Capítulo V

LOS RIESGOS ECONÓMICOS DE LA CIBERGUERRA

Henning Wegener

Resumen

La creciente aceptación e introducción de las tecnologías digitales en la planificación y el armamento militares da paso a la perspectiva de una ciberguerra en la cual, habida cuenta de la interdependencia global de las estructuras de red, podría, inevitable y profundamente, afectar a la economía y a esenciales activos de la sociedad.

La utilización militar hostil de estas tecnologías podría de hecho, y de derecho, no estar claramente diferenciada de los ciberconflictos de carácter general y despertar serias dudas sobre su control y legitimidad, abriendo así posibilidades ciertas de causar daños de importante consideración.

Existe el perenne dilema de que el crecimiento exponencial y el velocísimo desarrollo de las tecnologías cibernéticas y los nuevos usos sofisticados entren en conflicto con el crecimiento exponencial y la sofisticación de las posibilidades de ataques. El asombroso crecimiento cuantitativo y cualitativo de los sistemas y las infraestructuras cibernéticos hacia una *segunda revolución digital* viene acompañado de un crecimiento, igual o incluso superior, de posibles ataques y, con ellos, de vulnerabilidades.

Sin embargo, los beneficios de la era digital se acumulan solo si existe confianza en el funcionamiento, la fiabilidad, la integridad y la seguridad de las tecnologías subyacentes: es por ello que la seguridad digital se ha

convertido en un desafío global. Este artículo describe los presentes y posibles futuros desarrollos cibernéticos, así como el panorama de creciente amenaza en términos de nuevas formas de ataque, nuevos atacantes y nuevas dimensiones de riesgos y pérdidas económicas.

El artículo argumenta que el uso militar y deliberado de las nuevas tecnologías con fines cibernéticamente beligerantes o, cuando menos, su componente ofensivo debieran ser deslegitimados, o reducida su importancia; si bien el mejor proceder para todos los interesados, incluyendo los actores económicos, debería fundamentarse en optimizar las estrategias para evitar o reducir los posibles daños cibernéticos.

Los conceptos fundamentales –en toda forma de ciberconflicto– son: la autodefensa, la resistencia, la mejora en la seguridad de la industria de tecnologías de la información, la elaboración de normas que incluyan parámetros estándar de seguridad en la nube, redundancias técnicas, restricciones, cooperación nacional e internacional, respuestas de emergencia, intercambio efectivo de información y sistemas de alerta, incremento de los esfuerzos para armonizar las leyes penales y las sanciones en materia cibernética, avances en el refuerzo de la legislación internacional y el establecimiento de normas internacionales de conducta para la era cibernética. El artículo concluye subrayando la necesidad de crear una cultura de ciberseguridad y presenta unas líneas generales sobre los conceptos de ciberestabilidad y ciberpaz.

Palabras clave

Ciberguerra, ciberseguridad, ciberconflicto, ciberataque, infraestructura cibernética, infraestructura nacional crítica, nuevas tecnologías digitales, ciberlegislación, panorama de amenazas, resistencia, cultura de ciberseguridad, ciberley, ciberestabilidad, ciberpaz.

Abstract

The increasing acceptance and introduction of digital technologies in military planning and armament opens the perspective of a cyber warfare that, given the global interdependence of net structures, would unavoidably and deeply affect the economy and vital societal assets. Hostile military use of these technologies could, for factual and legal reasons, not be cleanly separated from cyber conflict in general and raises serious questions of controllability and legitimacy, thus opening up highly disturbing damage perspectives. There is the perennial dilemma that the exponential growth and ultra-rapid development of cyber technologies and new sophisticated uses are in conflict with the equally exponential growth and sophistication of attack options. The amazing quantitative and qualitative growth of cyber systems and cyber infrastructures in a *second digital revolution* comes accompanied by an equal or even superior growth in attack options and thus in vulnerabilities. Yet, the benefits of the digital age accrue only if there is trust in the functioning, reliability, integrity and safety of the underlying technologies: thus, cyber security has come to be a global challenge. The article describes actual and possible future cyber developments and the evolving threat landscape in terms of new attack modes, new perpetrators, and new dimensions of economic risk and loss.

The article argues that the deliberate military use of digital technologies in a cyber war mode should be delegitimized or that at least its offensive component be deemphasized, but that the best course for all stakeholders, including economic actors, would be to optimize strategies for the prevention and mitigation of cyber damage. The key concepts –for all forms of cyber conflict– are self-defense, resilience, security improvements in the IT industry, standard setting including standards for cloud safety, technical redundancies, constraint, national and international cooperation, emergency responses, effective information exchange and warning systems, increased efforts to harmonize cyber penal law and sanctions, advances in international law enforcement, and building international norms of behavior for the cyber age The article concludes emphasizing the need for a universal culture of cybersecurity, and offers an outline of a concept of cyber stability and «cyber peace».

Key word

Cyber war, cyber security, cyber conflict, cyber attack, cyber infrastructure, critical national infrastructure, new digital technologies, cyber law, threat landscape, resilience, culture of cyber security, cyber law, cyber stability, cyber peace.

Ciberguerra y ciberconflicto: la dimensión económica

Un número anterior de esta serie de *Cuadernos de Estrategia,* publicado en diciembre de 2010, centraba su análisis de las ciberamenazas en la dimensión de la seguridad nacional[1]; el presente ensayo examinará las consecuencias de la inseguridad cibernética y los ciberconflictos en la seguridad económica y en la inteligencia económica. Como quiera que las amenazas que subyacen son las mismas o similares, y considerando que la seguridad económica es, en definitiva, un ingrediente esencial para la seguridad nacional, este análisis servirá de aportación a la antedicha publicación, cuyo valor persiste con entera validez en el tiempo, no obstante lo cual, algunos desarrollos y cifras más recientes se han incorporado, como es natural.

Concebido literalmente, el tema que nos ocupa parece centrarse en los daños económicos que pueden resultar de un uso hostil de las tecnologías cibernéticas dentro de un contexto *militar,* lo cual podría suponer una relación directa entre la economía y la guerra.

Sin duda alguna, la historia nos demuestra que la guerra, tradicionalmente llevada a cabo con armas convencionales, ha representado siempre enormes riesgos y daños para los activos económicos de los países beligerantes:; tanto por sus efectos indirectos en las infraestructuras como en los hábitos de consumo, los procesos económicos y las relaciones comerciales, así como, en general, en el funcionamiento de las sociedades. También los daños secundarios «no intencionados», en los cuales los efectos sobre objetivos estrictamente militares han afectado ampliamente a la sociedad, incluyendo las infraestructuras básicas, así como aquellos que forman parte de una estrategia deliberada que persigue la destrucción de las redes de infraestructuras de países enemigos, con especial atención a la industria armamentística y la economía de guerra, o incluso aquellos destinados a quebrantar la moral del adversario y a minar el deseo de sus pueblos de luchar y resistir.

La guerra moderna ha absorbido de forma creciente a las sociedades en su conjunto. Su intencionado efecto destructivo y devastador culminó, sin duda, en la Segunda Guerra Mundial: una «guerra total» en la que el poder prácticamente ilimitado de los sistemas armamentísticos, incluidas las armas nucleares, y el deseo estratégico de los bandos supusieron la destrucción a gran escala de los territorios enemigos y sus activos económicos, incluyendo sus ciudades, poblaciones enteras, con nuevas dimensiones de violencia y sufrimiento humano.

[1] *Ciberseguridad, retos y amenazas a la seguridad nacional en el ciberespacio. Cuadernos de Estrategia,* n.º 149. Madrid: Instituto Español de Estudios Estratégicos, Ministerio de Defensa.

Al adentrarnos en la era digital, son otras las reglas que gobiernan. Los ataques digitales, incluyendo aquellos con objetivos militares, son, primordialmente, no violentos y de un coste relativamente bajo («bits en lugar de bombas»), y se desarrollan exclusivamente a través de la invasión electrónica de sistemas y estructuras de red. Esto es también aplicable a efectos militares. Las tecnologías de la información y comunicación (TIC) han revolucionado los asuntos militares, incluyendo la información sobre los campos de batalla y sus comunicaciones y los sistemas armamentísticos, al tiempo que han incrementado la vulnerabilidad a este tipo de invasiones.

Un ataque digital llega desde un enemigo invisible: es difícil de identificar y de seguir; es asimétrico, difícil de evaluar en lo que respecta a su amplitud y efectos finales, lo que hace incierto tratar de evaluar sus efectos más allá de las consecuencias económicamente mensurables. Si bien es cierto que de ello se desprende un menor derramamiento de sangre y una menor destrucción física, no lo es menos que sus consecuencias podrían, de hecho, ser desastrosas y dañar profundamente la economía.

En muchas ocasiones en las que autores se aventuran a definir la ciberguerra, esta es descrita como una acción política llevada a cabo por naciones cuyo fin es el de causar al adversario significativos daños militares: daños a redes informáticas militares, a sistemas de mando y control, a redes de defensa aérea y a sistemas de armamento centrados en redes, todo ello a través de medios digitales[2].

Más de cien países han reconocido haber establecido mandos cibernéticos y entendido que el ciberespacio es el quinto escenario bélico, tan esencial para las operaciones militares como las terrestres, marítimas, aéreas o espaciales. Es conocido que más de 30 han desarrollado doctrinas específicas sobre la ciberguerra y más de un centenar tienen la habilidad técnica para desarrollar ofensivas militares efectivas. El sentimiento generalizado es que la ciberguerra es una acción militar que supone una opción portentosa y real y, en consecuencia, debe ser tomada muy en serio; si bien los escenarios y predicciones acerca de su aceptación difieren.

Un asunto a tener en cuenta sobre esta materia es el crecimiento autónomo de los mandos cibernéticos y las doctrinas de ciberguerra aplicables que podrían seguir los esquemas militares al uso, que parecen padecer autismo, siendo así insensibles al contexto cibernético interconectado. El hecho de pensar en términos de ciberguerra podría conducir a una trampa terminológica; regresaremos a este preocupante aspecto.

[2] *Cyberwar*, Wikipedia. Ver también: GLENNY, Misha. «Das ende der nettigkeiten. Cyberkrieg und sicherheit im Internet». *Internationale Politik*, noviembre/diciembre de 2012, p. 80.

Sin embargo, una breve revisión y yuxtaposición de las diferentes definiciones de «ciberguerra» permite apreciar que estas clarifican poco y que, en el mejor de los casos, «ciberguerra» continúa siendo un término elusivo. La más simple y directa conclusión es que estamos hablando de ataques digitales a sistemas e infraestructuras cibernéticas.

Casi cualquier ulterior criterio de definición es susceptible de ser dudoso o ambivalente. ¿Ataques por motivos políticos?; si se trata de espionaje, incluido el ejercido contra industrias armamentísticas e infraestructuras nacionales, muchos de quienes los definen alegan que los motivos políticos y económicos están, por naturaleza, imbricados, por lo que el beneficio económico o los hurtos de datos informáticos bien pueden ser la causa principal[3].

El terrorismo informático (un concepto al que regresaremos en este análisis) tiene ciertamente motivaciones políticas, pero no persigue objetivos bélicos entre estados. ¿Acciones por parte de países o Gobiernos?; en efecto, los ataques pueden ser promovidos por países, pero el escenario más probable y efectivo es que una asociación criminal –si se quiere «mercenarios digitales»– son empleados, al menos como coadyuvantes, para infligir un desbaratamiento digital en perversas alianzas con estados turbios y el crimen organizado como proveedor de un «servicio de delitos».

Podrían darse ataques bajo «bandera falsa» cuando organismos estatales o no estatales llevasen a cabo un ataque informático haciéndose pasar por otros países: el malentendido resultante podría conducir a unas consecuencias que escapan a la imaginación, toda vez que los malentendidos que generalmente siguen a errores de atribución o a la imputación equivocada de una intromisión inocua pueden interpretarse como la preparación de un ataque a gran escala, que podría ser fatal.

Las ambigüedades son múltiples. ¿Objetivos militares? Indudablemente, si los Gobiernos dirigiesen un ataque concreto contra una nación enemi-

[3] Informes recientes acerca de la explotación cibernética por parte de China no solamente demuestran la enorme e indudablemente alarmante dimensión del espionaje cibernético procedente de aquel país, sino también la gran variedad de agentes que lo perpetran: grandes unidades de espionaje que roban borradores de proyectos tecnológicos, estrategias negociadoras, bases de datos corporativas y del Gobierno de los Estados Unidos del tamaño y cantidad de terabytes, los cuales son, en apariencia, oficiales contratados, en parte independientes, y, tal y como estos estudios afirman, están todos, si no conectados, al menos sí coordinados por una unidad del Ejército chino. Esta oscura relación muestra una mezcla de actores e intenciones que pone en duda la definición y convierte en ambivalente el término de «guerra cibernética». Ver: SANGER, David E., BARBOJA, David y PERLROTH, Nicole. «Chinese Army unit Is seen as tied to hacking against US» («Una unidad del Ejército chino es vista como ligada a hacking contra los Estados Unidos»). *New York Times,* 19 de febrero de 2013, y el *Mandiant report* allí citado y ampliamente comentado en otros órganos.

ga, los centros de cibermando podrían ser la punta de lanza de cualquier ataque; las instalaciones militares serían el centro de cualquier ataque, y los modernos sistemas militares centrados en redes serían con toda certeza el centro preferente.

Ahora bien, ¿qué hay del extenso espionaje militar e industrial? Un apunte esquemático de los principales escenarios prueba que el espectro de objetivos es mucho más amplio y que los planificadores militares de hecho incluyen la implicación de, como mínimo, las infraestructuras críticas, así como los sistemas de comunicaciones no militares dentro de sus listas de objetivos, en tanto que muchos de estos tienen un doble propósito.

Los cuatro escenarios más comúnmente mencionados en los análisis político-militares (la ciberguerra de Estonia de 2007, que incluía ataques masivos a instalaciones gubernamentales e importantes mediante una negación distribuida de saturación del servicio, la combinación de ataques cibernéticos y ataques convencionales en el conflicto de 2009 en Georgia, la persistente amenaza de bajo nivel de espionaje militar o la hipotética ciberguerra del «todo apagado» sobre los recursos de defensa, los gobiernos, la economía y las infraestructuras, tal y como lo describe de una forma un tanto sensacionalista en principio, pero a la postre realista, el análisis de Richard A. Clarke[4]) se definen como ataques con multiobjetivos: mitad civiles y mitad militares, y muestran que la ciberguerra en sentido estricto, desde su pura definición, es muy difícil de situar. La validez heurística del término «ciberguerra» y, en consecuencia, el concepto de la misma son muy limitados, por lo que una evaluación integral de conflictos y ciberamenazas resulta inevitable. Es exactamente esta perspectiva integral la que puede demostrar el enorme potencial destructor de un ataque informático de amplio espectro. Este autor no desea entrar en escenarios apocalípticos, pero la literatura que existe sobre posibles «Pearl Harbour» digitales no puede ser despreciada ni minusvalorada[5].

El factor clave que dificulta cualquier esfuerzo para definir la ciberguerra como una categoría distinta de conducta hostil subyace en la propia tecnología digital, ya que los medios de ataque civiles y militares son idénticos; casi siempre de doble uso, con independencia de los motivos u objetivos. Cualquier ataque a las omnipresentes estructuras de red afecta a todos los participantes digitales de forma imprevisible e incontrolable.

[4] CLARKE, Richard A. y KNAKE, Robert K. *Cyberwar. The next threat to national security and what to do about it* (La nueva amenaza a la seguridad y qué hacer con ella). Nueva York: 2010.

[5] Resulta difícil encontrar literatura reseñable que incluya cálculos y estimaciones fiables; no obstante, se puede dar por sentado que los Gobiernos y las instituciones de seguridad poseen amenazas sustanciales, ocultas los ojos del público.

Hasta ahora, uno puede lamentar la ausencia de una investigación sistemática del efecto cascada de un ciberataque militar limitado y de sus repercusiones internacionales; o, lo que es lo mismo, una escasez de predicciones acerca de la utilización básica de las armas cibernéticas[6]. La interdependencia digital entre varios sectores de la economía es susceptible de crear situaciones en las que el fallo de un sector no solamente puede dañar a otro, sino a varios al mismo tiempo, reforzando las retroalimentaciones. Por ello, está claro que el efecto cascada de cualquier ataque sobre los sistemas y estructuras de red en un mundo íntimamente interconectado puede ser enorme y, como quiera que los medios del atacante pueden también ponerse en riesgo, esto determina que, en el mejor de los casos, ese riesgo pueda ser disuasorio[7]. A lo largo de los tiempos, todos los esfuerzos para definir las «armas cibernéticas» han fracasado, aunque se ha conseguido identificar parcialmente algunos instrumentos de *software* dañino.

La realidad es, por consiguiente, que los ciberataques representan un mayor riesgo para la sociedad en su conjunto y para el tejido socioeconómico que lo que indica cualquier variante de las doctrinas, planificaciones y premoniciones militares.

La creciente dependencia de la tecnología digital sitúa a las instalaciones públicas y privadas, los suministros eléctricos, las telecomunicaciones, la banca y el mundo financiero, los transportes, la industria y las instalaciones médicas, la educación y los Gobiernos en la misma situación de riesgo que las instalaciones militares (más en las infraestructuras críticas que se detallan más adelante). Debemos hablar de una exposición integral de riesgos en nuestros países y sus economías. Desde esta perspectiva, las diferencias entre guerra, terrorismo y delitos cibernéticos se tornan borrosas, por lo que parece más adecuado hablar de ataques y

[6] El tan mencionado virus *stuxnet*, un *software* dañino muy sofisticado específicamente orientado a atacar los sistemas *software* de control producido por Siemens (SCADA) de las instalaciones de enriquecimiento nuclear en Irán, quiebra ese efecto cascada, y puede ser el precursor de ataques informáticos quirúrgicos muy precisos. En cualquier caso, los ataques mediante *stuxnet* no estaban orientados contra instalaciones militares y no aparecieron en Internet, sino que se produjeron a través de *pendrives* introducidos furtivamente en una planta en lo que representó más un problema de control de accesos físico y mal comportamiento interno. A este respecto, ver: FAREWELL, James P. y ROHOZINSKI, Rafal. «The new reality of cyber war» (La nueva realidad de la guerra cibernética). *Survival,* agosto-septiembre de 2012, p.107.

[7] El efecto cascada puede ser menos efectivo si los datos, por ejemplo datos militares, se gestionan a través de redes internas, o si otros elementos de segmentación de red han sido instalados. Sin embargo, el aislamiento es solo relativo, y la defensa de redes siempre debe combatir el mismo enemigo invisible. La misma lógica es aplicable con respecto a los presumibles planes de algunos países para operar por fuera de la estructura mundial de Internet, creando fronteras digitales nacionales en una era «ciberwestfaliana». Tales segmentaciones de red nacionales nunca se completarán, y serán, por ello, ineficaces.

conflictos cibernéticos cuando analizamos el amplio patrón de amenazas que crece ahora, y que influyen tan claramente en la economía. En lenguaje popular, la ciberguerra a menudo se ha entendido en amplio sentido como un reflejo del inespecífico y masivo pánico que un ciberconflicto despierta entre la ciudadanía. Estas intuiciones públicas demuestran que la seguridad, o mejor dicho, la inseguridad cibernética se encuentra entre uno de los grandes retos de nuestro tiempo.

Son estos amplios patrones de amenaza lo que más directamente afecta a la economía a través de una perspectiva integrada de riesgos, y en los que este ensayo se centrará a fin de mantenerse dentro del tema general objeto de este libro.

Un análisis realista del riesgo económico requiere un detallado e integrado análisis de todo el espectro de los riesgos cibernéticos, a través del cual, tanto si el objetivo primordial de un ciberataque es alcanzar un beneficio económico como si no lo es, el análisis debe constituirse en una estrategia integrada para combatir los ciberconflictos. La vital contribución que las tecnologías digitales representan en nuestra era, y especialmente en nuestra seguridad económica, depende del funcionamiento, la integridad y la fiabilidad de estas tecnologías, así como de la confianza que inspiran. En consecuencia, la ciberseguridad debe representar un tema central en este estudio, como sucedía en la publicación de 2010 citada anteriormente.

En consecuencia, indagaremos primero la dimensión hasta la que las tecnologías digitales han traspasado ya los segmentos económicamente relevantes de la sociedad. De manera predictiva, analizaremos, siquiera de forma especulativa, las posibilidades de crecimiento y de cambio del mundo digital en los años venideros. El siguiente capítulo se centrará en las vulnerabilidades y la exposición a riesgos generados por este mundo nunca antes tan interconectado y las subsiguientes amenazas de seguridad conforme estas se van generando. A continuación, se realizará un intento de medir los daños económicos resultantes y la escasamente clara relación existente entre ciberataques y ciberdefensa, como por ejemplo en la industria de seguridad.

En la segunda parte de este estudio, se hará hincapié en las contraestrategias, en mitigar los daños, en la prevención y en analizar en su totalidad la panoplia de la defensa digital. Se pondrá un especial énfasis en los aspectos legales, ya que son pocas las provisiones que se han destinado a ejercer un control normativo efectivo sobre la conflictividad cibernética; como mucho, existe una incipiente comprensión de cómo se aplicaría la legislación internacional[8].

[8] Más adelante se podrán encontrar referencias más detalladas al *Manual Tallin sobre la legislación internacional aplicable a la ciberguerra* (*Tallinn Manual on the international*

La cibernética como modelo de cambio del paradigma económico

Cualquier asesoramiento realista sobre amenazas precisa de una revisión panorámica de la tecnología de última generación empleada por actores económicos clave. Las tecnologías de la información y la comunicación (TIC) significativamente se están convirtiendo en el nuevo paradigma que domina todos los aspectos del esfuerzo humano, proporcionando el sistema operativo universal de las sociedades humanas. La tecnología cibernética se ha convertido en una característica que define nuestros tiempos: la casi dependencia total de las TIC proporciona una importancia vital sobre el rendimiento, la robustez, la seguridad, la fiabilidad de los sistemas y redes digitales y la confianza en su funcionalidad e integridad y en la protección de la privacidad. Estas condiciones se convierten en un entramado para el funcionamiento de la sociedad. Por tanto, la seguridad informática se debe considerar como un arquetípico desafío social de proporciones globales.

El progreso y el desarrollo de las TIC que podemos contemplar en la economía y en todos los foros, incluyendo los asuntos militares, son sobrecogedores y justifican ser designados como una segunda revolución digital.

Como ha sido mencionado por diferentes fuentes y estudios, los rápidos avances debidos a la densidad de integración y el desarrollo de circuitos digitales a gran escala que conforman la tecnología base en la era digital continuarán durante al menos una década más. La Ley de Moore, que duplica el desarrollo informático cada 18 años, se mantiene vigente. Como sucede que estos componentes digitales son crecientemente más pequeños y más baratos, algunos de estos componentes, como microprocesadores, sensores y actuadores, se integran en sistemas técnicos o físicos e interconectados a través de una variedad de redes. Según un reciente documento de Manfred Broy, actualmente, alrededor del 98% de todos los microprocesadores van integrados (y son invisibles) y están conectados a través de sensores (por ejemplo, RFID, identificadores de radiofrecuencia), y actúan con el mundo físico y con internet. Como Broy menciona, «... el mundo físico se funde con el mundo virtual del ciberespacio que conduce a sistemas ciberfísicos y a una Internet de las cosas, datos y servicios»[9]. Con más de 2.300 millones de ordenadores en línea y miles de millones de microprocesadores y microordenadores consiguientemente empleados en sistemas integrados, identificadores de radiofrecuencia y otros sensores, dispositivos móviles, tecnologías de red y de banda ancha en crecimiento, ultraminiaturización de circuitos

law applicable to cyber warfare. Cambridge University Press, 2013), el primer tratado minucioso sobre la materia.

[9] «Cyber physical systems» («Sistemas cibernéticos físicos»), parte 1. *IT. Information Technology,* número especial, 6/2012, pág. 255. Múnich: Manfred Broy, 2012. (*Parte 1).*

digitales y la ubicuidad resultante de nuevos elementos informáticos miniaturizados, y el incesante progreso hacia un «Internet de las cosas», con microordenadores insertados en tejidos o en las monturas de gafas, el espectro de una posible amenaza va infinitamente más allá de los ordenadores tradicionales o la actual Internet.

Básicamente, *todos* los dispositivos y redes digitales son vulnerables, y la creciente interconectividad de los sistemas digitales puede causar fácilmente un efecto «bola de nieve» (como ejemplos, la distribución de errores, deficiencias y fallos, o el daño causado por los ciberataques). Y estos son procesos en desarrollo; somos ya testigos de un crecimiento continuo de actores digitales, y de una curva de crecimiento exponencial en la interconectividad, y toda la penetrabilidad que de forma automática dispara un incremento paralelo de las vulnerabilidades.

El fenómeno de la migración de los procesos informáticos (de líneas telefónicas fijas a móviles y a voz sobre IP-VoIP), la gestión de *software* y el almacenamiento de datos desde ordenadores individuales y profesionales a enormes granjas o centros de servidores informáticos (en red en la nube) con capacidad de peta*bytes* y servicios informáticos en la nube –y convergencia– dan como resultado una indistinguible malla de sistemas móviles y fijos que se añaden a una inmensa estructura de redes global en un universo de conectividad .

Sumando los ordenadores tradicionales, los dispositivos móviles y los sistemas integrados –omnipresentes aunque sofisticados microprocesadores, a menudo miniaturizados al tamaño de un terrón de azúcar–, algunos analistas estiman que el número total de sistemas –civiles y militares– interconectados ha alcanzado o está a punto de alcanzar los 50.000 millones. La propensión exponencial de su potencial conectividad mutua, y por ello de su vulnerabilidad a los ciberataques salvo que se encuentren potencialmente protegidos, es difícil de calcular pero, en cualquier caso, es un asunto considerable y preocupante.

El desarrollo de dispositivos móviles es particularmente notorio. Recientes estadísticas indican que la comercialización a nivel mundial de los teléfonos inteligentes o *smart phones* habrá alcanzado los 650 millones de unidades en 2012, que elevarán la base de abonados a móviles a cerca de 8.500 millones en 2016; una cuota de crecimiento anual superior al 7%, con una penetración en el mercado que pronto superará el 100%. La facturación anual del negocio de telefonía móvil asciende aproximadamente a 250.000 millones de dólares[10], cifra que no incluye a otros dispositivos móviles ni al potencial de innovación de todos los sistemas móviles, como tablet PC, o *smart phones* con tecnología 3G. Estos convierten la informática en ubicua.

[10] Cifras de *Portio research report. Smartphone futures 2012-2016.*

En los países de la OCDE y en los mercados emergentes, casi todas las empresas están conectadas a Internet, y un porcentaje cada vez mayor del valor añadido de los negocios puede atribuirse a actividades relacionadas con Internet. Los países en vías de desarrollo se están poniendo al día cada vez más rápidamente, a menudo basándose en tecnologías móviles.

El aparato productivo de nuestras sociedades está ya en gran medida digitalizado. Equipos informáticos conectados por Internet que operan sistemas integrales de intercambio de información entre equipos dentro de las fábricas, a menudo interconectadas por protocolos inalámbricos conocidos como *sistemas de producción ciberfísicos,* y que crecientemente caracterizan los procesos productivos del hoy y del mañana constituyen la base de la cuarta revolución industrial, a pesar de que este desarrollo es aún incipiente. Los sistemas TI conectados a Internet e integrados, como los RFID, se convierten en motores de la innovación, reemplazando los antiguos modos de control y gestión centralizados de la producción por la autoorganización y los ajustes altamente definidos de los procesos.

Las *smart factories,* fábricas inteligentes, van de la mano de las *smart grids*, redes inteligentes para funciones esenciales de servicio público. Una economía energética adecuada debe moverse hacia el uso de redes inteligentes, un control de la producción y el consumo y unos sistemas de mando basados en el funcionamiento de millones de sensores. Los sistemas inteligentes no son, ni por asomo, propiedad de los países de la OCDE: Nueva Delhi ha introducido recientemente redes inteligentes para el mantenimiento energético de la metrópoli.

La *segunda revolución digital* se manifiesta también en el crecimiento cuantitativo del tráfico de datos, sin precedentes. La nueva dimensión en el almacenamiento, transmisión y procesamiento de la información y la nueva disponibilidad de nuevos servicios TIC se hace posible merced al inmenso crecimiento de los centros de datos, *big data* o «grandes volúmenes de datos», coloquialmente conocidos como *la nube,* que se han convertido en una guía principal del crecimiento económico. Los diversos servicios de la nube y su rápido crecimiento –infraestructuras como servicio (IaaS), *software* como servicio (SaaS)– permiten la reducción en la adquisición y mantenimiento del *hardware* y *software* de las empresas, y ofrecen flexibilidad, ahorro y plena disponibilidad de los datos de las empresas desde cualquier punto.

La explosión de la producción de datos es sin duda fomentada por el fenómeno de *la nube.* La computación en la nube es el segmento de las tecnologías de la información con un desarrollo más veloz que hace prever un crecimiento de datos en la nube multiplicado por seis en los próximos cinco años, de los cuales se espera que solo la Unión Europea pueda ge-

nerar unos ingresos adicionales de 600.000 millones de euros y la creación de dos millones y medio de puestos de trabajo a lo largo del proceso.

El mundo cibernético del mañana

Antes de apreciar en su totalidad las amenazas y los riesgos económicos del ciberconflicto, debemos valorar, siquiera de forma resumida, los avances en los desarrollos cibernéticos, a pesar de que predecir es una tarea arriesgada per se. Sin embargo, podemos trazar las líneas maestras conforme se desarrollan a partir de las tendencias actuales, siempre y cuando se construya un acelerador realista. Es seguro asumir que la miniaturización y la penetración de los dispositivos en el Internet de las cosas, basado en el mucho más potente protocolo IPv6 de Internet, avanzarán a un paso mucho más veloz que la ubicuidad y la penetración de la informática invisible, que el crecimiento de los datos se acelerará y que nuevas formas de informática conducentes a distintas y nuevas estructuras de procesamiento en las redes digitales, por ejemplo las redes neurales, evolucionarán.

Contemplaremos el desarrollo de minúsculos ordenadores con potencial de organizarse a sí mismos y capaces de conectarse con otros instrumentos digitales de forma autónoma, de nuevas comunicaciones hombre-máquina (por citar solo algunas de las tendencias informáticas de nueva generación)[11]. Estos desarrollos generarán una ola de continuo crecimiento explosivo de dispositivos digitales, haciendo pequeña la evolución cuantitativa que hemos conocido hasta ahora. El poder informático, especialmente a través de redes y nubes, se está convirtiendo en algo virtualmente ilimitado. La incorporación de modos *inteligentes* de procesamiento en la industria se acelerarán, y las *redes inteligentes,* todavía hoy en fase experimental, serán un componente habitual en el entorno económico.

La disponibilidad de banda ancha y la amplitud de banda se incrementarán hasta dar servicio a sociedades enteras, incluyendo el mundo en desarrollo, con acceso *on line* efectivo y sólido en muchos países del Tercer Mundo, primordialmente con técnicas móviles[12].

Contemplaremos conexiones de fibra de muy alta velocidad y nuevas conexiones inalámbricas de alta velocidad, dos tecnologías que conformarán el futuro próximo de la conectividad. Los aparatos móviles serán más sofisticados y versátiles, servirán como medios de pago sustituyendo a las contraseñas tradicionales e incluso a las tarjetas inte-

[11] Una relación más completa contemplaría los avances de las nanotecnologías, la ciencia material, la tecnología de sensores basados en semiconductores, la formación y gestión de sistemas virtuales, nuevos conceptos arquitectónicos, etc.

[12] Para ver las actuales cifras porcentuales, consultar *OCDE Internet economy outlook 2012 (Panorama económico de Internet 2012).*

ligentes, y tendrán capacidad de recibir televisión de alta definición en cualquier lugar.

Las tecnologías móviles serán tan eficientes que permitirán el trabajo desde casa con pleno acceso a los datos de las empresas como una de sus características normales, cambiando así la estructura laboral y permitiendo ahorros en infraestructuras y en viajes: *bring your own device* (BYOD) o *trae tu propio aparato*, una forma de trabajo en la que cada empleado podrá acometer sus tareas accediendo a datos y gestionándolos desde cualquier lugar, con plena conexión; lo que ya es factible en algunas compañías, y que se convertirá en un procedimiento rutinario. Nada volverá a ser como antes.

El desarrollo de las amenazas. La nueva realidad económica de la inseguridad cibernética

El anterior análisis ha subrayado el actual y el futuro crecimiento de los sistemas y sus actores, que, estando todos interconectados, constituyen el mundo cibernético. Es por ello evidente que la multiplicación de sistemas y de actores son los principales indicadores de las nuevas oportunidades que existen para poner en peligro la ciberseguridad a gran escala en los contextos militar y civil. El crecimiento de los objetos en este ritmo exponencial indica el crecimiento de las amenazas, igualmente exponencial. Debe tenerse presente que *cualquier* objeto digital, si no está protegido, puede ser objeto de un ataque, y si es parte de una red conectada, dispara múltiples potenciales infecciones y profusos daños.

El tremendo proceso de crecimiento que afecta simultáneamente a los sistemas cibernéticos, sus actores y las estructuras de red ha generado el célebre salto de la cantidad a la calidad. A diferencia de los tradicionales delitos informáticos a la vieja usanza, los ciberatacantes de hoy se aprovechan de la creciente dependencia en el día a día que tenemos de las TI y desarrollan estrategias creativas para explotar las vulnerabilidades de los sistemas de información tecnológica.

El cambio resultante no es sino dramático. Las diferentes dimensiones de la oleada de amenazas requieren ser evaluadas en su conjunto. El crecimiento explosivo de los sistemas y la interconectividad –que ya han sido aquí descritos–, la creciente intensidad, sofisticación y diversidad de los modos de ataque y la tecnología de los ataques, así como los cambios radicales en las características de los actores de ciberconflictos, interaccionan entre sí y multiplican los potenciales daños. Con la *segunda revolución digital*, nos adentramos en un nuevo mundo de peligros que hace ver el análisis de la ciberamenaza de, por ejemplo, hace diez años como idílica.

Todas las operaciones en los ciberconflictos tienen en común que intervienen en el funcionamiento de procesos digitales, ya afecten a los datos, a su almacenamiento, su manejo o su transmisión, ya minen la fiabilidad, la autenticidad, la integridad y la privacidad de los datos y los procesos.

Pero los objetivos de un ataque pueden variar; algunos dejan el normal funcionamiento de los sistemas y procesos informáticos intactos, pues su propósito es el de observar y posiblemente copiar (es decir, «robar») datos. Las aplicaciones clave son el espionaje militar e industrial en las que datos e identidades son robados. Si el ataque permanece sin descubrirse por un cierto periodo de tiempo, puede ser perseguido e incluso más datos se pueden recuperar conforme emerjan: el espionaje y el robo de datos apuntan a este tipo de operaciones encubiertas de larga duración, lo que se conoce como *amenaza persistente*, o en el caso de que sea llevado a cabo por un atacante del ámbito del crimen organizado y desarrolle esta actividad de forma sistemática a lo largo del tiempo, se denomina *amenaza persistente avanzada* (APT).

Otros ataques en los que se emplean, por ejemplo, «bombas lógicas» tienen como objetivo alterar o destruir las funciones del sistema atacado, falsificando su efecto (por ejemplo, las instrucciones operativas de un sistema de armamento) o haciéndolo inoperante. Aún más, otros ataques cambian las funciones operativas normales con propósitos abusivos o ilegales durante un cierto tiempo; por ejemplo, en los fraudes bancarios o de tarjetas de crédito, o de modo más permanente, modificando los sitios web. El envío masivo de *spam,* correo electrónico masivo no solicitado frecuentemente con contenidos comerciales y dirigido a un número indiscriminado de receptores, es a menudo empleado para enviar virus y otro *software* dañino como técnica para llevar a cabo robos financieros, de identidades, de datos y de propiedades intelectuales para fraudes o, simplemente, para llevar a cabo *marketing* engañoso.

Las nuevas formas de ataque

Las formas de conflicto que veremos a continuación, junto con sus tendencias de desarrollo y su dimensión evolutiva, pertenecen a alguno de los siguientes supuestos. Como quiera que el propósito de este estudio no es tratar sus características tecnológicas, las referencias se harán con carácter general. La información y las cifras de actualidad han sido recogidas y puestas a disposición por las compañías globales de ciberseguridad Symantec, Norton, McAfee, Microsoft, Kaspersky Labs, Panda Labs y CISCO, entre otras[13]. Además, muchos servicios de seguridad digital na-

[13] *Symantec Internet security threat report, Norton cybercrime report, McAfee threat report.* Estos informes se emiten periódicamente, y en 2011 y, en parte, en 2012 los datos y los desarrollos se encuentran recogidos en sus últimas ediciones.

cionales, como el alemán BSI, el Departamento de Seguridad Interior de EE. UU. y la agencia europea ENISA[14] recogen y a menudo publican datos.

Al tiempo que estas recopilaciones son extraordinariamente reveladoras, deben ser leídas con cierta cautela. Las empresas de seguridad de las TI, si bien son precisas y concienzudas en sus informes, tienden, no obstante, a realzar los peligros de los ataques en su propio interés. Además, las víctimas tienden a minimizar los incidentes sufridos: negocios como los bancos lo hacen para proteger la confidencialidad de sus operaciones, los particulares lo hacen por vergüenza o por la ausencia de interlocutores y los servicios nacionales de seguridad lo hacen especialmente cuando se trata de redes informáticas relacionadas con secretos militares, sistemas armamentísticos o cuando se ha violado algún dispositivo crítico de seguridad.

Pero es exactamente el aprovechamiento de las posibilidades de espionaje lo que ha mostrado últimamente uno de los factores de crecimiento más altos. Como el acceso a los sistemas de seguridad de los estados, las organizaciones y las empresas encuentran cada vez barreras más franqueables junto a la ubicuidad de las técnicas empleadas para acceder a estos datos, muchas de ellas desarrolladas por organizaciones criminales; es evidente que algunos estados hacen un uso cada vez más agresivo del ciberespionaje.

Existe información detallada de las operaciones cibernéticas de China en EE. UU., en las cuales los intrusos se concentran en infraestructuras corporativas clave con vistas al robo de propiedad intelectual[15].

Durante muchos años, China ha estado practicando espionaje nuclear, recopilando información altamente clasificada sobre largas y documentadas listas de cabezas nucleares, al tiempo que accedían a redes de altas instituciones de defensa y financieras. La forma más común de penetración es a través de ataques con troyanos, en los que se introduce un virus con instrucciones de recoger datos por amplios períodos de tiempo sin ser detectado por los sistemas operativos del objetivo. A la vez que las operaciones de explotación cibernética desarrolladas por China han recibido una publicidad especial por causa de su amplitud y agresividad, todo el resto de grandes potencias también se ven envueltas en intensas batallas de espionaje. Por el momento, los virus con funciones de espio-

[14] Informes de ENISA, como el *ENISA Threat landscape: Responding to the evolving threat environment,* de enero de 2013, que destaca por su amplia base de datos, que incorpora hallazgos de la mayoría de otros informes, y por sus sistemáticos y definitorios análisis de los diferentes tipos de riesgos y amenazas.

[15] Wikipedia, «Chinese intelligence operations in the US». *IISS Strategy Survey 2012, Intelligence agencies and the cyber world,* p. 33. Ver también INKSTER, Nigel: «Chinese intelligence in the cyber age». *Survival,* febrero-marzo de 2013, p. 45. Ver también nota 3 más arriba.

naje disfrutan de un ciclo de negocio positivo; últimamente, las variantes de *spylware madi* y *flame* se han hecho especialmente prominentes[16]: su aspecto muestra que incluso *spylware* relativamente simple es capaz de obtener información muy valiosa y sensible a gran escala. Desde las redes de espionaje manejadas por estados con alta penetración de troyanos, solo queda un paso para el ataque directo, la degradación de los sistemas armamentísticos y el sabotaje, por ejemplo a través de bombas lógicas durmientes, a pesar de que estas deben ser capaces de resistir la vigilancia y la constante actualización de *software* de la parte a la que se pretende atacar a corto plazo.

Todos los informes de las empresas de seguridad convienen en sus últimas ediciones que los ataques malintencionados continúan creciendo con rapidez y, según McAfee, actualmente han alcanzado el mayor punto de todos los tiempos en el quebrantamiento de bases de datos. Al mismo tiempo, existe una creciente sofisticación en los ataques y en el desarrollo de *software* dañino.

El software orientado a los dispositivos móviles se ha convertido en un nuevo foco de los ataques, y se ha casi duplicado en un período de un cuatrimestre.

Con el creciente número de vulnerabilidades en el espacio móvil subiendo –Symantec ha detectado un crecimiento de un 93% en un año– y los diseñadores de *software* dañino creando *software* orientado hacia las oportunidades de los móviles, 2011 fue el primer año en que el software dañino constituyó una amenaza tangible para empresas y consumidores, teniendo en cuenta que los trabajadores tienden a introducir sus *smart phones* y *tablets* en el ambiente laboral más rápidamente de lo que las empresas pueden garantizar su seguridad y gestión. BYOD representa unos enormes y nuevos retos de seguridad, y puede conducir a un posterior aumento a largo plazo de los quebrantamientos de datos. Los nuevos desafíos para los móviles se diseñan para actividades que incluyen la recopilación de datos, el envío de contenidos y el rastreo de los usuarios.

Existen saltos cuantitativos en todas las categorías de modos de ataque. Symantec por sí sola bloqueó más de 5.500 millones de ataques dañinos, con un incremento de un 81% respecto del año anterior. Además de ello, el número de variantes de *software* dañino aumentó hasta 403 millones en ese período.

[16] El virus *duqu*, a menudo citado en el contexto *flame*, reúne también excelentes propiedades para el espionaje y el robo de datos, pero es sustancialmente más complejo y está posiblemente relacionado en su estructura y orígenes con *stuxnet*. Su objetivo primordial es controlar *software* como SCADA. *Duqu* desaparece de los sistemas afectados en 36 días, lo que complica su detección.

El daño financiero a los bancos y a los clientes particulares (fraude con tarjetas de crédito, *phishing* y *carding, spearphishing*, extorsión financiera directa) continúa creciendo rápidamente. El pasado año, los delincuentes informáticos montaron un sistema automatizado de transferencias (ATS) que se empleó para atacar a instituciones financieras europeas y que estaba orientado a atacar una gran institución financiera multinacional de EE.UU. La «transferencia de dinero por móvil» (MMT), un término trampa para noveles sistemas financieros digitales que prestan servicios bancarios a millones de personas en el Tercer Mundo, mostrará, si no se regula rápida y eficientemente, el «lado oscuro» de las finanzas cibernéticas, y se convertirá en el terreno de juego para los ataques y el delito cibernéticos[17].

Dada la aún perdurable cuasimonocultura de los sistemas operativos en los que un productor domina el mercado, las vulnerabilidades que son inherentes a sus productos están ampliamente extendidas y, si se explotan, conducen a sustanciosos daños. La principal fuente de distribución de virus informáticos son, por consiguiente, los inocentes usuarios de ordenadores personales, y aquellos ordenadores de empresa cuyos operadores a menudo no son conscientes de los riesgos que comporta la red.

Los ataques con virus también han sido enormemente facilitados por la enorme presencia de «nuevas redes sociales» que operan como distribuidores gratuitos de la infección. Yendo más allá de los ataques de *spam,* los ciberdelincuentes se han orientado hacia estas redes sociales. Su apariencia muy inocente hace que los usuarios den –erróneamente– por sentado que no corren riesgos, y los atacantes están empleando estos sitios para apuntar a nuevas víctimas. Debido a las técnicas de ingeniería social y la naturaleza vírica de las redes sociales, es mucho más fácil que una amenaza se traslade de una persona a la siguiente. A pesar de todo, aunque el *spam* está ahora mejor controlado por los filtros anti*spam* de los proveedores de servicios de Internet y, además, en muchos países sujetos a legislación anti*spam,* este está todavía desenfrenado: en 2010, más del 86% del tráfico en Internet (62.000 millones de mensajes diarios globalmente) eran *spam* (con un porcentaje ligeramente inferior en 2011, un 75% que representó 42.000 millones de mensajes)[18], lo que supone que, al inundar las cuentas de Internet, causa un daño apreciable en tiempo de producción perdido, aparte del potencial existente para difundir los ataques de virus.

[17] BRONK, Christopher, MONK, Cody y VILLASEÑOR, John. «The dark side of cyber finance». *Survival,* abril-mayo de 2012, p. 129. Un virus específico, *gauss,* apunta a las transacciones financieras, pero existen otros.

[18] Cifras de Symantec. El *spam* puede haber crecido menos velozmente, también porque existe una mayor presión sobre los *spammers*; algunos *botnets* enormes especializados en *spam* se han retirado en los dos últimos años. Por el contrario, el contenido del *spam* delictivo se ha hecho más sofisticado.

Existe otro movimiento indiscriminado ajeno al *spam*: los atacantes individualizan sus ataques, centrándose en aquellas víctimas sobre las que han acumulado y procesado conocimientos a través de datos y robos personalizados. Un método de individualización es el *spear phishing:* el término denota un ataque vía correo electrónico orientado hacia personas que se sabe que frecuentan determinados negocios *on line* y de las que pueden poseer información relevante sobre cuentas bancarias, negocios concretos o cadenas de distribución. Se denominan así porque el movimiento hacia el objetivo es preciso y estrecho, como la punta de una lanza.

A pesar de que los datos de tarjetas de crédito no se pueden robar, las direcciones de correo electrónico se encuentran comprometidas y pueden ser vendidas en el mercado negro. Más aún, la información recolectada a través de *spear phishing* puede generar ataques de *phishing* más sofisticados a otros usuarios actuando sobre mensajes aparentemente legítimos procedentes de un minorista o un banco con el que mantengan relaciones comerciales. Los ataques dirigidos se orientan de manera creciente hacia pequeñas empresas, pues estas pueden estar peor protegidas u ocupan puestos importantes en determinadas cadenas de suministros.

Al mismo tiempo, el código dañino está cada vez menos programado para causar daños directos irreparables. Por el contrario, los atacantes tratan de someter bajo su control a los ordenadores para así poder continuar afectándolos a través de infecciones con troyanos y control remoto.

Un elemento importante y efectivo en esos esquemas son los ataques mediante DDoS (denegación de servicio distribuida). En este método de ataque, el atacante inunda al servidor con paquetes de datos inservibles para, de esta manera, sobrecargar los sistemas con el fin de provocar interrupciones comerciales en los sistemas y las estructuras de red de la víctima. En el contexto empresarial, tales ataques se pueden desencadenar por parte de competidores, personal insatisfecho o grupos de personas motivadas por otras razones. Obstruir masivamente la fluida operatividad de los sitios de red puede dar como resultado considerables consecuencias económicas, especialmente en empresas que hagan uso o estén basadas en el comercio electrónico. En escenarios de conflictos militares o políticos, los ataques DDoS –un elemento central del ataque ocurrido en Estonia en 2007, en el que, sin embargo, el daño económico fue menor– pueden paralizar instalaciones de defensa y comunicaciones y neutralizar o destruir sistemas armamentísticos, paralizar servicios gubernamentales, provocar fallos en infraestructuras críticas y sectores económicos y también, en consecuencia y en casos extremos, conducir a la pérdida masiva de vidas.

Mientras que los últimos informes de las empresas de seguridad apuntan a las nuevas amenazas, los dispositivos móviles –y a través de ellos todo

el universo interconectado– aún no han cuantificado las nuevas vulnerabilidades que surgen del explosivo crecimiento de los centros en la nube.

Más allá de la amenaza a los móviles, la inseguridad causada por la migración masiva de datos a la nube ha sido en los últimos tiempos un tema candente en discusiones sobre seguridad, como lo demuestran las palabras de un informe de 2009 de ENISA[19]: «Las concentraciones masivas de recursos y datos suponen un objetivo más atractivo para los atacantes», a pesar de que la agencia cree «que las defensas basadas en la nube pueden ser más robustas, escalables y coste-efectivas».

Esta lista de nuevos modos de ataque supone la emergencia de una amplia serie de nuevos y sofisticados programas de *software* destructivo que aparecen con una inaudita rapidez y sofisticación[20] y con precisión sobre los objetivos. Por descontado, las fronteras nacionales no son ya relevantes ante este tipo de amenazas, y resulta imposible circunscribir la protección de las tecnologías de la información y sus infraestructuras a las políticas nacionales. Los autores, vendedores y beneficiarios de los virus informáticos y otros códigos dañinos, operan globalmente, por lo que la defensa digital debe operar de igual modo.

El nuevo enemigo: actores colectivos del ciberconflicto

La delincuencia en Internet se conduce cada vez más de una forma profesional y comercial. Los ataques a objetivos son cada vez más frecuentemente realizados por delincuentes organizados. Los intereses financieros son la fuerza motriz. Los ciberconflictos se están convirtiendo en una poderosa rama de la escena internacional de la delincuencia organizada. Los consorcios de delincuentes comandan ejércitos de expertos cibernéticos y generadores de *software* dañinos, que sistemáticamente organizan campañas lucrativas de delincuencia organizada. Tras años de operar, han constituido equipos profesionales para el desarrollo de *software* dañino sofisticado, beneficiándose de los recursos generados por la delincuencia masiva. Esto da lugar también a ataques de magnitudes nuevas. Ya en 2004, el 16% de las actividades de *hacking* se orientaban contra empresas de comercio electrónico; esto representó un incremento de un 400% con respecto al año anterior, pero desde entonces, el *hacker* que operaba solo ha desaparecido en las tinieblas y las organizaciones han tomado el relevo.

---

[19] *Cloud computing: benefits, risks and recommendations for information security*. Noviembre de 2009, www.enisa.europa.eu.

[20] Un ejemplo es una nueva tecnología para segmentar el *software* dañino en minúsculos paquetes de datos que irrumpen en el sistema objetivo desconocidos por los cortafuegos y los sistemas antivirus, pero que se reconstruyen automáticamente una vez que han entrado en el sistema.

Estas sistemáticamente introducen troyanos en grandes cantidades de ordenadores, cada vez más, y también en dispositivos móviles, y de este modo tienen miles, incluso millones de equipos bajo su mando en los que pueden activar *software* dañino y emplearlo para sus ataques: las *botnets* –el término procede de las palabras robot y *net*– están creciendo.

Estos conjuntos de *ordenadores zombis* poseen distintos usos. Sus operadores, conocidos como *botherders*, pueden proceder directamente a generar dinero o bien a recoger inteligencia de espionaje, datos comprometedores o robos de identidades. Las *botnets* aportan una infraestructura efectiva y en creciente uso para distribuir programas de espionaje en una amplia gama de variantes, y a hacer negocios a través de bancos *on line.* Las *botnets* son la plataforma ideal para ataques DDoS, pues estos últimos precisan de un gran número de emisores de correo electrónico activos para alcanzar el deseado efecto de saturación a gran escala.

Las *botnets* pueden ser también alquiladas a otros delincuentes, o a Gobiernos, como mercenarios digitales, creando una opaca amalgama de actores estatal-no estatal. No son la única mercancía del mercado negro disponible para delincuentes y Gobiernos por igual; inmensos paquetes de *software* para ataques agresivos, de direcciones de correo electrónico y números de tarjetas de crédito están disponibles a precios casi de ganga. Tampoco hay escasez de zombis: se estima que uno de cada diez correos electrónicos están afectados por virus importantes y, en consecuencia, los *botherders* pueden sumarse en manadas, funcionando sin el conocimiento de sus propietarios. Ya en 2010, McAfee estimó que el número de ordenadores zombi crece alrededor cinco millones al mes.

En los mejores tiempos del virus Conficker, que era y es capaz de añadir de forma autónoma nuevos ordenadores a la *botnet,* la dimensión de tan solo esa red puede haber alcanzado a más de 10 millones de dispositivos. Sin el empuje que aportan los nuevos actores colectivos, este crecimiento sería inconcebible.

Un aspecto alarmante del nuevo escenario de delitos informáticos es la antes citada proeza técnica y financiera para desarrollar *software* dañino por delante de las ciberdefensas, y a pesar de la indudable eficiencia de la industria internacional de seguridad digital. Al mismo tiempo, la dependencia digital de las sociedades modernas es creciente, pues las infraestructuras son cada vez más dependientes de la red (por ejemplo las redes inteligentes). Incluso el aspecto estrictamente numérico es de por sí preocupante: los informes de McAfee indican que las variantes identificadas de *software* dañino se multiplican cada año por cinco.

En consecuencia, el eterno dilema entre ataque y defensa cobra un nuevo significado, especialmente a causa de estos nuevos operadores colectivos en el ciberespacio, y los defensores de un ciberespacio libre de

delitos no siempre prevalecen[21]. El potencial de ataque de estas fuerzas perversas y organizadas también da una idea de las posibilidades de una ciberguerra real si los estados y la delincuencia organizada cooperan.

Existen diversos análisis con teorías sobre los países o lugares de residencia de estas organizaciones delictivas y que se basan en parte en la URL de los mensajes atacantes. Sin embargo, habida cuenta de las ilimitadas posibilidades de saltar de una estación a otra y las entradas procedentes de varios países emisores, este estudio omite tales atribuciones.

Con todos estos desarrollos ha quedado evidentemente claro que el término *seguridad* ha alcanzado un significado completamente nuevo y una nueva dimensión en el ciberespacio: las fronteras nacionales ofrecen hoy menos protección que nunca antes. Conceptos tales como seguridad interna y externa resultan crecientemente difíciles de definir y, en muchos casos, pueden fundirse.

El ciberterrorismo puede también subsumirse bajo las nuevas amenazas colectivas. Bajo la definición más extendida, el terrorismo digital denota el empleo de ataques vía Internet por grupos ideológicos y políticos que apuntan hacia una quiebra a gran escala de los sistemas y las redes, generando potencialmente destrucción, alarma y pánico. Si el objetivo de estos terroristas no es conseguir un beneficio económico, no estarían de forma genuina dentro del contenido de este estudio. Si son motivos económicos, por ejemplo obtener fondos para la financiación de actividades terroristas, significa que esencialmente no son distintos de otros activistas criminales y solo formarían parte del ciberconflicto integral y del panorama de amenazas aquí descrito. En ningún caso esto significa que se trivialicen los peligros que representan, especialmente en los ataques contra infraestructuras críticas, y por ello están con todo derecho dentro de los objetivos de los Gobiernos en sus campañas antiterroristas y de seguridad en general[22].

Medir el coste del ciberconflicto: ¿es posible cuantificarlo?

Varias empresas internacionales de ciberseguridad periódicamente acometen poner un precio al daño económico global causado por el conflicto digital de acuerdo con sus propias actividades y predicciones.

[21] «Hay, y siempre habrá, una carrera permanente en el ciberespacio entre los atacantes y los defensores. Desgraciadamente, en este momento los atacantes van un paso por delante» –*ENISA Threat Landscape,* enero de 2013, antes citado.

[22] CANDAU ROMERO, Javier. «Estrategias nacionales de ciberseguridad. Ciberterrorismo». En: *Ciberseguridad, retos y amenazas a la seguridad nacional en el ciberespacio. Cuadernos de Estrategia,* n.º 149. Madrid: Instituto Español de Estudios Estratégicos, 2010.

El *Informe Norton de ciberdelitos* (*Norton cyber crime report 2012*) estima que las pérdidas financieras inmediatas alcanzan los 110.000 millones de dólares anuales en 24 países (Symantec alcanza los 114.000 millones), con 556 millones de víctimas afectadas; pero si se añaden a ello los fondos correspondientes al tiempo invertido en tratar de encontrar respuesta a los incidentes y resolver los delitos informáticos, la cifra alcanza aproximadamente los 390.000 millones de dólares.

Cualquiera que sea la metodología exacta para calcular estas cifras, es cierto que con independencia del número de países que esta cubra, el coste de los daños a largo plazo y la interrupción de los negocios, el dinero gastado directamente en responder a los incidentes y el daño causado a la reputación de las empresas no han sido totalmente considerados, y si así lo fuera, en todos los países alcanzaría importantes proporciones adicionales. Además, y como se ha señalado anteriormente, cualquier estadística sobre daños habrá de incluir el inmenso número de casos de ataques no identificados ni evaluados[23].

Tampoco parece que se cubran medidas preventivas y de defensa. Si tomamos como ejemplo los esfuerzos del Gobierno de EE. UU. por realzar sus capacidades en ciberseguridad (protegiendo infraestructuras críticas, operaciones de seguridad informática, compartiendo información y análisis, etc.), la asignación presupuestaria para el Departamento de Seguridad Nacional únicamente para estos fines asciende a 1.200 millones de dólares para el año fiscal de 2013[24], seguro que menos que el sector privado, donde todas las empresas incluidas deben invertir en seguridad y vigilancia cibernéticas. Se deben extrapolar estas cantidades a la comunidad internacional en su conjunto. La industria de la ciberseguridad por sí sola supone un negocio de miles de millones de euros o de dólares.

Calcular los presupuestos para salvaguardar instalaciones militares, sistemas de comunicaciones y armamento será incluso más difícil. Pero es evidente que la disponibilidad y mantenimiento de las propias comunicaciones militares y las estructuras de mando, junto con la capacidad de neutralizar acciones militares hostiles (ciberdefensa), deben ser contempladas –y lo son– en los cálculos y la planificación.

---

[23] La Comisión Europea, a través de su vicepresidenta Neelie Kroes, contempla en la actualidad que las empresas tengan la obligación legal de denunciar los ciberataques (*News agencies*, 26 de noviembre de 2012). La Comisión Europea prepara una directiva en este sentido. En los países de la UE, más de 40.000 empresas deberían cumplir con la obligación de informar. Esta iniciativa ha encontrado resistencia por parte de las industrias y los proveedores de servicios de información tecnológica. ENISA ha estimado que el 25% de los ataques en la UE y los EE. UU no se denuncian ante las autoridades legales. Para consultar una iniciativa reclamando la denuncia voluntaria por parte de las empresas, ver nota al pie n.º 55 más adelante.

[24] www.dhs.gov.

Considerando las incertidumbres de los cálculos, no sorprende que no se disponga de cifras globales fidedignas. No obstante, en la reciente primera Cumbre Mundial de Ciberseguridad organizada por el East-West Institute en Dallas, Texas, en 2010, portavoces autorizados valoraron el daño total de la inseguridad cibernética en alrededor de un billón de dólares anuales, y es esta la cifra estimada que desde entonces se ha barajado sin que haya habido serias objeciones. En la misma línea de magnitudes, un portavoz autorizado de la Cámara de Representantes de EE. UU. ha estimado que las pérdidas anuales causadas por el ciberespionaje –presumiblemente causadas por intrusos chinos– han alcanzado los 300.000 millones de dólares en 2012, sin pormenorizar las cifras[25]. En el Foro Económico Mundial de Davos 2013, se ha considerado como cierto que a lo largo de la próxima década existe un 10% de posibilidades de que se produzca un apagón digital de primera magnitud –de origen presumiblemente delictivo– que alcanzará el cuarto de billón de dólares[26]. Estas cifras, y al menos su orden de magnitud, son enormes.

Mientras que *la primera parte* ha analizado las actuales y futuras ciberamenazas y su enorme coste económico y ha subrayado el hecho de que una situación de riesgo integral requeriría también una respuesta integral y extensa, esta *segunda parte* se centrará en combatir los ciberconflictos, el desarrollo de estrategias para la ciberdefensa y el diseño de estrategias para mitigar las consecuencias.

Los límites legales a la ciberguerra *stricto sensu*

Pese a que hemos encontrado el concepto de ciberguerra ambiguo y de dudosa importancia para este análisis de riesgos económicos, se enumera un breve resumen de las restricciones del derecho internacional sobre acciones cibernéticas hostiles, pues estas pueden limitar la potencialidad de los daños.

El derecho internacional, y especialmente el derecho que rige los conflictos armados, precede a la era cibernética, pero dado que el ciberespacio es cada vez más considerado como un nuevo teatro de operaciones bélicas, se acepta generalmente que el *jus ad bellum* (el derecho sobre el empleo de la fuerza) y el *jus in bello* (el derecho en la guerra), adaptados adecuadamente, también gobiernan las hostilidades en el ciberespacio. Existe abundante literatura académica sobre las analogías que pueden y deben extraerse de la Carta de las Naciones Unidas, las Convenciones de La Haya y Ginebra, las Convenciones del Comité Internacional de la Cruz Roja, los protocolos adicionales y otros tratados sobre el derecho

[25] Artículo en *El País* y prensa de EE.UU., 21 de febrero de 2013.

[26] Citado por la vicepresidenta Kroes en la Conferencia sobre la Ciberseguridad Global en Bruselas, el 30 de enero de 2013.

humanitario, resoluciones de la Asamblea General de las Naciones Unidas anunciando principios generales de conducta para los países, la jurisprudencia internacional existente y el derecho consuetudinario internacional. Algunos Gobiernos han publicado manuales y estrategias que también definen restricciones, pero que igualmente proporcionan las bases para enormes inversiones en armamento cibernético. Gran parte del debate se centra en las definiciones de «ataque» y «ataque armado», pero también en las definiciones cibernéticamente adecuadas, asentadas sobre los principios de las leyes de los conflictos armados (necesidad, distinción, proporcionalidad, no discriminación, prohibición de atacar objetivos civiles y a ciertas personas, objetos y actividades, neutralidad, etc.)[27]. Los puntos de vista expresados abarcan desde la aceptación de amplias opciones de ataque, en las que apuntar a infraestructuras críticas se considera dentro de los márgenes de la legalidad[28], a interpretaciones más restrictivas[29].

No tiene sentido discutir estas diferentes perspectivas a la vista de que el principal trabajo de referencia es ya claramente el recientemente publicado *Tallinn manual on the international law applicable to cyber warfare*[30] (*Manual Tallin sobre la legislación internacional aplicable a la ciberguerra*) elaborado por el Grupo Internacional de Expertos invitado por el CCDCOE, Centro de Excelencia de Ciberdefensa Cooperativa de la OTAN. Este pormenorizado tratado busca establecer 95 «reglas» que puedan cubrir los principios de *jus ad bellum* y *jus in bello* para los ciberconflictos de forma exhaustiva.

El Manual posee un mérito obvio: la prestigiosa reunión de coautores propone bajo el régimen internacional de *lege lata* (según la ley existente) definiciones y reglas plausibles, y pone fin a muchas viejas controversias. Sin embargo, al tratar sobre las relaciones entre civiles y militares y al tratar de definir los valores de ambos así como debatir sobre la no

27 Para un resumen de estos asuntos, ver WESTBY, Jody R. «A call for geo-cyber stability», *en* la Unión Internacional de Telecomunicaciones (UIT) (Hamadoun Touré y el Panel Permanente de Seguimiento de la Seguridad de la Información, Federación Mundial de Científicos), *The quest for cyber peace,* Ginebra: UIT, 2011, pág. 66. En la misma publicación, ver: BARLETTA, G. A., BARLETTA, W. A. y TSYGICHKO, V. N. «Cyber conflict», pág. 53.

28 Para una evaluación prudente, que incide en la complejidad de diseñar las líneas en el debate sobre el uso de la fuerza, ver WAXMAN, Matthew C. «Cyber attacks and the use of force: Back to the future of art. 2(4)» («Los ataques informáticos y el uso de la fuerza del art. 2(4)»). *The Yale Journal of International Law*, vol. 36, 2011, p. 421.

29 AMATO, Anthony D. «International law, cybernetics and cyberspace» («Derecho internacional, cibernética y ciberespacio»). *76 International Law Studies,* 1999, pág. 59. En esta obra el autor predijo que «los ataques en Internet pronto serán vistos como claramente ilegales desde la legislación internacional y la legislación internacional consuetudinaria puede haber alcanzado ya ese punto»; pero ciertamente los desarrollos desde entonces no han ido por ahí.

30 Ver nota 7 al pie, más arriba.

discriminación, etc., han de admitir que las «armas» cibernéticas «por su propia naturaleza causan efectos que son imposibles de controlar y que, por ello, se pueden extender de forma incontrolada a ordenadores civiles, así como a otros ordenadores protegidos y a redes informáticas, creando una cadena de efectos incontrolables» (pág. 122), y que los objetivos más susceptibles de serlo, especialmente infraestructuras críticas y cibernéticas, son de doble uso, y que el ataque sobre las mismas origina más «daños colaterales» de aquellos que deben asumirse en un conflicto convencional.

¿Podría una infraestructura crítica de uso mixto, militar y civil, ser objetivo si apoyase a otros objetivos protegidos por las Convenciones de Ginebra? El Manual parece otorgar preferencia a los propósitos militares. Reglas tales como «la población civil como tal, así como los individuos civiles, no serán objeto de ciberataques» (regla 32) podrían, de este modo, perder su efecto protector. Las reglas 14 y 55, que especifican que las operaciones cibernéticas en legítima defensa deben ser necesarias y «proporcionadas», se empañarían si, por defecto de control sobre las mismas, la proporcionalidad sobre las mismas no pudiera medirse de forma fidedigna. Otras incertidumbres son las relativas a actores ocultos –no estatales–, al estatus de combatiente, a la definición de «objetos económicos que sostienen la guerra», la neutralidad y la autodefensa anticipativa: ¿cuándo podría ser considerado como inminente un ciberataque lanzado a velocidad del rayo?

Los autores han sido más afortunados al definir «ataque» y «ataque armado», empleando la regla de los «efectos» en el segundo caso (el hecho de que una operación cibernética constituya o no un ataque armado depende de su magnitud y sus efectos, regla 13)[31]. No obstante, incluso aquí las ambigüedades son alarmantes. La regla de «ataques armados» es tan amplia que reduce las barreras hacia la guerra; no es prudente y sí peligroso para la estabilidad internacional tratar conflictos que no supongan un riesgo evidente para las vidas humanas o un elemento de trastorno social como «ataques armados», con las consecuencias que ello conllevaría bajo el derecho internacional[32].

[31] El Manual también deja claro que no todos los ciberataques transfronterizos, ni tan siquiera aquellos dirigidos desde un Estado, constituyen una violación de la legislación de conflictos armados o, en general, de las leyes internacionales. Así pues, el ciberespionaje en tiempos de paz o en conflictos armados no está previsto en la legislación internacional (excepción hecha de casos especiales, por ejemplo, cuando se es indiferente a la inviolabilidad de los archivos y las comunicaciones diplomáticas). Uno de los elementos importantes de los ciberconflictos, la intrusión masiva en sistemas digitales con propósitos de espionaje, una amenaza avanzada persistente (APT), debe por ello ser juzgada bajo las leyes cibernéticas y sanciones nacionales, tal y como define la Convención de Budapest.

[32] BARLETTA, BARLETTA y TSYGICHKO, *op .cit.,* pág. 60.

En su conjunto, el Manual, lejos de limitar la opción de la ciberguerra cibernética, más bien subraya las grandes posibilidades de los ciberataques y el daño incontrolado que estos pueden infligir. Se han estipulado muy pocas restricciones: al contrario, las incertidumbres y el riesgo para las estructuras cibernéticas civiles se hacen más obvias. Esto se refiere específicamente a las infraestructuras críticas nacionales, que no solamente están mayoritariamente en manos privadas, o lo que es lo mismo, configuran buena parte de las economías nacionales, sino que indirectamente penetran en el tejido social, tanto que las economías dependen cada vez más de ellas. Los ataques cibernéticos sobre estas estructuras no solamente generan daños económicos masivos, sino que además comprometen seriamente la seguridad de la sociedad, poniendo en peligro la vida humana.

Más importante aún es que el Manual acepta la opción de la guerra en el ciberespacio de forma irreflexiva, y elude la cuestión sobre si el desenfrenado armamento cibernético que se prevé emplear en el futuro es un sabio camino a emprender por las naciones civilizadas. Naturalmente, el Manual comienza por asumir la afirmación subyacente de que hostilidades cibernéticas patrocinadas por los estados respetarán las directrices de Naciones Unidas y solo serán empleadas en legítima defensa. No obstante, la impresión final es que la transferencia al por mayor de la legislación tradicional sobre conflictos armados y el pensamiento en términos militares termina siendo un pretexto de legitimidad para las ciberguerras del futuro, y se desentiende del enorme dinamismo de los desarrollos digitales así como de la creciente vulnerabilidad social, con lo impredecible de sus consecuencias.

Una interpretación similar se puede detectar en los manuales cibernéticos que muchos Gobiernos han preparado, en la medida en que son públicamente accesibles.

Algunos países están incorporando capacidades ofensivas cibernéticas dentro de las estrategias bélicas convencionales, previendo respuestas militares convencionales o sabotaje a la información en Internet, incluso con independencia de que se produzca un «ataque armado» o bajas humanas. Otros reclaman el uso ilimitado de armas cibernéticas («explotar el potencial completo», «efecto máximo», «procesos de fuego conjunto», «represalia», «golpe de castigo»...) que indican que sus planeamientos siguen líneas militares («doctrina de combate») con sus correspondientes analogías y esquemas de pensamiento[33]. Sin embargo, conceptos como disuasión, represalia o reglas de enfrentamiento no tienen en cuenta la

[33] Una breve lista de las varias «modalidades de ciberguerra» ha sido ofrecido por el secretario general de la Unión Internacional de Telecomunicaciones, Touré, en «The international response to cyber war», *en The quest for cyber peace* («La respuesta internacional a la ciberguerra», en *La búsqueda de la ciberpaz*), *op. cit.* pág. 86.

especificidad de los ataques cibernéticos ni, por ejemplo, los problemas de atribución y proporcionalidad.

Afortunadamente, estos conceptos no permanecen sin contradecirse. El potencial de destrucción y la imprevisibilidad de las opciones de ciberataques son cada vez más reconocidos, y han matizado el punto de vista puramente militar o se encuentran yuxtapuestos al mismo. En muchos documentos de doctrina militar y política, la prevención de la ciberguerra, la priorización de la ciberdefensa y la cooperación de todos los agentes interesados están ahora avanzando hacia un primer plano. Un ejemplo interesante es la Estrategia de Operaciones en Ciberguerra del Departamento de Defensa de EE. UU., de julio de 2011, que opta claramente por la defensa digital, la estrecha colaboración entre agencias gubernamentales, el Gobierno y la industria y la cooperación internacional.

Documentos de la cumbre de la OTAN como la Declaración de Lisboa de 20 de noviembre de 2010 no ocultan las necesidades de defensa, y sin embargo, ponen especial énfasis en la protección cibernética central y en la optimización de la ciberdefensa colectiva y la alianza interna, así como en la cooperación internacional (§ 40). Es también significativo que los ciberataques no están subsumidos dentro del concepto de ataque recogido en el art. 5 del Tratado de la OTAN, sino más bien se menciona en el contexto del régimen consultivo contemplado en el art. 4[34].

Esto indica que el control de los ataques digitales está claramente admitido en muchos sectores como parte esencial de un nuevo paradigma de seguridad que coloca al frente la prevención, la resistencia y el fortalecimiento de infraestructuras digitales amenazadas, y a un entramado de nuevas y amplias redes de cooperación en defensa.

Como este artículo fundamentará más adelante, este movimiento hacia una posición defensiva debería llevarnos a introducir el concepto de ciberpaz como principio de una conducta pacífica en el ciberespacio.

Optar por el lado positivo de la antinomia guerra-paz implica un cambio importante en la perspectiva y la escala de prioridades, ya que orienta la

[34] Otro buen ejemplo de este emergente instinto de prudencia puede encontrarse en los informes actuales sobre un proyecto de directiva presidencial de los EE. UU. que incorpora disposiciones legales relativas a las Fuerzas Armadas en la defensa o la represalia contra un ciberataque importante, respetando plenamente el derecho internacional. Estas normas supuestamente otorgarán al presidente amplios poderes, incluso para un ataque preventivo, pero a la vista de las consecuencias y los problemas de atribuciones, reflejan también una actitud de moderación sustancial, excluyendo la represalia «automática» y reservando la prerrogativa del presidente para ordenar ataques en su condición de comandante en jefe. SANGER, David E. y SHANKER, Tom. «Broad powers seen for Obama in cyberstrikes». *New York Times,* 2 de febrero de 2013. Ver también CONDLIFFE, Jamie E. «Obama has signed a secret directive to stymie cyber attacks». *Washington Post,* 15 de noviembre de 2012.

mentalidad hacia los beneficios y el potencial positivo de la sociedad de la información y aporta un objetivo en este sentido, denunciando la connotación negativa de la ciberguerra y de los términos y calamidades afines –podríamos decir que la deslegitiman– y fomentando el movimiento dinámico hacia una cultura mundial de ciberseguridad.

En un intento por invertir las perspectivas beligerantes antes descritas, uno debe ser consciente de que las infraestructuras digitales son ahora omnipresentes, e inevitablemente también serán utilizadas con propósitos hostiles y no pacíficos.

En consecuencia, el objetivo último es restringir tales usos e incorporar los límites más estrictos para cualquier situación de ataque. Como el mismo término «ciberguerra» invita a pensar en categorías militares, debe hacerse un esfuerzo para combatir este automatismo mental y fundamentar una petición para lograr una conducta pacífica en el ciberespacio.

Ciberdefensa activa y pasiva

Si un país ejecuta un «ataque armado» –o si se piensa que tal ataque se ha producido–, la víctima, el país atacado, tiene, bajo la carta de las Naciones Unidas, el derecho a la legítima defensa proporcional. Pero si el ataque causa daños a intereses privados, por ejemplo a una empresa o a una infraestructura privada –energía, banca, aviación, etc. (para una definición más precisa, ver nota al pie 42)–, ¿puede el atacado responder a la agresión? ¿Y puede acaso hacerlo si existe incertidumbre en cuanto a la atribución y el atacante es, o puede ser, un actor no estatal o, simplemente, un delincuente informático común? Aquí entra en juego la legislación nacional sobre delitos cibernéticos, con sus sanciones penales y las herramientas de aplicación de la ley. El debate sobre si la defensa activa es legal, incluso si implica intrusión en los sistemas y redes y causa daños, se ha librado durante algún tiempo[35].

Algunas tácticas de defensa activa que han sido propuestas podrían incluir la intrusión en los sistemas para recuperar los datos, cerrando los sistemas, saboteando los datos, infectando al atacante con *software* dañino, apropiándose de la *botnet* del atacante o contratando una *botnet* para atacarle. Enviar datos a un atacante (siempre que no sea con *software* dañino) puede no ser ilegal, pero el resto de las acciones defensivas probablemente lo son. Emprender acciones contra un atacante delictivo en respuesta a un ataque criminal no es necesariamente legal en la mayoría de jurisdicciones. Más aún, estas acciones pueden desencadenar otras acciones legales (especialmente si existen *botnets* involucradas) tales

[35] Ver artículo de Jody R. Westby en el blog de *Forbes* http://www.forbes.com/sites/jodywestby/2012/11/29/caution-active-response-to-cyber-attacks-has-high-risk/.

como las que afectan a la propiedad intelectual, *spam*, fraude, legislación contractual y leyes de responsabilidad civil. Además, pueden causarse daños colaterales a sistemas de terceros[36].

Algunas de las justificaciones que se han sugerido para tácticas de defensa activa incluyen la autodefensa, la persecución y la propiedad de los datos robados. Sin embargo, ninguna de estas justificaciones son lógicas, la propia justicia no es válida y el camino a seguir es, por el contrario, hacer que los sistemas y las redes sean más resistentes, mejorar la ciberdefensa (pasiva) y aplicar las legislaciones nacionales e internacionales[37].

Un sistema emergente de gestión integral de la ciberseguridad

Tras la anterior excursión al territorio de la ciberguerra, con sus ambigüedades, déficits y aterradoras implicaciones, la discusión una vez más se centra en el panorama de la amenaza mundial, con los ciberconflictos procedentes de los estados, actores no estatales –o una combinación de ambos–, los grupos terroristas, consorcios de la delincuencia organizada y delincuentes informáticos en general.

Dada la penetración casi total de las tecnologías cibernéticas en nuestras sociedades, se puede observar cada vez más cómo las organizaciones internacionales, los Gobiernos, la economía en general, la industria de las tecnologías de la información y la industria de seguridad TIC, así como la sociedad civil –la *stakeholder community* o comunidad de intereses, término comúnmente aceptado– unen sus fuerzas para combatir y mitigar las amenazas en el ciberespacio. En un documento de longitud limitada, este movimiento, en parte concertado y en parte autónomo, es imposible de cubrir; por lo tanto, haremos un esfuerzo por enumerar y evaluar sus principales formas de manifestación. Las palabras clave primordiales son: ciberdefensa, autoprotección y resistencia (*resilience*).

Resistencia (*resilience)* es la política orientada a la defensa que maximiza la capacidad de los sistemas objetivo para prevenir, disuadir y resistir ciberataques y, si estos se producen, minimizar y mitigar sus efectos; es un concepto multidimensional que posee componentes técnicos, organi-

[36] Ejemplos tomados de Westby, anterior nota al pie.

[37] Si el origen de un ataque económico se atribuye con una certeza razonable, algunas contramedidas económicas, como la suspensión de relaciones, la negativa al suministro, la retirada de los beneficios comerciales o –en el caso de un Gobierno– la supresión del estatus de nación más favorecida u otras medidas comerciales punitivas pueden ser legítimas. En respuesta a la oleada actual de ataques informáticos sobre activos de empresas e infraestructuras de EE. UU., el presidente Obama ha hablado recientemente de tales medidas.

zativos, políticos y legales que precisan combinarse para ser eficaces[38]. Debatiremos a su vez los requisitos del marco legal, aquellos de legítima defensa a nivel de empresas y usuarios finales, la mejora del diseño técnico de resistencia a los ataques, la capacidad de establecer estándares y buenas prácticas, los beneficios de las redundancias, la asistencia y cooperación social, la cooperación internacional y el cumplimiento de las leyes, el papel del intercambio de la información, los sistemas de alerta y respuestas a emergencias y, lo que es de vital importancia, la protección de infraestructuras críticas, nacionales y transfronterizas.

Creación de un marco legal armonizado para combatir los ciberdelitos y ciberconflictos

El ciberespacio no podía continuar como un espacio alegal, y con la llegada de las tecnologías de la información y la comunicación los legisladores se han enfrentado a una doble tarea: introducir las nuevas tecnologías dentro de sus sistemas legales nacionales y proporcionar un marco legal internacional armonizado para las causas penales y las sanciones y el cumplimiento de la ley, puesto que los ataques informáticos pueden suceder en cualquier parte del mundo. La mayoría de los países industrializados tienen ahora leyes contra los ciberdelitos, muchas de ellas muy adecuadas, pero con variaciones significativas al definir lo que constituye un ciberdelito en su detección e identificación y en las disposiciones procedimentales aplicables, que hasta hace poco han dificultado significativamente la investigación de estos delitos. El Convenio sobre Delitos Informáticos del Consejo de Europa[39] (en la Convención de Budapest se firmó en 2001 y entró en vigor en 2004) ha supuesto un avance de primera magnitud en la armonización global de la legislación sobre ciberdelitos, y me uno al profesor González Cussac en su elogio a este instrumento; también estoy de acuerdo con él en que los nuevos desarrollos y modos de ataque digitales con el tiempo harán necesaria una revisión del texto, a pesar de su validez actual[40].

Sin embargo, al escribir este artículo, la Convención solo ha sido firmada y ratificada por 39 países, y están pendientes 10 ratificaciones. Son significativas las ausencias de Rusia, China y, como tantas veces, de Israel,

[38] La Comisión Europea, pionera en construir estrategias digitales para los 27 miembros de la Unión Europea unificando así sus políticas digitales y de defensa, utiliza el concepto de «resistencia» como una finalidad primordial, por ejemplo, creando –a través de ENISA– una Asociación Europea Público-Privada de Resistencia (EP3R), y sitúa su reciente borrador de la Estrategia de Ciberseguridad de la UE bajo la plataforma «Alcanzando la resistencia cibernética».

[39] www.conventions.coe.int.

[40] *Estrategias legales frente a las ciberamenazas*, *Cuadernos de Estrategia*, n.º 149, *op. cit.*, p. 116.

así como la mayoría de los países del Tercer Mundo, quizás, porque son reticentes a adoptar un documento de origen europeo. El juego de herramientas de la UIT para la legislación de la delincuencia informática (*toolkit for cybercrime legislation)* se ha desarrollado como una alternativa que propone un lenguaje jurídico armonizado con el Convenio y las normas jurídicas sobre delitos informáticos de las naciones industrializadas. La utilización creciente de estos textos o la adopción de un lenguaje autónomo comparable por parte de los países que aún no han suscrito el Convenio ayudarán a que este proceso de armonización avance pronto. Es crucial. La Convención, naturalmente, deberá traducirse conforme a la legislación nacional de los países que ratifiquen los compromisos jurídicos internacionales.

Autoprotección

La ciberdefensa comienza en el hogar o en la empresa. Entre las obligaciones evidentes de un director de sistemas, se encuentra la introducción de tecnologías avanzadas de cortafuegos, antivirus y de incidentes, cifrado de información confidencial, control de acceso a las instalaciones y los equipos que incluya una rigurosa y bien diferenciada gestión de contraseñas («necesidad de conocer»), así como otras técnicas sofisticadas de autenticación. Si se permite BYOD (*bring your own device*), controles rigurosos deberán controlar estos equipos. Se requiere especial vigilancia sobre los sistemas SCADA de las infraestructuras críticas pues son especialmente vulnerables a los ataques de actores estatales, no estatales y terroristas, con un propósito agresivo de tipo militar o de cualquier otro. Esto debería ser obvio; no obstante, la experiencia demuestra que el robo de información confidencial tanto en las empresas como en agencias gubernamentales es, sobre todo, debido a la negligencia de personal interno. Más de nueve de cada diez brechas de seguridad podrían haberse evitado si las organizaciones hubieran seguido las mejores prácticas sobre la protección de datos y seguridad de la información[41].

Una de las tres causas principales de pérdida de datos es el robo o la pérdida física de sus equipos. Además, un informe de la industria alemana muestra que solo una pequeña parte de los correos electrónicos que contienen información altamente sensible, como proyectos de diseño industrial, van cifrados. Se da una falta sistemática de cifrado de los dispositivos móviles de las empresas. En muchos casos, no se prevén sistemas redundantes que en caso de ataque puedan conservar o restablecer rápidamente la funcionalidad de los sistemas o las conexiones.

[41] Cifras de ENISA.

Diseñar para la seguridad

Una importante laguna para los atacantes, casi desde el inicio, es que los diseñadores de *hardware* y *software*, centrándose principalmente en los beneficios de diseño que surgen de los avances técnicos para un mejor desarrollo, han puesto menos interés y esfuerzo en la seguridad de la información y la privacidad.

Además, la construcción de la seguridad desde el principio puede acarrear un coste adicional que reduce los márgenes de beneficios. Tradicionalmente, ha existido una brecha entre la producción y las industrias de seguridad favorecida por la ausencia de conciencia de los usuarios finales de los riesgos para la seguridad de la información y la privacidad inherentes a sus equipos; durante mucho tiempo, ha existido una incongruencia entre la seguridad objetiva y la percibida. Muchas empresas pequeñas pueden no tener los medios o las habilidades profesionales para instalar los medios de protección por sí solas.

Estas brechas de seguridad se están llenando actualmente por una industria más consciente de la seguridad, por una mayor conciencia de los usuarios finales, mayor cooperación e incluso iniciativas comunes de las distintas partes interesadas (véase, por ejemplo, la reciente adquisición de la importante empresa de seguridad McAfee por parte de Intel).

Incluso sería erróneo no dar crédito a las principales alianzas industriales formadas para promover la seguridad y el desarrollo seguro de *hardware*, *software* y arquitectura de redes, ejercicios colectivos que comenzaron en los años noventa del pasado siglo. El más importante es el Trusted Computing Group, con más de 100 miembros, colaboradores o usuarios de la industria. Su módulo –*trusted platform module* (TPM)– está normalizado con la ISO/IEC[42].

No obstante, dado el panorama de las amenazas, la obligación de la industria de *hardware* y *software* de «diseñar para la seguridad» permanece, como también es permanente la responsabilidad de instituciones públicas y privadas y de los países de establecer contratos de seguridad y políticas y estándares de certificación de seguridad[43].

[42] www.trustedcomputinggroup.org. El TPM se usa en los sistemas operativos de la mayoría de los grandes suministradores. El Trusted Computing se enfrenta, sin embargo, a serias críticas por parte de la comunidad de *software* libre en la medida en que fideliza a los clientes.

[43] En su *Agenda de seguridad global,* la UIT se compromete al «desarrollo de estrategias para la creación de unos criterios mínimos de seguridad mundialmente aceptados, y esquemas de acreditación para aplicaciones y sistemas de *software* y *hardware*». Ver también el capítulo *Designing for security* in *information security in the context of the digital divide,* recomendaciones presentadas ante la Cumbre Mundial de la Sociedad de la Información (noviembre de 2005) por el Panel Permanente de Seguridad Informática de la Federación Mundial de Científicos, Doc. WSIS-05/TUNIS/CONTR/01, en www.itu.int.

Sería especialmente útil asegurar el diseño de sistemas SCADA a través de esfuerzos colectivos. Todo esto se basa en la percepción de que todavía existe una escasez de métodos de análisis y diseño, científicamente probados, para dominar las enormes complejidades de los futuros sistemas digitales interconectados, especialmente en lo que se refiere a la seguridad física, la fiabilidad, el funcionamiento y la seguridad. La industria de la seguridad de las tecnologías de la información requiere una alta cualificación para estar al día, a un nivel altamente profesional, de los desafíos que debe enfrentar cada vez más. Las compañías de seguridad representan un negocio en rápida expansión, altamente exigente y competitivo, de miles de millones de dólares.

Establecimiento de estándares y buenas prácticas

La actuación de los Gobiernos y la propia organización de las empresas han creado un universo de estándares técnicos y operativos para asegurar las estructuras de las infraestructuras IT. Muchas de estas son de carácter voluntario, pero un sistema de certificaciones ofrece incentivos para adoptar una visibilidad pública. Las empresas que no apuestan por la excelencia en este área y que, en consecuencia, sufren ataques e intromisiones en sus datos no solamente pierden dinero, sino también reputación y clientes. Los estándares más importantes para la gestión de las tecnologías de la información y la comunicación, de aplicación prácticamente mundial, han sido elaborados por ISO/IEL[44] en las series 27000 y 13335 para el antes citado trusted platform module, en sus normas 11889-1 a 11889-4 sobre tecnologías de la información (2009). En EE. UU., el establecimiento de normas está a cargo del American National Standards Institute (ANSI). Durante años, la comunidad de usuarios, desarrolladores y proveedores de tecnología de Internet se han unido a la Internet Engineering Task Force (asociada a la Sociedad Internet) para el desarrollo y la promoción de estándares para la infraestructura de Internet, enrutamiento y la seguridad del transporte de datos. Además, en los problemas específicos de la informática distribuida, existe el Open Grid Forum para el establecimiento de estándares en informática y arquitectura de redes.

El International Information Systems Security Certification Consortium (ISC) (Consorcio Internacional de Certificación de la Seguridad de Sistemas Informáticos), descrito como «la mayor organización mundial de seguridad de tecnologías de la información» («la seguridad trasciende a la tecnología»), promueve la idea de normalización mediante la concesión de certificados de excelencia en operaciones seguras de tecnologías de la información (*certified Information Security professional,* CISSP, profesio-

[44] www.iso.org, www.iec.ch. El miembro español de ambas es AENOR, que también establece estándares propios (en este contexto, ver UNE 71502) y otorga certificaciones.

nal titulado en Seguridad De La Información); las áreas de elección para estos certificados también incluyen el desarrollo de *software* y el diseño y la arquitectura de seguridad. Actualmente, 85.285 miembros de 143 países poseen estos certificados. Los emisores de certificados, más allá de las agencias normativas tradicionales, los institutos, las asociaciones, las empresas particulares o los organismos intergubernamentales, son muchos, lo que, obviamente, refleja la necesidad de reconocer la excelencia y la generación de confianza. Una recopilación indicativa en la página web de Wikipedia del CISSP reúne 70 certificaciones diferentes[45].

Protección de infraestructuras críticas

CIIP, la protección de infraestructuras críticas de información[46]. Ha estado durante muchos años en el centro de atención de las políticas de seguridad de la información y de las estrategias para mejorar la resistencia, tanto por parte de los Gobiernos y organismos internacionales como por los propios operadores de estas infraestructuras. De hecho, en un contexto de ciberguerra sería la pieza clave de las estrategias defensivas y de todos los esfuerzos para optimizar la resistencia de los sistemas. Dada su importancia vital para el funcionamiento de la sociedad, la creciente vulnerabilidad de las infraestructuras en un ambiente interconectado y dependiente de Internet y los posibles efectos cascada que sus fallos pueden producir, es fácilmente comprensible esta prioridad. Las infraestructuras críticas son de las primeras en la línea de fuego de un ataque militar, terrorista y de consorcios criminales (crimen organizado), en este último caso como base para el chantaje.

En EE. UU., las directivas presidenciales desde la época del presidente Clinton han ordenado las medidas de protección necesarias. Asegurar las infraestructuras críticas y los sistemas de información es una parte fundamental del mandato del Departamento de Seguridad Nacional (DHS), ampliamente dotado en cada presupuesto anual. Las políticas CIIP

[45] La *Revista de Seguridad en Informática y Comunicaciones*, www.revistasic.com, una excelente publicación y con certeza la mejor sobre seguridad informática en España, ayuda al lector no profesional a mantener la pista de estas diversas distinciones conforme son recibidas por empresas españolas. La editora de esta publicación, SIC, organiza también conferencias sobre ciberseguridad en España de forma periódica.

[46] Se entiende que estas infraestructuras generalmente, y en el más amplio sentido, incluyen la generación de transmisión y distribución de electricidad, la producción, transporte y distribución de gas, la producción, transporte y distribución de petróleo, las telecomunicaciones, el suministro de agua potable y no potable (alcantarillado), el filtrado de aguas de superficie (por ejemplo, diques y compuertas), la agricultura, la producción y distribución alimentaria, la calefacción (por ejemplo, gas natural, diésel, hospitales, sistemas de transporte por ambulancia, redes ferroviarias, aeropuertos, puertos o navegación interior), servicios financieros y servicios de seguridad (Policía y Ejércitos). El componente energético se considera la parte más vulnerable.

ocupan un lugar destacado en la página de DHS www.dhs.gov. Limitando intensos esfuerzos anteriores, el presidente de EE. UU., el 13 de febrero de 2013, firmó una orden ejecutiva (EO) *sobre la mejora de la ciberseguridad de las infraestructuras críticas* y una directiva presidencial de política (PPD) *sobre seguridad de infraestructuras críticas y resistencia* cuyas lecturas resultan instructivas.

Otro actor de la mayor importancia es la Comisión Europea, asistida por su Agencia Europea de Seguridad de las Redes y de la Información (ENISA). Consciente de las diferencias aún existentes en los sistemas y los niveles de protección en los 27 países miembros, la UE ha estado durante tiempo trabajando en CIIP y en la armonización de las normas de protección.

En 2009, la Comisión adoptó un Plan de Acción y Comunicación sobre CIIP[47] y organizó una Conferencia Ministerial sobre CIIP[48]. Ya hemos mencionado el European Public-Private Partnership for Resilience (Consorcio Europeo Público-Privado de Resistencia). ENISA ha venido organizando varios Ejercicios Europeos de Ciberseguridad, con amplia participación de Gobiernos y del sector privado, el último de ellos en 2012[49]. Con el objetivo de fortalecer la comunidad de gestión de incidentes informáticos. El 7 de febrero de 2013 la Comisión publicó, en un comunicado conjunto con los demás órganos principales de la UE, la Ciberestrategia de la UE, que en un amplio repaso persigue establecer unos requisitos comunes mínimos a nivel nacional para cada miembro de los sistemas de información y de red (NIS), incidiendo sobremanera en la resistencia y la protección de las infraestructuras[50]. El Parlamento Europeo está también activo, y celebró su última reunión sobre CIIP el 6 de febrero de 2013.

Durante más de una década, la Unión Internacional de Telecomunicaciones (UIT) ha estado trabajando en la protección de infraestructuras críticas desde una perspectiva global y, últimamente, en referencia con su *Agenda global de ciberseguridad,* a pesar de lo cual aún no se ha logrado concebir un marco regulador uniforme. Sin embargo, existe una gran cantidad de estudios, publicaciones e informes de conferencias que son fácilmente localizables en la página web de la UIT, así como en la de su rama ejecutiva, el Consorcio Internacional Multilateral contra las Ciberamenazas (International Multilateral Partnership Against Cyber Threats,

[47] COM/2009/149, incluida por el Consejo de Europa en su resolución 2009/C 321/01. Ver también la Directiva 2008/114/CE sobre la Protección de Infraestructuras Críticas Europeas.

[48] www.tallinnciipeu.eu/?id=conference.

[49] Para localizaciones clave, ver www.enisa.europa.eu.

[50] JOIN (2013 1 final). La Estrategia viene acompañada de un borrador de directiva sobre medidas destinadas a asegurar un alto nivel común de medidas de protección cibernética.

IMPACT)[51]. El estudio anterior no es sino indicativo, y complementarlo con una descripción de las iniciativas nacionales excedería las posibilidades de este capítulo. Aun así, muchos, si no la mayoría de los países que participan en el mundo cibernético, se ocupan de CIIP en sus organismos nacionales como complemento de los esfuerzos internacionales. La Agencia Federal Alemana de Seguridad de la Información, por ejemplo, maneja una plataforma de Internet especializada en CIIP y patrocina una serie de publicaciones[52].

Resistencia en la informática en la nube y los dispositivos móviles

Los rápidos avances de la informática en la nube en enormes centros de datos y la masiva migración hacia dispositivos móviles que se ha descrito en anteriores secciones de este capítulo plantean la utilidad de analizar la resistencia a los ataques de estos nuevos centros de gestión de datos y operaciones cibernéticas, y señalar las novedades al respecto.

La computación o informática en la nube es una nueva modalidad para suministrar recursos informáticos, no una nueva tecnología. La concentración de datos y la prestación de servicios, escalables según la demanda, ofrecen enormes beneficios económicos, y por ello han atraído inversiones masivas a nivel mundial. Las previsiones mundiales de servicios en nube en 2013 indican un volumen previsible de negocio de 44.200 millones de dólares. ENISA lo ha expresado de forma palpable: las economías de escala y flexibilidad de la nube son al mismo tiempo un amigo y un enemigo desde el punto de vista de la seguridad. La concentración masiva de recursos y datos ofrece un objetivo más atractivo a los atacantes, pero las defensas basadas en la nube pueden ser más robustas, escalables y rentables. Los ataques contra centros de datos de estas dimensiones ofrecen nuevas e importantes oportunidades a un ataque terrorista o militar, lo que incluye la manipulación del suministro de energía y supondría una pérdida masiva de datos (siempre que se superen las redundancias de suministro eléctrico), la destrucción física o la intrusión cibernética en las bases de datos. Los temores de los clientes aumentan, ya que las masas de datos se mueven de forma aparentemente arbitraria e imposible de seguir entre unos y otros paneles, y el personal supervisor se convierte en anónimo y la confianza en la integridad y la privacidad de los datos se torna más difícil de mantener. Los riesgos de la informática en la nube son serios y suponen un importante desafío en lo que concierne a la seguridad.

[51] www.itu.int; www.itu.int/ITU-D/cyb/cybersecurity/impact.html.

[52] www.bsi.bund.de, para la plataforma CIIP. Ver: www.kritis.bund.de.

Por todo ello, no resulta sorprendente que la seguridad en la nube se haya convertido en un tema central en el actual debate sobre seguridad informática. En un mundo tan competitivo como el de la nube, los suministradores y las compañías de seguridad se superan unas a otras en la generación de confianza. Sin duda, pueden demostrar que existe una prima en la gestión de la seguridad en la nube. Toda clase de medidas de seguridad resultan más baratas cuando se implantan a gran escala, y la misma cantidad invertida en seguridad consigue una mejor protección (un perímetro físico y control de acceso más barato, mejor escalado de los recursos, más oportunidades de respuesta rápida, una gestión más eficaz de la amenaza, etc.). Los clientes, entre los cuales están también los Gobiernos, toman sus opciones económicas en gran medida a la luz de la resistencia de los servicios de seguridad ofrecidos, la reputación de confidencialidad y la transparencia de los procedimientos internos.

Últimamente destaca un importante factor diferenciador de las empresas europeas, ya que estas juzgan la protección legal de los datos en Europa mejor que en EE. UU., habida cuenta de la política de datos más intrusiva del Departamento de Seguridad Nacional.

Hoy en día la seguridad en la nube parece ser un asunto de todos. Las referencias de este artículo al trabajo analítico y a las recomendaciones sobre la materia están por ello limitadas a los recientes estudios de ENISA: el *Cloud computing: benefits, risks and recommendations for information security* antes citado y el *Critical cloud computing: A CIIP perspective on cloud computing* (14 de febrero de 2013), ambos en www.enisa.europa.eu.

Antes se han citado cifras sobre el impresionante crecimiento del número de dispositivos móviles y las consecuencias derivadas de la migración hacia las tecnologías móviles. También se ha destacado que la amenaza hacia los móviles es desproporcionada, por lo que los ciberataques a móviles son una característica dominante del panorama actual de amenazas. A pesar de que son extraordinariamente vulnerables a los ataques, los dispositivos móviles han permanecido virtualmente desprotegidos durante mucho tiempo. Solo bajo esta coyuntura aparece en el mercado el *software* antiataque para los sistemas operativos de móviles. Sin embargo, el futuro no puede asentarse en la descarga de *software* en dispositivos móviles individuales, sino en la vigilancia centralizada de los clientes móviles desde la nube, como demuestra una alianza entre Vodafone y BAE Systems que se está introduciendo en el mercado a través de una asociación estratégica de cinco años[53]. La promesa de esta aproximación a la vigilancia de la nube es que no se refiere solo a *smart phones,* sino también a *tablets* y, eventualmente, a RFID, los sistemas de

[53] «BAE and Vodafone in cyber safety deal», *Financial Times,* «And news services», 18 de febrero de 2013.

control en fábricas inteligentes y otros sistemas ciberfísicos que podrían ser protegidos eficazmente.

Cooperación nacional e internacional en ciberseguridad

Habida cuenta de la naturaleza transparente y global de las estructuras de red digitales, un asunto de indudable necesidad es conseguir una amplia cooperación nacional e internacional de la comunidad de interesados en combatir y mitigar las consecuencias derivadas de ciberconflictos, como se reconoce a nivel mundial. Los patrones de cooperación existentes actualmente, y que deben mejorarse, incluyen intercambios efectivos de información, como la notificación de incidentes, asistencia mutua –también para activar redundancias–, respuestas a incidentes organizados, sistemas de alarma, puntos de contacto dentro y entre las naciones, mejora de la cooperación en el cumplimiento de las leyes y requisitos organizativos para hacer funcionar todos estos desiderátums.

Estas medidas, y otras relacionadas, parecen bastante sencillas, y su utilidad con vistas a una estrategia de prevención, defensa, sanción y mitigación de los incidentes propios de un conflicto digital es bastante evidente por sí sola. Por ello, no sorprende que las categorías y el número de actores involucrados en ellas sean enormes y muy diversas. Nos encontramos aquí con procesos de continua expansión, difíciles de resumir en un análisis breve. Baste con mencionar unos cuantos desarrollos que indican las próximas tendencias.

Encomendado por la Cumbre Mundial sobre la Sociedad de la Información para coordinar las respuestas internacionales sobre la ciberseguridad, la UIT ha elaborado una *Agenda global de ciberseguridad* que promueve muchas de las tareas de cooperación a nivel mundial, que culminan en un marco de una estrategia global de las múltiples partes interesadas para la cooperación y el diálogo internacionales. Esta agenda persigue sus objetivos de forma dinámica, como puede desprenderse de las páginas web de la UIT.

Un elemento importante de esta estrategia de cooperación es aquel que afecta a la información crítica a través de fronteras. El mecanismo clave es el enfoque «24/7» (24 horas durante 7 días), la disponibilidad permanente de puntos de contacto en caso de gestión de incidentes informáticos. El primer plan internacional se desarrolló con el G-8 en 1998: el grupo de G8 creó una red de expertos en el cumplimiento de las leyes de entre sus miembros, funcionando las 24 horas, pero también se unieron otros Gobiernos. En la UE, el primer programa 24/7 vino acompañado de la decisión marco del Consejo sobre ataques contra los sistemas de información de 2003. Un enfoque más sistemático forma parte del Convenio de Delitos Cibernéticos (Budapest) que, aparte de armonizar el derecho penal sustantivo de los delitos informáticos, ha aportado poderes

legislativos procesales necesarios para investigar y procesar delitos domésticos, pero también ha establecido un régimen ágil y eficaz de cooperación internacional y asistencia mutua (art. 23 y siguientes del Convenio) para el «seguimiento y rastreo» que incluye normas sobe la conservación expedita de los datos almacenados y en tráfico, etc. En el art. 35 se establece una red permanente 24/7 con equipos adecuados y personal capacitado a fin de asegurar la disponibilidad de apoyo inmediato con fines de investigación y procesamiento, incluida la recopilación de pruebas y la localización de sospechosos. Muchos Gobiernos participan en la puesta en marcha del 24/7, incluso más allá de las obligaciones que impone el tratado ya existente.

Un elemento de creciente importancia en la notificación de incidentes, asistencia mutua, alerta temprana, información de riesgo, etc. son los Equipos de Respuesta a Emergencias Informáticas (Computer Emergency Response Teams, CERT), también conocidos como Equipos de Respuesta a Incidentes de Seguridad Informática (Computer Security Incidents Response Teams, CSIRT). Liderados por la Universidad Carnegie Mellon y con fondos del Departamento de Defensa de EE. UU., los CERT nacieron en 1988 y son hoy una red de dimensiones globales. En muchos países existe una CERT del Gobierno central que se ocupa de la coordinación con otros CERT nacionales, y específicamente con asegurar infraestructuras digitales del Gobierno.

Los CERT son equipos de expertos en tecnologías de la información que siguen y procesan la información sobre incidentes informáticos; analizan, recomiendan, coordinan y prestan asistencia para combatir ciberataques y reparar los daños, y a menudo emiten boletines informativos y advertencias sobre nuevas amenazas. Por todo el mundo existen actualmente más de 250 organizaciones que emplean esta denominación, y que se ocupan de dar respuesta a la seguridad informática.

En muchos paises, la industria y las instituciones académicas han tomado la iniciativa de establecer CERT. En EE. UU., el Departamento de Seguridad Nacional ha establecido el US CERT, que coordina el CERT/CC, en parte financiado a nivel federal por la comunidad US CERT y liderado por la Carnegie Mellon. En Alemania, una tarea similar es llevada a cabo por el BSI, a través del CERT-Bund. En España, funciona el Centro de Respuesta a Incidentes de Seguridad TIC de INTECO, un órgano del Ministerio de Industria, y su oficina ejecutiva Red.es. Como parte de su *Agenda global de ciberseguridad,* la UIT apoya a los países en vías de desarrollo en la creación de sus CERT nacionales. En septiembre de 2012, la Unión Europea estableció un CERT-EU, en un principio para proteger sus propias entidades pero también para asociarse con CERT nacionales y gubernamentales del área de la UE. Al mismo tiempo, en su *Agenda digital* de 2010 la Unión Europea convocó a sus miembros a establecer sus propios CERT nacionales, un desarrollo que debía completarse en 2012,

allanando así el camino para una red comunitaria eficaz de respuesta a incidentes.

En un movimiento paralelo, en febrero de 2013, la UE ha creado un Centro Europeo de Delincuencia Informática (EC3), en EUROPOL, cuya finalidad se centra específicamente en grupos organizados que buscan grandes beneficios y un impacto hostil en infraestructuras con mayores poderes de investigación.

Para el futuro es necesario universalizar el movimiento CERT y hacer que los CERT sean más operativos y estén interconectados; pero también que, desde luego, constituyan un arma defensiva de primer nivel contra los ataques informáticos y para minimizar los ciberconflictos[54].

En el momento en que se elabora este capítulo, uno no puede sino observar un crecimiento de los ataques informáticos a Gobiernos e industrias, mayoritariamente con APT (amenazas persistentes avanzadas), como también una creciente toma de conciencia de que todos los interesados deben hacerse más activos y próximos en el intercambio de información y en compartir los recursos de defensa digital.

Un ejemplo notable de los amplios esfuerzos de autoayuda de la industria es la alianza colectiva para la ciberseguridad pilotada en Europa por René Obermann, consejero delegado de Deutsche Telecom, quien ha solicitado que se comuniquen voluntariamente más informes sobre incidentes y que haya una mayor transparencia[55].

Una cultura de ciberseguridad: normas de conducta en la era digital

Hasta el momento, solo *algunos* de los aspectos legales generales han sido considerados: el derecho internacional define con ambigüedad los límites de la ciberguerra y «ataque armado», así como la armonización de la legislación sobre delitos informáticos en sus dimensiones nacionales y transfronterizas. Naturalmente, aunque no se mencione, en la mayoría de países es válido un régimen de derecho civil que rige los daños y perjuicios, así como el pertinente derecho internacional privado.

[54] Desde 1990, los CERT están coordinando e intercambiando información desde una organización internacional informal, FIRST (Forum of Incident Response and Security Teams); pero existe espacio para una coordinación más efectiva. Ya en 2004, este autor recomendó que el enfoque CERT no solamente debería ser universal sino que, más allá de la asistencia y el procesamiento de información individuales, debería desarrollar un enfoque de «lecciones aprendidas». Ver: WEGENER, Henning. *Learning lessons from cyber attacks: Broadening the CERT framework*, en www.unibw.de/infosecur.

[55] Ver, por ejemplo: OBERMANN, René. «Uniting for cyber defence», *New York Times, op. ed.,* 21 de febrero de 2013.

Pero todo esto está lejos de cumplir los requisitos de un régimen de funcionamiento en el ciberespacio capaz de combatir y soportar los ciberconflictos. En términos legales, la nueva área del ciberespacio inicialmente era un vacío necesitado de un marco detallado de normas no solo para los estados, sino para todas las partes interesadas. La tarea consistía en desarrollar, con el tiempo, una serie de normas de conducta de convivencia –de una cultura de ciberespacio y de seguridad digital– que incluyese un marco legal global para gestionar y controlar el omnipresente e infinito potencial de las tecnologías digitales. En consecuencia, existe poca o ninguna capacidad para controlar por ley la escalada de ciberconflictos o garantizar el uso pacífico del ciberespacio y, como hemos visto, existen ambigüedades al concebir cómo debe aplicarse la legislación internacional existente. Sin duda, esto representa un peligroso y precario estado de cosas. El grupo sobre seguridad digital en el que sigo participando activamente, la Federación Mundial de Científicos, desde el principio reclamó que Naciones Unidas dirija los esfuerzos para la creación de una ley universal e integral del ciberespacio[56]. Sin embargo, por una serie de razones, un tratado único no ha demostrado ser una opción realista.

Afortunadamente, la reflexión colectiva sobre los procesos necesarios para la estrategia digital ha evolucionado notablemente. Para hacer corta una larga historia, una nueva era de diplomacia cibernética comenzó en torno a 2008, con un consenso internacional emergente manifiestamente hacia la concentración de los esfuerzos como una alternativa al establecimiento formal de tratados globales: la elaboración de medidas de fomento de la confianza o códigos de conducta como instrumentos normativos. Podemos estar asistiendo a un punto de inflexión en la diplomacia de seguridad informática.

La opinión predominante es que las CBM (*confidence building measures*) –las medidas de confianza– y los códigos de conducta abren una ventana a las oportunidades para progresar realmente hacia definiciones comunes y normas de comportamiento. Las CBM tienen capacidad para reducir amenazas, aumentar la transparencia y hacer predecible la conducta de los países; además, son flexibles, voluntarias y ofrecen una geometría variable en función de sus participantes –es posible incluir actores no

[56] *Towards a universal order of cyber space: Managing the threat from cyber crime to cyber war,* Doc. WSIS-03/GENEVA/CONTR/6-E, www.itu.int/dms_pub/itu-s/md/03/wsis/c/S03-WSIS-C-0006!!PDF-E.pdf, también en www.unibw.de/infosecur. Ver también: KAMAL, Ahmad. *The law of cyber space: An invitation to the table of negotiations.* Génova: UNITAR, 2005, www.un.int/kamal/thelawofcyberspace. Rusia ha abogado desde 1998, en una serie de resoluciones en Naciones Unidas, por un tratado, proponiendo contenidos hasta cierto punto conflictivos y probablemente de imposible aplicación. Ver Res. A/53/70 hasta A/65/41. Estas resoluciones, sin embargo, tuvieron el incuestionable mérito de mantener vivo el debate, en el sentido de que se requería un esfuerzo normativo universal a gran escala.

estatales– y seguimiento: a diferencia de la elaboración de tratados coherente, los participantes son libres para adoptar soluciones parciales y ponerlas en práctica sin demoras, independientemente o con otras partes interesadas que piensen de igual modo. Las CBM apoyadas por estados no requieren ratificación, invitan a la imitación y, en su grado máximo (y mejor), son políticamente vinculantes. Están por ello excepcionalmente indicadas para fomentar la creación de consenso internacional a escala evolutiva. Un paquete bien negociado de CBM con una masa crítica de participantes puede poner en marcha un proceso de cambio gradual y mayor sensibilidad. La clarificación de las normas de comportamiento puede servir como un incentivo para ir a más.

Actualmente existen numerosas actividades internacionales paralelas que conjuntamente contribuyen a la creación de un consenso. Baste con citar algunas. En 2011 se constituyó un grupo de expertos de Naciones Unidas, con el mandato concreto de «definir medidas cooperativas (...) incluyendo normas, reglas, principios de responsabilidad de los estados y mensajes de fomento de la confianza en el espacio de la información»[57], que informará en 2013. Los Gobiernos han proporcionado numerosas aportaciones al grupo a petición del secretario general de Naciones Unidas[58]; sus puntos de vista han apoyado firmemente la idea de identificar CBM. En poco tiempo, han surgido oleadas de declaraciones nacionales de otros países en este mismo sentido: desde Australia, el Reino Unido, Alemania y, al menos de manera implícita, EE.UU., entre otros[59]. Un portavoz autorizado de la India se ha unido al concierto[60]. China, Rusia, Tayikistán y Uzbekistán reflejaron los trabajos del Consejo de Cooperación de Shanghái y remitieron al secretario general de Naciones Unidas en septiembre de 2011 un borrador de código internacional de conducta sobre seguridad informática[61]. A pesar de que el documento, en virtud de la elección de sus autores, no desprendía un excesivo aroma de correc-

57 A/Res/66/24 de 13 diciembre de 2011.

58 A/66/152 y A/66/152, add.1.

59 Ver la anterior nota al pie y las expresiones positivas en la sesión del Diálogo de Shangri-La, *IISS news,* julio de 2012. Para Alemania, ver también «Challenges in cyber security: Risks, strategies and conference building», *Conference report.* Berlín: 13 y 14 de diciembre de 2011.
www.auswaertiges-amt.de/DE/Aussenpolitik/Friedenspolitik/Abruestung/Projekte/Cybersicherheit.html. El Ministerio Federal de Asuntos Exteriores de Alemania, además, apoya un proyecto de UNIDIR sobre ciberseguridad internacional y CMB en 2012.

60 GUPTA, Arvind. *CBMs in cyber space: What should be India's approach?* IDSA, Institute for Defence Studies and Analysis, 27 de junio de 2012.

61 A/66/359. Ver también el acuerdo entre los Gobiernos de los estados miembros de la Organización de Cooperación de Shanghái sobre Cooperación en el campo de la Seguridad Internacional de Información, firmado en Ekaterinburgo el 15 de junio de 2009.

ción política, el catálogo de compromisos ofrecidos mediante suscripción voluntaria no debe ser desdeñado.

Al mismo tiempo, los países miembros han organizado conferencias de prestigio internacional en las que se ha aireado la idea de las CBM y catálogos más o menos detallados con los contenidos o aportaciones a las CBM que han figurado en los resúmenes de las conferencias (Londres, Berlín, Pekín, Viena, Budapest). Además del ejercicio de las Naciones Unidas en curso, las organizaciones regionales también se están involucrando en el acto. Por ejemplo, el foro regional ASEAN, con sus miembros representativos y participantes, 27 naciones que trascienden sobradamente el ámbito geográfico de Asia, se ha inmerso de lleno en el tema CBM[62], y la OSCE, consciente de su anterior experiencia con CMB orientales y occidentales, está trabajando activamente en un borrador de código de conducta (ver *A comprehensive approach to cyber security*[63]).

También la APEC[64], así como la Organización de Cooperación de Shanghái[65], está trabajando en acuerdos regionales. El Consejo de Europa, famoso por su contribución a una ley penal mundial sobre delitos cibernéticos a través del Convenio sobre el Ciberdelito, ha adoptado 10 principios sobre la gobernanza en Internet[66], y el UNIDIR ayuda a suministrar el sustento académico para estos esfuerzos[67]. Las ONG en el área cibernética, así como investigadores individuales, ofrecen sus propios catálogos de conducta. Obviamente, estos catálogos no pueden reproducirse ni analizarse aquí, pero representan herramientas efectivas para estimular el debate y facilitar las negociaciones de CBM[68]. Es de esperar que el actual

[62] La secretaria de Estado, Clinton, en el encuentro de ASEAN en Pnom Penh el 12 de julio de 2012: «Este foro incluye algunos de los mayores actores cibernéticos del mundo. Por ello, es un lugar apropiado para un diálogo sostenido y lleno de contenidos sobre asuntos que atañen al ciberespacio. En los años que nos aguardan, debemos trabajar juntos en apoyo de normas y estándares responsables, y perseguir medidas prácticas para reforzar la confianza y reducir los riesgos». El ARF organizará un Seminario sobre Medidas de Fortalecimiento de la Confianza en el Ciberespacio en Seúl el próximo mes de septiembre. En mayo de este año, los ministros de Defensa de ASEAN han reclamado un «plan director ASEAN sobre conectividad segura».

[63] www.osce.org/event/cyber_sec2011.

[64] Ver el APEC TEL *Strategic Action Plan* (Plan de Acción Estratégica 2010-2015, www.apec.org).

[65] No se pudo detectar ninguna página web en inglés. Resulta mejor recoger la información de las páginas web de los países miembros.

[66] www.coe.int.

[67] El UNIDIR (United Nations Institute for Disarmament Research, www.unidir.org) organiza conferencias y participa en otras. Particularmente relevante es la conferencia 2012 sobre *The role of confidence-building measures in assuring cyber stability (El papel de las medidas de fomento de confianza en la garantía de ciberestabilidad).*

[68] Para una posible lista de principios que debieran incorporarse a un código de conducta global, ver: WEGENER, Henning. *La 'ciberguerra' se puede evitar.* Madrid: Política Exterior, n.º 146, marzo-abril de 2012, p. 140; del mismo autor, *Die diplomatie des cy-*

dinamismo en promover negociaciones sobre tales medidas de fomento de la confianza y códigos de conducta se mantenga y que pronto se alcance un acuerdo sobre un escenario apropiado para la negociación.

Con el fin de aportar al lector al menos algunas ideas sobre los contenidos de los actuales esfuerzos normativos, se incluye una breve referencia de una corta lista publicada por el secretario General de la UIT:

1. Todos los Gobiernos deben comprometerse a dotar a su pueblo del acceso a las comunicaciones.
2. Todo Gobierno se comprometerá a proteger a su pueblo en el ciberespacio.
3. Todo Gobierno se comprometerá a no acoger terroristas ni delincuentes en su territorio.
4. Todos los países deben comprometerse a no ser los primeros en lanzar un ataque cibernético contra otros países.
5. Todos los países deben comprometerse a colaborar entre sí dentro de un marco de cooperación internacional para asegurar la paz.

Para la UIT, esta concisa lista constituye la esencia de la ciberestabilidad, y una parte importante de la paz digital. En el mismo sentido se orienta la Declaración Erice *sobre principios de ciberestabilidad y ciberpaz,* que emana de la Federación Mundial de Científicos, cuya lista de principios culmina en un llamamiento a «evitar el uso del ciberespacio para el conflicto». La ciberguerra puede evitarse, y no debería ser considerada como un instrumento legítimo de conflictos militares. Eso supondría un largo camino para aliviar la ambivalencia de la tecnología cibernética y podría reducir sensiblemente los riesgos y las preocupaciones económicas. La paz en el ciberespacio –la *ciberpaz*– es la mejor elección[69].

ber-friedens, 2011, en www.unibw.de/infosecur, y también: «Regulating cyber behavior: Some initial reflections on codes of conduct and confidence-building measures» («Regulando la conducta cibernética: algunas reflexiones Iniciales sobre códigos de conducta y medidas de fomento de confianza»), agosto de 2012. *The science and culture series,* Sigapur: World Scientific, 2013, en prensa.

[69] Ver también WEGENER, Henning. *A concept of cyber peace in the quest for cyber peace, op. cit.*(«Un concepto de paz cibernética en la búsqueda de la paz cibernética»), 2011. En la misma publicación, la Declaración de Erice está también reimpresa.

Composición del grupo de trabajo

Coordinador:	**Don Eduardo Olier Arenas** *Presidente del Instituto Choiseul España* *Director de la cátedra de Geoeconomía de la Universidad CEU San Pablo*
Vocal y secretaria:	**Doña María José Caro Bejarano** *Analista principal del Instituto Español de Estudios Estratégicos*
Vocales:	**Don Antonio M. Díaz Fernández** *Profesor titular de Ciencia Política y de la Administración de la Facultad de Derecho de la Universidad de Cádiz*
	Don Christian Harbulot *Director de l'École de Guerre Économique de París* *Socio gerente de la empresa Spin Partners*
	Don José L. González Cussac *Catedrático de Derecho Penal de la Facultad de Derecho de la Universidad de Valencia*
	Don Fernando Palop Marro *Cofundador de Triz XXI* *Profesor asociado de la Universidad Politécnica de Valencia*

Don Henning Wegener
Exembajador de Alemania en España.
Presidente del Observatorio Permanente para la Ciberseguridad de la Federación Mundial de Científicos

Cuadernos de Estrategia

01 La industria alimentaria civil como administradora de las FAS y su capacidad de defensa estratégica

02 La ingeniería militar de España ante el reto de la investigación y el desarrollo en la defensa nacional

03 La industria española de interés para la defensa ante la entrada en vigor del Acta Única

04 Túnez: su realidad y su influencia en el entorno internacional

05 La Unión Europea Occidental (UEO) (1955-1988)

06 Estrategia regional en el Mediterráneo Occidental

07 Los transportes en la raya de Portugal

08 Estado actual y evaluación económica del triángulo España-Portugal-Marruecos

09 Perestroika y nacionalismos periféricos en la Unión Soviética

10 El escenario espacial en la batalla del año 2000 (I)

11 La gestión de los programas de tecnologías avanzadas

12 El escenario espacial en la batalla del año 2000 (II)

13 Cobertura de la demanda tecnológica derivada de las necesidades de la defensa nacional

14 Ideas y tendencias en la economía internacional y española

15 Identidad y solidaridad nacional
16 Implicaciones económicas del Acta Única 1992
17 Investigación de fenómenos belígenos: método analítico factorial
18 Las telecomunicaciones en Europa, en la década de los años 90
19 La profesión militar desde la perspectiva social y ética
20 El equilibrio de fuerzas en el espacio sur europeo y mediterráneo
21 Efectos económicos de la unificación alemana y sus implicaciones estratégicas
22 La política española de armamento ante la nueva situación internacional
23 Estrategia finisecular española: México y Centroamérica
24 La Ley Reguladora del Régimen del Personal Militar Profesional (cuatro cuestiones concretas)
25 Consecuencias de la reducción de los arsenales militares negociados en Viena, 1989. Amenaza no compartida
26 Estrategia en el área iberoamericana del Atlántico Sur
27 El Espacio Económico Europeo. Fin de la Guerra Fría
28 Sistemas ofensivos y defensivos del espacio (I)
29 Sugerencias a la Ley de Ordenación de las Telecomunicaciones (LOT)
30 La configuración de Europa en el umbral del siglo XXI
31 Estudio de «inteligencia operacional»
32 Cambios y evolución de los hábitos alimenticios de la población española
33 Repercusiones en la estrategia naval española de aceptarse las propuestas del Este en la CSBM, dentro del proceso de la CSCE
34 La energía y el medio ambiente
35 Influencia de las economías de los países mediterráneos del norte de África en sus respectivas políticas defensa
36 La evolución de la seguridad europea en la década de los 90
37 Análisis crítico de una bibliografía básica de sociología militar en España. 1980-1990
38 Recensiones de diversos libros de autores españoles, editados entre 1980-1990, relacionados con temas de las Fuerzas Armadas
39 Las fronteras del mundo hispánico
40 Los transportes y la barrera pirenaica
41 Estructura tecnológica e industrial de defensa, ante la evolución estratégica del fin del siglo XX

42 Las expectativas de la I+D de defensa en el nuevo marco estratégico
43 Costes de un ejército profesional de reclutamiento voluntario. Estudio sobre el Ejército profesional del Reino Unido y (III)
44 Sistemas ofensivos y defensivos del espacio (II)
45 Desequilibrios militares en el Mediterráneo Occidental
46 Seguimiento comparativo del presupuesto de gastos en la década 1982-1991 y su relación con el de Defensa
47 Factores de riesgo en el área mediterránea
48 Las Fuerzas Armadas en los procesos iberoamericanos de cambio democrático (1980-1990)
49 Factores de la estructura de seguridad europea
50 Algunos aspectos del régimen jurídico-económico de las FAS
51 Los transportes combinados
52 Presente y futuro de la conciencia nacional
53 Las corrientes fundamentalistas en el Magreb y su influencia en la política de defensa
54 Evolución y cambio del este europeo
55 Iberoamérica desde su propio sur. (La extensión del Acuerdo de Libre Comercio a Sudamérica)
56 La función de las Fuerzas Armadas ante el panorama internacional de conflictos
57 Simulación en las Fuerzas Armadas españolas, presente y futuro
58 La sociedad y la defensa civil
59 Aportación de España en las cumbres iberoamericanas: Guadalajara 1991-Madrid 1992
60 Presente y futuro de la política de armamentos y la I+D en España
61 El Consejo de Seguridad y la crisis de los países del Este
62 La economía de la defensa ante las vicisitudes actuales de las economías autonómicas
63 Los grandes maestros de la estrategia nuclear y espacial
64 Gasto militar y crecimiento económico. Aproximación al caso español
65 El futuro de la Comunidad Iberoamericana después del V Centenario
66 Los estudios estratégicos en España
67 Tecnologías de doble uso en la industria de la defensa
68 Aportación sociológica de la sociedad española a la defensa nacional