ieee.es
Instituto Español de Estudios Estratégicos

Documento
Opinión

74/2011 18 octubre de 2011

*Luis de Salvador*

INGENIERÍA SOCIAL Y OPERACIONES PSICOLÓGICAS EN INTERNET

# INGENIERÍA SOCIAL Y OPERACIONES PSICOLÓGICAS EN INTERNET

## Resumen:

Las técnicas de ingeniería social son aquellas que se emplean para influenciar el pensamiento y acción de un individuo o un grupo. Su uso tiene una larga tradición y se emplean ahora en Internet, que es un nuevo canal de comunicación, denominándose hacking no técnico. La novedad de su uso en Internet reside en que, gracias a la naturaleza de la red de datos, pueden ser utilizadas con éxito por un pequeño grupo de individuos con muy pocos recursos y contra un colectivo muy amplio de forma simultánea. En este caso, la ingeniería social se ha empleado habitualmente con objetivos fraudulentos, como el phising, pero podría ser usada aún con más efectividad como una nueva arma en el soporte a operaciones psicológicas en los conflictos asimétricos. Surge entonces la cuestión de hasta qué punto estamos preparados para comprender, detectar, detener y contrarrestar los efectos de estas operaciones.

*Abstract:*

*The social engineering techniques, that allow influencing over a person or group, have a large tradition. These techniques are applied in Internet, a new communication channel with new rules, and they are called no-tech hacking. The main difference when these techniques are used in Internet is that they can be developed by small teams, need few resources and affect many people. Social engineering has been used for fraud purposes with great success, like phising. But, it is currently used with effectiveness like a weapon in asymmetric warfare psychological operations. Then, we have to take into account if we are ready to understand, detect, defeat and strike back this kind of attacks.*

## Palabras clave:

Ingeniería social, operaciones psicológicas, conflicto asimétrico, Internet, ciberguerra.

*Keywords:*

*Social engineering, psychological operations, asymmetric warfare, Internet, cyber war.*

## INTRODUCCIÓN

En España, los ciudadanos que utilizan de forma habitual Internet suponen el 58,4% de la población, aproximadamente 20 millones de personas[1]. A nivel europeo, un 33% de las personas declaran que no podrían vivir sin Internet y, en general, las personas dedican a la red unas 1,7 horas diarias[2]. Más aún, el 55% de los usuarios toman decisiones de compra en función de la información que encuentran en Internet. Estas cifras muestran cómo nuestra dependencia de la red crece día a día.

En febrero de 2011, unos estudiantes decidieron analizar cuán vulnerables podrían ser sectores de la población a la manipulación a través de Internet y qué complejidad o dificultades se podrían encontrar. Dentro de un proyecto universitario resolvieron llevar a cabo un experimento para comprobar hasta qué punto se podía crear un estado de opinión en un determinado colectivo utilizando técnicas de ingeniería social.

Planificaron una operación muy limitada con los siguientes pasos: en primer lugar elegir una audiencia objetivo y un tema de interés dentro de la misma. Naturalmente, era necesario marcar una serie de límites, como que el tema elegido no fuera excesivamente polémico y que la distorsión no cayese dentro de la ilegalidad. Se seleccionó como audiencia el sector de compradores de un determinado producto electrónico de gran consumo y el tema elegido era dar testimonio de cómo los clónicos de dicho producto, que se podrían comprar por Internet, estaban configurados con un supuesto troyano de fábrica que remitía toda la actividad del usuario (comunicaciones, información personal, etc.) a un servidor situado en Asia.

A continuación, fue necesario estudiar ese colectivo de usuarios para conocer sus sesgos a la hora de tomar decisiones y analizar en qué entorno se nutrían de información sobre temas relacionados con su producto de interés. Es decir, del conjunto total de recursos de Internet cuáles eran sus canales de información y comunicación: qué foros, páginas, redes, blogs, medios de comunicación en versión electrónica[3], etc. Conjuntamente, se estudió cuán vulnerables eran todos esos medios[4], la forma más adecuada para dar verosimilitud a una información para dicha audiencia y la de influir en los blogs de especialistas en el tema para

[1] Instituto Nacional de Estadística *Encuesta sobre equipamiento y uso de tecnologías de la información y comunicación en los hogares*, 2010.
[2] EIAA *European Media Landscape Report*, diciembre 2010.
[3] Muchos medios incluyen foros en los que los ciudadanos, como cartas al director, pueden expresar su opinión.
[4] Se comprobó que, excepto los casos en los que los mensajes llamasen mucho la atención, el filtrado de contenidos que se realiza en periódicos digitales y foros de gran difusión es muy pobre, sino nulo.

extenderla. Es importante destacar que estamos hablando de vulnerabilidades ante un ataque social, no de vulnerabilidades desde un punto de vista técnico (agujeros de seguridad). Lo que se pretendía era conocer las facilidades que proporcionaban los distintos canales en Internet para propagar una noticia, qué mecanismos se empleaban para contrastar la información, o si se realizaba un análisis crítico de la misma antes de publicarla.

Para lanzar la información era necesaria una semilla, un origen, una o varias personas que inicien la difusión de la misma, y para ello nada mejor que utilizar las posibilidades que da Internet para levantar personalidades ficticias, los "ganchos". Las personalidades virtuales tenían que ganar verosimilitud y, para ello, se le dotó de una imagen, una historia, unas relaciones y, sobre todo, de un pasado: blog personal, perfiles en redes sociales, historial de actividad, rastro de su existencia en diversos sitios, comentarios en fechas pasadas, etc.

A su vez, para dar más cuerpo a la historia, había que dar una evidencia que cualquiera pudiera comprobar, lo que en este caso suponía demostrar que realmente dicho troyano estaba actuando. En un país con un idioma poco corriente se levantó un servidor de bases de datos que era el teórico destino de la información robada por el troyano. Deliberadamente, se introdujo una vulnerabilidad técnica que permitía acceder al contenido de la base de datos saltándose los controles de acceso de la misma, vulnerabilidad que sería divulgada por los colaboradores virtuales. Y dicha base de datos se rellenó de información ficticia generada de forma automática, pero que daba la sensación que procedía de los dispositivos infectados[5].

Tras toda esa preparación, sólo quedaba lanzar los personajes al aire y darles un poco de vida: el protagonista virtual principal, tras varias vicisitudes prolíficamente detalladas durante varios "meses", adquiría dicho producto, descubría el troyano, a su vez daba con el servidor y, actuando como hacker, se introducía en el mismo, desvelando un secreto que daba a conocer al mundo. Por supuesto, el resto de personalidades virtuales, menos elaboradas, actuaban como meros "ganchos" para extender la noticia.

El resultado fueron más de 10.000 visitas directas al blog del personaje virtual para consultar su descubrimiento, miles al servidor ficticio, y muchas más visitas indirectas por la propagación de la noticia en los principales foros de seguridad. Diversos colectivos divulgaron la información a través de la red y se generó una reacción de empatía de cientos

[5] Un análisis riguroso de la misma hubiera evidenciado que estaba formada por patrones que se repetían de forma continua.

de personas[6] hasta tal punto que algunas de ellas detallaban cómo les estaba afectando dicho troyano imaginario e incluso proporcionaban nuevas evidencias del suceso. La respuesta tuvo un ámbito global y llegó hasta la materialización de denuncias ante las Fuerzas de Seguridad por un supuesto robo de información.

Todo ese impacto se consiguió en tan sólo tres días de existencia en Internet, de existencia virtual, y con el trabajo de tres personas. Aunque el experimento estaba planificado para ser realizado durante tres meses, la repercusión fue tan grande que decidieron detenerlo nada más nacer, pues la velocidad de propagación superó cualquier expectativa.

**INTERPRETACIÓN**

Lo llevado a cabo en el estudio mostrado en el apartado anterior es un ensayo de psicología social construido sobre los servicios de Internet empleando técnicas de ingeniería social. Existen muchos precedentes que han explorado la utilización de los nuevos canales de comunicación (radio, televisión, etc.) con los mismos propósitos. Podríamos remontarnos a 1938, a *La guerra de los mundos* de Orson Wells[7], para estudiar fenómenos parecidos[8] que se han repetido de forma recurrente[9] sobre todo con propósitos de marketing[10]. Este mismo año 2011, en la localidad mexicana de Veracruz, se generó un pánico debido a la propagación de mensajes falsos que informaban sobre avisos de bomba en varios colegios de la ciudad utilizando Twitter. El resultado fueron decenas de accidentes automovilísticos, cuando los padres acudieron a salvar a sus hijos de las escuelas de la ciudad, y el colapso de las líneas telefónicas de emergencia[11].

Hay algunas diferencias entre estas experiencias con el fenómeno Wells. La más evidente es que, en este último, el impacto social fue un efecto colateral no deseado[12], mientras que en el proyecto mostrado el efecto era deliberado. Pero donde reside la principal novedad no es

[6] El personaje virtual recibió invitaciones y ofertas de trabajo y, cuando se le hizo desaparecer, surgieron incluso teorías conspirativas.
[7] CRUZ Gilbert, *Orson Welles' War of the Worlds*, Time Enterteinment, disponible en http://www.time.com/time/arts/article/0,8599,1855120,00.html.
[8] WRIGHT Peter, *Alternative 3 (review),* Science Fiction Film and Television - Volume 2, Issue 2, Autumn 2009, pp. 318-322 ISSN: 1754-3770.
[9] *Universal Sued for The Fourth Kind Viral Marketing Misfire*, disponible en http://www.filmjunk.com/2009/11/16/universal-sued-for-the-fourth-kind-viral-marketing-misfire/
[10] Recientemente utilizando técnica de marketing viral. Los Angeles Times, *"Alien" bus-stop ads create a stir*, disponible en http://articles.latimes.com/2009/jun/19/entertainment/et-district19.
[11] *Los 'twitterroristas' de México se enfrentan a 30 años de cárcel*, disponible en http://www.elmundo.es/america/2011/09/05/mexico/1315239774.html.
[12] Por lo menos 6 millones de personas oyeron la emisión y 1 millón de ellas se asustaron o inquietaron, generalmente los pertenecientes a los sectores de ingresos y educación más bajos, que habían llegado a confiar más en las noticias difundidas por la radio antes que en los periódicos.

en los resultados, sino en los recursos empleados. Si para el programa de Wells se necesitó utilizar un programa de radio, de éxito ya consolidado (con el desgaste de credibilidad que eso le impuso), dentro de una cadena de cobertura nacional; para el ensayo descrito aquí se necesitó muy poco personal implicado en un equipo ad-hoc durante poco tiempo y utilizando medios muy sencillos. El coste fue nulo, el impacto global, el anonimato garantizado por los recursos de la red y las herramientas técnicas empleadas al alcance de cualquiera.


The New York Times.

NEW YORK, MONDAY, OCTOBER 31, 1938.

MEAD STANDS PAT AS A NEW DEALER IN BID FOR SENATE

Democratic Candidate Opposes Any Except Minor Changes in Labor and Security Laws

Radio Listeners in Panic, Taking War Drama as Fact

Many Flee Homes to Escape 'Gas Raid From Mars'—Phone Calls Swamp Police at Broadcast of Wells Fantasy

OUSTED JEWS FIND REFUGE IN POLAND AFTER BORDER STAY

Exiles Go to Relatives' Homes or to Camps Maintained by Distribution Committee

Imagen 1: Impacto en los medios de las consecuencias del programa de Wells

Es más, realizar una acción más ambiciosa está al alcance de aquellos que tengan la suficiente motivación y que empleen un poco de imaginación, cualidades presentes en la fuente de nuestras amenazas[13]. A diferencia de la televisión, la radio o los periódicos, Internet es un recurso que está fuera de control estatal o de las corporaciones que poseen los medios de comunicación. Las armas que emplea, aunque se sustentan sobre la tecnología, se basan en los principios de la ingeniería social. Su objetivo final depende tan sólo de la voluntad de los atacantes, y puede ser científico, comercial, terrorista o formar parte de una operación psicológica a mayor escala.

## INGENIERÍA SOCIAL

La psicología social es la ciencia que intenta explicar la influencia que la presencia[14] real o implícita de otras personas tiene en las ideas, los sentimientos y la conducta de los individuos. Nació para estudiar fenómenos como el sucedido en 1938[15].

[13] ALONSO Rogelio, *La innovación terrorista: desafíos para la prevención y contención del terrorismo yihadista*, Documentos de opinión del IEEE Nº 08/2011.
[14] La presencia, no ha de ser física, se puede manifestar con acciones o palabras.
[15] Hadley Cantril escribió un estudio sociológico sobre dicho fenómeno y fue el que fijó los principios de la psicología social.

La misma diferencia que existe entre ciencia y técnica la encontramos entre la psicología y la ingeniería social. Las técnicas de ingeniería social son aquellas que permiten ejercer influencia y dirigir el pensamiento y la acción de un individuo o un grupo. Su uso es tan antiguo como el hombre[16], tiene una larga tradición en política, diplomacia e inteligencia[17], aunque su estudio sistemático corre paralelo al desarrollo de la psicología.

La ingeniería social es un ataque dirigido en dos fases[18]. En la primera, el ingeniero social (el origen del ataque) recaba información sobre la persona o entidad a atacar (el objetivo). El origen ha de tener el suficiente conocimiento del objetivo antes de realizar cualquier tipo de contacto para poder seleccionar la mejor táctica de ataque.

Una vez completada esta fase, el atacante comenzará la explotación del objetivo directamente, bien para alcanzar un conocimiento más profundo del mismo (en el caso de que el objetivo mismo es una escucha), bien para conseguir los elementos necesarios para infiltrarse en la red (humana o digital) de una organización u obtener el objeto que desea. Si el atacante no consigue sus propósitos de un primer objetivo, puede usar las piezas conseguidas para adquirir una mayor credibilidad frente a un segundo[19]. En definitiva, se pretende inducir una conducta sobre el objetivo y el grado de refinamiento del ataque dependerá de la complejidad de dicha conducta y de la vulnerabilidad del objetivo.

Los métodos de ataque son tan numerosos o específicos como objetivos y objetos, pero todas tienen en común el explotar los siguientes tres rasgos genéricos del ser humano: el miedo, la confianza y la ingenuidad[20]; ejecutadas dentro del marco creado por los sesgos cognitivos utilizados en la toma de decisiones[21]. Asociados a estos tres rasgos hay técnicas que los explotarán de forma combinada hasta conseguir suficiente información para realizar el ataque definitivo.

El miedo es la emoción que más fácilmente permite controlar a los seres humanos. Hay muchos tipos de miedo (al rechazo, a lo extraño…) pero el más apropiado para inducir una

[16] El timo del nigeriano, que tan actual nos parece cuando recibimos correo spam, en el siglo XVI ya se conocía como el timo del prisionero español.
[17] Por ejemplo, en las actividades de HUMINT.
[18] Estas dos fases podrían solaparse, pero su naturaleza es diferente por lo que tienen que considerarse distintas.
[19] US-CERT *Cyber security tip ST04-014.*
[20] COLE Ray, et al. *Social engineering: the human element in information warfare* CS4235A Information Warfare Group.
[21] CORTADA DE KOHAN Nuria, *Los sesgos cognitivos en la toma de decisiones*, International Journal of Psychological research 2008, ISSN: 2011-7922.

conducta es el miedo a perder[22] o codicia, que se puede concretar en el chantaje (más o menos explícito, más o menos emocional) y en el soborno.

La confianza puede ser de dos tipos: apropiada o ganada. En la primera se suplanta la identidad de alguien o algo con quien el objetivo tiene confianza de forma previa. Las técnicas utilizadas pueden ser muy diversas, yendo desde presentarse en persona asumiendo la personalidad de, por ejemplo, un médico, a enviar un correo electrónico que parece proceder de nuestra entidad bancaria. En la segunda, no se oculta la identidad sino que se trabaja una relación de confianza de la que se derivará un abuso de la misma o se aprovechará de una relajación de las medidas de seguridad. Puede tomar la forma de un amigo en el bar o una amistad a través de Internet.

Esta última es una técnica que puede ser más costosa en tiempo, y muy peligrosa para atacante y objetivo si sale a la luz. Métodos para acelerar el proceso de confianza mutua son utilizar la reciprocidad, el proporcionar al objetivo algo que desea pero que no tiene, o bien utilizar el principio de "no pasa nada" cuando se adopta por parte del origen el rol de ser parte indiferente en el entorno en que dicha información es relevante[23].

Explotar la ingenuidad, en sus distintas formas de negligencia, compasión o curiosidad es la forma menos arriesgada de ingeniería social. Sus técnicas incluyen, la búsqueda en fuentes[24] abiertas[25], en el material desechado o en la basura[26], el robo de material y su inversa la cesión de material[27] o cualquier forma de interceptación de comunicaciones. Esta última puede tomar formas más sutiles, como la de explorar el historial de reenvíos en correos

[22] Es uno de los tres errores en toma de decisiones que se formulan en la teoría de las perspectivas desarrollada por Amos Tversky y Daniel Kahneman, la aversión a perder, que señala que el dolor por una pérdida es mayor que la alegría por una ganancia. Se implementa en estrategias de marketing en las que se presenta el producto no como una oportunidad de ganar, sino como una oportunidad de no perder. De ahí la frase "Oferta válida hasta…". Los otros dos errores que formula la teoría son las preferencias de riesgo asimétricas y la estimación errónea de probabilidades.

[23] Por ejemplo, ¿qué puede pasar cuando le hablo al chofer, al camarero o al portero de mis problemas en un proyecto?

[24] OSINT en terminología militar o googlear en terminología de un hacker.

[25] En el documento del DoD "Website OPSEC discrepancies" se hacía referencia a un manual de Al Queda capturado en Afganistán en el que directamente se declaraba que el uso del fuentes públicas de información, sin necesidad de recurrir a métodos ilegales, puede proporcionar el 80% de la información necesaria sobre el enemigo.

[26] Se denomina dumpster diving, y si antes se limitaba a la búsqueda de papeles ahora su principal fuente son discos duros, CD's o memorias que no han recibido un procedimiento de borrado seguro de la información.

[27] En 2007, se dejaron en un aparcamiento de Londres varias unidades USB infectadas con un troyano bancario. El virus Stuxnet se propaga de una forma similar. The Economist *The Stuxnet worm. A cyber-missile aimed at Iran?* disponible en http://www.economist.com/blogs/babbage/2010/09/stuxnet_worm.

electrónicos[28].

Los sesgos cognitivos, en los que se enmarcan estos rasgos, son aquellos errores de razonamiento causados por la utilización de una estrategia de procesamiento de la información simplificada. Estas estrategias son necesarias para tomar decisiones rápidas en la vida diaria, pero muestran "agujeros" que pueden ser explotados. Existen muchos tipos de sesgos cognitivos: en la toma de decisiones, de memoria, de comportamiento, sociales, etc. Sesgos que han funcionado en el experimento anteriormente descrito han sido: el de anclaje[29] en la imagen del servidor, el de arrastre ante las opiniones de los demás (los "ganchos"), el de encuadre al presentar la información en el canal en el que se espera, el de confirmación al apoyarse en una hipótesis preconcebida, el del experimentador al permitir comprobar algo que ya creían que es cierto y la heurística de disponibilidad[30] cuando se descubre el contenido del servidor "rompiendo" su seguridad sin llegar a analizar su contenido, etc.

Antes de que los atacantes tuvieran acceso a las nuevas tecnologías, para aplicar las técnicas de ingeniería social era necesario acceder a cada víctima potencial de forma individual por contacto directo, por correo, fax o telefonía tradicional. Estos métodos requerían una inversión importante en tiempo y dinero, y limitaban su impacto. En el nuevo escenario de Internet esto cambia, se puede realizar un ataque global, como en el caso del phising, por lo que ya no se habla de objetivo si no de audiencia objetivo.

## OPERACIONES PSICOLÓGICAS

Las operaciones psicológicas o PSYOPS suponen un instrumento importante en la estrategia de seguridad y parte del arsenal no-letal de cualquier Estado, permitiendo rellenar el espacio que existe entre la diplomacia o las relaciones públicas y el uso de la fuerza. Las PSYOPS son uno de los elementos que forman parte de las operaciones de información (IO), junto con la guerra electrónica (EW), las operaciones a través de la red de ordenadores (CNO), el engaño (MILDEC) y las operaciones de seguridad (OPSEC)[31], y pueden tener carácter ofensivo o

[28] Es muy habitual encontrar en un correo electrónico reenviado el historial de la conversación, con datos ajenos a la última respuesta y un historial de direcciones de correos electrónicos de reenvío, lo que da información sobre la relación entre las personas.
[29] Fijarse en un rasgo destacado para dar autenticidad de una fuente, como un logo, una imagen de marca, etc.
[30] Es una evaluación errónea al centrarse en el suceso más destacado, más familiar o emocionalmente cargado.
[31] *Information Operations*, Joint Staff JP3-13 2006. La versión de 1998 de dicho documento incluía el ataque físico y su relación con las relaciones públicas.

defensivo.

En la Segunda Guerra Mundial, las operaciones psicológicas se definían como un medio para "aproximarse a la mente del individuo a través del engaño y con ficciones bien elaboradas calculadas para que bajen la guardia y se alimente su egoísmo, deslealtad y motivos personales de los individuos", "inventan hechos, dispersan rumores y tratan de racionalizar los recelos, las dudas y los restos de individualismo de los soldados… pueden incluso movilizar los motivos más patrióticos contra ellos mismos…"[32].

En las modernas operaciones de paz, el objetivo de las operaciones psicológicas es ganar los "corazones y mentes" de la población en general (no sólo del elemento militar, pues nos encontramos en conflictos asimétricos) de forma que se proporcione al mando apoyo eficaz con el fin de comunicarse directamente con el elemento humano en el campo de batalla. Para ello, las operaciones psicológicas han de proyectar una imagen favorable de un ejército, amplificar los efectos de una demostración de fuerza, evaluar las actitudes e impresiones, apoyar a las operaciones de engaño, desmoralizar e interrumpir al enemigo y realizar evaluaciones de la zona. Por lo tanto, son críticas para el éxito sobre el terreno.[33]

Tradicionalmente, estas operaciones necesitaban conseguir acceso a medios de comunicación corporativos o estatales (estaciones de TV, radio) o la puesta en marcha de campañas de divulgación (emisoras, altavoces, carteles, anuncios, panfletos, buzoneo). Esto supone poner ingentes recursos en marcha[34] y/o que las campañas se realicen con un marco temporal amplio. En muchos casos, precisa de la entrada o la connivencia de personas en "territorio enemigo" y, además la operación se realiza en la superficie, es decir, notoriamente visible a todo el mundo.

[32] Memorándum firmado por el Brigadier-General Robert A. McClure, Jefe del PWD/SHAEF, en relación a la política y métodos de propaganda negra contra Alemania, 1944.
[33] SANTANA HERNÁNDEZ Manuel, *Curso básico de operaciones psicológicas* Campus Internacional de Seguridad y Defensa, y conferencia sobre "*Operaciones Psicológicas en Países Islámicos: el ejemplo de Afganistán y El Líbano*" de las Jornadas sobre Seguridad, Defensa y Geo-Estrategia.
[34] Poner una gran campaña en marcha supone contar con un gran equipo, muchas veces disperso, con distintos grados de compromiso y por lo tanto más difícil de controlar.


Imagen 2: Unidad PSYOPS de la KFOR en Kosovo[35]

El uso de Internet y, en general las tecnologías de la información y las comunicaciones (TIC), simplifica mucho la utilización de las operaciones psicológicas y las convierte en armas mucho más potentes.

Las operaciones psicológicas "llegarán a ser el arma dominante en la forma de intervención en los medios de comunicación y a través de las TIC…los adversarios de la cuarta generación de guerra manipularán los medios para alterar la opinión pública mundial y local para doblegar la voluntad de lucha. El objetivo principal será el soporte popular al gobierno y a la dirección de la guerra"[36]. Los nuevos teóricos chinos, en su doctrina establecen que "En las acciones militares, la principal misión es atacar a las mentes; atacar fortificaciones es una misión secundaria. La guerra psicológica es la cuestión principal. El combate es secundario"[37].


Imagen 3: Poster Serbio de propaganda distribuido a través de Internet

[35] LUNGU Angela María, *The Internet and PSYOPS*, War.com Spring/Summer 2001.
[36] LIND William S., *The changing face of war: Into the fourth generation* Marine Corps Gazette October 1989, Pages 22-26.
[37] THOMAS Timothy L., *Human Network Attacks* Foreign Military Studies Office, Fort Leavenworth, KS. Military Review, Septiembre-Octubre 1999.

## INGENIERÍA SOCIAL Y PSYOPS EN INTERNET

El ciberespacio es considerado ya un campo de batalla[38] en el que "las ciberamenazas están creciendo rápidamente en número y sofisticación"[39]. Pero no sólo habrá que luchar contra las amenazas puramente técnicas como los virus, la doctrina norteamericana ve con claridad que "el ciberespacio será el entorno elegido por nuestros adversarios para influir en el apoyo de los individuos a su causa y para crear una atmósfera de miedo, haciendo uso de técnicas de persuasión y tecnología"[40]. Los desarrollos tecnológicos han hecho posible llegar a todos los ciudadanos con una ofensiva de información, desde el hombre de la calle a los jefes de estado[41].

El factor humano es la parte más importante de un sistema de defensa, y más concretamente en la seguridad de los sistemas de información[42] que, en definitiva, soportan las infraestructuras y servicios tanto civiles como militares. Es más, dicho factor es el eslabón más débil de cualquier estructura defensiva y el único medio que permite romper cualquier estrategia de seguridad[43], introduciendo una variable impredecible que no puede controlarse por medios técnicos.

La ingeniería social aplicada a través Internet pretende explotar esta vulnerabilidad, de ahí que se denomine hacking no técnico, refinándose cada vez más la naturaleza de los ataques, haciéndolos más personales y con un mayor conocimiento de los objetivos[44]. A su vez, los servicios que proporciona la red crecen en complejidad. Por un lado, el fenómeno Internet engloba o se interconecta con multitud de servicios como son la telefonía fija y móvil (SMS, mensajería blackberry[45] o bluetooth), televisión y radio digital, RFID, internet de las cosas (web 3.0), servicios de geolocalización, Wifi y similares. Por otro lado, dentro de Internet se

---

[38] CARO BEJARANO M.J., *Nuevo concepto de ciberdefensa de la OTAN* Documentos informativos del IEEE Nº 09/2011
[39] North Atlantic Council, *Lisbon Summit Declaration* Lisboa 2010.
[40] BAKER Prentiss O., *Psychological operations within the cyberspace domain*, 2010 Air War College University, Alabama.
[41] THOMAS Timothy L. opt.cit.
[42] La norma ISO 27001-2007, sobre el sistema de gestión de seguridad de la información, dedica su capítulo 5.2.2 a la concienciación, formación y captación del personal, así como su anexo 8 a los controles de seguridad ligados a los recursos humanos, clasificando los controles en aquellos a ejercerse antes, durante y en la finalización de la relación contractual. Así mismo, en el apartado 9 hace alguna referencia a los mismos en relación a los controles de acceso físico. En el Esquema Nacional de Seguridad encontramos una trasposición de dichos principios en los artículos 5, 14 (sobre gestión de personal) y 15 (sobre profesionalización). A pesar de ello, no se recalca la importancia fundamental que tiene.
[43] The Economist *The Stuxnet worm* opt.cit.
[44] Cisco security white paper, *E-mails attacks: This time is personal,* Junio 2011.
[45] El mundo.es, *El MI5 intenta localizar a los autores de los mensajes que convocaron los saqueos. La mayoría enviados a través de Blackberry*, martes 16 de agosto de 2011.

encuentran multitud de canales distintos (e-mail, foros, blogs, páginas, P2P, redes sociales, Skype, etc.) que son medios para establecer relaciones sociales, grupos de interés… en definitiva redes[46] entre personas, que se solapan unas a otras e interrelacionan sobre dichos recursos[47].

Las operaciones psicológicas basadas en internet se iniciaron con la ofensiva propagandista en la guerra de Kosovo de 1999. En Estonia, en 2007, se demostró la viabilidad de realizar un ataque tecnológico a gran escala contra un Estado. En Georgia[48], en el año 2008, ya se coordina la acción militar con los ataques tecnológicos y propagandistas. Anonymous[49] y Wikileaks[50] en 2010 son ejemplos de acciones coordinadas internacionalmente para dar sensación de inseguridad, vulnerabilidad y fragilidad en nuestros sistemas y servicios nacionales. La utilización de técnicas virales en redes sociales para la expansión de protestas en 2011 ha demostrado su impacto en países tan distintos como los árabes (Egipto, Túnez…) y los occidentales (España, Gran Bretaña…).

Pero todavía queda dar un paso más allá en el conflicto cibernético. Este consiste, no sólo en emplear Internet para tareas de comunicación, propaganda blanca, reclutamiento, financiación, mando y control o ataque tecnológico (elementos de la clickskrieg[51]), sino en la utilización de las técnicas de ingeniería social para implementar operaciones psicológicas a gran escala ocultando el origen y la intención última del ataque, es decir, para implementar una acción de propaganda negra[52].

Este tipo de ataque no sustituirá a los métodos habituales de las operaciones psicológicas, sino que los reforzará al crear las condiciones idóneas para su desarrollo potenciando los sesgos cognitivos como son: primera impresión, conocimiento, aceptación y simpatía por la causa. Estas acciones, introducidas en los canales y formatos en los que la audiencia objetivo

[46] Una colección de actores (más de dos) pares (iguales entre sí) que de forma continua y duradera mantienen relaciones entre sí. Podolny Joel M. et al., *Network Forms of Organization* Annual Review of Sociology.
[47] EILSTRUP-SANGIOVANNI Mette et al. *Assessing the danger of illicit networks*, International Security, Vol. 33, No. 2 (Fall 2008), pp. 7–44.
[48] GANUZA ARTILES Néstor, *Situación de la ciberseguridad en el ámbito internacional y en la OTAN*, Ciberseguridad retos y amenazas a la seguridad nacional en el ciberespacio. Cuadernos de Estrategia. IEEE – IUGM – Ministerio de Defensa, diciembre 2010.
[49] El Mundo.es, *Anonymous afirma haber conseguido más de 1GB de datos de la OTAN*, 21 de julio de 2011.
[50] DE SALVADOR Luis, *Internet, filtraciones y Wikileaks*, Documentos de opinión del IEEE, nº 25/2010 www.ieee.es.
[51] Término acuñado en el artículo de SATCHELL Michael, *Captain Dragan's Serbian Cybercorps (Serbs Used Internet For Propaganda, While NATO Drops Leaflets)* U.S. News & World Report 126, 10 Mayo 1999.
[52] Información falsa que se supone que procede de una fuente en conflicto, pero que realmente procede de otra diferente, que ha utilizado alguna estrategia para ocultar su origen. TAYLOR Philip. M. *Strategic Communications and the Relationship between Governmental 'Information' Activities in the Post 9/11 World*, Journal of Information Warfare Volume 5, Issue 3.

tenga más confianza, permitirán que el mensaje sea aceptado en los lugares donde no habría sido siquiera invitado.

En el caso del empleo de técnicas de ingeniería social para atacar sistemas de ordenadores o redes, normalmente la segunda fase del ataque ha sido un ataque tecnológico: introducir un virus, troyano o cualquier mecanismo para romper, por ejemplo, un sistema de cifrado. Pero, en este caso, se mantendrán las dos fases del ataque en el plano humano, extendiéndose a la red de mentes. El objetivo será, entonces, manipular las emociones.

Las técnicas de ingeniería social que se utilizan en este tipo de operaciones, y las herramientas informáticas que les dan soporte, son conocidas, fáciles de emplear y muchas son de tipo "point and click[53]". En sí mismas no son novedosas, es más, actualmente se divulgan libremente en los foros especializados, conferencias y páginas de los ingenieros sociales más especializados y están al alcance de cualquiera. Están concebidas para permitir configurar los ataques maximizando la dispersión de la amenaza, su independencia de cualquier centro de control, así como su capacidad de adaptación y maniobra dentro de los canales de comunicación en Internet[54]. La novedad residirá en su utilización masiva y coordinada.

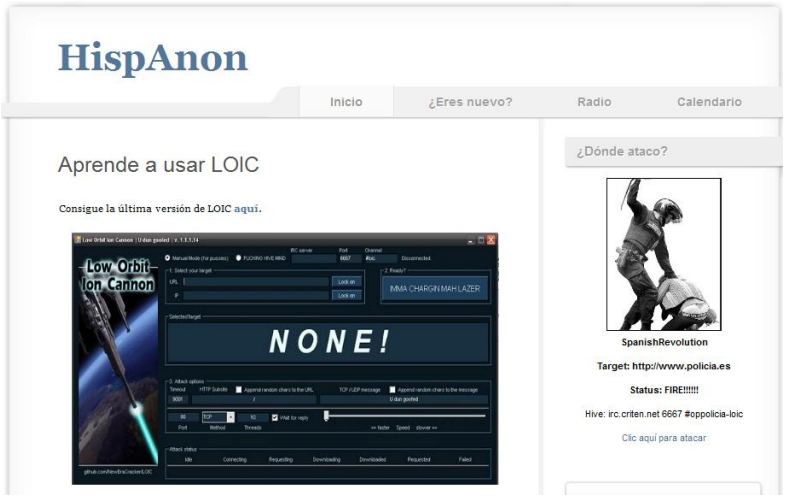


Imagen 4: Página en la que se ofrece la descarga de herramientas para realizar ataques coordinados a través de la red. Origen en el portal www.hispanon.com

[53] VACCA John R., *Computer and Security Handbook*, ed. Seymor Bosworth.
[54] LIND William S. opt.cit.

La ingeniería social, empleada a través de Internet tiene varias particularidades:

- Por un lado, permite acceso instantáneo a grandes grupos de población.
- Por otro lado, puede aplicarse selectivamente a segmentos de población (menores, adolescentes, grupos de interés, tribus urbanas…), y por tanto no ser visible para la totalidad de la población en sus primeros estadios.
- Tiene una rápida velocidad de propagación, en algunos casos exponencial como ocurre en el caso de trabajar sobre las redes P2P.
- El mensaje es persistente, una vez se ha lanzado a la red resulta difícil eliminarlo de forma completa, pues se replicará múltiples veces.
- Es un arma de reutilización limitada. Una vez empleada, los objetivos se encuentran saturados de información por dicho canal y son conscientes de la amenaza[55]. Si dicho instrumento se emplea a discreción por otros actores en el conflicto su poder desaparece, o se asocia a los primeros que lo utilizaron, teniendo un efecto contraproducente[56]. Esto le obliga a mutar de estrategia o de forma continuamente.
- Existe una simplificación del canal de comunicación. Simplicidad no técnica, pero sí comunicativa. Un correo, una llamada o una conversación en chat, limita o cercena gran parte de los canales verbales y no verbales de la comunicación. Al interlocutor no se le ve, no se le oye de forma normal o no se le oye en absoluto, en los chat, los ritmos normales de la conversación desaparecen. Por lo tanto, todo el conjunto de parámetros que utilizamos de forma consciente e inconsciente para discriminar la veracidad de las informaciones que nos ofrecen se reducen drásticamente quedando únicamente el criterio racional, crítico y objetivo para distinguir si una información es verdadera o falsa, mecanismos muy difíciles de emplear cuando se han distorsionado los puntos de referencia.
- Dependiendo de la estrategia utilizada, los individuos de la audiencia objetivo tendrán la ilusión de haber establecido una comunicación uno a uno, lo que facilitará la aceptación del mensaje.

Al ser el ciberespacio un dominio que enlaza las tres dimensiones del entorno de información del individuo (el físico, el informativo y el cognitivo), la deformación de dicho dominio es el camino ideal para alterar la percepción de la audiencia objetivo. Sobre todo en los casos en los que son empleadas en el marco de un conflicto asimétrico. El actor asimétrico será un atacante no necesariamente más débil o no-estatal, sino será aquel que empleará medios novedosos, con grupos irregulares, que eviten el enfrentamiento directo, al que será difícil de responder con las mismas armas y de identificar, y que se basará

[55] A menos que se emplee un tiempo prudencial para que la memoria colectiva desaparezca, como fue la repetición del fenómeno Wells en 1998, coincidiendo con su 60 aniversario en México y Portugal, con un gran impacto en el primero.

[56] Como ocurrió con el lanzamiento de panfletos por parte de la OTAN en la guerra de Yugoslavia, que los serbios asociaron a los panfletos lanzados por las fuerzas invasoras alemanas en la Segunda Guerra Mundial PSYOPS in Kosovo.

siempre en lo inesperado[57]. Tendrá mucha más libertad de acción que el ejército convencional para realizar acciones de este tipo por las siguientes razones:

- La gran mayoría de la audiencia objetivo es urbana y altamente dependiente de los canales de comunicación digitales.
- Hay un impulso creciente que empuja a los ciudadanos, instituciones, empresas y administraciones públicas[58] al uso de nuevas tecnologías, en el que se intenta simultanear libertad de expresión, privacidad, seguridad y comercio electrónico[59].
- Una intervención por un actor asimétrico no estará sujeto a las limitaciones legales[60] que se imponen en el uso de los sistemas de telecomunicación.
- No estarán limitadas por el temor a atravesar fronteras nacionales y el impacto que eso podría producir a países limítrofes o al entorno internacional.
- No estarán limitadas por el riesgo a influir en su propia población.
- Tienen expedito el camino a los medios de comunicación de la audiencia objetivo, pues resulta prácticamente imposible limitar el acceso desde terceros países al territorio nacional de forma sistemática (siempre en el caso de los países occidentales).
- A la hora de reaccionar, resultará más complejo y lento realizar las intervenciones de las comunicaciones, pues su privacidad está protegida como un derecho fundamental.
- Al ser un ataque social, la propia sociedad reaccionará de forma negativa a cualquier reacción sobre el mismo ataque, por lo que se debilitará la posibilidad de defensa.

Imagen 5: Mensaje de Anonymous difundido a través de Youtube en relación a la Operación Telefónica del 26 de junio[61]

Sin pretender ser exhaustivo, entre otras cosas porque sería inútil ya que en este campo la innovación es constante, ejemplos de técnicas y herramientas que ya han sido empleadas de

[57] GRAY Colin S., *Thinking Asymmetrically in Times of Terror* Revista Parameters 2002.
[58] Como puede ser la ley 11/2007 de acceso electrónico de los ciudadanos a los servicios públicos.
[59] CARO BEJARANO M.J., *La estrategia internacional para el ciberespacio* Documento Informativo IEEE 21/2011.
[60] Como son leyes de protección de datos, comercio electrónico, de telecomunicaciones o anti-spam.
[61] Este mensaje aparecía en la web "Los ataques a sus webs se realizarán este Domingo 26 de Junio, y previsiblemente colapsarán temporalmente la red. Estáis avisados. Se pide la colaboración de todos los internautas información para todos los interesados en participar: La operación se sincronizará a través del canal irc.anonops.li.

forma limitada son:

- Ganar el control, suplantar o replicar canales[62] en los que confía la audiencia objetivo, desde portales gubernamentales a foros. Para ello se utilizan técnicas combinadas como DoS[63] que permiten anular un servidor confiable y sustituirlo por un "dummy" que tome control de las conexiones abiertas, DNS spoofing para redireccionar a sitios web distintos del auténtico, páginas replicadas (mirrors) que se mimetizan con las reales, etc.
- Generar corrientes de opinión en foros, blogs, encuestas online o por televisión, sms, y redes sociales mediante el uso de "ganchos", chat bots que simulan mantener conversaciones y otro tipo de personajes virtuales.
- En relación al anterior, el robo de identidades en la red para suplantar la personalidad de personajes reconocidos y así dar mayor verosimilitud a los mensajes transmitidos[64].
- Utilización de medios masivos de distribución de información, que pueden ser centralizados como Youtube, distribuidos como son las redes P2P, de acceso controlado como Wikileaks, o ilícitos como botnets[65].
- Empleo de técnicas de marketing viral, una estrategia de publicidad que incentiva que los individuos transmitan rápidamente un mensaje para crear un crecimiento exponencial en la exposición de dicho mensaje. Son técnicas de publicidad que se propaga a sí misma.[66]
- El secuestro y redirección de tráfico de Internet[67] a través de áreas controladas para monitorización, filtrado y manipulación de opiniones y contenidos.
- Generación de imágenes y voces simuladas o reproducidas, discursos desorientadores realizados por dirigentes virtuales o realidad distorsionada[68].
- La utilización de los banners publicitarios en los sitios de internet, mediante inserción directa o manipulación de los servicios de subasta on-line, para la propagación de mensajes.
- Etc.

---

[62] Muchas de estas técnicas no son novedosas, ya se han utilizado anteriormente aunque con medios técnicos más limitados. Durante la Guerra Civil Española, el Ministerio de Propaganda Alemán levantó una falsa emisora de radio republicana para operar al servicio del General Franco. NEWCOURT-NOWODWORSKI Stanley, *La propaganda negra en la Segunda Guerra Mundial*, Ed. Algaba, 2006.

[63] Ataque por denegación de servicio. También empleado por activistas pro serbios en paralizar los servidores de la OTAN durante el conflicto de Kosovo.

[64] La Tribuna de Ciudad Real, *Las redes sociales, el paraíso de los suplantadores digitales. Algunas personalidades de la política y la cultura españolas han comprobado y denunciado cómo diversos cibernautas anónimos se han hecho pasar por ellos para todo tipo de fines*, 27 de julio de 2009.

[65] Las botnets permiten convertir millones de ordenadores distribuidos por el mundo en generadores de spam (información) u otro tipo de ataques de forma transparente para los propios dueños de las máquinas.

[66] WILSON Ralph F., *The Six Simple Principles of Viral Marketing*, Web Marketing Today, February 1, 2005.

[67] El País.com, *China secuestró en abril el 15% del tráfico de Internet. Durante 18 minutos se desviaron rutas para que en vez de seguir el camino más corto, cruzasen el país asiático*, 17 de noviembre de 2010.

[68] THOMAS Timothy L. opt.cit.

Imagen 6 Foto distribuida por Reuters en relación a un ataque israelí sobre el Líbano. El patrón de humo (círculo) es repetitivo y los edificios destruidos (cuadrados) están repetidos para dar mayor sensación de destrucción[69].

**MECANISMOS DE DEFENSA**

La defensa frente un ataque de este tipo tiene que ir mucho más allá de la mera búsqueda de responsabilidades legales, que será siempre a posteriori y difícil de concretar. Ha de ser una defensa que minimice el impacto de dicho ataque, lo que resultará una tarea complicada debido a dos factores: su rápida velocidad de propagación y la propia naturaleza social del ataque.

El primero obliga a disponer de un servicio específico para la detección de este tipo de amenazas en tiempo real, lo que supone monitorizar el contenido[70] de Internet[71], y, una vez detectado, una acción que contrarreste con una contraprogramación los efectos del ataque. La detección en tiempo real supone mantener un sondeo constante de blogs, foros, tweets, redes sociales, Skype[72] y cualquier otro canal, nuevo o no, que pueda surgir en un momento dado. Aún más lejos, puede suponer un control, siempre con garantías, del anonimato en Internet[73], o incluso del contenido de las comunicaciones, contemplando la obligación de no

[69] *Reuters admits altering Beirut photo*, disponible en http://www.ynetnews.com/articles/0,7340,L-3286966,00.html
[70] La Gaceta, *Reino Unido y EEUU vigilarán a los jóvenes en la redes sociales*, viernes 12 de agosto de 2011
[71] Telecinco, *India quiere monitorizar el acceso a Internet*, disponible en www.telecinco.es/informativos/tecnologia/noticia/3187555/.
[72] El País.com, *Microsoft patenta un sistema para espiar Skype*, 29 de junio de 2011.
[73] Ya se están levantado voces contra el anonimato en Internet, precisamente de las empresas con más presencia en la misma como Facebook, RTVE, *Randi Zuckerberg: el anonimato en Internet tiene que*

vulnerar los derechos fundamentales a la privacidad, intimidad y secreto de las comunicaciones que garantiza la Constitución[74] y sin llegar a los límites de los países que no respetan los más elementales derechos humanos.

La reacción a un ataque muchas veces no podrá ser contrarrestada empleando los cauces gubernamentales o tradicionales, debido a dicho carácter social y a los perfiles de la audiencia objetivo ya mediatizada por las estrategias de ingeniería social. La propia naturaleza del ataque les restará credibilidad y el atacante se desvinculará[75] de la acción, incluso planteará problemas políticos[76]. La respuesta ha de ser realizada por los mismos medios, o medios que tengan la misma credibilidad para dicha audiencia, por lo que se ha de tener previsto recursos y equipos para llevarla a cabo.

Es importante plantearse si resulta adecuado realizar un apagón o bloqueo controlado de determinados portales o incluso redes de comunicación en situaciones de crisis. Hay que tener en cuenta que, en caso de que "se haya desatado un conflicto étnico, nacionalista, terrorista, criminal o una guerra social en la red, los protagonistas serán los más interesados en mantener la red activa"[77]. Esto supone identificar cuáles son los elementos críticos a eliminar[78], realizarlo con la velocidad suficiente y con eficacia técnica. Más aun, sería necesario hacer operaciones de microcirugía sobre la red, de forma que se pueda intervenir en ella sin anular todos los servicios de comunicaciones ni violar de forma sistemática los derechos de los ciudadanos.

Esto último ya ha sido planteado por el gobierno británico a la luz de los sucesos de violencia que han sacudido Londres en agosto de 2011. Facebook, Twitter y RIM han sido contactados por dicho gobierno para, en un futuro, realizar intervenciones estatales a dichos medios en caso de inestabilidad social[79]. Pero la eficacia de estas intervenciones no es tan fácil como pueda parecer. Detener la propagación de ficheros en una red P2P es muy difícil sin la

---

*desaparecer,* disponible en http://www.rtve.es/noticias/20110801, o Google en el lanzamiento de su red social Google+.

[74] Art. 18 de la Constitución Española. desarrolladas entre otras en la Ley 32/2003 General de Telecomunicaciones, la Ley 25/2007 de Conservación de Datos de Tráfico o la Ley Orgánica 15/1999 de Protección de Datos.

[75] Como ya está ocurriendo. El Mundo Digital, *China niega ser el estado detrás de los ciberataques descubiertos por McAfee. Califica las acusaciones de irresponsables*, 5 de agosto de 2011.

[76] El País.com, *Los eurodiputados suscriben una declaración en contra del tratado ACTA. Pide que la UE impida obligar a los proveedores de Internet al filtrado de tráfico*, 9 de septiembre de 2010.

[77] Networks and netwars: The future of terror, crime and militancy, J.Arquilla, D. Rondfelt, ed. RAND ISBN: 0-8330-3030-2 MR-1382-OSD, 2001.

[78] En el caso de la guerra contra Yugoslavia, los medios de comunicación tradicionales serbios fueron destruidos, pero no así los accesos a Internet, que fueron utilizados por los mismos serbios para realizar el contraataque informativo.

[79] Iniciativa que ya ha tenido una contestación social y política.

intervención de IP particulares[80]. Eliminar las entradas DNS de páginas fuera de un país no impide acceder a las mismas a través de portales de navegación anónima. Se han empleado sistemas de filtrado de contenidos, que muchas veces son ineficaces ya que su utilización implica un análisis del propio mensaje y generar las reglas que los identifiquen, lo que retarda su aplicación. También se ha utilizado el filtrado de origen, en particular bloquear el tráfico procedente de las redes de anonimización.

La rapidez de reacción es vital. Cualquier maniobra de este tipo será vista como una acción de censura que reforzará el mensaje si éste ya ha llegado a la audiencia objetivo. Además, hay que contar con la velocidad de adaptación que se supone va a tener el atacante[81] lo que obliga a adaptarse a su ritmo.

Finalmente, todas estas acciones han de tener la oportuna cobertura legal que proporcione precisamente lo que antes se comentaba: legitimidad, garantías, velocidad y flexibilidad de actuación.

**CONCLUSIÓN**

Los sucesos recientes que se han producido en Egipto, Túnez o Gran Bretaña (graves conflictos que han llegado a derribar gobiernos) han demostrado que el gran desafío que presentan las nuevas tecnologías se ha materializado, no en la forma de amenazas técnicas como virus o troyanos, sino en la forma de amenazas sociales.

En estos sucesos se han utilizado con profusión las facilidades que ofrecen estas técnicas para la propaganda y la coordinación. Han servido de soporte, conductor y potenciador de un malestar ya existente en la sociedad, permitiendo el estallido del mismo y proporcionándole un efecto multiplicador, y han demostrado que los sistemas de comunicación cada día ofrecen nuevos canales y formas novedosas de interrelacionar a individuos y grupos, con nuevas reglas y nuevos lenguajes.

Pero esto es sólo una primera fase del potencial existente en la manipulación de las modernas redes de telecomunicaciones, se ha demostrado que hay abierto un camino que podría llegar mucho más lejos. En cualquier país, sobre todo en los más avanzados técnica y democráticamente, ya existe una vulnerabilidad a nivel social que es susceptible de ser

[80] Imposible si los ordenadores de la red, todos, no están en un país en el que sea posible la intervención.
[81] Cuando el gobierno serbio cerró las estaciones de radio de la oposición a Milosevic éstos las recondujeron a través de Internet. De igual forma hicieron los serbios cuando sus estaciones fueron bombardeadas. Más recientemente, los intentos de cerrar los servidores de Wikileaks terminaron en un fracaso, ya que rápidamente cambiaron su hosting.

explotada por terceros para implementar operaciones psicológicas de gran alcance utilizando técnicas de ingeniería social que permitan crear desestabilizaciones artificiales en momentos de crisis. Las técnicas y los principios están ahí. Ensayos limitados, principalmente con propósitos de marketing, han sido los primeros ejemplos.

Internet, sus tecnologías y canales de comunicación asociados, puede ser un servicio libre pero no puede seguir tratándose como un recurso social totalmente fuera de control[82]. Es necesario adoptar medidas preventivas y correctivas para evitar que estas amenazas se materialicen. Es preciso monitorizar el pulso social que se está gestando en cada momento en los distintos planos de comunicación, sobre todo cuando éste puede ser inducido desde el exterior, y disponer de herramientas para la toma de decisiones de forma ágil, dinámica y selectiva. Todo ello dentro de un marco jurídico que proteja los derechos fundamentales relativos a la libertad, intimidad y privacidad de los ciudadanos.

*Luis de Salvador*
Doctor en Informática

[i] **NOTA:** Las ideas contenidas en los ***Documentos de Opinión*** son de responsabilidad de sus autores, sin que reflejen, necesariamente, el pensamiento del IEEE o del Ministerio de Defensa.

[82] LUNGO Angela M., *War.com: The Internet and psychological operations*, Naval War College, Newport, R.I.