad entera, o enviar información falsa a las computadoras del adversario e inutilizar sus baterías antiaéreas instantes antes de disparar, o penetrar una red informática ilegalmente e introducir virus capaces de infectar miles de computadoras en sólo segundos, sin prácticamente riesgo de ser detectado ni detenido, por no hablar de las pérdidas que podrían ocasionar y los efectos psicológicos que podrían producir entre la ciudadanía.

De ahí que, cada vez más, los Estados desarrollados estén prestando más atención a sus sistemas de ciberseguridad. Es más, muchos de ellos se han dedicado a crear toda una infraestructura de seguridad cibernética. Aunque también es cierto, que aún son muchos los países que no son conscientes de las consecuencias potenciales de un posible ataque cibernético, es más no muestran intención de prepararse para ello. Por lo tanto, a lo largo de este artículo nos hemos dedicado a analizar que es la ciberguerra, y hasta qué punto estos dos últimos fenómenos cibernéticos que se han producido, Stuxnet y Anonymous, pueden ser considerados como conflictos de una guerra cibernética.

2. La ciberguerra

La ciberguerra puede ser entendida como una agresión promovida por un Estado y dirigida a dañar gravemente las capacidades de otro para imponerle la aceptación de un objetivo propio o, simplemente, para sustraer información, cortar o destruir sus sistemas de comunicación, alterar sus bases de datos, es decir, lo que habitualmente hemos entendido como guerra, pero con la diferencia de que el medio empleado no sería la violencia física sino un ataque informático que va desde "la infiltración en los sistemas informáticos enemigos para obtener información hasta el control de proyectiles mediante computadores, pasando por la planificación de las operaciones, la gestión del abastecimiento", etc (Colle, 2000). No obstante, para los que consideran que la *cyberwar* y la *netwar* son una misma cosa, hay que puntualizar: la ciberguerra es la utilización de todas las herramientas electrónicas e informáticas para derrumbar los sistemas electrónicos y de comunicación del enemigo y mantener operativos los propios (Sánchez Medero, 2008: 15).

En todo caso, si tuviéramos que enumerar las características de una guerra cibernética éstas serían: complejidad, asimetría, objetivos limitados, corta duración, menor daño físico para los soldados, mayor espacio de combate y menor densidad de tropas, transparencia, lucha intensa por la superioridad de la información, aumento de la integración, mayores exigencias impuestas a los comandantes, nuevos aspectos de la concentración de fuerzas, reacción rápida, e igual de devastadora que una guerra

convencional (Thomas, 2001). Pero tal vez, de todas ellas, la más importante sea la de asimetría, porque la guerra cibernética proporciona los instrumentos necesarios para que los más pequeños puedan enfrentarse, incluso vencer y mostrarse superiores a los más grandes, con unos riesgos mínimos para ellos, sólo siendo necesario un ordenador y unos avanzados conocimientos informáticos. Más, cuando los objetivos de este tipo de guerra son: 1) Dañar un sistema o entidad hasta el punto en que ya no puede funcionar ni ser restaurado a una condición útil sin que lo reconstruyan por completo; 2) Interrumpir o romper el flujo de la información; 3) Destruir físicamente la información del adversario; 4) Reducir la efectividad o eficiencia de los sistemas de comunicación del adversario y sus capacidades de recolección de información, 5) Impedir al adversario acceder y utilizar los sistemas y servicios críticos; 6) Engañar a los adversarios; 7) Lograr acceder a los sistemas del enemigo y robarles información; 8) Proteger sus sistemas y restaurar los sistemas atacados; 8) Responder rápidamente a los ataques o invasiones del adversario.

3. La ciberseguridad

El término "ciberseguridad" se define normalmente como la protección de datos, información y sistemas conectados a Internet. No es fácil englobar una materia tan compleja en una definición tan sencilla, pues el concepto extiende el de seguridad clásica a otras nociones más propias del ciberespacio, como integridad, disponibilidad, autenticidad, confidencialidad o la mencionada denegación del servicio. Tal es así, que en un primer momento, la ciberseguridad obedecía a un enfoque de protección de la información (*Information Security*) donde solamente había que proteger la información de los accesos, usos, revelaciones, interrupciones, modificaciones o destrucciones no permitidas (Fojón, 2010, 2). Mientras que ahora, este enfoque está evolucionando hacia la gestión de riesgos del ciberespacio (*Information Assurance*) donde la ciberseguridad consiste en la aplicación de un proceso de análisis y gestión de los riesgos relacionados con el uso, procesamiento, almacenamiento y transmisión de información o datos y los sistemas y procesos usados basándose en los estándares internacionalmente aceptados (Fojón, 2010, 2). Por tanto, es importante para los Estados disponer de estructuras organizativas nacionales, regionales e internacionales, para fortalecer su ciberseguridad y luchar contra la ciberdelincuencia.

Así, ante el temor de las posibles consecuencias de un hipotético ataque cibernético, países como EEUU, Francia, el Reino Unido, Israel y Corea del Sur, y algunas organizaciones internacionales como la ONU y la OTAN, estén tomando conciencia de la importancia y necesidad de un ciberespacio seguro y, por ello, se están desarrollando marcos normativos, planes y estrategias específicas para la defensa del ciberespacio (Fojón, 2010, 2), es decir, medidas y acciones dirigidas a: educar, formar y concienciar a todos los agentes de la ciberseguridad; establecer estructuras que puedan funcionar como centro de alerta y de gestión de crisis a nivel nacional; agrupar los medios a implementar para utilizarlos y compartirlos para un conjunto de países o para una región; imponer sistemas de vigilancia y control; desarrollar las competencias de un equipo de ciberpolicía que pueda contribuir a la persecución e investigación de los delitos informáticos en el ámbito de la cooperación internacional; proponer soluciones tecnológicas en lo que se refiere a la gestión de identidades, el control de acceso, la utilización de plataformas materiales y de aplicaciones informáticas seguras, las infraestructuras de respaldo, los protocolos criptográficos y la gestión operacional, etc (UIT, 2007: 13). Y todo con el fin de establecer una línea de defensa común y homogénea, mejorar las capacidades de detección y reacción, concienciar y proporcionar apoyo a los ciudadanos para hacer más segura su actividad en línea (on-line), así como reforzar la capacidad de las fuerzas y cuerpos de seguridad del Estado para combatir el cibercrimen y fortalecer el entorno futuro de la ciberseguridad.

Por otro lado, países como China, Irán, Corea del Norte, Rusia y Pakistán han reconocido su interés estratégico en el ciberespacio como vehículo para alcanzar posiciones de liderazgo económico y político en sus áreas geográficas de influencia, y lo están concretando en la definición de políticas, en la ejecución de grandes inversiones económicas destinadas a recursos TIC y en la formación de recursos humanos, con el objetivo de establecer "una defensa beligerante" de su ciberespacio (Fojón, 2010, 2). Para ello, se están dedicando a incrementar el número de especialistas en seguridad de las TIC, impulsar y coordinar los esfuerzos de investigación y desarrollo de productos de seguridad y ataque nacionales, y definir estrategias que disuadan la actividad hostil o dañina en el ciberespacio.

4. Ataques cibernéticos

Hoy en día todavía no ha habido ningún ataque que nos permita hablar de ciberguerra propiamente dicha, ya que no se ha registrado ninguno que haya afectado a las instalaciones o infraestructuras críticas. Eso sí, cada día se producen miles de ataques e intrusiones que, sin generar los efectos y las características que se atribuyen a la guerra cibernética, causan daños políticos, económicos y psicológicos, como se puede comprobar en los siguientes ejemplos que se han producido en los últimos años:

Década de 1980
La National Security Agency (NSA) intercepta mensajes encriptados de Libia, Irán y de decenas de países, gracias a sus tratos con la empresa Suiza Crypto AG, que vende programas de criptología con puertas traseras sólo conocidas por la agencia norteamericana.
La NSA pone en marcha la red Echelon (con precursoras conocidas desde 1952), destinada a espiar las comunicaciones telefónicas, por satélite e Internet.
En plena guerra fría, cinco hackers alemanes robaron información de sitios militares norteamericanos y franceses, y la vendieron a la KGB.
Un grupo terrorista conocido como "Middle Core Faction" atacó el sistema que controlaba los ferrocarriles de alta velocidad japoneses. Para ello, en primer lugar, cortaron el suministro eléctrico y los cables de control informatizados del ferrocarril, y posteriormente, interceptaron y perturbaron las radiocomunicaciones de la policía para anticipar y ralentizar la capacidad de respuesta de las autoridades. Aunque nadie resultó herido con la acción, ésta afectó a 6´5 millones de usuarios del ferrocarril japonés y costó a la compañía aproximadamente 6 millones de dólares.
Década de 1990
La Guerra del Golfo es considerada tradicionalmente como el inicio de la era de la infoguerra. En ella, aviones armados con municiones de precisión atacaron la red de telecomunicaciones y energía eléctrica de Bagdad, con especial saña contra los centros informáticos de la policía secreta iraquí. Además, según el Pentágono, un grupo de hackers holandeses se ofreció a Saddam para romper el sistema militar norteamericano en Oriente Medio.
Según los medios de comunicación, alguien penetró en los servidores militares estadounidenses y alteró los archivos médicos de los soldados. Entre otras cosas, cambiaron los tipos de sangre, información crucial para una transfusión durante una batalla.
El grupo guerrillero tamil Liberation Tigers fue el primer grupo terrorista en atacar, a través de Internet, objetivos estadounidenses lanzando un "mailbombing" contra ordenadores gubernamentales.
La Whale and Dolphin Conservation Society, una organización británica para la

preservación de los mamíferos marinos, detectó intentos de entrada en sus ordenadores provenientes de la Marina de los Estados Unidos. El objetivo era robar un informe sobre delfines adiestrados para fines militares en el Mar Negro
El grupo Masters of Downloading aseguraba haber robado programas militares para submarinos, satélites GPS y redes informáticas del Pentágono. El presunto terrorista Khalid Ibrahim, del grupo separatista indio Harkat-ul-Ansar, intentó contactar con uno de ellos por IRC para cobrar una recompensa a cambio de algunos programas.
Guerra Serbia-Croacia en la red. El grupo de hackers serbios Black Hand atacó el Centro de Informática de Kosovo, universidades y la versión en línea del periódico "Vjesnik". La respuesta croata fue entrar en el sitio web de la Biblioteca Serbia. La reacción del Black Hand fue robar el fichero de contraseñas del Rudjer Boskovic Institute, incluso se rumoreó que consiguieron entrar en el proveedor de acceso más importante de Croacia. Por el contrario, los hackers croatas se introdujeron en dos servidores serbios.
La guerra de Kosovo también se produjo en la red. Hackers rusos, yugoslavos y norteamericanos llenaron páginas de grafitis a favor y en contra de Milosevic o la OTAN. La red se utilizó para poner en contacto a los de dentro y los de fuera del territorio. Nacieron nuevos foros de discusión. La información de la guerra voló por las listas, discutiéndose en ellos todos los sucesos acontecidos. La red se llenó de propaganda.
Década de 2000
La ciudad de New York quedó sumida en el caos como consecuencia del mayor apagón en la historia de Estados Unidos, que afectó a casi toda la región noreste del país, además de Canadá.
Un apagón de 34 minutos en el sur de Londres trastornó la red del metro de la ciudad y el sistema de trenes en el sur de Inglaterra, afectando a medio millón de personas y la mayoría de los servicios en el centro de la capital británica. El 60 por ciento de las estaciones del metro tuvo que cerrar, sobre todo en el sur de la ciudad. La Policía dijo que alrededor de 270 semáforos se apagaron, y aunque esta falla se remedió con rapidez, no dejó de añadir su dosis de estrés en las calles afectadas.
Guerra de Gaza. En el portal de Youtube el ejército israelí colgó vídeos en los que se insistía en que Hamas era una organización terrorista que usaba a los civiles como "escudos humanos" y a las mezquitas, para esconder armas. Su vídeo más visto fue, con más de 600.000 visitas, un ataque israelí contra un centro de almacén de misiles palestinos "destinados a civiles inocentes". Los palestinos contraatacaron subiendo al portal PalTube vídeos donde se denunciaba la "masacre" que estaba cometiendo el ejército israelí en Gaza.
En Estonia las páginas oficiales de varios departamentos estonios, las del Gobierno y las del gobernante Partido de las Reformas quedaron paralizadas por ataques informáticos provenientes del exterior. Al mismo tiempo que los sistemas de algunos bancos y periódicos resultaron bloqueados durante varias horas por una serie de ataques distribuidos de denegación de servicio (DDoS), hecho que se produjo justo después de que Rusia presionara a Estonia por la retirada de las calles de Tallin de un monumento de la época soviética. De ahí que Estonia acusará al gobierno ruso de estar detrás de estos ataques, aunque el Kremlin siempre negó su implicación en el asunto.
Una red informática del Pentágono sufrió un ataque lanzado por hackers desde China que se convirtió en "uno de los ciberataques de más éxito" al Departamento de Defensa de los Estados Unidos. Aunque es cuestionable la cantidad de información confidencial que se robó, el incidente aumentó el nivel de preocupación, al poner de relieve cómo se podían interrumpir sistemas en momentos críticos.
El prestigioso semanario alemán Der Spiegel indicó que se pensaba que China había

atacado sistemas informáticos de la Cancillería alemana, así como sistemas de tres ministerios, e infectado las redes con programas espía. Los supuestos ataques se dirigieron a los ordenadores de la Cancillería y de los Ministerios de Asuntos Exteriores, Economía e Investigación.
En India, el Centro Nacional de Informática (NIC) sufrió ataques desde conexiones telefónicas a Internet en China. Destacados miembros del servicio de inteligencia afirmaron que los hackers accedieron a las cuentas de correo electrónico de 200 ministros, burócratas y funcionarios de defensa, y continuaron atacando servidores indios al ritmo de tres o cuatro al día. China ha negado todas las acusaciones de estar detrás de los ataques.
Asia Pacific News informó de que unos hackers chinos habían intentado supuestamente acceder a las redes informáticas estatales de alto secreto de Australia y Nueva Zelanda, como parte de una operación internacional más amplia para conocer secretos militares de países occidentales.
Google denunció el 12 de enero de 2010 que había sido blanco de ciberataques, probablemente procedentes de China, para acceder a la correspondencia de disidentes y robar a la empresa códigos y secretos comerciales.
Un experto en informática "hackeó" temporalmente el sitio de microblogs Twitter.com, redireccionando a los usuarios a una página en Internet y señalando que representaba un grupo que se hace llamar Ejército Cibernético de Irán.

Fuente: Elaboración propia.

Por tanto, se puede decir que hasta el momento se está haciendo un uso pasivo de la red que se limita, en la mayoría de los casos, al espionaje, a dañar sistemas de comunicación, generar confusión y desinformación, bloquear páginas web, es decir, pequeñas acciones si las comparamos con las acciones que podría generar una verdadera guerra cibernética.

5. Stuxnet

Durante el año 2010 se descubrió una ciberamenaza que cambiaría las reglas de juego del ciberespacio desatando la alarma de los expertos a medida que es analizado y se constata la extremada sofisticación de su diseño. Se trata de Stuxnet, un software malicioso que es detectado por primera vez en junio de 2010, por la empresa VirusBlokAda (empresa de seguridad radicada en Bielorrusia), aunque se presupone que puede haber estado trabajando en la sombra durantes meses e incluso años. Stuxnet es el primer gusano informático que, aprovechando la vulnerabilidad MS10-0466 de los sistemas operativos Windows CC, empleados en los sistemas SCADA (*Supervisory Control and Data Acquisition*), fabricados por Siemens, se emplea para atacar las infraestructuras críticas tales como el control de oleoductos, plataformas petroleras, centrales eléctricas, centrales nucleares y otras instalaciones industriales con el objetivo de sabotearlos (Joyanes, 2010). Este tipo de troyano no utiliza Internet para propagarse, sino que lo hace a través de lápices de memoria de tipo USB. Primero, el virus se oculta mediante un *rootkit*[2] a nivel de *kernel*[3] firmando con certificados robados a los fabricantes de hardware JMcron y Realtek, lo que implica también que previamente tuvo que realizarse un ataque a estas empresas para substraer dicho material criptográfico. Después, queda camuflado y latente en el equipo infectado hasta que su autor decide activarlo, entonces es cuando comienza a multiplicarse a sí mismo, pasando de un ordenador a otro, permitiendo al intruso mantener el acceso al programa, para accionar o extraer información sensible de forma remota, reprogramar los controladores lógicos programables y ocultar los cambios realizados. No obstante, hay que

[2] El rootkit es un programa que sirve para acceder de manera ilícita a un sistema informático.
[3] Es un software que se emplea para facilitar el acceso seguro a los distintos programas.

señalar que los métodos que emplea para propagase son: 1) Mediante el fichero *"autorun.inf"*, vulnerabilidad conocida desde hace tiempo, y que sólo se utilizaba en las primeras versiones del malware. –a través de una "nueva vulnerabilidad LNK"[4] aprovechando una de las vulnerabilidades de *"dia 0"*[5] que provocaba que, con solo visualizar en Windows "Explorar los ficheros de acceso directo", se ejecuta automáticamente el código del fichero al que hace referencia dicho acceso directo (Pastor, 2011: 81), y 2), a través de recursos de red compartidos, en los que la máquina infectada tiene permisos de escritura, aprovechando una vulnerabilidad conocida y utilizada por otros gusanos como *"conficker"*[6].

Pero lo que hace realmente original a este troyano es que es el primer *rootkit* diseñado específicamente para atacar el sistema SCADA, y principalmente, explota hasta cuatro vulnerabilidades de "días 0", es decir, vulnerabilidades aún desconocidas en las aplicaciones informáticas. Lo curioso es que este tipo de troyanos no están destinados a la infección masiva de ordenadores domésticos sino que están pensados para atacar un programa concreto de la marca Siemens (sistema SCADA) que se utiliza para controlar las infraestructuras críticas, de tal manera, que se podría aumentar o disminuir el caudal de un oleoducto o dañar una central nuclear (Joyanes, 2010).

Así, Stuxnet ya es considerado como la mejor arma cibernética jamás creada, al haber dejado fuera de combate a un 20% de las centrifugadoras. Téngase en cuenta que Israel siempre se ha mostrado contraria a la proliferación de este tipo de armamento entre el resto de países de la región, al considerarlo que amenaza su propia existencia como país. Por eso ha hecho todo lo que ha estado en su mano para impedir este desarrollo. Incluso ha llevado a cabo ataques aéreos preventivos por sorpresa contra reactores nucleares en Irak, Siria, Sudán, etc. El problema es con Irán, porque su ruta área es mucho más larga. Además deberían sobrevolar naciones neutrales y, encima, sus instalaciones de enriquecimiento se encuentran bajo tierra. Una operación militarmente posible pero que podría tener más coste que beneficio, dado el riesgo operativo y el coste político. Por tanto, Stuxnet se ha convertido en un arma casi perfecta. En primer lugar, ha provocado daños en las centrifugadoras, como han reconocido los propios iraníes, con todo lo que ello supone para la carrera nuclear que está llevando a cabo Irán: bloqueo y retraso. En segundo lugar, la creación de este troyano habría llevado seis meses para un equipo de cinco personas, por lo tanto, estamos hablando de unos costes muy bajos para un Estado. Y en tercer lugar, puede alcanzar unos objetivos que son invulnerables por otros medios, y además el uso de esta ciberarma no limita el empleo simultáneo de tácticas más convencionales. De ahí que no sea de extrañar que en futuro muy próximo se utilicen ciberarmas como alternativa a las operaciones militares clásicas. Es más, ya tenemos una nueva versión del patógeno gusano, al que los expertos en seguridad han denominado *"Duqu"*, un virus que está diseñado para robar la información necesaria para organizar un ataque como el llevado a cabo por su predecesor.

5. Anonymous

Anonymous es un seudónimo que emplean diferentes grupos e individuos en todo el mundo para realizar acciones informáticas en su nombre en aras de la libertad de expresión, de la independencia de Internet y en contra de diversas organizaciones. En un primer

[4] La vulnerabilidad LNK (archivos de acceso directos) permite la ejecución del código aunque el Autoplay y Autorun se encuentren desactivados.
[5] Los ataques día-cero ocurren cuando una vulnerabilidad tiene una ventana de tiempo existente entre el tiempo en el que se publica la amenaza y el tiempo que se publican los parches para solucionarla.
[6] Es un gusano informático que explota una vulnerabilidad en el servicio Windows Server.

momento Anonymous sólo actuaba en la red, pero con el tiempo ha combinado sus acciones en Internet con la programación y organización de manifestaciones en la calle. En todo caso, Anonymous se organiza de manera difusa en la red, no tiene líderes, ni tampoco instancias controladoras, ni jerarquías, su poder reside en la fuerza colectiva de sus participantes individuales. Por lo tanto, resulta muy difícil de ser contrarrestada y bloqueada por las fuerzas de seguridad y orden.

Las acciones de Anonymous son llevadas a cabo de forma que no parecen seguir una agenda única compartida ni sincronizada. En todo caso, si hoy conocemos a Anonymous es por la campaña de protesta que protagonizó contra la Iglesia de la Cienciología. El proyecto Chanology organizaba ataques de denegación de servicio contra las páginas web de la mencionada iglesia, pero también realizándoles bromas telefónicas, o envíos de "faxes negros", o colgando videos en youtube en los que convocaban protestas o explicaban su posición contra esta organización. Pero también han atacado a la plataforma youtube, al subir varios videos pornográficos que fueron disfrazados como contenido para niños usando tags como "Jonas Brothers"; o a la compañía Aiplex Software por no responder a la advertencia de cierre, o a las web del Senado Español, el Partido Popular, la Academia del Cine, la Diputación de Jaén, como reacción a la aprobación de la Ley Sinde; o a las páginas de las web del Ministerio de Información egipcio y del partido del Presidente Hosni Mubarak como una forma de apoyar a las manifestaciones que pedían la dimisión del presidente; o a la empresa Sony como respuesta a las acciones emprendidas por la mencionada empresa contra los usuarios "Geohot" y ""Graf-Chokolo", los cuales lograron hackear la PS3; o a la web del Ministerio de Interior y de Justicia en Colombia en represalia por un proyecto de ley, impulsado por dicho ministerio, que buscaba dar cárcel a quien incurriera en la piratería en Internet; etc. Pero Anonymous no solo se ha dedicado a atacar webs, sino que también ha hecho diversas reivindicaciones de apoyo, como han sido a las manifestaciones árabes, las protestas del 15-M o Wikileaks, etc; o de protesta contra las redes sociales por sus reiteradas violaciones de la privacidad y por vender información a los usuarios de forma ilegal, y contra todos los gobiernos, organizaciones o agencias que traten de coartar la libertad en la red.

Así, podemos llegar a afirmar que Anonymous son una especie de cibersoldados que luchan en la red por unos principios que consideran necesarios defender, en aras de un Internet libre y sin cortapisas. Un ejército difícil de contrabandear, y que cada día parece contar con un mayor número de adeptos. Un ejército que ataca y se esconde, pero que de momento se ha limitado a realizar acciones de bloqueo o de desinformación, causando daños económicos y políticos pero, en ningún caso, pérdidas humanas ni materiales. Por tanto, una guerra en la red pero no una ciberguerra.

6. Conclusiones

Hoy en día Internet conecta a millones de redes, incluidas aquellas que hacen funcionar infraestructuras y servicios esenciales. De modo que la economía y la seguridad nacional dependen en gran medida de las tecnologías de la información y de la infraestructura de comunicaciones. Es cierto, como se ha dejado patente a lo largo de este artículo, no se ha producido ningún conflicto que se pueda calificar como una verdadera ciberguerra, aunque los casos de Stuxnet y Anonymous se encuentran cerca de ello. Por tanto, es lógico que estas dos cuestiones, la ciberdefensa y el ciberataque, hayan entrado a formar parte de la agenda política de los gobiernos, dada cuenta que, como sostiene William Crowell, exsubdirector de la Agencia para la Seguridad Nacional, "en el curso de los próximos veinte

o treinta años, el papel de los ciberataques en caso de guerra cobrará cada vez más importancia".

Y para garantizar la seguridad de los ordenadores no hay nada mejor que apagar el ordenador. El problema es que hoy en día eso parece imposible y, por eso, se están activando otras acciones que pueden contribuir a frenar este tipo de ataques y sus consecuencias, como dotarse de medios de seguridad especializados en ciberdefensa para reducir las amenazas y las vulnerabilidades de los mismos, aunque siempre considerando que existe la posibilidad de que sean vulnerados. En este sentido, el intercambio de información entre los actores víctimas de ataques puede ser fundamental, aunque eso siempre es difícil por el miedo que existe a que se filtren datos confidenciales, se conozcan las vulnerabilidades, etc. Otra posible operación es establecer planes de asistencia mutua entre los diferentes componentes de las infraestructuras críticas, de modo que se reduzcan los efectos en cascada debido a su interrelación. Eso sí, todos estos planes deben ser coordinados por un órgano superior a nivel nacional, que debe depender directamente del Departamento Gubernamental encargado de la seguridad del ciberespacio (Puime, 2009: 57). Otra es identificar las vulnerabilidades e individualizar los peligros existentes y potenciales que dichas debilidades permiten. Esto sólo se puede conseguir con la ciberinteligencia. El problema que se plantea es que Internet carece de fronteras y el contenido ilícito circula de un país a otro en milésimas de segundos. Además existe una escasa o nula regulación de los cibercafés, locutorios, salas de informática públicas, bibliotecas, centros educativos, máquinas populares de acceso a Internet y otras donde de forma anónima las personas puede conectarse y realizar actividades ilícitas (Sánchez Medero, 2009). Lo mismo ocurre con las redes inalámbricas libres al alcance de equipos con conexiones capaces de conectarse a esas redes con el anonimato de la no pertenencia al grupo autorizado (Ruiloba, 2006). Otra posible solución es empezar a endurecer la legislación que hace referencia a los delitos informáticos para paliar las posibles deficiencias jurídicas que existen en algunos países. Y otra, como algunos investigadores considera, es crear una segunda red extraordinariamente controlada y separada del Internet comercial (Waston, 2007).

Bibliografía

FOJÓN CHAMORRO, Enrique y SANZ VILLALBA, Ángel F. (2010). "Ciberseguridad en España: una propuesta para su gestión", en *ARI*, nº 101, junio. En: http://www.realinstitutoelcano.org/wps/wcm/connect/c1360e8042e4fcf49e51ff5cb2335b49/ARI102-2010_Fojon_Sanz_ciberseguridad_Espana.pdf?MOD=AJPERES&CACHEID=c1360e8042e4fcf49e51ff5cb2335b49

JOYANES AGUILAR, Luis. (2010). "Introducción. Estado del arte de la Ciberseguridad", en Cuadernos de Estrategia, *Ciberseguridad. Retos y amenazas a la seguridad nacional en el ciberespacio*, nº 149, diciembre, pp. 13-49.

PUIME MAROTO, Juan. (2009). "El ciberespionaje y la ciberseguridad", en CESEDEN, *La violencia del Siglo XXI. Nuevas dimensiones de la guerra*. Monografías del CESEDEN, nº 112, octubre, p. 42/70.

RUILOBA CASTILLA Juan Carlos. (2006). "La actuación policial frente a los déficits de seguridad de Internet", en *Revista de los Estudios de Derecho y Ciencia Política de la UOC*, nº 2.

SÁNCHEZ MEDERO Gema. (2008). "Ciberterrorismo. La guerra del Siglo XXI", en *El Viejo Topo*, nº 242, marzo, pp. 15-23.

SÁNCHEZ MEDERO Gema, (2009) "21st Century to two new challenges: Cyberwar and Cyberterrorism", en *Nómadas. Mediterranean Perspectives*, nº 1, mayo, pp. 1-10.

SÁNCHEZ MEDERO, Gema. (2009). "Ciberguerra y Ciberterrorismo ¿realidad o ficción? Una nueva forma de guerra asimétrica", en AMÉRIGO CUERVO-ARGANGO, F. y DE PEÑARANDA ALGAR, J. (Comp.) *Dos décadas de Posguerra Fría. Actas de I Jornadas de Estudios de Seguridad*. Madrid: Instituto Universitario General Gutiérrez Mellado-UNED, pp. 215/241.

UNIÓN INTERNACIONAL DE TELECOMUNICACIONES (UIT). (2007) *Guía de ciberseguridad para los países en desarrollo*. En: http://www.itu.int/ITU-D/cyb/publications/2007/cgdc-2007-s.pdf

WASTON Steve. (2007). "Científicos usamericanos quieren desembarazarse de la red de Internet", en *Rebelión*. En http://www.rebelion.org/noticia.php?id=49932.