UNIR
Universidad Internacional de La Rioja

TRABAJO FIN DE MÁSTER

Máster Oficial Universitario en

Intervención social en las sociedades del conocimiento

Título: # ¿Cuál es la amenaza real del Ciberactivismo (o Ciberterrorismo)?

Trabajo: **Investigación sobre cómo influyen las ciberacciones en el sistema global de medios y en la opinión pública.**

Apellidos González Rodrigo

Nombre María

Fecha Entrega 15/10/2012

ÍNDICE

1. INTRODUCCIÓN

En la sociedad moderna, cada vez más dependiente de los sistemas informáticos, la posibilidad de causar graves perjuicios a un Estado a través del asalto a nódulos de comunicación por medio de ataques cibernéticos se ha convertido en una amenaza real con un riesgo creciente. Este tipo de agresiones se agrupan bajo la denominación de ciberterrorismo, término acuñado hace aproximadamente una década por el profesor Barry C. Collin, del Institute for Security and Intelligence, y definido por la doctora Denning, de la Universidad de Georgetown, como el "ataque ilegal contra ordenadores, sus redes y la información contenida en ellos cuando se lleva a cabo con la finalidad de coaccionar a un gobierno o a su población para conseguir objetivos políticos o sociales".

Junto a los avances de la informática y las comunicaciones en los últimos años, ha surgido una hueste de apasionados de estas tecnologías, que armados con sus ordenadores y conexiones a redes como Internet, ha logrado humillar a instituciones tan potencialmente seguras como el Pentágono y la NASA. Hay que tener en cuenta que todos somos dependientes de los sistemas electrónicos e informáticos, somos una presa fácil para cualquier ataque cibernético, cuyos objetivos son paralizar la capacidad militar y el servicio público de un país. Pueden comenzar con ataques a los mercados financieros, para continuar con un ataque a los sistemas informáticos gubernamentales. Hoy en día se hace patente que en la medida que los avances tecnológicos van generando la sistematización y automatización de las tareas de primordial interés para el correcto funcionamiento de un Estado (gobierno, población y territorio), se hacen más vulnerables a un ataque ciberterrorista.

Y por ello hemos querido estudiar la amenaza que supone el ciberterrorismo para el sistema global de medios, desde la creación del término en los años 80, hasta la actualidad. En la que se ha convertido en un problema real y ha obligado a los Estados desarrollados a elaborar programas de seguridad en materia de ciberterrorismo para evitar, lo que se ha denominado como una catástrofe a nivel mundial.

Y para ello analizaremos, en primer lugar, las influencias de la Red en el desarrollo de la vida económica, pública y política de un país, para llegar a entender hasta que punto un ataque en Red a un Estado puede ser tan importante como para paralizar un país. Llevaremos a cabo un detallado análisis sobre el ciberterrorismo, entendido

como una amenaza para los Estados, derivada de la monopolización y el poder, tanto político como económico en los diferentes Estados, que convierten el ciberterrorismo en un método de acción contra las grandes estructuras de poder. Una vez explicado y detallado el ciberterrorismo, nos centraremos en definir el ciberactivismo, y por supuesto en la relación entre ambos, así como en examinar los principales casos y acciones relacionadas con el ciberactivismo, haciendo un especial hincapié en la actualidad del tema y en las respuestas de los diferentes Estados en materia ciberactivista.

Por último concluiremos tratando de responder a una difícil cuestión a modo de conclusión: ¿Cómo las posibilidades de la web 2.0 y la amenaza del ciberterrorismo influyen en el sistema global de medios? Y para tratar de responderla nos centraremos en las precauciones y medidas abordadas por los distintos países, cuyo análisis nos aclarará la gravedad y relevancia real del asunto, y nos permitirá conocer los países con sistemas de medios más desarrollados y también aquellos que más temen por su sistema. Trataremos de recoger los efectos del ciberterrorismo así como los casos más significativos con el objetivo de dar a conocer las consecuencias que puede generar en un país para demostrar la amenaza real que supone y hasta qué punto.

Y para resolver todas estas cuestión hemos llevado a cabo el método de investigación convencional, planteando un enfoque para el tema, y una serie de hipótesis a resolver una vez concluida la investigación expuestas ya arriba, y recurriendo a diversas fuentes para desarrollar el contenido de la investigación, principalmente a Internet, pues al tratarse de un tema de estudio relativamente novedoso, es escasa la bibliografía en papel publicada al efecto, sin embargo sí hemos recurrido a diversos ensayos y publicaciones que abordaban el tema así como manuales y trabajos de investigación sobre ciberterrorismo.

2. OBJETIVOS

En la investigación que vamos a llevar a cabo, hemos determinado un objetivo general, así como varios secundarios.

En este trabajo queremos estudiar la amenaza que puede suponer el ciberterrorismo desde la creación del término en los años 80 hasta la actualidad, como ya hemos adelantado en la introducción, por lo que este será el objetivo general.

Los objetivos secundarios de este estudio pretenden responder a la cuestión sobre cómo las posibilidades de la web 2.0 y la amenaza del ciberterrorismo influyen en el sistema global de medios. Otros objetivos secundarios son conocer la gravedad del ciberterrorismo y la relevancia real de esta nueva forma de actuación social como protesta.

Para conseguir alcanzar estos objetivos se llevará a cabo una metodología enfocada a ellos que se detallará en un apartado específico, justificando cada estudio y método

3. MARCO TEÓRICO

Para poder hablar sobre ciberterrorismo, debemos hacer un repaso no sólo de este hecho en concreto si no de la importancia de la Red en nuestras vidas, por lo que detallaremos el papel de Internet en la vida pública, política y económica de un país para contextualizar el tema. En segundo lugar, hablaremos del término en concreto repasando y revisando las obras de autores que acuñan este término. Finalmente concretaremos las teorías que conforman este marco teórico sobre el tema de estudio.

3.1. Contexto

Internet es una de las palabras más nombradas en los últimos tiempos. Con más de 200 millones de usuarios en todo el mundo, Internet se ha convertido en el medio de comunicación más extendido en toda la historia de la humanidad. Constituye una fuente de recursos de información y conocimientos compartidos a escala mundial. Es también la vía de comunicación que permite establecer la comunicación entre un gran número de comunidades y grupos de interés, distribuidos por todo el planeta. Esta influencia a nivel global ha fomentado que Internet se haya convertido en la herramienta fundamental a emplear en materia de desarrollo político y económico.

a) El papel de la Red en la vida pública:

Sin lugar a dudas, a lo largo de la historia mundial hemos asistido a multitud de cambios sociales a los que nos hemos tenido que amoldar y, con ello, hemos configurado la sociedad actual.

No obstante, en la actualidad, hemos asistido al mayor cambio social de la historia de la humanidad con el apogeo y auge de internet y las redes sociales. Todo lo que podemos encontrar en la calle, ya está disponible a través del pc (compras, relaciones sociales, ofertas de trabajo, jugar, aprender, negociar… y un largo etcétera interminable). Internet es toda una revolución: no sólo en el plano tecnológico, sino también en relación a las implicaciones que tiene en los diferentes ámbitos que definen o estructuran una sociedad.

Internet puede considerarse una sociedad orientada a las personas. Permite comunicarse y participar a millones de personas de todo el mundo. Nos comunicamos enviando y recibiendo correo electrónico, o estableciendo una conexión con el ordenador de otra persona y tecleando mensajes de forma interactiva. Es mucho más

que una red de ordenadores o un servicio de información: es una ventana abierta a la comunicación y a la sociedad.

Dentro de los cambios sociales, se encuentra el cambio de la interacción con las personas de forma física por una de forma virtual, dando algunas ventajas como la facilidad, bajo costo y accesibilidad de poder dialogar con personas que viven en lugares remotos o de acceso limitado permitiéndonos conocer un poco hasta las culturas y personas a las que antes no se podían llegar cómodamente.

Internet ha cambiado espectacularmente el mundo en que vivimos, eliminando las barreras del tiempo y la distancia y permitiendo a las personas compartir información y trabajar en colaboración.

Las nuevas aplicaciones permiten acceder a todo tipo de información de manera cada vez más veloz, realizar transacciones económicas de forma segura y proporcionan nuevas oportunidades para el comercio. Y además las nuevas tecnologías aumentan la velocidad de transferencia de información, lo que hace posible que en segundos se pueda conversar o incluso visualizar a la persona.

Uno de los aspectos en los que ha influido decisivamente Internet es en el ámbito de la educación, suponiendo una revolución en todo el mundo, y posibilitando no sólo el poner la educación al alcance de todos, sino facilitando el acceso al conocimiento y permitiendo acceder a información de todo tipo.

Internet ha redefinido: nuestra manera de informarnos, la forma de llegar a las personas e influir en ellas, la manera de influir en el cambio político y social, el espacio privado de las personas y la forma de relacionarnos con los demás, con la sociedad.

b) El papel de la Red en la política:

Internet ha cambiado la forma de hacer política. Las nuevas tendencias políticas han recibido muchos nombres como e-política, política 2.0 o política online. Pero el fundamento de todas ellas es el mismo, el contacto más directo, rápido y efectivo con el ciudadano.

La e-política o política 2.0 son aquellas estrategias de gestión pública que se desarrollan a través de Internet. En realidad el concepto es muy amplio y, aunque desde la revolución Obama y el uso de las redes sociales para su campaña política se ha utilizado este término fundamentalmente para hablar de las acciones llevadas a

cabo por el Gobierno o por los partidos políticos, también se pueden englobar en esta categoría las propias iniciativas de los ciudadanos.

Jürgen Habermas formuló, antes de la revolución de Internet, en su teoría sobre la política deliberativa un sistema más democrático en el que se pudiera llegar a consensos a través del entendimiento mutuo. La política 2.0 engloba esta idea y así los foros, los blogs y las páginas de Internet, y sobre todo las redes sociales, se han convertido en los principales canales de discusión de los ciudadanos y los políticos. En España, las elecciones de 2008 fueron el germen de esta política online. Todos los partidos abrieron perfiles de sus líderes políticos y las campañas a través de Internet se multiplicaron. Aunque después del periodo electoral se ha perdido parte del interés, se siguen dando ejemplos del uso político de Internet.

Internet puede afectar el quehacer político en diferentes aspectos. En el Poder Ejecutivo está la posibilidad de facilitar la vida de los ciudadanos con el gobierno electrónico, desburocratizando y facilitando la transparencia en cuentas públicas (al colocar el material disponible en Internet). En cuanto a comunicación, se han generado nuevos mecanismos de marketing político especializados en Internet. Y como tercer punto, está la participación de la gente, ya sea para apoyar a políticos o para movilizarse para sus propias causas.

Para la política 2.0, los ciudadanos son un elemento esencial del proceso pues se han convertido en los principales sujetos en la formación de la opinión pública. Además las nuevas tecnologías generan una mayor demanda de información y están obligando a los gobiernos a publicar más información sobre su gestión. Internet es una valiosa herramienta que ha permitido a los ciudadanos ir tomando poco a poco más parcelas de poder reforzando la llamada sociedad civil. Movimientos asociativos, páginas que promueven acciones conjuntas o, simplemente, la creación de fuertes corrientes de opinión han hecho cambiar muchas decisiones políticas.

Hasta tal punto se equipara el sistema que los políticos ya no tienen una posición de superioridad y su opinión es tan solo una opinión más. Serán los propios internautas quienes decidan qué opiniones merecen mayor credibilidad. De ahí que una acción colectiva a través de Internet pueda tener una repercusión en la política estatal. Internet no es, por tanto, un simple lugar de intercambio de opinión, sino que es también el origen de medidas concretas realizables en el mundo real, tanto positivas como catastróficas, como es el caso del ciberterrorismo o el ciberactivismo.

Las nuevas tecnologías han supuesto el antes y el después en la sociedad, diferenciándola de la idea tradicional y ofreciendo nuevas hipótesis planteadas por autores como Marshal McLuhan o Daniel Bell. La forma de denominar a estas sociedades pasa por llamarse desde aldea global (McLuhan, 1996), sociedad de la información (Bell, 1991 y 2001), sociedad de la tercera ola (Toffler, 1986), telépolis (Echeverría, 1999), sociedad de la vigilancia (Lyon, 1995 y 2001),sociedad del conocimiento (Drucker, 1993), sociedad red (Castells, 1999 y 2001), sociedad interconectada (Martin, 1980), sociedad de la inteligencia interconectada (Tapscott, 1996), sociedad digital (Mercier, 1980; Terceiro, 1986; Negroponte, 2000), cultura virtual o cibercultura (Levy, 2001; Picistelli, 2002), entre otras.

Vemos como Internet es un espacio para los movimientos sociales en el que surge un tipo de acción política no convencional. De este modo, debemos preguntarnos cuáles son las consecuencias sobre la democracia y esta acción que denominamos convencional en la política. Numerosos grupos demandan la llamada "ciberdemocracia" (grupos como Anonymous o Hacktivistas, en España), una democracia que consiste en la utilización de las nuevas tecnologías para llevar a cabo procesos básicos como las elecciones, el voto electrónico, toma de decisiones, según expresa Chadmwick (2006). En España, ya existen iniciativas de este tipo que quieren llevar esta forma de actuar al Congreso y al Senado, como podría ser la iniciativa española Democracia 2.0. o los partidos piratas, como el alemán.

La idea que mantienen es que los ciudadanos influyan en la toma de decisiones de los gobernantes y que las herramientas digitales del más voz a la soberanía popular, de modo que la toma de decisiones públicas se canalizaría a través de medios digitales.

Internet no sólo ha abierto este camino, si no que también es una nueva forma de desobediencia civil. Los movimientos sociales han visto esta herramienta como una nueva forma de protestar, llevándose al extremo del ciberterrorismo. Autores como Además Mccaughey y Ayers (2003) señalan que estas nuevas herramientas de participación han supuesto redefiniciones del propio activismo, identidad colectiva, cambio democrático, entre otros términos.

c) El papel de la Red en la economía:

Internet esta cambiado por completo la economía mundial. Hoy en día, cualquier persona con buenas ideas, con conocimientos que otras personas en cualquier parte del planeta puedan necesitar o con una gran pasión por cualquier cosa, puede crear

su propio negocio en Internet. Un negocio que se puede gestionar desde cualquier parte del mundo, siempre que tenga un ordenador y una conexión a Internet.

Internet se ha extendido por todo el mundo de forma imparable. Esta expansión significa que con nuestro ordenador podemos viajar a cualquier otro ordenador del mundo, para consultar por ejemplo, la evolución de los índices de la NYSE, los precios de cierre del barril de petróleo en Europa, o las bases de datos que contienen los artículos de revistas científicas y noticias de actualidad…etc. Hasta es posible buscar y encontrar un trabajo en Internet sin salir de casa.

La facilidad con la que obtenemos esta información ha permitido el avance de nuevas tecnologías, beneficiando al usuario y consumidor final. Producto de esta transformación la economía ha cambiado de actores y de escenario. El mercado se transforma en el ciberespacio, las necesidades tradicionales continúan existiendo dentro del ciberespacio, los ofertantes y demandantes se convierten en cibernautas, y el desarrollo del comercio y sus transacciones se realizan de forma digital sin papeles, quedando registros de las aprobaciones, comprador, vendedor, mercadería o servicio, fecha y hora, etc.

Las nuevas tendencias tecnológicas se perfeccionan día a día con la cotidianeidad de su utilización, y con el mayor aprovechamiento de altos estándares de productividad de las grandes corporaciones globalizadas, estas realizaron un estudio de utilización promedio de Internet y concluyeron que 5 de cada 10 personas en el mundo tienen acceso directo e indirecto a la red. Esta cifra da con facilidad un amplio espectro de consumidores y ofertantes, es por ello que estas corporaciones no escatiman esfuerzos científicos ni económicos para desarrollar nueva tecnología con el fin de acaparar una parte más grande de este mercado.

La digitalización significa que toda la información, se pueda utilizar en cualquier orden y se pueda organizar como se desee. Esta es probablemente una de las mejores novedades del sistema moderno, poder manipular la información a gusto y necesidad tanto del ofertante como del demandante, esto es que al momento de poder comprar como vender se pueda poseer la mayor cantidad de información referente al producto como del proveedor, para tomar la mejor decisión al cerrar una transacción de compra o de venta.

Se ha llegado a la conclusión que uno de los mayores impactos de la tecnología de la información se produce en el comercio y los servicios financieros. El negocio

conectado a la red o comercio electrónico ha modificado los hábitos de las finanzas y el de los comerciantes y consumidores, a la vez que produce cambios sustanciales en los medios de pago tradicionales.

Son tres factores fundamentales los que hacen realidad esta nueva economía de Internet:

Con la llegada de Internet, y la continua mejora de las infraestructuras y la velocidad de las conexiones, podemos conectar con casi cualquier persona del mundo. Esto hace que se pueda contratar un programador en la India, un asistente personal en Filipinas, o vender productos y servicios para el mundo entero desde cualquier lugar.

Ya no es necesario tener una audiencia gigante para tener éxito. Por muy pequeño o específico que sea tu nicho de mercado, la conectividad y capacidad de distribución que nos ofrece Internet hace que sea posible encontrar una base de clientes suficientemente grande para que el negocio funcione y sea rentable.

Gracias a los nuevos dispositivos móviles como el iPhone o la Blackberry hemos pasado a un estado de conectividad total. Ahora estamos conectados en el momento que queramos en cualquier lugar, lo que incrementa exponencialmente las posibilidades de conectar con nuestros clientes potenciales.

La nueva economía exige una rápida adaptación a los cambios. En general se reconoce que la economía de los países ha evolucionado de la era industrial basada en la transformación de materias primas a una nueva economía basada en el manejo de información a través de los ordenadores, de la inteligencia artificial y de los recursos de la comunicación. La era de la información ha transformado radicalmente las bases sobre las que descansa la economía de todo el mundo. Por esto el comercio se ha visto afectado por la tecnología en una proporción muy considerable.

El ritmo acelerado de la tecnología y el crecimiento vertiginoso de los nuevos modelos de comercio electrónico, así como la cada vez mayor competencia en los mercados, han hecho patente la necesidad de adoptar estrategias que den respuesta a estas necesidades. Y primero que nada, este nuevo panorama debe incluir a todos y cada uno de los miembros de la organización. El cambio en el comportamiento conllevará no solo un uso más adecuado de los recursos innovadores, sino una nueva visión de la atención y el servicio al cliente. La Economía Digital, trae no solo cambios en el plano meramente económico, sino en el uso de la tecnología, que debe tender a

facilitar los procesos.

El uso de una buena plataforma operativa y tecnológica, permite que las empresas funcionen como una red, capaz de tener un alcance global, que incluye a los clientes y a la información que de estos se pueda extraer. Esto hace que se penetre más fácilmente en los distintos sectores y se implanten estrategias más acertadas, que conducirán finalmente a uno mejores volúmenes de negocios, mayor flujo de dinero y una valoración real del mercado.

En este esquema digital, las fronteras de la industria son inexistentes, porque las necesidades de los usuarios son cada día distintas y además se trabaja de la mano de otras industrias, para compartir experiencias, conocimientos y crear alianzas que les hagan obtener mutuos beneficios.

3.2. Ciberterrorismo

En los años 80, Barry Collin, un investigador senior del Institute for Security and Intelligence en California acuñó el término *cyberterrorism* para referirse a "la convergencia del ciberespacio con el terrorismo". Al igual que ya que ocurrió con conceptos como Web 2.0 o *hacktivismo*, el término "Ciberterrorismo" se nos presenta ahora como una nueva palabra derivada del continuo desarrollo que la Red está sufriendo constantemente. Y es que ya sabe que todas las posibilidades que ésta nos ofrece son infinitas y que, evidentemente, los límites son prácticamente inexistentes.

En consonancia con esto mismo, hace su aparición en escena este moderno vocablo que no hace sino llevar a Internet algunas prácticas que se aplicaban fuera de ella, entre las que se incluyen la extorsión y el chantaje.

Veamos, pues cuál es el significado más popularizado de Ciberterrorismo, partiendo de las discrepancias existentes a la hora de dar una definición exacta del mismo. Aún así, podríamos definirlo como "el uso de medios, de tecnologías informativas y de la comunicación conjuntamente con la informática y la electrónica con el propósito de generar un cierto tipo de terror entre una población, una clase dirigente o un gobierno, y causando con ello una violación a la libre voluntad de las personas. Los principales fines que se persiguen con ello son económicos, políticos o religiosos".

Aún así, varias han sido las críticas que reivindicaban el empleo de este término no como algo únicamente negativo, sino como también una forma de expresar el desacuerdo con el sistema actual en la red de las redes. Sin embargo, esta opinión es

minoritaria, ya que para ello existen otros mecanismos y procedimientos bajo el nombre de ciberactivismo, un punto a tratar en este mismo trabajo.

Para conseguir abordar de un modo más completo todo lo relacionado con el terrorismo en la red, se hará una clase de apartados que tratarán más profundamente las diversas cuestiones que han ido surgiendo a la par del desarrollo de esta práctica informática.

a) Una práctica en auge

La generalización de las Tecnologías de la Información y las Comunicaciones (TIC) ha supuesto toda una revolución en el plano de lo social, lo político y lo económico. Internet se nos presenta hoy día como la mayor de las herramientas que, junto a la globalización, se ha ido extendiendo a un ritmo vertiginoso desde su aparición en los años 70. Precisamente es en este punto donde se encuentran las virtudes y los pecados de este medio, ya que su potencial para dar voz a todos los grupos no ha pasado desapercibido para otras prácticas políticamente menos ortodoxas, como las llevadas a cabo por hackers y, en lo que aquí nos ocupa, por los grupos de ciberterroristas.

En 1986, un libro llamado "Softwar" afirmaba que los países del Pacto de Varsovia podrían incapacitar al mundo occidental lanzando ataques contra las computadoras militares y financieras de Estados Unidos y la OTAN. Tres años más tarde, la Guerra Fría terminó, pero para varios integrantes de organismos de inteligencia estadounidense, el peligro de un ataque electrónico siguió latente. Las hipótesis se ampliaron: ya no se trataba sólo de que algún país enemigo buscara atacar o inutilizar las instalaciones militares, sino que además se comenzó a especular con algún tipo de ataque contra la infraestructura civil de la nación.

De este modo, y a pesar de no contar con un espacio informativo relevante, el ciberterrorismo no debe ser subestimado, al igual que tampoco debe serlo el empleo de Internet como plataforma. Visto queda si tenemos en cuenta que, desde los atentados en Nueva York del 11-S por la red terrorista Al Qaeda, las miradas hacia este entorno han sido mayores de lo que cabría esperar, descubriendo con ello las infinitas posibilidades que ofrece a todos aquellos que pretendan difundir el terror.

Así, Estados Unidos endureció desde entonces su legislación sobre el uso de Internet y reforzó el Centro Nacional de Protección de Infraestructuras (NIPC – National Infraestructure Protection Center). Fue a partir de entonces cuando comenzó a

acuñarse este término de un modo más definitivo, si bien es cierto que desde aquella primera definición ofrecida en los años 80 por Barry Collin, la designación de Ciberterrorismo ha sufrido multitud de transformaciones.

En la actualidad, el concepto aparece definido de un modo más completo, entendiendo como ciberterrorismo "la ejecución de un ataque sorpresa por parte de un grupo (o persona) terrorista, extranjero subnacional, con objetivo político, utilizando tecnología informática e Internet para paralizar o desactivar las infraestructuras electrónicas y físicas de una nación, provocando de este modo la pérdida de servicios críticos, como energía eléctrica, sistemas de emergencia telefónica, servicio telefónico, sistemas bancarios, Internet y otros muchos ... El objeto de un ataque ciberterrorista no es solo impactar sobre la economía de una región o país, sino amplificar los efectos de un ataque terrorista físico tradicional provocando confusión y pánico adicionales en la población en general".

El estudioso Dan Verton, comenta sobre ciberterrorismo que "es la nueva cara del terrorismo. Es un juego de inteligencia que aplica las tácticas violentas del viejo mundo a las realidades y vulnerabilidades de la nueva era tecnológica. (…) El terrorismo ahora implica atacar de forma indirecta, inteligente y bien planeada los tendones electrónicos de una nación."

En cuanto a la materialización de esta práctica, son varias las oportunidades que organizaciones terroristas ha aprovechado, existiendo constancia de ello. Por ejemplo, el uso del correo electrónico para la comunicación interna de estos grupos es una realidad, empleando programas de encriptación y de protocolos seguros, a los que se le unen las técnicas de enmascaramiento y ocultación, la utilización de comunicaciones de voz sobre IP y el empleo de dispositivos móviles de conexión a través de puntos de acceso inalámbricos vulnerables.

Además, las TIC favorecen las relaciones y colaboraciones entre las diversas organizaciones, aumentando la guerra psicológica al darse un incremento de la desinformación y la difusión de amenazas, así como de los canales de financiación y reclutamiento. Ejemplo de ello son los vídeos con mensajes propagandísticos de Osama Bin Laden o los numerosos comunicados de la organización terrorista ETA.

Sin embargo, el más sofisticado de estos ataques se produjo en octubre de 2001 en EE.UU, afectando a 9 de los 13 grandes servidores raíz de la red. El FBI NIPC informó sobre la evidencia de que un grupo terrorista se encontraba preparando un ciber

ataque al sistema de aprovisionamiento de agua en el país.

El incremento del ciberterrorismo en los últimos años ha venido dado por sus ventajas con respecto al terrorismo tradicional. Además de las nombradas anteriormente, habría que añadir unas fundamentales: el ciberterrorismo no comporta riesgo físico al terrorista, su ámbito de actuación geográfica es ilimitado, las acciones alcanzan una gran repercusión sobre la Red y, evidentemente, un efecto propagandístico inmediato. Y todo ello con una relación coste-beneficio bastante óptima. Sin embargo, los inconvenientes de este nuevo terrorismo son escasos, por lo que resulta previsible que las organizaciones terroristas amplíen sus procedimientos de ciberterrorismo.

Conscientes de ello, los propios Estados han comenzado a emplear el ciberterrorismo como una nueva arma de defensa que ofrece una gran cantidad de posibilidades de un modo económico y eficaz. Entre estos países, China se encuentra a la cabeza, liderando el poderío de estas iniciativas.

Según Ned Moran, miembro del Terrorism Research Center, "Un país como China se da cuenta que en vez de armar una red de espías para robar información, puede hacer lo mismo a muy bajo costo y con menos riesgos mediante los ciber-ataques". En Estados Unidos, tal y como afirma Moran, muchas sociedades de armamento privadas han sido atacadas de esta manera. Los piratas han tenido éxito en varias oportunidades, en ataques que comenzaron al menos desde 2003 contra Estados Unidos y probablemente en 2005 contra Gran Bretaña. Prueba de ello es que sitios sensibles de los gobiernos estadounidense, francés, alemán y británico, entre ellos el Pentágono y el ministerio de Defensa francés, fueron objeto en los últimos meses en ofensivas por internet. El experto asegura que, siguiendo la línea actual, otros estados encontrarán sus propios medios para utilizar la ciber-guerra.

b) Ciberterrorismo y Defensa en España

En el ámbito español, el mayor de los ejemplos de ciberterrorismo lo encontramos de la mano de la banda terrorista ETA, que tradicionalmente ha tenido entre sus objetivos repetidores de radio y televisión, subestaciones eléctricas, infraestructuras ferroviarias, entidades financieras, abriles y de comercio e instalaciones de los operadores de telefonía.

En España las responsabilidades en el ciberespacio están fragmentadas en diferentes organismos. La dotación presupuestaria se considera crítica si se quieren llevar a cabo

las líneas de acción que se plantean como posibles soluciones para reducir la amenaza, ya que la aproximación debe ser a todos los niveles: en el sector público, la industria, los ciudadanos y los aliados internacionales.

En los últimos años se ha detectado un incremento constante de vulnerabilidades y amenazas sobre los sistemas y tecnologías de la información y comunicaciones. Estas amenazas, evolucionan continuamente y representan un verdadero desafío para los responsables de proporcionar servicios electrónicos. Además, en la actualidad los ataques se pueden llevar a cabo desde cualquier parte del mundo y, en muchos casos, las posibilidades de descubrir su origen, e incluso su presencia, son muy remotas. Por ello, ningún sistema, incluidos todos los de la Administración, está a salvo de sufrir un ataque de graves consecuencias como el robo, pérdida, destrucción o extracción de dispositivos de almacenamiento; destrucción o modificación de datos almacenados, etc.

Debido a ello, muchos países están desarrollando estrategias nacionales de Ciberdefensa mediante el intercambio de información de alertas, vulnerabilidades, amenazas y eventos; la mejora de las capacidades de contrainteligencia, la seguridad de sus productos y tecnologías, y la formación de sus ciudadanos y servidores públicos en TIC.

En nuestro país, durante los últimos 10 años se han desarrollado iniciativas parciales (criterios de seguridad, conservación y normalización, Centro Criptológico Nacional, infraestructuras críticas, Instituto Nacional de Tecnologías de Comunicación o esquema nacional de seguridad) con las que se intenta mitigar el riesgo de recibir cualquier tipo de ataque procedente de este nuevo tipo de amenaza.

De entre todos los organismos existentes, es necesario destacar la labor realizada por la Secretaría de Estado de Seguridad (SES), que se encarga de la dirección, coordinación y supervisión de la protección de infraestructuras críticas (PIC) nacionales, de la creación del Centro Nacional de Protección de Infraestructuras Críticas (CNPIC), como órgano director y coordinador de dichas actividades, y de la determinación, clasificación y actualización del Catálogo de Infraestructuras críticas.

Cualquier estrategia de seguridad en estas infraestructuras debe tener como objetivo principal prevenir posibles ataques, disminuir la vulnerabilidad y, en el caso de que se produjeran situaciones de crisis que afectaran a las infraestructuras esenciales, minimizar los daños y el periodo de recuperación.

Sin embargo, la legislación se centra especialmente en los ataques físicos a las infraestructuras críticas; la única referencia disponible en el borrador a ciberataques es la plasmada en la realización del análisis de riesgos y en la redacción de los planes de protección específicos, por lo que sería necesario la contemplación en mayor profundidad de las amenazas relacionadas con el ciberespacio. Únicamente, los ciberataques se plantean en el sector de Tecnologías de Información y Comunicaciones y en los sistemas de información y comunicaciones que soportan otros sectores estratégicos como los de la Administración y los sistemas SCADA (Supervisory Control And Data Acquisition).

Aún así, sería necesario tener en cuenta que la seguridad del ciberespacio es un objetivo estratégico de la seguridad nacional, teniendo implicaciones sociales y económicas en el país. Según Luis Joyanes, "la próxima Estrategia Española de Seguridad deberá contemplar la seguridad en el ciberespacio y debería constituir el punto de partida de una Estrategia Nacional de Ciberseguridad. Posteriormente, debería centralizarse la gestión de la ciberseguridad con la creación de un organismo responsable de coordinar a todas las entidades públicas y privadas implicadas en España".

Por tanto, teniendo en cuenta este análisis, se llega a la realización de una serie de propuestas que podrían ser esenciales para el desarrollo de una estrategia de ciberseguridad teniendo en cuenta los retos y amenazas actuales. Entre los diversos puntos, destacaría alguno como el establecimiento de una plataforma de ciberseguridad, fomentar la cultura de ésta en todos los niveles, así como la colaboración público-privada en el campo de la seguridad y las infraestructuras, abogar por Sistemas de Gestión de Seguridad de TIC y formar al ciudadano en general para que comprenda lo necesario de esta Ciberseguridad. De hecho, el propio jefe del Centro Nacional de Inteligencia, el general Félix Sanz, reconoció en un congreso celebrado en noviembre del pasado año en Madrid que algunas nuevas amenazas les pillan "casi sin experiencia y sin capacidad de reacción".

Aunque hay que decir que a un nivel menos exhaustivo, España ya comienza a prevenir los posibles ataques de esta nueva amenaza. De este modo, el pasado mes de febrero, el secretario de Estado de Seguridad, Antonio Camacho, anunciaba la elaboración de un Real Decreto por parte del Gobierno para proteger las infraestructuras de un posible ataque cibernético. "Ya no es suficiente con proteger físicamente una central energética o una vía de transporte, los riesgos son ahora

cibernéticos", explicaba Camacho. En definitiva, y en lo que a España se refiere, aún queda mucho por hacer en el terreno de la ciberdefensa, comenzando por considerar este nuevo terrorismo como una auténtica amenaza, y siguiendo por encontrar soluciones al mismo.

3.3. Casos más sonados

Cuando Collins habló por primera vez de ciberterrorismo, lo hizo elaborando una serie de hipótesis sobre posibles actos ciberterroristas. Esas hipótesis fueron usadas masivamente por periodistas, políticos y funcionarios de organismos de seguridad, para referirse a esta nueva amenaza, contribuyendo a formar una determinada idea acerca de las posibles consecuencias de un atentado terrorista informático. Las hipótesis de Barry Collin son las siguientes:

- Un ciberterrorista podría acceder remotamente a los sistemas de control de procesamiento de una planta elaboradora de cereales, cambiar los niveles de suplementación de hierro, y enfermar (e incluso eventualmente matar) a los niños de Estados Unidos mientras disfrutan de su desayuno. También podría realizar alteraciones similares en plantas de alimentos para bebés. La supuesta ventaja potencial para el ciberterrorista de este tipo de ataque es que no tendría que estar en la fábrica para ejecutar ese tipo de atentado.

- Un ciberterrorista podría interferir a los bancos, las transacciones financieras de dinero y los centros bursátiles. Esa manera, los habitantes del país perderían su confianza en el sistema económico.

- Un ciberterrorista podría atacar a la próxima generación de sistemas de tráfico aéreo, y hacer que dos grandes aeronaves civiles choquen entre sí, y señala que maniobras similares pueden ser realizadas con las líneas de ferrocarriles.

- Un ciberterrorista podría alterar las fórmulas de remedios o productos farmacéuticos, causando una gran cantidad de pérdidas humanas.

- Un ciberterrorista podría cambiar remotamente la presión de los gasoductos, causando fallas en las válvulas, y desencadenando una serie de explosiones e incendios.

Según Collin, y en vista de todas estas posibilidades, las personas encargadas de velar por la seguridad de la Nación no estarían advertidas ni podrían anular al

ciberterrorista, que probablemente se encontrará en el otro lado del mundo. En este punto, Pollitt introduce la idea de que, a pesar de las vulnerabilidades, los efectores devastadores de un ciberataque no son tantos, aunque advierte que "A medida que incorporamos más y más tecnología en nuestra civilización, debemos asegurarnos de que exista el suficiente control e intervención humana como para salvaguardar a aquellos a quienes la tecnología sirve".

En este apartado es fundamental nombrar que Al Qaeda y las Farc son los grupos que más activos se han mostrado en este tipo de ataques cibernéticos, aunque, tal y como indicaba el informe Fortinet de junio de 2009, el 40, 57% de los ataques se 'fabrica' en EEUU. El resto procedía de países asiáticos, mientras que Japón, Taiwán, China y la India se repartían el mercado. En este año, EEUU recibió el 22, 25% de los ataques y España el 6, 26%.

Pues ahora bien, veremos cuántas de estas hipótesis han permanecido como tal y cuántas han llegado a cumplirse, basándonos en los ejemplos más representativos de ciberterrorismo.

- Noviembre de 2001: Treinta países firman en Budapest la primera Convención Internacional contra el 'Cibercrimen'
- Abril de 2002: la Comisión Europea propone penas de cárcel para combatir el cibercrimen.
- Marzo de 2003: El Gobierno estadounidense diseña un posible ataque informático contra Irak, pero anuncia la penalización a aquellos 'ciberpiratas' que realicen incursiones ilegales por su cuenta.
- Junio de 2006: Los países miembros del G-8 acuerdan en Moscú cooperar para combatir el terrorismo informático con una propuesta: ayudar a las instituciones competentes a "controlar los sitios de Internet dedicados a la difusión de propaganda terrorista".
- Agosto de 2006: son detenidos en Indonesia dos hombres acusados de utilizar tecnología informática para ayudar a grupos terroristas.
- Junio de 2007: un desconocido penetra en uno de los sistemas de correo electrónico del organismo del Pentágono y obliga a desconectar 1.500 ordenadores.
- Agosto de 2010: Microsoft asegura que Stuxnet había infectado a más de 45.000 ordenadores en el mundo. Según la firma de seguridad informática estadounidense Symantec el 60% de las máquinas estaban alojadas en Irán, el 18% en Indonesia y el 8% en India.

- Septiembre de 2010: el troyano Stuxnet afecta a 30.000 ordenadores en Irán, aunque las asegura que sus instalaciones nucleares consiguen mantenerse a salvo. Stuxnet se dirige a un programa concreto de la marca Siemens que se utiliza en el control de oleoductos, plataformas petroleras, centrales eléctricas y otras instalaciones industriales, con el objetivo de sabotearlos.
- Febrero de 2011: El Nasdaq, el mercado electrónico estadounidense en el que cotizan los grandes titanes tecnológicos, sufre durante el asalto repetido de hackers, que penetran en los ordenadores de la compañía que gestiona sus operaciones.
- Marzo de 2011: el Congreso de los Diputados español aprueba la Ley de Infraestructuras Críticas, que establece los procedimientos para proteger las más de 3.500 instalaciones del país que, si dejaran de funcionar, pondrían en grave peligro servicios esenciales para la ciudadanía.
- Abril de 2011: La autoridades de Corea del Sur responsabilizan a Corea del Norte de un ataque informático que inhabilita los sistemas del banco surcoreano. La caída del sistema informático afecta a millones de clientes, que no son capaces de usar sus tarjetas de crédito y cajeros automáticos en más de una semana.

Como no es oro todo lo que reluce, no todos los ataques producidos por hackers se pueden considerar como ciberterrorismo. Aun teniendo en cuenta esto mismo, es necesario añadir que son muchos los actos perpetrados por ciberterroristas y que no han sido ni serán destapados por los servicios de inteligencia de los países en los que se produjeron. De igual modo, y por razones de seguridad, tampoco se desvelan aquellos que se han logrado evitar antes de que el ciberterrorista consiguiera llevarlos

4. METODOLOGÍA

Para resolver las cuestiones que se han detallado en los objetivos y que dan sentido a este trabajo, hemos llevado a cabo el método de investigación convencional. Para ello hemos planteado una serie de hipótesis a resolver:

1. El ciberactivismo y el ciberterrorismo se ha convertido en un problema real para los Estados, obligándoles a desarrollar programas de seguridad en estas dos materias.

2. Los Estados tienden a ver estos movimientos como una amenaza, idea derivada de la monopolización del poder, tanto político como económico.

3. Los Estados diferencian el ciberactivismo del ciberterrorismo según quién realice la acción, otorgando la diferencia de terrorismo a las acciones cometidas por grupos terroristas convencionales.

4. Las acciones y efectos del ciberterrorismo y ciberactivismo provocan cambios en la sociedad que pueden beneficiar o afectar a la ciudadanía en materia de participación democrática.

5. Las ciberacciones o los actos ciberterroristas no consiguen su fin si no son publicados en los medios de comunicación.

4.1. Técnicas de producción de datos

Para analizar y estudiar este tema, hemos recurrido a diversos ensayos y publicaciones que abordaban el tema, tanto de carácter público como privado. Los Estados no son los únicos interesados en este tipo de acciones digitales (textos más enfocados al Ciberterrorismo), pues algunas entidades privadas también han sido hackeadas y comienzan a preocuparse y a realizar informes sobre seguridad digital y Ciberactivismo.

Es un tema de estudio relativamente novedoso, por lo que hemos recurrido principalmente a Internet para buscar publicaciones que aborden el tema puesto que en papel todavía es escasa la bibliografía producida sobre este tema.

Hemos hecho un repaso por la obra de autores que han tratado este tema, tratándose de ensayos muy recientes y de sociólogos jóvenes.

Además de estas técnicas convencionales, también hemos realizado entrevistas a miembros de movimientos sociales que realizan ciberacciones y periodistas especializados en movimientos sociales. Para conseguir los datos, hemos elegido el paradigma cualitativo, pues la información que recopilemos de esta manera será más rica para completar los objetivos secundarios.

Entrevistas cualitativas semi-estructuradas

El método de investigación cualitativa de la entrevista es adecuado en esta investigación porque lo que se pretende es comprender la propia visión de las personas sobre la situación sobre el tema en concreto.

La entrevista ofrece un espacio común relacional en el que juegan factores como la intimidad, un marco que nos permite acercarnos a la realidad subjetiva, que aporta nuevos datos al estudio.

Con esta técnica, podremos valorar la forma en la que hablan los entrevistados, el modo de expresarse, las palabras que utilizan, los gestos, además de la información que ofrecen oralmente. Todo ello supone una información muy valiosa que complementará en todo momento la investigación.

El entrevistador, a la hora de hacer estas entrevistas, ha mantenido un papel dialogante y empático que permite comprender la realidad del entrevistado. El encargado de realizar la entrevista ha sido aclarador y ha potenciado el discurso de forma que se pueda profundizar en las ideas que ofrece el entrevistado.

Una vez se ha realizado la entrevista, se han analizado los datos de la información, siempre evitando la manipulación.

La población objeto de esta investigación se diferencia en dos tipos:

1. Miembros de asociaciones o movimientos sociales que ponen en marcha ciberacciones para pronunciarse sobre algún tema. Concretamente hemos entrevistado a un miembro de Anonymous España y a dos hacktivistas que han participado en dos acciones distintas, una referida al grupo #OpEuribor (plataforma encargada de investigar la estafa del Euribor y el Libor), y otra al #15MpaRato (colectivo que ha conseguido presentar en la Audiencia Nacional

una querella contra el señor Rodrigo Rato, expresidente de Bankia).

2. Periodistas encargados de cubrir información social y especializados en movimientos sociales. Los profesionales son Luis Giménez San Miguel y Elena Herrera, del diario *Público* y Jairo Vargas Martín, fotógrafo y periodista freelance colaborador en varios medios como el citado anteriormente, *Vice* o *Diagonal*, entre otros.

Se trata de un muestreo opinático, que ha seguido el criterio de la voluntariedad, puesto que se han propuesto otras entrevistas pero no han querido pronunciarse sobre este tema. En total, se han realizado seis entrevistas.

Se realizaron contactos con varios medios de comunicación con la intención de dar una visión general sobre este tema, sin embargo, sólo en el diario *Público* contestaron.

Por otra parte, los miembros de las plataformas respondieron positivamente a la hora de proponerles hacer una entrevista para la investigación.

El guion de la entrevista debe garantizar la objetividad del conocimiento que se obtiene a través de este trabajo, dado que la naturaleza del muestreo es opinática.
El esquema que hemos seguido a la hora de plantear las cuestiones durante la entrevista es:

El esquema de distribución de preguntas en la entrevista es el siguiente:

1 Fase social: Presentación y petición a la persona de un relato breve biográfico.
2. Bloque de preguntas sobre el ciberactivismo: Se plantea a los miembros de las plataformas y a los periodistas cuál es el significado que otorgan a este término.
3. Bloque de preguntas sobre qué papel tiene el ciberactivismo en la actualidad: Tanto los periodistas como los miembros de los colectivos tienen las mismas preguntas.

4.a. Bloque específico para participantes en ciberacciones: Se persigue saber qué pretenden conseguir.

4.b. Bloque específico para periodistas: Cómo interactúan las plataformas y sus miembros con los medios de comunicación para que se publiquen sus acciones y sus propuestas.

5. Se termina la entrevista retomando las cuestiones que hayan podido quedar sin

resolver o que no estén claras.

4.2. Técnicas de análisis de datos

Para desarrollar esta investigación se utilizarán técnicas de investigación descriptivas principalmente, pues esta técnica permitirá que el objetivo principal se desarrolle convenientemente.

Se utilizarán técnicas explicativas para intentar entender la realidad social a la que nos referimos. Para ello, cruzaremos los datos obtenidos, tanto e las entrevistas como en los ensayos y estudios consultados, y se intentarán ahondar en el estudio, de forma que se aporten nuevos datos.

Para los ensayos y estudios, tendremos en cuenta la perspectiva histórica, muy corta en este caso pues abordamos un tema con una trayectoria muy corta. Compararemos los datos y pondremos de manifiesto la evolución de los términos que vamos a tratar y del tema en específico.

Concretamente, para el análisis de la entrevista, se utilizarán distintas estrategias:

1. Lectura teórica de la entrevista: Los conceptos que tratamos en este estudio (ciberterrorismo y ciberactivismo, principalmente, ampliando a términos como: democracia, sociedad, participación ciudadana). Los términos están en el marco teórico de esta investigación.
2. Deconstrucción de la entrevista: Se analizarán partes concretas de cada una de las entrevistas para ver cómo surgen, de vez en cuando, contradicciones en relación a lo objetivo y a lo subjetivo.
3. Interpretación del significado: Plantea la búsqueda de significados profundos de lo extraído en la entrevista. Para este tipo de interpretación, se tendrán en cuenta las interpretaciones que realizaron los entrevistados durante el momento de la entrevista.
4. Condensación del significado: Permite organizar temáticamente las declaraciones que se han realizado de forma resumida, de modo que se puede realizar comparaciones entre unas entrevistas y otras.

5. RESULTADOS

En los últimos años ha llegado a ser invasora la cantidad de material a cerca del uso social de las nuevas tecnologías digitales. En concreto de su última conquista: las redes sociales. El término uso social se refiere al que hacen de ellas los movimientos sociales. Tal y como se ha reflejado a lo largo del análisis, no puede ignorarse que está habiendo un cambio en la forma de comunicación y de organización social. Pero no se ha convertido en un fenómeno social solo por su potencial global, sino porque ha sido capaz también de influir, de alguna manera, en la agenda mediática actual, tan estancada desde hace tiempo. Es necesario explicar esta idea con un caso concreto, el de las revoluciones árabes. Este es un claro ejemplo del ideal de la acción política en Internet: "la culminación en una movilización en la calle de un proceso de discusión social llevado a cabo por medios electrónicos de comunicación y publicación personales en el que se rompe la división entre ciberactivistas y movilizados".

Como pasó en 2006 con las "sentadas por una vivienda digna", o las revueltas en 2005 contra el CPE en Francia, las movilizaciones de las revueltas en el mundo árabe se convocaron y agilizaron gracias a Internet. Pero frente a la escasa cobertura que los medios de comunicación hicieron de las acciones de la "Plataforma por una Vivienda Digna" (más significativa en el caso de las revueltas en Francia), la lucha social en Túnez, Egipto, Barhéin, Libia, Marruecos, Siria, etc. ha tenido y está teniendo mayor reflejo en los medios. Desde que empezaran en Túnez, no ha dejado de estar en la agenda informativa de los medios.

Lo que interesa de esto es constatar la influencia que pueden tener los movimientos sociales que funcionan empleando Internet como herramienta, en la agenda pública. La blogsfera y las redes sociales pueden modificar la agenda pública. Así lo demuestran las revoluciones culminadas. La importancia que han demostrado las redes sociales con su capacidad de convocatoria y difusión ha interesando mucho a los comunicadores. Ahora el ciberactivismo forma parte de la "agenda setting". Existe dentro del proceso de tematización de los medios de comunicación y, por tanto, existe para la opinión pública (las revueltas árabes han sido Trending Topic en Twitter, ha tenido gran presencia en los medios de comunicación y se han abierto multitud de debates públicos al respecto) Esto implica una modificación en el sistema global de medios, pues, como ya se ha dicho, la agenda informativa está desde hace tiempo muy encorsetada y "amaestrada" por grupos de presión con lo que, el sistema global de medios estaba también estancado y resultaba inaccesible para nuevos sujetos.

Con la trascendencia de las acciones sociales en la agenda mediática y pública, se están empezando a abrir huecos en la suerte de corsé anquilosado que es el Sistema Global de Medios.

Es paradójico que el ciberactivismo culmine con 100% de éxito una acción cuando, a parte de trascender la división entre ciberactivistas y movilizados gracias a una movilización física de los ciudadanos en la calle, trasciende en los medios de comunicación de masas tradicionales. Es decir, la acción habrá alcanzado todos sus objetivos si, finalmente, influye en la agenda mediática pública, y por tanto, si a través de los medios de comunicación se sitúa en la opinión pública como tema de debate. El siguiente logro es que estos temas recién instalados en el debate público verdaderamente se integren como cambios futuros en la agenda política. No hay nada más democrático que la efectiva influencia de la ciudadanía en la actividad institucional.

5.1. Movimientos sociales en la Red. *Ciberactivismo.*

Que con la evolución de la *Web* y la llegada de las redes sociales algo está cambiando, de eso no hay duda. Y es un cambio que afecta de manera directa a la constitución del tejido social, y que transforma los procesos de relación. Pero más allá de esto, no parece saberse bien en qué consiste exactamente esta reestructuración social, a dónde nos lleva ni que hay de bueno o malo en todo ello. Es un cambio todavía en proceso.

Algunos de los efectos reales de esta nueva forma de organización y comunicación social si los estamos viendo ya. El ciberactivismo se presenta como un ejemplo de las posibilidades de organización y movilización social de la Red. Una serie de movimientos sociales, en el marco de la sociedad de la información y el conocimiento, que van desde actos simbólicos de “ciberprotesta” hasta revoluciones, están sabiendo emplear la *Web* como herramienta de comunicación y organización social. Y el uso de esta herramienta se resume en un hecho muy sencillo: la difusión masiva de mensajes desde la Red y a través de la Red.

Internet es una herramienta, no un sujeto para los movimientos sociales. Estos usan la Red, pero no tienen su origen en ella. Esto es importante mencionarlo ya que, con las últimas revoluciones, por ejemplo, que están teniendo lugar en los países árabes, algunos medios de comunicación se recrean al llamar a estos movimientos

"revoluciones *Twitter*" y publican líneas y líneas que atribuyen la razón de las revueltas a la herramienta. Esto es un error, la razón está en la situación, que crea el descontento y lleva a la sociedad a perseguir el cambio. Las redes sociales, si, son una herramienta potente que facilita la acción, sobre todo por su gran poder de convocatoria. Esta claro que el uso de Internet como herramienta de comunicación, trabajo y convocatoria modifica el proceso de trabajo, y éste cambia si cambia la herramienta con la que se trabaja, de eso no hay duda. Internet resulta un elemento decisivo en la organización social porque tiene un carácter global como ninguna otra. Facilita enormemente la globalidad a la que aspiran los movimientos sociales. Cambia la forma de trabajo y también la forma de organización, pero este hecho no implica que la utilización de la red por los movimientos sociales para sus acciones políticas o sociales esté dando lugar a nuevos sujetos antes no existentes.

Internet da voz y convierte en líder de opinión a quienes antes no lo eran. No crea sujetos, sino que da voz a aquellos que en la forma de comunicación centralizada jamás la tuvieron. David Ugarte dice en su libro "El poder de las redes" que con las redes sociales, "las personas normales podemos ganar independencia". El cambio en la estructura de la información que provoca Internet da lugar a nuevas formas de distribución de poder. El empoderamiento ciudadano, en este caso, tiene además un gran impacto en el actual Sistema Global de Medios. Se multiplican los emisores y en la Red ganan fuerza medios de información alternativos a los tradicionales. Aunque estamos hablando aún de una mínima influencia a escala mundial de estos "medios alternativos". Pero la diferencia fundamental es que esos infinitos nuevos emisores, están interconectados entre sí, se comunican ahora sin necesidad de pasar antes por un equipo central. Aquí es importante destacar otro concepto que explica David Ugarte en su libro, el de red "distrubuida": "Internet permite que millones de ordenadores, jerárquicamente iguales, se conecten y comuniquen, pasando así de un mundo de poder descentralizado a otro de poder distribuido".

Con lo que sabemos, lo verdaderamente interesante es ver como los movimientos sociales, partiendo de un real "empoderamiento ciudadano" están empleando Internet para sus acciones políticas. Escapando del control al que los medios de comunicación de masas tradicionales están sometidos, los movimientos sociales han encontrado un arma muy fuerte en Internet y las posibilidades de la "Red distribuida".

El primer ejemplo de actividad social en Internet (ciberactivismo), lo ha protagonizado

la *Blogsfera.* Los blogs como soportes personales que dan voz a sujetos individuales pero que pueden distribuirse por la Red y llegar a una masa colectiva importante.

Puede decirse que existen dos fases en el ciberactivismo: una expositiva o deliberativa, en la que a través de los blogs y los foros se intentan incluir determinados temas en una especie de agenda global en Internet y así abrir el debate; y otra de movilización, en la cual a partir de las redes sociales, *e-mails* y mensajes de móvil se llega a movilizar físicamente a la gente en la calle.

En la primera fase encontramos referentes a día de hoy ya muy importantes. Algunos ejemplos pueden ser blogs tan populares y "mediáticos" como el de la activista cubana Joani Sanchez: www.desdecuba.com/generaciony. Esta activista cubana mantiene un blog en el que denuncia y crítica las acciones represivas del gobierno cubano y se ha convertido en un *site* muy visitado en occidente. Durante los últimos años ha tenido lugar una verdadera explosió de páginas e iniciativas individuales de la ciudadanía. Ya sean blogs o acciones en Internet.

La Red también ha permitido una tipología de *blogs* capitaneados por periodistas pero que en esta ocasión escriben al margen de los medios de comunicación oficiales. Representan así versiones alternativas y lanzan al público cibernético asuntos de actualidad que no cubren dichos medios oficiales.

Ejemplos de esta tipología pueden ser el blog de la periodista Olga Rodríguez: http://minotauro.periodismohumano.com/ o el de Alberto Arce www.albertoarce.com.

Existen también espacios como http://globalvoiceonline.org:
"Es una red internacional de bloggers que traducen, reportan y defienden a los blogs y medios ciudadanos de todo el mundo". Plataformas así reflejan la tendencia en la Red a interconectar todo infinitamente.

Antes de pasar a la segunda fase, la de movilización física, encontramos multitud de acciones que tienen repercusiones en la Red. Son las que ya se han mencionado anteriormente, como los "Ciber-ataques" de Anonymous a las *Web* institucionales de Túnez y Egipto. En esta fase, los movimientos sociales, conscientes de la fuerza e importancia de Internet como arma, llevan a cabo acciones desde y destinadas a la propia Red. En este caso, atacaban *webs* oficiales de gobiernos que estaban limitando el uso de Internet a sus ciudadanos para poder manipularles y controlarles a sus anchas. El ciberactivista tiene entre sus objetivos asegurar la disposición pública de las herramientas para que éstas devuelvan a los ciudadanos el poder que hoy monopolizan las instituciones, medios de comunicación de masas tradicionales y los grupos de poder económicos y políticos.

Respecto a la fase de movilización de la ciudadanía en la calle, lo más importante aquí es destacar es el poder de convocatoria de las Redes Sociales y la potente capacidad de difusión de Internet. Lo importante de la tecnología es que está supeditada a la forma de organización que representa y esto es lo decisivo para los movimientos sociales, porque se trata de una tecnología que está a completa disposición pública. Las redes sociales no son el sujeto actor de las acciones políticas ni de las revoluciones actuales, como se confunde en ocasiones, pero si es la vía mediante la que se han facilitado. La clave del para el éxito para que una convocatoria en Internet se convierta en una verdadera movilización es establecer un lugar y una hora concretos, junto con unos objetivos escuetos y contundentes. Para el éxito de una acción, se han de poner al servicio de los usuarios las herramientas e instrucciones necesarias para que secunden dicha iniciativa. Para esto no hay nada más efectivo que Internet: la "Red Distribuida".
A continuación se van a exponer algunos ejemplos y casos concretos para ilustrar todo lo explicado.

a). Ciberactivismo: iniciativas concretas de movilización social en la Red.

En los últimos meses han sido muchas las organizaciones no gubernamentales que

han optado por este ejemplo de movilización por Internet para conseguir sus propósitos. Lo muestran como la manera más fácil de participar puesto que solo es necesario un equipo electrónico que permita acceso a Internet y la propia conexión. Sobre todo está sirviendo para que los jóvenes que no tienen poder real en la sociedad pidan e incluso exijan democracia y que puedan presionar a los que sí tienen el poder de cambiar situaciones que consideran injustas. Para ello utilizan todo tipo de herramientas 2.0, así consiguen incitar a la gente a participar y aprovechar la libertad que ofrece el ciberespacio, y transformarlo en un claro detonante de reivindicaciones.

Las campañas que se emprenden cada día pueden estar motivadas por diversas causas: la búsqueda de respeto a los Derechos Humanos, detención de acciones nocivas para el medio ambiente, imposición de una situación de democracia, muestra de desacuerdo político, y se realizan usando la libertad de expresión que ofrece Internet. Las acciones pueden proceder de una organización que considera el ciberactivismo la mejor manera de crear presión en ese momento o en cambio, de otra que basa la mayoría de sus campañas en las nuevas tecnologías y formas de divulgación como las redes sociales. Además pueden ser acciones que promuevan la movilización en el plano real o solo en el plano virtual.

En muchos casos, la buena organización y la apropiada difusión han conseguido resultados positivos en las campañas. Amnistía Internacional ha evitado que se lleven a cabo penas de muerte mediante este activismo al igual que Periodistas sin Fronteras han conseguido la liberación de profesionales de los medios de comunicación.

Tres ejemplos de campañas concretas:

- <u>"Brazil: „Expediente limpio'"</u>

  Esta campaña la llevó a cabo Avaaz, una organización que ha basado la mayoría de sus propuestas en la presión social de las firmas digitales de los participantes. Ha emprendido más de 40 millones de acciones desde enero de 2007 y tiene casi 9 millones de miembros en 193 países.

  Iniciaron la campaña "Brazil: „Expediente limpio'" ("Ficha limpa" en portugués) en julio de 2010. Buscaban conseguir que en Brasil los políticos que hubieran

sido condenados por delitos graves no pudiesen presentarse como candidatos a cargos públicos.

La idea era que se crease una ley que regulase esta propuesta, es decir, llegar hasta el Congreso y que éste aprobase la iniciativa de forma legal.

Teniendo en cuenta que el 25% de los miembros del Congreso estaban bajo investigación por actividades delictivas, como la corrupción, no había muchas expectativas la ley se aprobase.

A través de su página web, con el envío de esta propuesta con información sobre ella a los miembros inscritos y, además, con la divulgación mediante redes sociales, para que se conociese esta acción, se consiguieron "más de 2 millones de firmas, 500.000 acciones online y decenas de miles de llamadas telefónicas". Así, el resultado fue la aprobación de la ley que ha excluido a más de 330 candidatos a cargos públicos.

- "Exige al Banco Santander que no financie una central nuclear en una zona de riesgo sísmico"

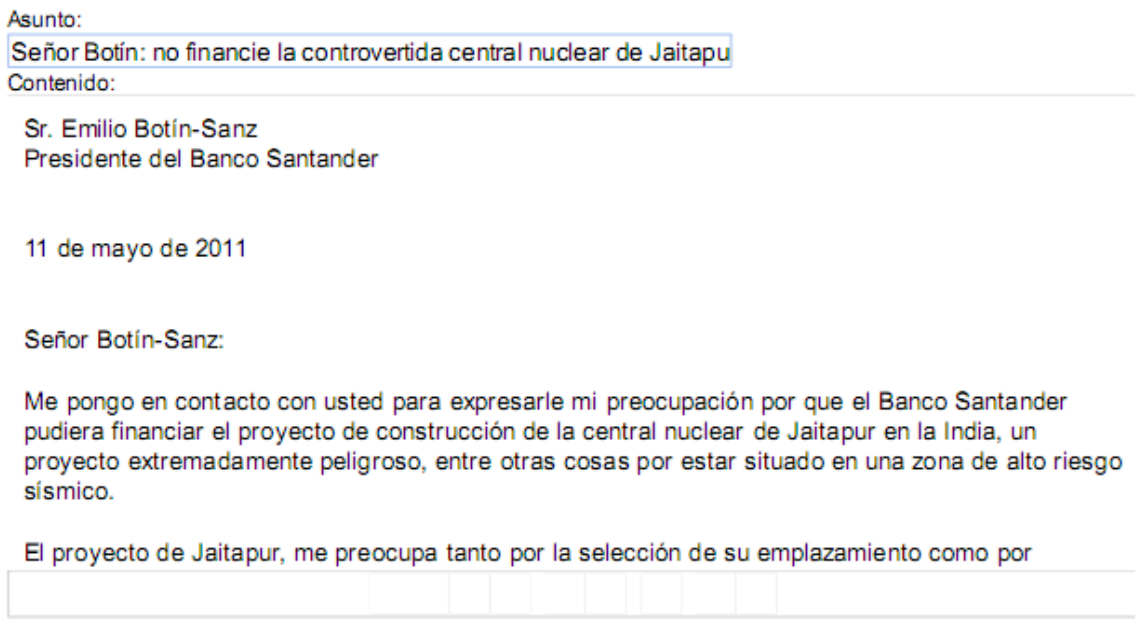
Greenpeace es otra de las organizaciones que promueven habitualmente el ciberactivismo para todos aquellos que no sean activistas en las acciones físicas que llevan a cabo, pero quieran ayudar de alguna manera. En la mayoría de sus acciones para ejercer la presión social oportuna, utilizan el envío masivo de correos con peticiones a los que tienen la autoridad de cambiar la situación demandada.
Según Greenpeace España ser ciberactivista es "movilizarse activamente en la defensa del medio ambiente desde tu ordenador." Promueven la participación incidiendo de la importancia que tiene cada uno de los participantes "aún nos quedan muchas metas por logras y tú eres una parte necesaria para conseguirlas" y lo fácil qué es: "¡Sólo necesitas tener una dirección de correo electrónico y un minuto de tu tiempo!". Su lema es que cada firma "es una valiosa herramienta para la lucha por el medio ambiente".

Una de las últimas campañas pretende evitar la construcción de una central nuclear en

Jaitapur (India), una zona con alto riesgo de terremotos, recordando el

antecedente de lo que ha sucedido en Japón. La construcción de esta central, que será la mayor del mundo, se va a realizar con financiación bancaría, entre las entidades participantes está el Banco Santander. Además del peligro, también supone un "enorme impacto negativo en el desarrollo social y medioambiental de la región". Y añaden que "el proceso de obtención de la licencia ambiental para este proyecto ha violado la legislación vigente en la India".

Ante esta situación Greenpeace ha decidido utilizar todas las ventajas que Internet le ofrece. Para empezar ha propuesto a los ciberactivistas enviar una carta directa a Emilio Botín, Presidente del Banco Santander para que "no financie la construcción de la central nuclear de Jaitapur". El formato de la carta


Asunto:
Señor Botín: no financie la controvertida central nuclear de Jaitapu
Contenido:

Sr. Emilio Botín-Sanz
Presidente del Banco Santander

11 de mayo de 2011

Señor Botín-Sanz:

Me pongo en contacto con usted para expresarle mi preocupación por que el Banco Santander pudiera financiar el proyecto de construcción de la central nuclear de Jaitapur en la India, un proyecto extremadamente peligroso, entre otras cosas por estar situado en una zona de alto riesgo sísmico.

El proyecto de Jaitapur, me preocupa tanto por la selección de su emplazamiento como por

está prediseñado y el ciberactivista solo tiene que rellenar los datos personales, lo que facilita y agiliza la acción. Para que el número de participantes sea mayor, propone que todos compartan esta información por las redes sociales como Twitter, Tuenti o Facebook. De momento la campaña está en marcha y pleno momento de difusión y divulgación.

- <u>"Campaña „Zapatero, ¡lo dijiste! Cúmplelo'"</u>

Intermón Oxfam hace un uso bastante repetido de las acciones a través de Internet. Su apartado más juvenil llamado Dale La Vuelta Al Mundo propuso una campaña de ciberactivismo a todos sus miembros el año pasado.

> Se titulaba “Zapatero, ¡lo dijiste! Cúmplelo” y hacía referencia a las promesas que el Presidente realizó cuando se encargaba de la presidencia de la Unión Europea durante el primer semestre de 2010. Se pretendía que llevase a cabo un plan antipobreza.
>
> Su ideal era “un plan que garantice el cumplimiento del 0,7%, que luche contra la evasión fiscal que traba el desarrollo de los países y que proponga medidas eficaces para paliar la situación mundial de hambre”.
>
> Consiguieron mover a exactamente 31.335 personas para que firmasen ese recordatorio para el Presidente. Esas firmas fueron entregadas personalmente al Presidente por parte de la portavoz de Intermón Oxfam. Pero, como dice la organización “sus promesas de lucha contra la pobreza han quedado en buenas intenciones.”
>
> Aunque no se consiguió un cambio en la política que llevó a cabo José Luis Rodríguez Zapatero durante la presidencia española, la presión social se hizo evidente con esas peticiones y con su entrega en mano, además del gran número de participantes que comentaron en el blog de la campaña.

El ciberactivismo ofrece formas fáciles de colaborar por la consecución por un ideal, de realizar acciones sociales, dando la oportunidad de participar a todos aquellos que incluso les gustaría hacerlo más activamente pero no pueden y evitando que la gente se pueda excusar en lo poco que pueden hacer desde su posición. Y todo esto de una forma internacional, sin barreras idiomáticas ni límites geográficos.

Lo cierto es que no siempre surgen efecto las campañas propuestas, no obstante el hecho de que tan fácilmente se pueda movilizar a mucha gente por un objetivo común debería poner en alerta a los grandes grupos de poder, además de hacerlos conscientes de que la presión en un futuro puede ser aún mayor. Internet no tiene dueño, es un espacio virtual de libertad en el que estas acciones se pueden seguir llevando a cabo pero para conseguir manifestaciones y movimientos en el mundo real, como se ha demostrado recientemente.

El factor fundamental en muchos casos es la divulgación apropiada a través de los Medios de Comunicación fuera de Internet. Por supuesto, esto debe ocurrir después de una amplia difusión por Internet, después de que la *ciberacción* se haya llevado a cabo. Cuando el número de participantes y el alcance de sus acciones sean noticia.

Es en el momento en el que se muestra al mundo real lo que se ha estado haciendo en el virtual, cuando la presión ejercida es la máxima y los buenos resultados pueden darse y los fines de la campaña cumplirse con mayor facilidad.

b) La acción de Anonymous

Mención especial se merece el grupo de activistas de "Anonymous". Conocidos por algunas de sus polémicas acciones, entre las que destacan la caída de cuatro sitios de Colombia en protesta por el proyecto de Ley de protección de derechos de autor en Internet, han sido acusados de ciberterroristas en más de una ocasión.

Si bien es cierto que sus métodos no son siempre los más apropiados, la plataforma se defendía de las duras críticas en un comunicado en vídeo a mediados de abril en el que reivindicaba su lucha. Esta reacción vino provocada en respuesta a las acusaciones que las autoridades habían realizado señalando que el responsable de los ataques a estos sitios webs estatales había sido identificado.

El grupo, que aclara no ser „de hackers', como se les ha denominado en los medios, dirige el vídeo al gobierno colombiano, pero comienza con un mensaje a los medios, en el que manifiesta su desagrado por "las acusaciones perpetradas por algunos medios „desinformativos', que basándose en un gran desconocimiento y en su infinito afán por conjeturar, nos han tildado de ciberterroristas, denotando una total y completa falta de profesionalidad".

Además, explica que si bien las acciones de Anonymous llegan a inhabilitar servidores web temporalmente, no generan daños, ni robo de información, ni ataques de virus o malware a los sitios web, "así algunos de sus miembros dispongan de los medios y el conocimiento para hacerlo, porque no son ciberterroristas".

Anonymous exige libertad de expresión y de información en Internet, que considera un derecho fundamental, e insiste en que su enemigo es la censura y quienes la promuevan. "Nuestros objetivos son nobles y nuestra lucha pacífica se libra por la necesidad de impedir que intereses particulares atenten contra la libertad de expresión y de información".

Sin embargo, y siguiendo los criterios que definen a una auténtica acción ciberterrorista, Anonymous no es considerado como tal, ya que sus acciones están encaminadas a la libertad de expresión y a la concienciación de la ciudadanía en todo

lo relacionado con este mismo aspecto, y no en el boicoteo y sabotaje continuo de las plataformas estatales y gubernamentales.

5.2. Una nueva amenaza para los Estados

Como ya hemos visto antes, Internet tiene una influencia en muchos ámbitos, y todos ellos afectan directamente a la ciudadanía. Internet está en el desarrollo de la vida pública, en la política y en la economía. Dicho esto, estas esferas están expuestas a nuevas amenazas, peligros que pueden llevarse a cabo con las nuevas herramientas tecnológicas. Como los casos anteriormente explicados en los que se ha detallado en qué consistían, son casos de ciberactivismo o ciberterrorismo que intentan cambiar y "atentan" contra regímenes dictatoriales o situaciones globales injustas.

La preocupación por esta nueva vulnerabilidad de los sistemas informáticos nació en los años 80, ya que los hackers comenzaban a acceder ilegalmente a redes conectadas, consiguiendo así información o incluso, algunas veces, conseguían cambiar el contenido de estas redes. Por lo tanto, se planteó en Estados Unidos la posibilidad de que los grupos terroristas pudieran cometer atentados a través de estas nuevas herramientas tecnológicas, lo que les permitía no estar en el lugar del atentado directamente, sino que con los medios tecnológicos se pudieran realizar acciones terroristas a distancia. Así nació el término de ciberterrorismo.

En este mundo globalizado actual en el que Internet difumina las fronteras y los recursos tecnológicos y los nuevos dispositivos móviles fomentan la transferencia de información, resulta muy difícil luchar contra todo tipo de terrorismo sin tener en mente la cooperación internacional. Todos estamos conectados a Internet, o por lo menos todos los habitantes de países desarrollados o en vías de desarrollo, se ha convertido en una necesidad cotidiana según Camilo José Dacach. Como dice este profesor e ingeniero en telecomunicaciones, “la más grande multinacional o simplemente un habitante del mundo está conectado a Internet”. Estos usuarios y empresas se conectan a través del correo electrónico u otras aplicaciones sencillas, pero no sólo existen estas relaciones en Internet, sino que hay soluciones más complejas como por ejemplo la video vigilancia que se da a través de Internet.

Hay que enfatizar que cada vez que el mundo ha aumentado su nivel de globalización, también han aumentado la amenaza potencial del ciberterrorismo. ¿Por qué? Sencillamente porque al estar todos más conectados es más sencillo causar más daño

global a más personas, a gobiernos a los sistemas globales. Vemos así el ejemplo que nos ofrece el profesor Camilo José Dacach en su análisis "Ciberterrorismo: Historia de nunca acabar":

"La perdida económica causada por un ciberataque puede causar desastre en sistemas financieros mundiales, apagones nacionales y el colapso de infraestructuras clave de información tecnológicas que apoyan muchos departamentos gubernamentales".

Sin embargo, hay que tener en cuenta que a los Estados, en muchos casos, no les interesa tanto estas molestias tipificadas como actos ciberterroristas que pueden afectar a los ciudadanos, sino que lo realmente molesto es la gran capacidad que ofrece Internet para dirigirse a grandes audiencias y poder reclutar, movilizar y realizar una propaganda anónima a través de los medios tecnológicos actuales y la conexión en red global que existe hoy en día.

Según la profesora Beatriz Busaniche, de la Universidad de Buenos Aires, los estados han tipificados el ciberterrorismo como una nueva forma de atentar contra el estado, sin embargo podemos creer que en realidad lo que se está haciendo es controlar más férreamente a la ciudadanía imponiendo medidas penales para controlar la información que se da en las redes globales. De forma que, en lugar de englobar el ciberterrorismo dentro de las leyes en las que se pena el terrorismo, se crean unas nuevas para poder crear un régimen más controlable.

5.3. Posibles soluciones de los Estados

Los estados proponen distintas soluciones para estos ataques tan molestos para los ciudadanos, así que, en nombre de la seguridad ciudadana crean nuevas legislaciones para controlar las acciones a través de las nuevas tecnologías. Hay quien cree que no existen nuevos los ciberdelitos, sino que sólo existen los delitos. No es totalmente cierto, según la profesora Beatriz Busaniche, que sea necesario modificar el código penal para construir una sociedad de la información más segura. Se está creando un riesgo que muchas veces no es real, ya que las iniciativas del ciberterrorismo o ciberactivismo, muchas veces parten de situaciones injustas que pretenden ser denunciadas a través de estas plataformas. Lo que consiguen los estados con estas nuevas leyes es controlar el sistema de información para evitar estos movimientos que afectan al control de las masas.

Se pretende instaurar un régimen de control sobre la ciudadanía en el ámbito de las comunicaciones hablando de ciberseguridad, cuando lo que se da realmente es, según Busaniche, "una flagrante violación a los derechos humanos".

No sólo los estados apoyan esta forma de tipificar estos delitos tradicionales con nuevas herramientas dentro de una nueva legislación, sino que la ONU también cree que esto es necesario. De hecho, esta entidad ha emitido una serie de documentos en los que clasifica los delitos informáticos según el tipo (fraude, falsificación y sabotaje) como se puede ver en el marco del Décimo Congreso de las Naciones Unidas sobre Prevención del Delito y Tratamiento del Delincuente Viena, 10 a 17 de abril de 2000. En el contenido de este texto podemos leer: "dado que las computadoras y las redes pueden ser objeto a la vez de uso legítimo y de uso ilícito, se impone la conclusión de que entre quienes exploran las oportunidades del nuevo medio hay personas y grupos impulsados por motivos delictivos". Por lo tanto, las conclusiones que podemos sacar de esto y del contenido de estos textos de Naciones Unidas es que esta herramienta, así como podrían ser muchas otras, pueden tener este mismo objeto. A lo mejor debería darse una nueva tipificación para el uso de cuchillos, ya que, si planteamos esta lógica tan sencilla a esta herramienta tradicional, podemos pensar que hay personas que pueden utilizarla de forma lícita (para comer, por ejemplo) y otras personas o "grupos impulsados por motivos delictivos" puedan utilizar esta herramienta de forma ilícita (como por ejemplo, para matar a alguien). De forma que, se presupone que existiendo este riesgo hay que paliarlo de alguna forma para evitar las consecuencias que puedan tener, mientras que en otros casos la tipificación que se da tiene en cuenta el delito y no la herramienta.

Para definir "delito cibernético" las Naciones Unidas dicen que "se entiende todo delito que puede cometerse por medio de un sistema o una red informáticos, en un sistema o una red informáticos o contra un sistema o una red informáticos. En principio, el concepto abarca todo delito que puede cometerse en un medio electrónico. En este marco, la palabra delitos denota formas de comportamiento generalmente definidas como ilegales o que probablemente serán declaradas ilegales en breve plazo". Por lo tanto, se mantiene el sentido tradicional de la palabra delito, pero se regula y se legitima esta nueva ley por la herramienta que se va a utilizar.

Por otro lado, otra de las soluciones que plantean los gobiernos (más sencilla que la anterior) es la desconexión total o parcial de Internet, consiguiendo así resolver el problema totalmente. Sin embargo, esto logra solucionarse a través de otros medios

de transmisión de información ya que actualmente se cuenta con más mecanismos para vencer estos obstáculos, como los que se han señalado al analizar los casos prácticos de ciberactivismo.

5.4. Ciberdefensa frente a ciberterrorismo

Este concepto se presenta como solución al ciberterrorismo, engloba las soluciones que el estado debe dar para combatir estas situaciones. Según Fernando Acero Martín, Teniente Coronel del EA Diplomado del Estado Mayor, los gobiernos de Francia y Reino Unido, impusieron a todos los proveedores de servicios de Internet firmar un acuerdo de auto-censura en el que se comprometían a retener, durante al menos por un año, las conversaciones de correo electrónico u otros datos que pudiesen ser sospechosos de contener información que "evidenciara" actividad terrorista.

También nos dice que en otros países europeos, como Suecia y Dinamarca, han realizado acciones similares ya que han permitido que la policía tuviera un acceso rápidamente, inmediatamente después de un ataque, sin orden judicial. Además, también permitían instalar rastreadores en los proveedores de servicios de Internet para controlar e interceptar correos electrónicos con contenidos que puedan estar relacionados o sean sospechosos de actividad ciberterrorista.

En China, uno de los países con el control más férreo de información, se ha intentado controlar el crecimiento de cibercafés, los únicos sitios en los que se puede acceder a esta red global. Lo que se ha hecho ha sido intentar atrapar a "disidentes y criminales", según Fernando Acero Martín, que utilizaban Internet para planear o infringir daños. La censura que realiza China es para "asegurar la estabilidad del régimen", es decir sólo emiten propaganda y evitan todo tipo de críticas provenientes de cualquier medio web.

En el informe que crea Reporteros Sin Fronteras para el Día Mundial contra la Cibercensura se dice que los países que deben ser considerados como "enemigos de Internet" son Burma, China, Cuba, Irán, Corea del Norte, Arabia Saudí, Siria, Turkmenistán, Uzbekistán y Vietnam. Por lo tanto, en estos países se está dando un control como el que hemos descrito en el ejemplo de China. Sin embargo, hay otros países en los que este concepto, "cibercensura", también existe por increíble que nos parezca, ya que utilizan la excusa del ciberterrorismo como riesgo al que hay que paliar con la ciberdefensa, generándose así un alto nivel de cibercensura, como en los

casos de los países europeos que hemos detallado anteriormente.

En el monográfico de Fernando Acero Martín, se dice que “es muy importante que todas las naciones hagan una revisión cuidadosa y completa de sus leyes concernientes a este problema y que fortalezcan las medidas de seguridad relacionadas con el Internet, sin importar que tan tecnológicamente avanzado este el país, para prevenir que los terroristas encuentren refugio en donde tendrían mayor libertad para cometer actos de ciberterrorismo”. Por lo tanto, este concepto de ciberdefensa se refugia en este posible peligro para poder controlar a la ciudadanía violando derechos de privacidad, entre otros derechos.

Estados Unidos no es una excepción en todo el tema de ciberdefensa, de hecho, es el país que se sitúa en cabeza. A partir de los atentados del 11-M, Estados Unidos ha creado un programa denominado “carnívoro” que es capaz de rastrear contenidos que puedan contener información relacionada con acciones terroristas. Sin embargo, también existe programas encriptadores que permiten mantener la confidencialidad y que por lo tanto ceden un espacio a los terroristas a crear sus planes y mantenerlos en total secreto.

Estamos partiendo de la idea tradicional de riesgo. Hay un nuevo riesgo en este mundo globalizado, ya no sólo existen los delitos, sino que también hay ciberdelitos. Sin embargo, todo se agrava, existen incluso los ciberterroristas. Para combatirlo, no nos importa ceder parte de nuestra privacidad o confidencialidad, no importa renunciar a parte de nuestro derechos mientras que el nuevo término de ciberdefensa tenga sentido en el sistema global y pueda hacer que nos sintamos más seguros frente a este nuevo riesgo al que nos enfrentamos cada uno de los internautas. Quizás deberíamos plantearnos quienes son realmente los ciberterroristas, si pequeños grupúsculos o incluso grandes grupos formados o gobiernos que acceden y controlan el flujo de la información de las redes globales.

6. CONCLUSIONES GENERALES

6.1. Ideas principales

Teniendo en cuenta los resultados presentados, podemos ver que los términos "ciberterrorismo" y "ciberactivismo" están separados por una delgada línea. El criterio para diferenciar estos dos términos proviene de quién realiza la acción, de modo que si la organización que lo protagoniza es un grupo terrorista tradicional, se considera la acción como "ciberterrorista", sin embargo, en el caso de que sean organizaciones no gubernamentales o movimientos sociales más pequelos, se tratará de una "ciberacción".

La definición que ya hemos señalado de Barry Collins sobre "ciberterrorismo" se mantendría tras conocer estos datos, puesto que señala que es "la convergencia del ciberespacio con el terrorismo". Sin embargo, hay que tener en cuenta que las acciones de los activistas y terroristas en la web pueden tener consecuencias similares y se les están dando dos valoraciones diferentes.

Los miembros de colectivos entrevistados para este estudio tienden a referirse a sus acciones como un acto de "ciberactivismo", descartando tajantemente el "ciberterrorismo".

Los hackeos que ponen en marcha estas organizaciones no distan demasiado de las que ejecutan las organizaciones terroristas. El fin de las dos organizaciones es interferir en la vida pública y situarse en la opinión pública a través de los medios de comunicación.

Los colectivos y las asociaciones que realizan hackeos o ciberacciones suelen delegar la comunicación en un grupo de personas, según nos cuentan los miembros de las plataformas Anonymous en España y Hacktivistas, así como los periodistas entrevistados.

Los periodistas hacen hincapié en que muchas veces las acciones que proponen no tienen la suficiente magnitud ni relevancia para ser noticia y que son los propios miembros de las plataformas quienes reconocen que no han conseguido el objetivo.

Los movimientos sociales actuales están utilizando las redes sociales y los medios técnicos digitales para propagar sus noticias y darse a conocer. El miembro hacktivista

de la plataforma 15MpaRato, colectivo encargado de la querella contra Rodrigo Rato en la Audiencia Nacional, subraya la importancia de las redes sociales y asegura que su actividad en Twitter "fue definitiva para conseguir que los casos particulares se pusieran en contacto con la plataforma para conseguir presentar la querella contra Rato". Por otro lado, el miembro del colectivo #OpEuribor señala que el hackeo que realizaron contra los bancos españoles que manipularon el Euribor, así como la acción contra el sitio web de Bankia en acuerdo con #15MpaRato fue una acción que les dio visibilidad en la prensa y que consiguió que dos temas económicos de relevancia se instauraran en la agenda setting y llegaran a personas "que generalmente no están interesadas por esos temas".

La sociedad de la información de la que habla Daniel Bell ha potenciado que las acciones de unos países se empiecen a llevar a cabo en otras localizaciones geográficas más lejanas. La aldea global a la que se refiere Marshal McLuhan también recoge este tipo de acciones globalizadas que entrar en la agenda setting y empiezan a calar en la mente de la audicencia.

No sólo las acciones empiezan a formar parte de la opinión pública, si no que los temas que reivindican cada una de esas acciones comienza a situarse dentro de la opinión pública.

Para los Gobiernos es una amenza real que existan pequeños grupos de hacktivistas que realicen ciberacciones, puesto que estas podrían alterar el orden general y además podrían plantear nuevas ideologías o pensamientos lejanos o distintos a la idea que quiere transmitir el Estado. Los miembros de las plataformas a los que hemos entrevistado detallan que no tienen por qué ser "Gobiernos autoritarios" y ponen de ejemplo al Gobierno español. Señalan que varios de sus compañeros y ellos mismos han sido identificados en varias ocasiones y que sus cuentas de correo electrónico han sido rastreadas por la Policía para evitar nuevas acciones. De esta manera, justifican que los Gobiernos ven como una amenaza real las acciones que puedan cometer estos pequeños grupos sociales.

La influencia de las ciberacciones en el sistema global de medios es cada vez mayor, según señalan los periodistas entrevistados. "Muchas veces no puedes medir la magnitud al principio, pero hay otras que sabes que algunas acciones van a tener un gran peso y mucha fuerza mediática", asegura Jairo Vargas Martín, periodista freelance entrevistado y especializado en movimientos sociales, sobre todo en la zona

de Madrid y en ciberacciones.

Elena Herrera y Luis Giménez invitan a realizar un seguimiento en los medios de comunicación sobre este tipo de acciones y aseguran que están en auge. “Cada vez recibes más llamadas de los gabinetes de las plataformas o de los encargados de estas acciones y te das cuenta de que están muy bien organizados”, señala Luis Giménez.

Ambos aseguran que las plataformas saben la magnitud que pueden llegar a tener y la importancia de que sus acciones aparezcan es los medios es fundamental. “El fin de las ciberacciones es alterar a la ciudadanía, despertarla y concienciarla de nuevos problemas, si las acciones no aparecen en las páginas de los medios de comunicación, en los boletines de radio o en las televisiones, estás acciones no sirven para nada”, señala Elena Herrera.

De esta forma, podemos constatar que existe una relevancia real entre las ciberacciones como actuaciones sociales como protesta.

6.2. Futuras líneas de investigación

Esta investigación puede desencadenar nuevas líneas de actuación. Se podría plantear cuál es la magnitud de la influencia que se deriva de las noticias publicadas en medios sobre este tipo de acciones.

Por otra parte, también se podría determinar cuál es el papel del periodista en este tipo de informaciones, señalando cómo debe dar la información y cómo debe tratar la objetividad y a los entrevistados, puesto que en numerosas ocasiones los miembros de los colectivos no ofrecen sus datos personales por miedo a que les acusen o les multen, por lo que las fuentes no siempre son constatables.

También se podría llevar a cabo un estudio sobre qué es lo que entiende la población por ciberterrorismo y ciberactivismo, de forma que se constataría que estas ideas están en la idiosincrasia general y, además, se conocería la diferencia que le otorga la población a estos dos datos.

6.3. Aplicabilidad del estudio

Esta investigación tiene valor tanto para entidades públicas como privadas. La información que ponemos de manifiesto tras analizar distintos datos y realizar

entrevistas interesa tanto a entes estatales como privados, ya que no es sólo una amenaza para los Gobiernos, si no que también constituye una forma de atacar a las entidades privadas.

Cambiar la idiosincrasia, la agenda setting o la opinión pública a la ciudadanía a través de estas acciones es una amenaza real para los Gobiernos. Sin embargo, para las empresas algunas campañas de concienciación también pueden afectar la productividad, la imagen o el prestigio de algunas entidades con ánimo de lucro, como es el caso de Bankia, después de las noticias que se han publicado sobre su gestión y las acciones que se han llevado a cabo para poner de manifiesto este aspecto desde pequeños grupos y que se han llevado a cabo a través de la Red.

7. BIBLIOGRAFÍA

MINISTERIO DE DEFENSA. *CUADERNOS DE ESTRATEGIA. Ciberseguridad, retos y amenazas a la seguridad nacional en el ciberespacio* [en línea]. Instituto nacional de estudios estratégicos e Instituto Universitario General Gutiérrez Mellado. Cuadernos de estrategia 149. Diciembre 2010. [Consulta: 15 de junio de 2.012]. Disponible en Web: http://www.portalcultura.mde.es/Galerias/publicaciones/fichero/CE_149.pdf. ISBN: 978-84-9781-622-9.

CABRERA M. Y CUPAIUOLI L. *La influencia de Internet en la sociedad actual* [en línea]. SOLO CIENCIA.COM (El portal de ciencia y tecnología en español). [Consulta: 15 de junio de 2.012]. Disponible en Web: http://www.solociencia.com/informatica/influencia-internet-sociedad-actual-origen-evolucion-historica.htm

PROFESORADO DE TECNOLOGÍA ELECTRÓNICA. *Internet: influencia y problemática en la educación.* (en línea). Universidad Nacional de San Luis. Facultad de ciencias físico matemáticas y naturales. 2.009. [Consulta: 5 de julio de 2.012]. Disponible en Web: http://www.slideshare.net/ea_perez/internet-influencia-y-problemtica

FERNANDO GUTIÉRREZ, C. *Comprendiendo la economía digital* (en línea). Razón y palabra (Primera revista electrónica en América Latina especializada en comunicación). Número 20. Estado de México. Noviembre 2.000 – Enero 2.001. [Consulta: 5 de julio de 2.012]. Disponible en Web: http://www.razonypalabra.org.mx/anteriores/n20/20_fgutierr.html.

HUAYAMAVE BETANCOURT, X. *La economía digital* (en línea). MONOGRAFÍAS.COM. [Consulta: 5 de julio de 2.012]. Disponible en Web: http://www.monografias.com/trabajos14/econodigital/econodigital.shtml.

BENÍTEZ, J.L y LUND, D. *Internet visto por los ojos de los ciudadanos del mundo* (en línea). Reporte de Opinión y Política. Serie 10. Número 12 Estudio Internet BBC. Mund Group. México 06760 D.F. Investigación en Demografía Global. 10 de marzo, 2010. [Consulta: 5 de julio de 2.012]. Disponible en Web:

http://www.mundgroup.com/Serie_10_Numero_12_Internet_en_perspectiva_mexicana_y_global.pdf.

ORIOL PRATS, J. Y DEL ÁLAMO, O. *Democracia electrónica: concepto, tipos y posicionamientos* (en línea). Número 4. Volumen 1. Futuros (revista trimestre latinoamericana y caribeña de desarrollo sostenible). 2.003. [Consulta: 5 de julio de 2.012]. Disponible en Web: http://www.revistafuturos.info/futuros_4/democr_elect_1.htm. ISSN 1913-6196.

ORDUZ, Rafael. *Internet y política* (en línea). El espectador.com. 11 de junio de 2.008. [Consulta: 5 de julio de 2.012]. Disponible en Web: http://www.elespectador.com/opinion/columnistasdelimpreso/rafael-orduz/columna-internet-y-politica

DEL PASO, Ana. *España se arma contra el ciberterrorismo* (en línea). www.belt.com. [Consulta: 5 de julio de 2.012].Disponible en Web: http://www.belt.es/expertos/HOME2_experto.asp?id=1872.

ANÓNIMO. *El 'ciberterrorismo': una amenaza del futuro muy presente* (en línea). Globedia. 24 de febrero de 2.010. [Consulta: 5 de julio de 2.012]. Disponible en Web: http://es.globedia.com/ciberterrorismo-amenaza-futuro-presente.

SÁNCHEZ-AGUILA COLLANTES, J.J. *Ciberterrorismo. La amenaza fantasma.* (en línea). Colegio Oficial de Ingenieros de Telecomunicaciones. Noviembre-diciembre 2.002. [Consulta: 5 de julio de 2.012]. BIT 136. Disponible en Web: http://www.coit.es/publicac/publbit/bit136/rincon.pdf.

GONZÁLEZ PRIETO, G. *Ciberterrorismo: el lado oscuro de la red.* (en línea). RTVE. Informe semanal. Junio de 2.010. [Consulta: 5 de julio de 2.012]. Reportaje. Disponible en Web: http://www.rtve.es/noticias/20100611/ciberterrorismo-lado-oscuro-red/335212.shtml.

ANÓNIMO. *Estudio de caso: la amenaza potencial del ciberterrorismo* (en línea). Projects by Students for Students. ORACLE. Think quest (education foundation). [Consulta: 5 de julio de 2.012]. Disponible en Web: http://library.thinkquest.org/05aug/00533/lowres_content_spanish/lowspan_content_typ

es4.htm.

Estados Unidos con la administración Barack Obama contra el ciberterrorismo (en línea). Vía Digital: tecnología, Internet y ciencia. 10 de septiembre de 2.009. [Consulta: 5 de julio de 2.012]. Disponible en Web: http://www.vidadigitalradio.com/barack-obama-ciberterrorismo/.

ANÓNIMO. *Ciberterrorismo* (en línea). Wikipedia. [Consulta: 15 de junio de 2.012]. Disponible en Web: http://es.wikipedia.org/wiki/Ciberterrorismo.

SALELLAS, L. *Delitos informáticos. Ciberterrorismo* (en línea). SR Hadden Security Consulting. [Consulta: 5 de julio de 2.012]. Disponible en Web: http://www.cabinas.net/informatica/ciberterrorismo_informatico.asp.

JEFATURA DEL SERVICIO DE INFORMACIÓN. *Ciberterrorismo* (en línea). Unidad central especial nº 3. Revista Seguridad del Estado. Dirección General de la Guardia Civil. Enero-febrero 2.006. [Consulta: 27 de junio de 2.012]. Disponible en Web: http://www.revista-ays.com/DocsNum01/SeguridadEstado/GuardiaCivil.pdf.

MASANA, S. El ciberterrorismo: ¿una amenaza real para la paz mundial?. Escudé, C. Facultad Latinoamericana de Ciencias Sociales. 8 de julio de 2.002. [Consulta: 21 de junio de 2.012]. Tesis de maestría (relaciones internacionales). Disponible en Web: http://www.argentina-rree.com/documentos/ciberterrorismo.pdf.

JARAMILLO MARÍN, M. *"No somos ciberterroristas": Anonymous* (en línea). www.enter.co. 19 de abril de 2.011. [Consulta: 1 de julio de 2.012]. Disponible en Web: http://www.enter.co/internet/no-somos-ciberterroristas-anonymous/.

Anonymous: ¿Comienza la caber guerra? (en línea). www.anmtvla.com. 25 de abril de 2.011. [Consulta: 2 de julio de 2.012]. Disponible en Web: http://www.animefansclub.org/fans/index.php?option=com_content&view=article&id=260:reportaje-anonymous-icomienza-la-ciber-guerra&catid=1:latest-news&Itemid=50.

CUÉLLAR MANUEL. *El ideario político de los 'ciberactivistas' Anónimos (en línea).* Edición digital. Elpaís.com internacional. 9 de diciembre de 2.010. [Consulta: 1 de julio de 2.012]. Disponible en Web:

http://www.elpais.com/articulo/internacional/ideario/politico/ciberactivistas/Anonimos/elpepuint/20101209elpepuint_16/Tes.

RAYA, JAVIER. *Randy Pitchford llama a jugadores a solidarizarse con Sony* (en línea). www.levelup.com/noticias. 13 de mayo de 2.012. [Consulta: 16 de junio de 2.012]. Disponible en Web: http://www.levelup.com/noticias/13185/Randy-Pitchford-llama-a-jugadores-a-solidarizarse-con-Sony/.

LAURENCE, JEREMY. *Corea del Norte, tras un ciberataque a banco surcoreano: fiscal* (en línea). Pinedo, Emma. Thomson Reuters. 3 de mayo de 2.011. [Consulta: 4 de julio de 2.012]. Disponible en Web: http://lta.reuters.com/article/internetNews/idLTASIE74217L20110503.

DE LEÓN, ÁNGEL. *Robo y fraude a través de la red* (en línea). Digital. Diario de Sevilla. 9 de mayo de 2.011. [Consulta: 17 de junio de 2.012]. Edición digital. Disponible en Web: http://www.diariodesevilla.es/article/opinion/970511/robo/y/fraude/traves/la/red.html.

DÍAZ, CARLOS ALBERTO. *Hackean el sitio en el que Anonymous coordina sus ataques* (en línea). www.enter.co. 10 de mayo de 2.011. [Consulta: 6 de julio de 2.012.]. Disponible en Web: http://www.enter.co/internet/hackean-el-sitio-en-el-que-anonymous-coordina-sus-ataques/.

PINEDA, JULIOS CÉSAR. *Terrorismo y la ONU* (en línea). Digital: Opinión. Caracas. El Universal. 12 de mayo de 2.011. [Consulta: 2 de julio de 2.012.]. Disponible en Web: http://www.eluniversal.com/2011/05/12/terrorismo-y-la-onu.shtml

LOPEZ RODRÍGUEZ, B. y otros. *Las violencias del siglo XXI. Nuevas dimensiones de la guerra* (en línea). Centro Superior de Estudios de la Defensa Nacional. Ministerio de Defensa. Gobierno de España. Octubre de 2.009. [Consulta: 30 de junio de 2.012]. Monografías del Ceseden 112. Disponible en Web: http://www.portalcultura.mde.es/Galerias/publicaciones/fichero/Monografia112.pdf.
ISBN: 978-84-9781-501-7.

MINISTERIO DE DEFENSA. *CUADERNOS DE ESTRATEGIA. Los actores no estatales y la seguridad internacional, su papel en la resolución de conflictos y crisis.*

[en línea]. Instituto nacional de estudios estratégicos e Centro Nacional de Inteligencia. Cuadernos de estrategia 147. Agosto 2010. [Consulta: 15 de junio de 2.012]. Disponible en Web: http://www.portalcultura.mde.es/Galerias/publicaciones/fichero/CE_147.pdf. ISBN: 978-84-9781-606-9

AFP. *El ciberterrorismo, nueva arma de Estado económica, discreta y eficaz* (EN LÍNEA). error98.blogspot.com.es. 13 de septiembre de 2.007. [Consulta: 30 de junio de 2.012].Disponible en Web: http://error98.blogspot.com/2007/09/el-ciberterrorismo-nueva-arma-de-estado.html.

POZZI, SANDRO. *Los 'hackers' se pasean por el Nasdaq* (en línea). Elpaís.com economía. 5 de febrero de 2.011. [Consulta: 27 de junio de 2.012]. Disponible en Web: http://www.elpais.com/articulo/economia/hackers/pasean/Nasdaq/elpepueco/20110205elpepueco_1/Tes

EL PAÍS. *El jefe del CNI reconoce que algunas nuevas amenazas les pillan "casi sin experiencia y sin capacidad de reacción"* (en línea). Elpaís.com actualidad. Madrid. 22 de noviembre de 2.011. [Consulta: 17 de junio de 2.012]. Disponible en Web: http://www.elpais.com/articulo/espana/jefe/CNI/reconoce/algunas/nuevas/amenazas/les/pillan/experiencia/capacidad/reaccion/elpepuesp/20101122elpepunac_19/Tes.

REVENTÓS, LAIA. *Un 'troyano' muy sofisticado* (en línea). Elpaís.com archivo internacional. Barcelona. 28 de septiembre de 2.010. [Consulta: 12 de julio de 2.012]. Disponible en Web: http://www.elpais.com/articulo/internacional/troyano/sofisticado/elpepiint/20100928elpepiint_7/Tes.

ESPINOSA. ÁNGELES. *Un potente ataque informático afecta a 30.000 ordenadores en Irán* (en línea). Elpaís.com internacional. 27 de septiembre de 2.010. [Consulta: 12 de julio de 2.012]. Disponible en Web: http://www.elpais.com/articulo/internacional/potente/ataque/informatico/afecta/30000/ordenadores/Iran/elpepuint/20100927elpepuint_4/Tes.

CEBERIO BELAZA, MÓNICA. *Una ley protege 3.500 instalaciones contra catástrofes o ciberterrorismo* (en línea). Elpaís.com archivo España. 17 de marzo de 2.011.

[Consulta: 12 de julio de 2.012]. Disponible en Web: http://www.elpais.com/articulo/espana/ley/protege/3500/instalaciones/catastrofes/ciberterrorismo/elpepiesp/20110317elpepinac_13/Tes

REUTERS. *Marruecos desmantela una célula que planeaba ataques en el extranjero* (en línea). Elmundo.es. Digital. 27 de diciembre de 2.010. [Consulta: 12 de julio de 2.012]. Disponible en Web: http://www.elmundo.es/elmundo/2010/12/27/internacional/1293454783.html.

AGENCIAS. *Corea del Sur culpa al vecino del norte de un importante 'ciberataque' a un banco* (en línea). Elmundo.es. Digital. 4 de mayo de 2.011. [Consulta: 12 de julio de 2.012]. Disponible en Web: http://www.elmundo.es/elmundo/2011/05/04/navegante/1304493700.html.

EFE. *Un 'ciberataque' obliga a desconectar 1.500 ordenadores del Pentágono* (en línea). Elmundo.es. Digital. 22 de junio de 2.007. [Consulta: 12 de julio de 2.012]. Disponible en Web: http://www.elmundo.es/navegante/2007/06/22/tecnologia/1182500094.html.

EFE. *Juntos contra el 'ciberterrorismo'* (en línea). Elmundo.es. Digital. 16 de junio de 2.006. [Consulta: 12 de julio de 2.012]. Disponible en Web: http://www.elmundo.es/navegante/2006/06/16/seguridad/1150459726.html.

CERNUDA, OLLALLA. *EEUU, listo para la 'ciberguerra'* (en línea). Elmundo.es (navegante.com). Digital. 1 de marzo de 2.003. [Consulta: 12 de julio de 2.012]. Disponible en Web: http://www.elmundo.es/navegante/2003/03/17/esociedad/1047923716.html.

EUROPA PRESS. *Bruselas propone penas de cárcel para combatir el cibercrimen* (en línea). Elmundo.es (navegante.com). Digital. 25 de abril de 2.002. [Consulta: 12 de julio de 2.012]. Disponible en Web: http://www.elmundo.es/navegante/2002/04/25/esociedad/1019731964.html.

EUROPA PRESS. *Treinta países firman la primera Convención Internacional contra el 'Cibercrimen'* (en línea). Elmundo.es (navegante.com). Digital. 26 de noviembre de 2.001. [Consulta: 12 de julio de 2.012]. Disponible en Web:

http://www.elmundo.es/navegante/2001/11/26/esociedad/1006766268.html.

Dos detenidos bajo cargos de ciberterrorismo en Indonesia (en línea). Lavanguardia.com tecnología. Digital. 23 de agosto de 2.006. [Consulta: 12 de julio de 2.012]. 24 de agoto de 2.006. Disponible en Web: http://www.lavanguardia.com/tecnologia/20060823/51280597278/dos-detenidos-bajo-cargos-de-ciberterrorismo-en-indonesia.html.

Agosto registra el mayor número de ataques informáticos hasta la fecha (en línea). Lavanguardia.com tecnología. Digital. 4de septiembre de 2.002. [Consulta: 12 de julio de 2.012]. 30 de mayo de 2.006. Disponible en Web: http://www.lavanguardia.com/tecnologia/20020904/51262760464/agosto-registra-el-mayor-numero-de-ataques-informaticos-hasta-la-fecha.html.

NAVARRO, SANTIAGO. *En defensa de una red soberana* (en línea). Elpaís.com archivo. 1 de mayo de 2.011. [Consulta: 12 de julio de 2.012]. Disponible en Web: http://www.elpais.com/articulo/Pantallas/defensa/red/soberana/elpepurtv/20110501elpepirtv_1/Tes.

ANÓNIMO. *Ciberactivismo* (en línea). Wikipedia. [Consulta: 15 de junio de 2.012]. Disponible en Web: http://es.wikipedia.org/wiki/Ciberactivismo.

GREENPEACE. *Ser ciberactivista* (en línea). Greenpeace España. www.greenpeace.com. [Consulta: 10 de julio de 2.012]. Disponible en Web: http://www.greenpeace.org/espana/es/Que-puedes-hacer-tu/Ser-ciberactivista/.

GREENPEACE. *¿Qué es un ciberactivista?* (en línea). Greenpeace España. www.greenpeace.com. [Consulta: 10 de julio de 2.012]. Disponible en Web: http://www.ciberactuacongreenpeace.es/?cmd=CNTN&content=CyberWhat.

GREENPEACE. *Exige al Banco Santander que no financie una central nuclear en una zona de riesgo sísmico* (en línea). Greenpeace España. www.greenpeace.com. [Consulta: 10 de julio de 2.012]. Disponible en Web: http://ciberactuacongreenpeace.es/?cyberid=126.

TOSCO, P. *Dale La Vuelta Al Mundo, la web joven de Intermón Oxfam, termina su*

andadura después de cuatro años de grandes experiencias (en línea). INTERMON OXFAM. [Consulta: 10 de julio de 2.012]. Disponible en Web: http://dalelavueltaalmundo.intermonoxfam.org/.

Avaaz: Información básica (en línea). Avaaz.org el mundo en acción. [Consulta: 8 de julio de 2.012]. Disponible en Web: http://www.avaaz.org/es/pressfaq.php.

DACACH, CAMILO JOSÉ. *Cyberterrorismo, la historia de nunca acabar* (en línea). Quito, Ecuador. Centro Internacional de Estudios Superiores de Comunicación para América Latina. Marzo 2.004. [Consulta: 8 de julio de 2.012]. Revista latinoamericana de comunicación Chasqui número 85. Disponible en Web: http://redalyc.uaemex.mx/redalyc/pdf/160/16008509.pdf. ISSN 1390-1079.

JANCZEWSKI, LECH y COLARIK, ANDREW M. *Managerial Guide For Handling Cyber-Terrorism And Information Warfare* (en línea). Estados Unidos. Idea Group Publishing. 2.005. [Consulta: 8 de julio de 2.012]. Disponible en Web: http://books.google.es/books?hl=es&lr=&id=V9UnYi6qggMC&oi=fnd&pg=PR1&dq=cyber+terrorism+solutions&ots=LizQQE9d6l&sig=FRuHhboln8sg0FoEaHlxRAwdMO4#v=onepage&q=cyber%20terrorism%20solutions&f=false. ISBN 1-59140-583-1.

COLARIK, ANDREW M. *Cyber Terrorism: Political And Economic Implications* (en línea). Estados Unidos. Idea Group Publishing. 2.006. [Consulta: 8 de julio de 2.012]. Disponible en Web: http://books.google.es/books?hl=es&lr=&id=V9UnYi6qggMC&oi=fnd&pg=PR1&dq=cyber+terrorism+solutions&ots=LizQQE9d6l&sig=FRuHhboln8sg0FoEaHlxRAwdMO4#v=onepage&q=cyber%20terrorism%20solutions&f=false. ISBN 1-59904-021-2.

TRUJANO RUIZ, Patricia, DORANTES SEGURA, Jessica y TOVILLA QUESADA, Vania. Violencia en Internet: nuevas víctimas, nuevos retos. *Liber.* [online]. Enero – junio de 2009, vol.15, no.1 [citado 16 Mayo 2011], p.7-19. Disponible en Web: <http://www.scielo.org.pe/scielo.php?script=sci_arttext&pid=S1729-48272009000100002&lng=es&nrm=iso>. ISSN 1729-4827.

Décimo Congreso de las Naciones Unidas sobre Prevención del Delito y Tratamiento del Delincuente Viena, 10 a 17 de abril de 2000.