recibido: 16.09.13 / aceptado: 01.10.13

Las ciberguerras, un tema en ascenso en el periodismo internacional

Josep M. Sanmartí
Universidad Carlos III de Madrid

Palabras clave

Ciberguerra, ciberataques, *hackers*, daños, periodismo internacional, alarmismo

Resumen

El objetivo de este artículo es señalar las principales dificultades con se encuentran los periodistas de información internacional al tratar el tema de las ciberguerras o los ciberataques, dificultades que obviamente se trasladan a las audiencias.

Las nuevas tecnologías de la información y la comunicación han desarrollado, en efecto, su propia capacidad destructiva en forma de ciberataques. Estos pueden ser aplicados a otros conflictos existentes o establecer sus propias estrategias por actores brumosos que incluyen desde superpotencias hasta *hackers* aficionados. Tal como admiten abiertamente personalidades e instituciones mundiales, su potencialidad para causar grandes daños, su escaso coste, su anonimato habitual, su implicación con el espionaje estatal y empresarial, etc., han convertido los ciberataques en una amenaza, que, sin ser sangrienta hasta ahora, es parecida a la nuclear, solo que mucho más confusa. Por esta razón, algunos expertos y medios hablan de una nueva Ciberguerra Fría.

La sección de Internacional de todos los medios refleja este temor difuso aunque real y de consecuencias imprevisibles. Los periodistas se enfrentan a un tipo de información fácilmente espinoso, de alcance ignorado, con agentes con frecuencia desconocidos, fuentes sospechosas, campañas de intoxicación, tecnologías sofisticadas, etc. y que sin embargo puede ser muy trascendente. Es fácil constatar, por ejemplo, que la ciberguerra incide abiertamente en las relaciones entre países, incluso entre países aliados. Por esto, una de las consecuencias más corrientes es el alarmismo, que a su vez acrecienta las dificultades objetivas propias del tema.

DOI: http://dx.doi.org/10.6035/2174-0992.2013.6.7

E-wars, an increasing subject in international journalism

Keywords

E-wars, cyber attacks, hackers, damages, international journalism, alarmism

Abstract

The aim of this article is to point out the main difficulties that journalists of international information have to discuss about the subject of the cyber wars (e-wars) or cyber attacks, difficulties who obviously are transferred to the audiences. Indeed, new technologies of information and communication have developed their own destructive capability in the form of cyber-attacks. These can be applied to other conflicts or establish their own strategies for foggy actors ranging from superpowers to amateur hackers.

As they openly admit personalities and institutions worldwide, its potential to cause big damages, their low cost, their usual anonymity, his involvement with State and corporate espionage, etc., cyber attacks have become a threat, which, without being bloody so far, is similar to nuclear war, only that much more confusing. For this reason, some experts and media speak of a new Cyber Cold War.

All media international section reflects this diffuse fears although real and with unpredictable consequences. Journalists are facing a type of information easily thorny, with an ignored scope, frequently unknown agents, suspicious sources, campaigns of black propaganda, sophisticated technologies, etc. and which can however be very transcendent.

It is easy to see, for example, that e-war, often affect relationships between countries, even among allies. For this reason, one of the most common consequences is alarmism, which in turn increases the objective difficulties of the subject.

Autor

Josep M. Sanmartí Roset [josemaria.sanmarti@uc3m.es] es periodista y profesor titular en el Departamento de Periodismo y Comunicación Audiovisual de la Universidad Carlos III de Madrid y doctor en el Programa de Relaciones Internacionales de la UCM. Coordina la materia de Periodismo internacional I: la información global en la UC3M, y es miembro del grupo de investigación PASEET.

DOI: http://dx.doi.org/10.6035/2174-0992.2013.6.7

1. Introducción

La sección de Internacional de los medios de comunicación se ha ido convirtiendo durante los últimos años en un cajón de sastre de asuntos diversos, que reflejan de forma sistemática la complejidad, la interconexión y la velocidad que distinguen al mundo actual. Sin embargo, siguen predominando los temas relacionados con conflictos, especialmente los bélicos, a causa tanto de la sensibilidad instalada en la opinión pública hacia los sufrimientos y las destrucciones ocasionadas por las guerras, como por la larga tradición que tiene esta información en la historia del periodismo desde el siglo XVI.

En esta área han aparecido desde los años 90 las noticias y los comentarios basados en las ciberguerras o los ciberconflictos (*e-war*, en terminología inglesa*)*, noticias que ciertamente se han acelerado en los dos o tres últimos años y que están adquiriendo un protagonismo cada vez más destacado. Se trata de la información relacionada con acciones llevadas a cabo a través de las tecnologías de la información y la comunicación y las telecomunicaciones actuales con una finalidad destructiva a gran o a pequeña escala. Es decir, que la progresiva sofisticación de la Red ha servido también para amplificar y ramificar los efectos de estas operaciones perturbadoras. El WorldEconomicForum (WEF) sitúa los ataques en un mundo hiperconectado entre las cinco amenazas principales para 2013, al lado de las medioambientales, las económicas, las geopolíticas y las sociales.

> «Mientras que sus beneficios son evidentes y están bien probados, nuestro hiperconectado mundo es capaz asimismo de expandir rápidamente información viral que intencionadamente o sin proponérselo sea distorsionadora o provocadora con serias consecuencias»(World Economic Forum, 2013: 23).

Por todo ello, ya se habla abiertamente de una Guerra Fría cibernética (Andrades, 2013: 1).

Más concretamente, el 11 de octubre de 2012 el entonces Secretario de Estado de Defensa de los EEUU, León Panetta, pronunció una sonada conferencia en Nueva York en la que hizo público y oficial que agentes extranjeros estaban explorando las redes informatizadas de compañías norteamericanas consideradas decisivas con el fin de preparar ataques cibernéticos dirigidos contra instalaciones químicas, eléctricas, plantas de agua potable y de transportes a lo largo y ancho de todo el país. Un ataque cibernético múltiple sería capaz de conducir a «un ciber Pearl Harbor, que podría causar destrucciones físicas y pérdidas de vida, paralizar y desorganizar el país, así como provocar una nueva y profunda sensación de vulnerabilidad».

Panetta apuntó que países como China, Rusia e Irán podrían estar detrás de estas operaciones. Por ello, el gobierno norteamericano ya estaba tomando medidas defensivas de distinta índole, algunas de las cuales enunció (Reed, 2012).

Cinco meses más tarde, el 11 de marzo de 2013, la Comisión de Inteligencia del Senado norteamericano conoció un amplio informe presentado por el Director de la Inteligencia Nacional, James R. Clapper, sobre las amenazas mundiales. El do-

DOI: http://dx.doi.org/10.6035/2174-0992.2013.6.7

cumento anunciaba que una de las más graves era precisamente la ciberseguridad (Clapper, 2013). Entre estos ataques citaba los experimentados por bancos y mercados de valores norteamericanos y especialmente por la petrolera SaudiAramco en 2012. Las sospechas se centraron de nuevo en Irán, actuando como represalia a los ciberataques sufridos por la central nuclear de Natanz en 2010 a través del virus Stuxnet. En todo caso, parece que el epicentro, o por lo menos su parte más visible, de estas ciberguerras es el programa nuclear de Irán y en segundo lugar las tensiones nucleares entre Corea del Norte y Corea del Sur.

La experiencia en curso indica que continúan las guerras tradicionales de baja o media intensidad y además que permanecerán, y el caso actual de Siria es un buen ejemplo de ello, pero hay razones poderosas para creer que muchos conflictos geoespaciales, económicos, militares, religiosos, culturales, etc. se trasladarán al ciberespacio. La mayor peculiaridad que identifica a las ciberguerras es que en teoría tienen capacidad para desencadenar efectos tan letales como las guerras clásicas (colapso de territorios —incluso de países enteros— o de sectores estratégicos, bloqueo de redes informáticas básicas, expandir información falsa y desinformar, causar alarmas sociales masivasy gratuitas, anular o contrarrestar sistemas defensivos tradicionales o informatizados, etc.), pero no tienen por qué ser (o por lo menos parecerlo) sangrientas, son mucho más baratas (sólo se requiere la debida tecnología y un puñado de expertos) y reflejan además una gran capacidad tecnológica aplicable a muchos otros terrenos, por ejemplo industriales. Por otra parte, esta tecnología de relativamente bajo coste es susceptible de ser instalada de forma ubicua y en distintos lugares, si se tercia hasta en el interior del país agredido, lo que hace muy difícil, si bien no es imposible, su detección y acometer las acciones para contrarrestarla.

En su documento para una Estrategia de Seguridad de 2011 el gobierno español afirmaba que

> «los ciberataques son una amenaza en crecimiento con la que los posibles agresores —terroristas, crimen organizado, empresas, Estados o individuos aislados— podrían poner en dificultad infraestructuras críticas. Existen precedentes (Estonia en 2007, Georgia en 2008 o Irán en 2010) de cómo la pérdida de disponibilidad de las mismas puede causar serios daños a un país. El ciberespacio es asimismo un ámbito para el espionaje por parte tanto de agentes criminales como de otros Estados» (Gobierno de España, 2011: 65).

Es decir, que no sólo subrayaba la creciente gravedad del asunto, sino que admitía explícitamente la participación activa de estados en estas acciones. En la revisión efectuada en mayo de 2013, el gobierno español añadía que el espacio cibernético ya no es solo una amenaza por sí misma, sino que se ha transformado en el terreno propicio para llevar a cabo muchas otras de signo distinto y con objetivos diferentes. Y es que Internet no es segura.

> «Tecnológicamente, Internet fue creada para ser útil y sencillo, no para ser segura. La creciente interconexión de la Red, incluyendo necesariamente las infraestructuras, suministros y servicios críticos, incrementa los niveles de riesgos sobre éstos. El anonimato y la dificultad para rastrear los ciberataques son factores añadidos que entorpecen su neutralización» (Gobierno de España, 2013: 26).

DOI: http://dx.doi.org/10.6035/2174-0992.2013.6.7

Lo cierto es que la atención requerida por las ciberguerras es cada vez mayor entre los países desarrollados y algunos en vías de desarrollo, lo que dispara su traducción informativa. La propia OTAN se rige en este terreno por un extenso estudio, el *Manual Tallinn*, redactado por un grupo de expertos que además de examinar el tema, realizó una serie de recomendaciones. Entre ellas, el Capítulo 5 está dedicado a la protección de los periodistas y sus instrumentos informáticos, aunque admite la posibilidad de que éstos sean confiscados si son utilizados con fines armamentísticos (Schmitt, 2013: 180).

De momento, según Mª José Caro

> «el estudio de los recientes ciberataques a Corea del Sur destaca cuatro verdades sobre los ciberconflictos, una vez analizados. Las implicaciones de tres de ellas son obvias, la cuarta todavía no es así: 1) los ciberconflictos son perjudiciales, 2) pero están lejos de la guerra, 3) los ciberconflictos son cada vez más fáciles de predecir y la nación responsable a menudo es perfectamente obvia, 4) sin embargo, para detener este tipo de ataques asimétricos, a veces hay que utilizar un enfoque tradicional» (Caro, 2013: 3).

2. Pero, ¿qué son las ciberguerras?

La primera dificultad con la que se encuentra el periodista es la definición y catalogación de las ciberguerras. Una cosa son los ataques a cargo de activistas más o menos aislados, que van desde los ciberterroristas (muy abundantes y cada vez más capacitados, por cierto) hasta los *hackers* aficionados, y otra son los impulsados de alguna manera por gobiernos o instituciones oficiales, como por ejemplo servicios de inteligencia.

«Es cierto que diariamente se producen ataques a sistemas operativos de diferentes organismos o instituciones, pero no pueden ser considerados propiamente como ciberguerra o ciberterrorismo, sino más bien como acciones realizadas por hackers», afirma acertadamente. Xavier Servitja.

No olvidemos que recientemente el gobierno turco ha considerado como acciones terroristas las llamadas a la revuelta efectuadas en las redes sociales, asimilando distintos conceptos como la agitación, el terrorismo, el ciberactivismo y el uso libre de Internet.

Para Gema Sánchez, las ciberguerras se caracterizan por su complejidad, su asimetría, sus objetivos limitados, su corta duración, su menor daño físico para los soldados, su mayor espacio de combate y su menor densidad de tropas, su transparencia, su lucha intensa por la superioridad y el control de la información, su aumento de la integración, sus mayores exigencias impuestas a los comandantes, sus nuevos aspectos de la concentración de fuerzas, su reacción rápida e igual de devastadora que una guerra convencional. La asimetría, según ella, es el factor más importante en la medida en que países pequeños pueden poner en serios aprietos e incluso *derrotar* a las potencias, o sea forzar decisiones no deseadas de antemano (Sánchez Medero, 2012: 125).

DOI: http://dx.doi.org/10.6035/2174-0992.2013.6.7

Habitualmente los redactores de Internacional dan por sentado que detrás de los ciberataques hay algún Estado promoviéndolos o por lo menos mostrándose tolerantes. O dicho de otra manera, cuando no es una iniciativa propia los grandes Estados tienen en principio capacidad técnica y política para desarticular las iniciativas agresoras y si no lo hacen es porque sacan réditos propios. Al menos 12 de las 15 principales potencias militares del mundo están construyendo actualmente programas de guerra cibernética, según James Lewis, experto en ciberseguridad del Centro para Estudios Estratégicos e Internacionales(Goldman, 2013), y se calcula que por lo menos 50 países están implicados en acciones de este tipo.

En términos generales los países *agresores* pretenden

> «utilizar el ciberespacio como arma de ataque por razones de seguridad o actividad militar. En esta dirección, la ciberseguridad se puede utilizar para propósitos de espionaje, de sabotaje o de subversión, entre otras actividades» (Servitja, 2013: 6).

Por el contrario, la ciberdefensa sirve para proteger la infraestructura tecnológica, sus servicios y la información que canalizan. Se ha comprobado fehacientemente que el ciberespacio ofrece amplias posibilidades para actuar contra la seguridad y la defensa de muchos países, lo que obliga a éstos a activar complejos mecanismos de protección, que van desde el espionaje y el contraespionaje hasta las acciones de subversión y sabotaje. En esta lucha la identificación del atacante y el análisis de sus técnicas son de gran importancia tanto en el campo estrictamente cibernético como en el de la seguridad y en el político.

Es lógico que tanto a escala estatal como internacional se estén tomando medidas de todo orden para contrarrestar los efectos negativos de los ciberataques. La previsión es que los Estados amenazados destinen grandes sumas de dinero para organizar estas líneas defensivas (y ofensivas, si es preciso) y que incluso deleguen en terceros estas funciones. Israel, por ejemplo, parece cumplir esta función supletoria en determinados momentos y campos relacionados con la situación en el Próximo y Medio Oriente. En síntesis, se pretende preparar y formar a todos los implicados en la ciberseguridad; organizar infraestructuras destinadas a dar la alarma y gestionar las posibles crisis; crear redes de cooperación entre Estados y organizaciones; perseguir los delitos informáticos a todos los niveles; mejorar y desarrollar los servicios informáticos pertinentes; y aprobar normativas específicas que eviten en lo posible el uso fraudulento de la Red con objetivos destructores.

Sin embargo, no es fácil tomar medidas sobre todo a escala mundial por el choque de intereses nacionales distintos y por el peligro que se corre de desvirtuar las esencias de Internet, por lo menos tal como está concebida actualmente.

> «Incluso si la imposición de tales límites fuera posible, ¿a qué autoridad podríamos confiar su ejecución? Al proponer la revisión del tratado de 1988 que rige la Unión Internacional de Telecomunicaciones, la Conferencia Mundial de las Telecomunicaciones Mundiales en Dubaiencendió una polémica en diciembre de 2012 al argumentar los críticos que las normas técnicas aparentemente inocuas podían tener consecuencias negativas inesperadas. Normas

DOI: http://dx.doi.org/10.6035/2174-0992.2013.6.7

> claramente adoptadas para cualquier asunto desde combatir los *spam* hasta garantizar la calidad del servicio del tráfico en Internet, podrían ser utilizadas por gobiernos en solitario con el fin de entorpecer la marcha de las comunicaciones entrantes o filtrar los contenidos específicos que desean detener. Cuando algunas medidas de los tratados revisados fueron consideradas como una autorización para la censura de los Estados, la regulación de Internet y de redes privadas, los Estados Unidos rechazaron firmar el tratado reformado, decisión que siguieron Canadá y alguno Estados europeos», explica el Global RisksReport2013 (WorldEconomicForum, 2013: 26).

3. Los misterios que conducen al miedo

Uno de los grandes inconvenientes con que se encuentra el periodismo de Internacional respecto a las ciberguerras son los grandes misterios y la confusión que rodean este asunto en general, con la inestimable ayuda, todo hay decirlo, de películas como *La jungla de cristal 4* con Bruce Willis de protagonista. Muchos de estos ciberataques se relacionan además con oscuras operaciones de inteligencia y espionaje, como por ejemplo las 18 detenciones de chiíes (uno de ellos libanés y otro iraní) que tras un incidente cibernético en la empresa SaudiAramco efectuó el gobierno de Arabia Saudí el 20 de marzo de 2013, acusándolos de trabajar para los servicios secretos iranís. Ni que decir tiene que ello fue inmediatamente desmentido por el gobierno de Irán. Pero es que por las mismas fechas en Teherán fueron juzgados otros 18 individuos bajo la acusación de asesinar al menos a cinco expertos nucleares iranís siguiendo instrucciones de los servicios secretos de Gran Bretaña, EEUU e Israel (Servitja, 2013: 3). Se ha dado el caso incluso del uso de medios informáticos por parte del servicio secreto chino para espiar al servicio secreto australiano (Reinoso, 2013: 1).

Los países sospechosos de patrocinar o alentar ciberataques niegan sistemáticamente su participación y ocultan posibles pistas. Por el contrario, las guerras clásicas son reivindicadas y hechas públicas por sus agentes que movilizan fuerzas regulares identificadas y en principio sometidas a regulaciones nacionales e internacionales. Incluso las armas nucleares tienen dueño declarado y reglas estatales e internacionales. Es un ámbito de portavoces y gabinetes de comunicación, en el que el periodista debe analizar las fuentes y los contenidos informativos, pero partiendo de una base conocida. Los mecanismos, el lenguaje, los desarrollos son mucho más públicos, y en este método ha crecido el periodismo bélico a lo largo de los siglos.

Ahora bien,

> «los agresores cibernéticos pueden actuar por motivos políticos, pero, al contrario de lo que ocurre con la guerra, suelen estar muy interesados en evitar la reivindicación. Los actos subversivos siempre han prosperado en el ciberespacio porque conservar el anonimato es más fácil que atribuir un acto de forma inequívoca. Ese es el origen del problema político: creer que unos cuantos estados van a ponerse de acuerdo en limitar las armas cibernéticas es tan realista como pensar en un tratado que prohíba el espionaje y tan práctico como declarar ilegal la subversión general del orden establecido» (Rid, 2012: 5).

DOI: http://dx.doi.org/10.6035/2174-0992.2013.6.7

4. Y sin embargo, no hay destrucciones a la vista

Otro planteamiento novedoso de las ciberguerras es que no tienen que causar víctimas mortales directamente, pero tampoco está excluido del todo y mucho menos en fases posteriores al posible ataque. En todo caso, hasta el momento no constan bajas por este motivo. Esta circunstancia da de nuevo un carácter ambiguo a las informaciones relacionadas en la sección de Internacional. Por un lado, se resalta la extrema gravedad de estos ciberataques, pero por el otro no se contabilizan víctimas mortales, que sí aparecen incluso en gran número en conflictos bélicos de media intensidad. Dicho de otro modo, las guerras clásicas siguen siendo mucho más mortíferas que las ciberguerras, por lo menos de momento.

> «No se sabe de ningún ataque cibernético que haya causado la pérdida de vidas humanas. Ningún delito informático ha herido jamás a una persona ni ha provocado daños en un edificio. Y, si un acto no tiene al menos la posibilidad de ser violento, no es un acto de guerra. Separar la guerra de la violencia física la convierte en un concepto metafórico; significaría que no hay manera de distinguir, por ejemplo, entre la Segunda Guerra Mundial y las guerras contra la obesidad y el cáncer. Sin embargo, estos últimos son males que, a diferencia de los ejemplos de guerra cibernética, sí matan a las personas» (Rid, 2012: 2).

Y añade Eugene Kaspersky que

> «Los programas maliciosos avanzados más destructivos descubiertos hasta el momento — Stuxnet, Duqu, Flame, y Gauss— han sido en realidad relativamente benignos, en el sentido de que no han causado muertos de forma directa. La próxima vez que oigamos hablar de un acto de ciberguerra, no obstante, este podría venir acompañado de un resultado con víctimas mortales. Y la razón es que los ciberataques tienen efectos colaterales impredecibles. La infraestructura electrónica mundial se ha vuelto tan interconectada que el daño causado a un solo objetivo puede extenderse rápidamente por todo el planeta, incluso por error. Las autoridades estadounidenses temen, con razón, que un arma de destrucción masiva pueda caer en las manos equivocadas. Pero deberían preocuparse también por la mucha más probable posibilidad de que haya terroristas que adquieran unaciberarma. Una simple metedura de pata podría posibilitar que cualquiera pudiera robar, copiar o adaptar ciberarmamentosupuestamente secreto, volviéndolo contra sus creadores» (Kaspersky, 2012: 1).

Para algunos los escasos daños ocasionados, por lo menos los conocidos, se explican por el escaso interés de los Estados (China y Rusia en especial) en desencadenarlos, ya que no se vislumbra la ventaja adquirida, y por otra parte porque podrían ocasionar represalias más destructivas aún. «No creemos que haya una ciberguerra sin cuartel, a pesar de que es posible», según Wade Baker, jefe de la división de seguridad de la empresa Verizon (Goldman, 2013). Además, en un mundo hiperconectado la interrupción de determinados sectores sensibles en alguna de las potencias derivaría fácilmente en disfunciones más o menos serias en la red informática del país atacante. Por ello, en la actualidad las acciones se mantienen más en el terreno del espionaje y las amenazas, y los ciberataques registrados hasta ahora se centran en empresas e instalaciones no vitales o esenciales para la población. Sin contar con que los países que se muestran más decididos a utilizar estos ciberataques desde plataformas controladas por ellos, principalmente Irán, no parecen disponer de la suficiente capacidad tecnológica. Parece ser que la gran ventaja tecnológica y económica sigue estando del lado de

DOI: http://dx.doi.org/10.6035/2174-0992.2013.6.7

los EEUU y sus aliados, Gran Bretaña, República Federal de Alemania, Francia e Israel, mientras que China, Rusia e Irán, sus mayores competidores, muestran aún importantes debilidades en distintos aspectos.

Por lo demás, a medida que se han incrementado las amenazas cibernéticas, también se han mejorado los mecanismos tecnológicos de defensa, y algunas compañías especializadas afirman que una ciberguerra a gran escala es tecnológicamente muy difícil por no decir que imposible. Igual que existen escudos antimisiles, hay ya sofisticados escudos antivirus.

> «El que haya más programas maliciosos no significa que los ataques sean más fáciles. De hecho, debería ser más difícil realizar ataques con capacidad de ser perjudiciales o verdaderamente peligrosos. ¿Por qué? Los sistemas más delicados suelen tener incorporados sistemas de redundancia y seguridad, de modo que el objetivo más probable de un atacante no será cerrar el sistema, porque el mero hecho de obligar a cerrar un sistema de control, por ejemplo una central eléctrica, puede desencadenar un atasco y que los operadores empiecen a buscar el problema. Para ser un arma eficaz, los programas maliciosos deben poder influir en un proceso activo, pero no interrumpirlo por completo. Si la actividad maliciosa se prolonga demasiado, tiene que ser sigilosa. Y eso es más difícil que apretar el botón de apagado virtual» (Rid, 2012: 2).

Y resulta muy complicado repetir los ciberataques con las mismas herramientas informáticas, habida cuenta de que una vez utilizadas son analizadas y contrarrestadas por los especialistas con relativa rapidez. O sea que cada ataque debe ser distinto, multiplicando así las dificultades técnicas y encareciendo los procesos de agresión. No obstante, es preciso insistir en que no hay nada claro del todo, ya que para determinados expertos norteamericanos hoy por hoy los Estados y las empresas atacadas no son capaces de adaptar sus mejores instrumentos de defensa con la diligencia suficiente. Para ellos, la conclusión parece evidente: los atacantes informáticos suelen tener ventaja sobre los defensores como mínimo la primera vez.

Estas consideraciones han conducido a algunos analistas, como Bruce Schneier, a pensar que el peligro de las ciberguerras ha sido exagerado tanto por intereses políticos y económicos, como por el halo de misterio que las rodea y que las convierte en un asunto muy apetitoso para las secciones de Internacional (Molist, 2011: 1). La sensación instalada en la opinión pública es que se corre un riesgo permanente y potencialmente grave, sin que se conozcan ni las advertencias previas, ni el sitio y las instalaciones amenazadas, ni el nivel de peligro que se corre, ni la identidad de los agentes, ni las consecuencias que puede conllevar. La rocambolesca historia del grupo Jester así lo demuestra.Casos mediáticamente muy sonados, como la explosión de un gasoducto siberiano en junio de 1982 equivalente, dicen, a una pequeña bomba atómica, no han sido documentados ni por el país afectado, ni por el atacante.

En numerosas ocasiones los ciberataques transcurren a través de empresas, con frecuencia multinacionales, con intereses diversos y celosas siempre de preservar sus estrategias tecnológicas, financieras y comerciales. En otras, los Estados

DOI: http://dx.doi.org/10.6035/2174-0992.2013.6.7

operan a través de agentes privados, lo que entorpece aún más descubrir todo lo que hay detrás de los ciberataques. Michael Moynihan explica que

> «en algunos casos los *hackers* pueden estar trabajando directamente para el beneficio de gobiernos, incluso cuando la extensión de las conexiones con estos gobiernos resulta discutible. Por poner un ejemplo, nadie sabe si el Ejército Electrónico Sirio —un grupo pro-Assad de *hackers*, en cierta ocasión reivindicado por el dictador como *un arma virtual en el ciberespacio*—forma parte o no del gobierno al que apoya. (Recientemente esta organización reivindicó haber usado la cuenta en Twitter de la AssociatedPress para tuitear que había habido una explosión en la Casa Blanca, provocando un breve retroceso en la Bolsa. También penetró en las cuentas de TheOnion, que se ha burlado con frecuencia de la dictadura siria, y de Justin Bieber. Y en Israel, agentes gubernamentales han admitido que el grupo intentó infructuosamente entrar en la red de ordenadores que controla el suministro de agua en Haifa). Sin embargo, aunque un gobierno no disponga de una organización como el Ejército Electrónico Sirio en la que apoyarse, puede buscar los servicios de otro *hacker*» (Moynihan, 2013: 5).

5. Conclusiones

Al contrario que las guerras tradicionales, con una larga tradición en los medios de comunicación y unos métodos narrativos muy asentados, las ciberguerras son un fenómeno informativo relativamente reciente en Periodismo Internacional, aunque se está intensificando a gran velocidad.

En estas informaciones existe casi unanimidad en que las ciberguerras tienen la posibilidad de ocasionar grandes daños materiales y que incluso podrían causar víctimas mortales, por lo menos de forma indirecta. Sin embargo, hasta ahora no consta que se hayan producido ni los destrozos, ni las bajas temidas, más allá de inconvenientes temporales y molestias puntuales y referidas más a empresas concretas que a sectores, infraestructuras e instalaciones básicas. Con todo, los medios deben subrayar la extrema gravedad del problema y a renglón seguido no dudan en crear y propiciar un clima de miedo y de desconcierto, acrecentado además por el misterio y la confusión que rodea los ciberconflictos. Con escasas excepciones estos ciberataques no son reivindicados, se desconoce su alcance exacto e incluso cuando, donde y en qué condiciones se producen, y con frecuencia llegan a los medios con retraso y mal documentados. En numerosos casos los ciberataquesestán relacionados con episodios de espionaje de todo tipo, operaciones propagandísticas y maniobras políticas o económicas de gran complejidad y siempre oscuras, y también con el *hackerismo*puro. Para los periodistas de Internacional resulta muy difícil contrastar las noticias y disponer de fuentes fiables y estables, tal como sucede con otros asuntos de las mismas páginas de Internacional.

Aunque con alguna excepción, la información sobre las ciberguerras transcurre, pues, en un esquema de fuerte tensión por su importancia y sus posibles consecuencias, y al mismo tiempo de falta de fiabilidad y de seguimiento. Esto conduce a referenciar exageraciones, recoger errores e incluso mentiras, sucumbir a manipulaciones de toda laya, sin riesgo a ser descubiertos por lo menos a corto plazo a causa de la oquedad de los temas tratados. En resumen, un asunto de

DOI: http://dx.doi.org/10.6035/2174-0992.2013.6.7

gran impacto del que los medios, y de rechazo la opinión pública, conocen aún muy poco.

Referencias bibliográficas y recursos electrónicos

Andrades, Fran (2013).Cinco escenarios de ciberguerra en el nuevo orden mundial. Disponible en: http://www.eldiario.es/turing/escenarios-ciberguerra-nuevo-orden-mundial_0_129837338.html (8/05/2013).

Caro, Mª José (2013). Algunas reflexiones sobre la ciberguerra. En: *Documento informativo del Instituto Español de Estudios Estratégicos,* 13/2013 de 24 de abril.

Clapper, James R. (2013).Worldwide Threat Assessment of the US Intelligence Community. En: *Office of the Director of National Intelligence*, de 12 de marzo. Disponible en: http://intelligence.senate.gov/130312/clapper.pdf. (27(05/2013).

Gobierno de España (2011). *Estrategia Española de Seguridad*. Disponible en: http://www.lamoncloa.gob.es. (10/05/2013).

Gobierno de España (2013). *Estrategia de Seguridad Nacional: un proyecto compartido*. Disponible en: www.lamoncloa.gob.es. (10/05/2013).

Goldman, David (2013). 2013, ¿año de la ciberguerra? En: *CNNMoney.com*. Disponible en: http://money.cnn.com/.(07/01/ 2013).

Kaspersky, Eugene (2012). Ciberespeluznante: amenazas en la Red. Disponible en: http://www.fp-es.org/ciberespeluznante-amenazas-en-la-red. (11/12/ 2012).

Molist, Mercè (2011). Los gobiernos exageran sobre la ciberguerra. Disponible en: www.*elpais.com*. (20/03/2011).

Moynihan, Michael (2013). You're Being Hacked. Cyberspies are everywhere. But who are they helping? En: *Newsweek /The Daily Beast,*May 29. Disponible en:http://www.thedailybeast.com/newsweek/2013/05/29/hackers-are-spying-on-you-inside-the-world-of-digital-espionage.html.(30/05/2013).

Reed, John (2012). U.S. energy companies victims of potentially destructive cyber intrusions. Disponible en: http://killerapps.foreignpolicy.com/(27/05/2013).

Reinoso, José (2013). Los espías australianos, espiados por los chinos. Disponible en: www.*elpais.com*. (28/05/2013)

Rid, Thomas (2012): Depende: Ciberguerras. Disponible en: http://www.fp-es.org/depende-ciberguerra. (06/03/2012).

Sánchez Medero, Gema (2012). La ciberguerra. Los casos Stuxnet y Anonymous. En: *Nueva Época* nº 11 de Septiembre-Noviembre.

DOI: http://dx.doi.org/10.6035/2174-0992.2013.6.7

Schmitt, Michael (dir.) (2013).*Tallinn Manual onthe International LawApplicabletoCyberWarfare.* Cambridge: UniversityPress

Servitja, Xavier (2013). Ciberseguridad, contrainteligencia y operaciones encubiertas en el programa nuclear de Irán: de la neutralización selectiva de objetivos al "cuerpo ciber" iraní. En: *Documento de Opinión del Instituto Español de Estudios Estratégicos,* vol. 42/2013 de 7 de mayo.

World Economic Forum (2013). *Global Risks 2013.* Eight Edition.

Referencia de este artículo

Sanmartí Roset, Josep M. (2013). Las ciberguerras, un tema en ascenso en el periodismo internacional. En: *adComunica. Revista Científica de Estrategias, Tendencias e Innovación en Comunicación*, nº6. Castellón: Asociación para el Desarrollo de la Comunicación adComunica, Universidad Complutense de Madrid y Universitat Jaume I, 103-114. DOI: http://dx.doi.org/10.6035/2174-0992.2013.6.7

DOI: http://dx.doi.org/10.6035/2174-0992.2013.6.7