Revista Iberoamericana de las Ciencias Sociales y Humanísticas

RICSH

ISSN: 2395 - 7972

https://doi.org/10.23913/ricsh.v8i16.179

Artículos Científicos

Perfil psicosociológico en el ciberdelincuente

Psychosociological profile in the cybercriminal

Perfil psicossociológico no cibercriminoso

Juan Carlos Fernández-Rodríguez
Universidad Antonio de Nebrija. Madrid, España
jfernanr@nebrija.es
https://orcid.org/0000-0003-3312-861X

Fernando Miralles Muñoz
Universidad San Pablo CEU, España
f.miralles@ceu.es
https://orcid.org/0000-0003-3382-5343

Luis Millana Cuevas
Universidad Antonio de Nebrija. Madrid, España
lmillana@nebrija.es
https://orcid.org/0000-0002-7824-6313

Resumen

En el presente artículo se estudian las características más importantes de los conceptos que hoy conocemos como *ciberdelincuencia*, *ciberterrorismo* y *ciberguerra*. En relación con la ciberdelincuencia y el ciberterrorismo, se proporcionan datos sobre los posibles perfiles existentes y sobre distintos arquetipos de personas que tienen estas conductas delictivas. En lo concerniente a la ciberguerra, y debido al reducido número de estudios planteados sobre este fenómeno, se exponen los datos más relevantes sobre este hecho y se resalta la falta de estudios para describir a sus actores desde un prisma de carácter psicosociológico.

Palabras clave: cibercrimen, ciberdelincuencia, ciberguerra, ciberterrorismo.

Revista Iberoamericana de las Ciencias Sociales y Humanísticas

RICSH

ISSN: 2395 - 7972

Abstract

In the present paper we study the most important characteristics of the concepts that we know today as cybercrime, cyberterrorism and cyberwar. Regarding cybercrime and cyberterrorism, data are provided regarding possible profiles and also about the different archetypes of people who perform these forms of criminal behavior. Regarding the cyberwar, and because of the small number of studies on this phenomenon presented the most relevant data on this fact and highlights the lack of studies that describe their actors from a prism of psychosociological character.

Keywords: cybercrime, cybercrime, cyberwar, cyberterrorism.

Resumo

Neste artigo, estudamos as características mais importantes dos conceitos que conhecemos hoje como cibercrime, ciberterrorismo e guerra cibernética. Em relação ao crime cibernético e ao ciberterrorismo, são fornecidos dados sobre possíveis perfis existentes e sobre diferentes arquétipos de pessoas que têm esses comportamentos criminosos. No que diz respeito à guerra cibernética, e devido ao pequeno número de estudos levantados sobre esse fenômeno, são apresentados os dados mais relevantes sobre esse fato e destacam-se a falta de estudos para descrever seus atores a partir de um prisma de natureza psicossociológica.

Palavras-chave: crime cibernético, crime cibernético, guerra cibernética, ciberterrorismo.

Fecha Recepción: Marzo 2019 **Fecha Aceptación:** Julio 2019

Introducción

En la sociedad tecnológica global la ciberdelincuencia es un fenómeno que ha aumentado considerablemente en los últimos tiempos. Esto sucede en medio de un contexto donde las personas son cada vez más dependientes de las tecnologías de la información y comunicación (TIC), de ahí que sea necesario aumentar los estándares en materia de seguridad digital para prevenir potenciales ciberdelitos que no solo pueden afectar a los individuos, sino también a las empresas, las organizaciones y los gobiernos.

En el año 2015, por ejemplo, fueron registrados 81 307 delitos, de los cuales 74.4 % se relacionaron con fraudes informáticos (estafas), mientras que 13.9 % se vincularon con amenazas y coacciones (Ministerio del Interior, 2017). Asimismo, en 2014 se registraron más de 317 millones de novedosos códigos maliciosos (troyanos, gusanos, virus, etc.), es decir, casi un millón de amenazas emitidas por día en el ciberespacio (Symantec Corporation, 2015, citada por Guilabert, 2016).

Un caso emblemático de ciberdelincuencia fue el realizado por el ingeniero John Draper, quien fue arrestado en 1972 por fraude contra las compañías telefónicas. Según se sabe, todo comenzó cuando un amigo invidente de Draper (Joe Engressia) le comentó que obstruyendo la salida de aire de uno de los oficios del silbato que añadía una famosa empresa (Quaker Oaks) en sus cajas de cereales se podía generar un tono puro de 2600 Hz, frecuencia que era igual al tono realizado por el sistema telefónico para advertir la conclusión de una llamada.

Emitido el tono de 2600 Hz, uno de los extremos de la línea se desconectaba y el lado conectado entraba en modo de operador, con lo cual se podían "escuchar" los tonos especiales que definían la llamada. Esto le sirvió a Draper para idear un aparato que imitaba distintos tonos registrados por la centralita, de modo que podía controlar y modificar su comportamiento para su propio beneficio. La producción de este artefacto, conocido como *blue box 35* o *caja azul*, se convirtió en el primer gran caso del llamado *phreaking* o *hacking telefónico*. Esta estrategia de Draper fue usada por una gran cantidad de usuarios, quienes pudieron realizar gratuitamente llamadas telefónicas de larga distancia, lo cual no solo ocasionó grandes pérdidas a las compañías telefónicas, sino que también colaboró con el ascenso del movimiento *hacker*.

Este acontecimiento provocó gran entusiasmo en las universidades de ingeniería electrónica; de este modo llegó a ser conocido por Steve Woznkiak, un talentoso de esa disciplina, quien empezó a reproducir esas cajas para venderlas y conseguir capital con su socio Steve Jobs.

Otro ejemplo de estos delitos electrónicos fue el gran robo cibernético bancario realizado en febrero de 2016; este consistió en la extracción de 81 millones de dólares del banco central de Bangladesh, los cuales estaban depositados en el Banco de la Reserva Federal de la ciudad de Nueva York. Este crimen fue materializado gracias a un *malware* que reproducía transferencias legales de fondos mediante una aplicación llamada SWIFT, la cual es empleada por todos los bancos para realizar operaciones entre ellos (Leetaru, 2016).

Objetivos

Es habitual que en los distintos medios —sean especializados o no— se empleen distintas expresiones o vocablos, pero con diferentes significados, lo cual puede alterar no solo el significado de la información que se quiere trasmitir, sino también la manera en que es interpretada por el receptor, de ahí que sea necesario explicarlos con mayor detalle. Debido a ello, el objetivo del presente trabajo es procurar una clarificación de términos como

ciberdelincuencia, *cibercrimen*, *ciberdelito* y *ciberterrorismo*, así como exponer las cualidades psicosociológicas más sobresalientes de estos fenómenos y las posibles clases de delincuentes según las categorías mencionadas.

Metodología

Para cumplir con los anteriores objetivos se ha realizado una búsqueda bibliográfica, la cual se concretó en febrero de 2019. En ese proceso se incluyeron los términos usados como palabras clave. Los resultados se han restringido a la información recabada en lengua española.

Resultados

Con bastante regularidad se utilizan los términos *ciberdelincuencia* y *cibercrimen* para referirse a situaciones similares. De hecho, y siguiendo a Roca (2014), el ciberdelito se asocia a aquellas actividades ilegales que se ejecutan mediante el uso de los actuales sistemas de comunicación e información. Según el *Diccionario* de la Real Academia Española (RAE), el vocablo *delito* posee tres significados: 1) culpa, quebrantamiento de la ley; 2) acción o cosa reprobable, y 3) acción u omisión voluntaria o imprudente penada por la ley. Estas tres acepciones se pueden trasladar a los crímenes realizados mediante las TIC. Igualmente, la palabra *delincuencia* se vincula con un "conjunto de delitos", de ahí que sea posible asociarla en los ámbitos adecuados con el término *ciberdelincuencia*. Igual suele suceder con la palabra *cibercrimen*.

Según la RAE, *crimen* es la "acción voluntaria de matar o herir gravemente a alguien". Por tanto, no parece un concepto que pueda aplicarse al mundo de las comunicaciones, aunque sí es correcto emplear la primera acepción referida porque un crimen no solo es un "delito grave", sino también una "acción indebida o reprensible", lo cual se puede trasladar al entorno virtual de la informática y de las comunicaciones.

Para Miró (2012,), ciberdelincuencia o cibercrimen es cualquier delito en el que las TIC "juegan un papel determinante en su concreta comisión, que es lo mismo que afirmar que lo será cualquier delito llevado a cabo en el ciberespacio, con las particularidades criminológicas, victimológicas y de riesgo penal que de ello se derivan" (p. 44). Según esta postura, los términos *ciberdelincuencia* y *cibercrimen* parecieran emplearse de manera indistinta (en el caso de cibercrimen, se refiere a la totalidad de acciones delictivas realizadas en el ciberespacio). En este sentido, se pueden considerar sinónimos los vocablos *ciberdelito* y *cibercrimen* (como acción concreta: "Se ha cometido un cibercrimen").

Ahora bien, desde una perspectiva psicosocial, el terrorismo se vincula con un modo de crear caos y zozobra en la población civil (Fernández-Rodríguez y Miralles, 2016). Esta manera de violencia, trasladada al mundo del ciberespacio, da origen al denominado *ciberterrorismo*, forma de delincuencia que se materializa en la Web no solo por organizaciones terroristas tradicionales que se apoyan en sus creencias religiosas para comentar distintos actos punibles, sino también por nuevos grupos o bandas organizadas de ciberdelincuentes que promueven protestas políticas o ideológicas y cuyos miembros son conocidos como *hacktivistas* (Mateos, 2013).

Ciberdelincuencia y ciberdelincuentes

La denominada *ciberdelincuencia* se ha expandido sustentada en el desarrollo de las nuevas tecnologías, espacio sin fronteras bien establecidas en el cual se pueden cometer una serie de actos vandálicos sin las restricciones que se imponen en el entorno tradicional. Esto ha exigido el surgimiento de una sociedad de la información que se enfoque en la prevención, la investigación, la prueba y la represión del hecho criminal superando las trabas que presentan las jurisdicciones de los distintos países.

Al respecto, sin embargo, vale acotar que el gran reto de la justicia penal en las democracias de nuestros días consiste en alcanzar un equilibrio entre seguridad y libertades individuales para que no sean sacrificadas las garantías de los ciudadanos (Francés, 2005).

Para tener una visión más amplia de la ciberdelincuencia en España, resulta preciso referir el informe sobre ese fenómeno en dicho país correspondiente al año 2017 y publicado el Ministerio del Interior (Ministerio del Interior, 2017). Para la redacción de este informe se tomó como fuente la información estadística recabada sobre la delincuencia conocida, la cual es registrada por las distintas fuerzas y cuerpos de seguridad (Policía Nacional, Guardia Civil, Policía Foral de Navarra y múltiples cuerpos de policía local). Esta información se puede encontrar en el Sistema Estadístico de Criminalidad (SEC) y en el Centro Nacional de Protección de las Infraestructuras Críticas (CNPIC). En dicho informe se incorpora una radiografía de la sociedad de la información, así como otros tipos de datos estadísticos, como el número de detenciones/imputaciones, los hechos conocidos por categorías delictivas, la distribución territorial de la cibercriminalidad, el perfil de la víctima y del responsable, los incidentes registrados por el CERTSI, etc.

Aunado a esto, se añaden cifras en torno a la manera en que la sociedad española en general emplea las tecnologías, así como comparaciones entre esos usos y los realizados por otros estados de nuestro entorno. Este tipo de resultados se obtiene gracias a encuestas y

estudios de opinión que realizan distintos organismos tanto a nivel nacional (Instituto Nacional de Estadística de España [INE]) como europeo (Eurostat). Algunos de los datos más sobresalientes son los siguientes (Ministerio del Interior, 2017):

a. La cifra total de detenciones o de personas investigadas por las fuerzas y los cuerpos de seguridad del Estado fue de 4912, de los cuales 77.04 % eran hombres.
b. Del análisis de las distintas tipologías delictivas recogidas en este informe, entre los detenidos/imputados hombres sobresalen las amenazas, las estafas, la pornografía de menores, así como el descubrimiento y la revelación de secretos; mientras que las amenazas, las estafas, las injurias y la usurpación del estado civil son predominantes en las mujeres detenidas/imputadas.
c. La mayor parte de los detenidos/imputados por ciberdelincuencia son españoles (84.6 %), mientras que los detenidos/imputados de otros países son predominantemente de nacionalidades rumana, marroquí (también ocurre con las víctimas), nigeriana, colombiana y ecuatoriana. El colectivo de los detenidos/imputados de entre 26 y 40 años ejecuta con frecuencia más elevada los delitos de amenazas, fraudes informáticos y coacciones. En cuanto a los menores de edad, se observa una preponderancia en delitos de amenazas, coacciones, acceso e interceptación ilícita y delitos sexuales.

De acuerdo con Mateos (2013), existe un número elevado de estudios que apuntan a que el perfil típico del ciberdelincuente se corresponde con una persona de sexo masculino, entre los 25 y 35 años de edad y con ciertos conocimientos tecnológicos e informáticos que le facultan para usar Internet como fórmula perfecta para ejecutar sus actividades, aunque vale acotar que la edad de inicio en la ciberdelincuencia es cada vez menor, por lo que se deben estudiar cuáles son los precipitantes de este hecho (González y Campoy, 2018).

Un ciberdelincuente o *hacker*, de forma general, desconfía de la autoridad (a la cual habitualmente considera opresora) y cree que el acceso a todo tipo de información debería ser gratuito e ilimitado; sin embargo, es preciso saber que este tipo de delincuentes tienen características y comportamientos que sirven para ofrecer distintas categorizaciones, como se explican a continuación (Mateos, 2013):

a. *White hat hacker*: Conocidos habitualmente como los *hacker* tradicionales o *hacker* éticos. Su mayor maldad consiste en dejar una tarjeta de visita para informar al administrador del sistema de los fallos y vulnerabilidades encontrados tras un ataque o entrada en su sistema, o realizando —en el peor de los casos— solo algunas

modificaciones para lograr el anonimato. En algunas circunstancias, los *white hat hacker* son personas que han pertenecido a los *black hat hacker*, pero que decidieron modificar sus determinaciones maliciosas para luchar contra el cibercrimen y apoyar a los administradores de los sistemas de seguridad. Los términos *black hat* y *white hat* proceden de las antiguas películas del oeste donde los buenos portaban sombrero blanco y los malos llevaban siempre un sombrero de color negro (Meseguer, 2013).

b. *Black hat hacker*: Son aquellos a los que comúnmente se les nombra como *hacker* habituales. Se les identifica porque no siguen ninguna ética y porque buscan el beneficio económico y personal. El *hacker* negro intenta colapsar los servidores, penetrar en zonas prohibidas o tomar el control de sistemas y redes. En este caso, sin embargo, también se pueden referir algunas excepciones, como sucedió con un *hacker* ruso que en un importante foro expresó su malestar y antipatía por quienes atacaban sistemas de salud pública. En efecto, en los círculos clandestinos rusos existe un cierto "código ético" que deja a dichos centros asistenciales fuera de ese tipo de ataques, independientemente de si se encuentran en países que suelen ser objetivo de sus campañas y ciberataques (McAfee, 2016). Estas personas se sienten orgullosas cuando demuestran sus habilidades, de modo que su grado de autorrealización es más elevado cuando mayor es el impacto del perjuicio provocado.

c. *Grey hat hacker*: Son sujetos con una ética ambigua. Estas personas poseen conocimientos equiparables a los de un *black hat hacker*, aunque también los usan para localizar vulnerabilidades o fallos de seguridad, los cuales son aprovechados para más tarde ofrecer una solución a cambio de una compensación económica.

d. *Cracker*: Se podrían incluir dentro del grupo de los *black hat hacker*. Se les toma como el grupo más agresivo y quizás más peligroso. Su objetivo único es "reventar sistemas" informáticos o electrónicos. Los *cracker* poseen gran experiencia en programación y utilizan sus conocimientos para modificar el comportamiento de redes y sistemas, aprovechando cualquier tipo de vulnerabilidad encontrada. Actúan de forma casi insaciable y obsesiva, dirigidos por su afán destructivo y ególatra.

e. *Lammer*: Rechazados dentro del colectivo *hacker*, son sujetos que se dedican a recopilar información y ejecutar códigos maliciosos buscando el reconocimiento social como *hacker* sin poseer un conocimiento real del impacto de sus acciones ni del funcionamiento del código ejecutado. Pueden llegar a suponer una molestia, aunque sus acciones no suelen causar daños graves.

f. *Phreaker*: Colectivo dedicado casi por entero al mundo de los sistemas telefónicos, incluyendo también la telefonía móvil y voz sobre IP (VoIP). Tienen un gran

conocimiento del funcionamiento de dichas tecnologías y de sus protocolos de comunicación, por lo que se dedican a alterar el comportamiento de los sistemas, algunas veces por placer y en otras con fines económicos.

g. *Scriptkiddie***:** Son simples usuarios de Internet que se interesan por temas de *hacking*, aunque con un conocimiento poco profundo. Pueden utilizar programas o *malware* que descargan de Internet y que ejecutan sin mayor conocimiento o estudio, por lo que en algunos casos pueden infectar sus propios sistemas.
h. *Wannaber*: Son aspirantes a *hacker* con baja capacidad técnica y escasa perseverancia, lo cual en la mayoría de los casos los convierten en inofensivos. Suelen utilizan sus bajos conocimientos informáticos para obtener el prestigio social fuera de la Red.
i. *Newbie*: Son conocidos como aprendices de *hacker*. Son los usuarios novatos que comienzan a leer y a experimentar con la información encontrada. En ocasiones realizan incursiones en sistemas débiles aunque sin mayor trascendencia debido a sus escasos conocimientos en el área. Normalmente su único objetivo es aprender.
j. *Piratas informáticos*: De forma habitual se confunde esta denominación con la del término *hacker*. Sin embargo, los piratas informáticos solo se dedican a la copia y distribución de manera ilegal de *software*, música, juegos y demás contenido, con lo cual atentan contra la propiedad intelectual y los derechos de sus propietarios.
k. *Bucaneros*: Hacen el papel de comerciantes en la Red. Se dedican a comprar y vender material ilegal obtenido por medio de otros, tales como identidades, tarjetas de control de acceso, *software* craqueado, etc.

A partir de lo anterior, se puede indicar que un ciberdelincuente es todo aquel que puede ser acusado de ejercer la ciberdelincuencia o el cibercrimen. De igual forma, se consideran ciberdelincuentes a aquellos sujetos cuya actividad ilegal ha evolucionado con la tecnología, como puede ser el caso de pederastas, proxenetas, etc.

Aunado a esto —y aunque se han nombrado las características de los distintos tipos de *hacker* o de sujetos dedicados a la ciberdelincuencia—, se puede considerar relevante agregar algunos perfiles adicionales que han surgido en la actualidad, los cuales se pueden hallar en diferentes artículos tecnológicos, entre los que se destacan el Informe sobre Criminología Virtual de la compañía de seguridad informática McAfee, los cuales se explican a continuación (McAfee, 2009, citado por Mateos, 2013):

a. *Instaladores de bots*: Son aquellos usuarios que buscan conseguir el control de un equipo remoto gracias a la instalación de un *software* malicioso. Para alcanzar dichos propósitos utilizan un *malware* preprogramado, el cual es embebido de manera oculta en todo tipo de interacciones que el usuario realiza mientras navega por la Web.
b. *Carders*: Esta clase de ciberdelincuentes se centran de forma exclusiva en la sustracción de identidad y en la consecución de fraudes mediante tarjetas de crédito en la Red. Los *carders*, por tanto, pueden ser considerados como una evolución virtual de los carteristas callejeros tradicionales. Una vez lograda la información necesaria, pueden realizar transacciones y compras en línea encubriendo su identidad y cargando el coste a su víctima.
c. *Ciberpunks*: Sin llegar a tener un objetivo lucrativo en sus actos, los *ciberpunks* —denominación surgida del movimiento literario con el mismo nombre— pueden generar grandes pérdidas a sus víctimas tanto económicas como de imagen. Considerado como el ciberdelincuente travieso, el *ciberpunk* se dedica a alterar sistemas públicos —como una página web— para mofarse y ridiculizar a distintos usuarios.
d. *Insiders*: Son empleados o exempleados que actúan desde dentro de las propias compañías en las que trabajan o han trabajado para acceder, distribuir información confidencial o perjudicar de algún modo a sus empresas. Sus motivaciones suelen ser tanto económicas como personales, incluso con fines de venganza.
e. *Phisher, spammer*: Usuarios especializados en utilizar el correo electrónico como forma o vía de comunicación con sus víctimas. Intentan lograr un beneficio económico a través de engaños y señuelos que confunden a los cibernautas despistados, a los cuales se les muestran como fuentes aparentemente confiables.

El individuo que comete este tipo de actos punibles no es considerado un delincuente común, ya que se diferencia de este último en el mecanismo y en el medio empleado para producir el resultado. En este sentido, es importante mencionar que no existe un perfil individual para describir a estos ciberdelincuentes, aunque se ha intentado extraer una serie de características comunes (Garrido, Stangeland y Redondo, 2006). En otras palabras, se puede afirmar que las personas que cometen estas conductas delictivas poseen ciertos rasgos que los delincuentes tradicionales no tienen, es decir, disponen de altas habilidades en el manejo de sistemas informáticos y normalmente en su puesto de trabajo gozan de información de carácter sensible (Gallego, 2012).

En concordancia con esta idea, y según una investigación realizada en la Universidad de Yale para estudiar las características de los ciberdelincuentes, se ha demostrado que las personas que cometen fraudes informáticos reúnen las siguientes características: la mayoría son hombres de edad media mayor, casados y económicamente estables porque disponen de un puesto fijo de trabajo. Además, tienen un alto nivel de educación, buena consideración de sí mismos y no se consideran delincuentes (Garrido, Stangeland y Redondo, 2006, citados por Dinca, 2016). Igualmente, y tomando en consideración los estudios de tipo criminológico que se han ocupado de estudiar los perfiles de estos delincuentes, se puede decir que poseen unos conocimientos mínimos del medio informático, sin los cuales no podrían acceder a los distintos sistemas (De La Cuesta y Pérez Machío, 2010).

Otra de las características que hacen a las nuevas tecnologías atractivas para los ciberdelincuentes, en especial para cometer ciberataques de diferente tipo, es el efecto masivo que podrían conseguir con sus acciones. Por ejemplo, con el uso de troyanos en miles de ordenadores se pueden realizar ataques de forma simultánea con consecuencias realmente graves. Lo lamentable y paradójico de esta acción, sin embargo, se halla en que en muchos casos resulta muy difícil señalar al autor de los ataques, ya que existen técnicas que permiten camuflar y ocultar hasta cierto punto la dirección de algunos equipos (Roca, 2014).

Un tipo de ciberdelincuente particular es aquel que opera desde dentro de las empresas. Puede ser que estos no sean expertos en tecnología, pero conocen las vulnerabilidades en la seguridad tecnológica de una organización, lo cual es aprovechado para conseguir los datos que buscan. Entre estos delincuentes se hallan los *insiders*, los cuales pueden ser ejecutivos que cambian de trabajo y se llevan consigo en cualquier dispositivo de almacenamiento la base de datos de los clientes con quienes han trabajado (*Portafolio*, 2013). A continuación, se explican algunos de estos casos:

a. Personas con conocimientos de usuario y de redes que utilizan constantemente los ordenadores sin explicar qué hacen y sin compartir ese conocimiento. Estos incluso pueden menospreciar a los demás por su competencia informática.
b. Empleados que trabajan horas extras sin razón aparente, que no disfrutan de vacaciones o que no hacían uso frecuente de los ordenadores, pero que de manera súbita empiezan a usarlos sin motivo alguno.
c. Una situación de alerta se presenta cuando personas cuyas tareas laborales no se relacionan con los ordenadores (p. ej., encargados de limpieza) se encuentran en las oficinas utilizándolos.

d. Sujetos que aprovechan espacios sociales para interesarse por datos de clientes y demás información de uso restringido o particular.
e. Personal que instala programas espías sin autorización de la organización.
f. Sujetos que desactivan el *software* del antivirus en equipos de trabajo.
g. Personas que sin autorización utilizan ordenadores o dispositivos de los demás miembros de la organización.
h. Personas sin experiencia, pero que tienen el conocimiento sobre la vulnerabilidad de ciertos puntos en la seguridad tecnológica de la empresa, lo cual aprovechan para conseguir los datos que necesitan.

Siguiendo el estudio de Digiware (Gallo, 3 de mayo de 2016), en nuestros días los ciberdelincuentes ya no actúan de manera aislada, pues en muchos casos operan para grandes organizaciones criminales alrededor de todo el mundo, las cuales atacan unas 600 000 veces al día, en especial al sector financiero y a los gobiernos. Según Digiware, la mitad de las bandas dedicadas al cibercrimen están compuestas usualmente por seis o más personas, de las cuales 76 % son hombres cuyas edades oscilan entre los 14 (8 %) y los 50 años (11 %), con una media de 35 años (43 %). Sobre este aspecto, cabe resaltar que cerca de la mitad los ciberdelincuentes han realizado estas operaciones durante más de seis meses, mientras que 25 % lo ha hecho durante medio año o menos. Estas actividades son realizadas principalmente en Norteamérica y Sudamérica, con 19 % del total de ataques a escala mundial.

Digiware igualmente afirma que la mayoría de ataques efectuados en el interior de las empresas son cometidos por un *hacker* de forma premeditada y con intervención directa en los sistemas internos de las organizaciones. Estos accesos en 9.3 % se producen por negligencia de los colaboradores y en 7.3 % por accidentes de los integrantes de la empresa. Digiware destaca que los ataques a las marcas son los más utilizados por los delincuentes para rebajar el valor de las acciones o para afectar seriamente la imagen de las compañías a través de fraudes hacia sus clientes. También, se intenta interrumpir servicios digitales, como el bloqueo a accesos de correos electrónicos o *hackeos* de sitios web. Sobre estas acciones vale comentar que tienen diferentes tarifas; por ejemplo, 25 dólares por el robo de una cuenta de Skype o de 200 dólares por acceder a datos en redes sociales o extraer información de tipo profesional.

En definitiva, cualquier persona con conocimientos suficientes de informática e impulsado por ansias económicas puede prestar su labor a empresas de seguridad o usarlo para su propio beneficio. Asimismo, también es preocupante que el perfil de estos *black hats* se asocia de forma más frecuente a jóvenes y, principalmente, a menores de edad, lo que limita

el que asuman las consecuencias por sus hechos, ya que la responsabilidad penal de los menores (en el caso de España) se exige a las personas mayores de catorce años y menores de dieciocho años por la comisión de hechos tipificados como delitos o faltas en el Código Penal o en las leyes penales especiales.

En este contexto, se debe agregar que aún es difícil dibujar un perfil único del ciberdelicuente, lo cual se puede explicar por la íntima relación que comparte el ciberagresor con el ciberdelito, cuestión a la que hay que añadir la dificultad que presenta la persecución judicial de este tipo de delincuentes. Además, se debe destacar que la carencia de estudios criminológicos, cuantitativos y cualitativos sobre perfiles concretos no contribuye a ofrecer una única conclusión general (Miró, 2012).

Por ejemplo, y siguiendo a Di Piero (2012) en el caso del cibercriminal económico, este perfil no se corresponde con el de una persona individual y concreta, sino con el de una organización criminal, siendo el paradigma de esta ciberdelincuencia el *hacker*, sobre el que se explica la transformación que ha sufrido.

En el caso de la cibercriminalidad política, destaca la diferente organización que presenta en relación con los agentes delictivos del mundo físico, con acento sobre su organización horizontal, y no vertical, con un objetivo central al que se unen distintos sujetos que participan de ideologías sin que exista un alto conocimiento técnico de forma necesaria y, por tanto, prescindible. Igualmente, no se descarta la posible actuación individual fuera de toda relación organizativa. Finalmente, la cibercriminalidad social puede ser la más compleja debido a la existencia de múltiples motivaciones en el sujeto activo, aunque siempre con la singularidad que le otorga el ciberespacio.

Ciberterrorismo y ciberterroristas

Aunque diversos estudiosos consideran que ambos términos son equiparables, el ciberterrorismo trasciende a la ciberdelincuencia. De hecho, si bien es cierto que en varios aspectos estas palabras poseen cierta vinculación semántica, pues en múltiples ocasiones los ciberterroristas realizan actividades delictivas en la Red, las causas que motivan sus acciones y los beneficios que esperan recibir unos y otros son diferentes.

El ciberterrorismo es la confluencia del terrorismo y el ciberespacio, es decir, la manera en la que el terrorismo usa las tecnologías de la información para coaccionar, intimidar o causar daños a grupos sociales con fines políticos-religiosos. En otras palabras, viene a ser la evolución que resulta de cambiar las armas, las bombas y los misiles por un ordenador para planificar y ejecutar ataques que produzcan los daños más graves posibles a la población civil.

El ciberterrorismo, por ende, busca originar el mayor daño posible por razones normalmente político-religiosas, mientras que las acciones del cibercrimen están encaminadas a conseguir un beneficio principalmente de tipo económico (Sánchez Medero, 2012).

¿Cómo se puede conocer al ciberterrorista? Debido a su conocimiento de la técnica, en principio se pudiera considerar como una persona con un alto coeficiente intelectual, pero esta observación pudiera ser errada, pues el ciberterrorista puede llegar a actuar incluso sin poseer un perfil excelente en el manejo de la informática. Por ello, resultan ilustrativas las ideas de Patrón (2013), quien explica algunas cualidades del terrorista informático:

a. Es una persona que a través de sus acciones causa pánico y terror con la finalidad de debilitar y desacreditar a gobiernos, a la sociedad, a una creencia, etc.
b. Es un sujeto con un carácter estratégico, pues es capaz de captar tanto la atención como el apoyo de la comunidad (colegios, universidades, iglesias, etc.). En este caso, utiliza los medios informáticos y las redes sociales.
c. Es un sujeto que tiene claramente marcados sus objetivos tanto de ataque como de población diana (público objetivo).
d. Su perfil criminal está lejos del parámetro del "criminal de cuello blanco", como señalara el sociólogo estadounidense Edwin Sutherland (1943) para referirse a un criminal informático. Con el avance de los tiempos, pensar que solo las personas con alto poder adquisitivo pueden ser cibercriminales es cometer un claro error ante la perspectiva mundial y su avance progresivo. Cualquiera puede estar capacitado para ser un terrorista informático o para diseñar páginas web, pues solo se necesita un ordenador y la intención de aprender.
e. Es una persona con un fuerte resentimiento hacia la sociedad o un grupo dentro de ella, elemento clave para que en muchos casos surja el terrorismo.
f. Por último, conoce las maneras de atacar utilizando los diferentes medios informáticos. Este punto se entiende como el saber cuáles programas manejar, cómo captar a las personas a través de los medios informáticos y cómo llegar a sus diversos fines con el uso de la Red.

Ciberguerra

Antes de precisar qué es la ciberguerra se deben establecer sus diferencias con la ciberdelincuencia. Esta última se enfoca en atacar para conseguir una retribución económica o causar daños en las víctimas sin tener en cuenta alguna ideología activista (Pantano, 2014). La ciberguerra, en cambio, puede ser definida como un tipo de agresión promovida por un Estado y dirigida a dañar de forma grave las capacidades de otro Estado para imponerle la aceptación de un objetivo propio, para apropiase de determinada información o para alterar o destruir sus sistemas de comunicación y modificar sus bases de datos. En pocas palabras, la ciberguerra se vincula con lo que tradicionalmente se conoce como guerra, pero con la diferencia fundamental de que el medio empleado no sería la violencia física, sino un ataque digital que va desde "la infiltración en los sistemas informáticos enemigos para obtener información hasta el control de proyectiles mediante computadores, pasando por la planificación de las operaciones, la gestión del abastecimiento, etc." (Colle, 2000, *Guerra informática*, párr. 4). La ciberguerra, entonces, supone la utilización de todas las herramientas electrónicas e informáticas para derrumbar los sistemas electrónicos y de comunicación del enemigo y mantener operativos los medios propios (Sánchez, 2008).

Sin duda, el campo de batalla de la ciberguerra es el ciberespacio, lugar donde se establecen los elementos de poder. Es un ámbito en el que el beneficiado es el que toma la iniciativa. La oportunidad del actuar, de la respuesta y de la contrarrespuesta son variables de desbalance en la disuasión, donde la inacción facilita la escalada de la agresión de quien busca el efecto asimétrico como estrategia de acción (Arteaga, Ballesteros, Cerpa, Cervantes y Díaz, 2019). Para este fenómeno, por sus especiales características, no se han encontrado datos sobre los perfiles de sus distintos actores.

Conclusiones

Internet se ha convertido en un espacio perfecto para la implantación de la ciberdelincuencia y el ciberterrorismo, pues no suele estar regulado por ningún tipo de leyes bien definidas. Aunado a ello, estas prácticas delictivas se pueden desarrollar de forma anónima y con un altísimo impacto que se puede conseguir con poca inversión y riesgo para quien comete el crimen. En este sentido, vale recalcar que a pesar del trabajo realizado por las agencias o secretarias de seguridad de los Estados, es muy complicado garantizar la integridad de los sistemas informáticos.

Evidentemente, se pueden implementar acciones regulatorias como las impuestas en algunos países como China, Corea del Norte o Arabia Saudita, los cuales, paradójicamente, han sido acusados frecuentemente por realizar ciberataques. Asimismo, se podría optar por no conectarse a Internet, aunque esto sería casi impensable en la actualidad porque muchas de las actividades diarias se realizan gracias a ese medio digital. Por ello, pareciera que la opción más viable sería identificar las vulnerabilidades y los peligros potenciales para fortalecer los sistemas informáticos. Sin embargo, hasta el momento no parece que tengan resultados positivos el aumento del control de las comunicaciones o la creación de agencias específicas (cibervigilantes).

Aunado a ello, y de acuerdo con la documentación revisada, hasta el momento resulta complejo describir el perfil concreto de los ciberdelincuentes y los ciberterroristas, pues la información disponible solo sirve para ofrecer una simple descripción de características generales e imprecisas, lo cual es insuficiente para controlar o impedir la actividad de estas personas en la Red.

En todo caso, como se ha descrito a lo largo del presente trabajo, la ciberdelincuencia, el ciberterrorismo y los Estados se están volcando en la Web para ejercer, extender y desarrollar sus actividades aunque, desde luego, con objetivos y fines diferentes.

Los ciberdelincuentes usan la Red para dañar y bloquear con el propósito de conseguir una rentabilidad económica o alcanzar sus intereses fuera de la ley. En este sentido, los grupos terroristas están trasladando sus organizaciones difusas al ciberespacio porque de ese modo se pueden diluir en un lugar donde a las autoridades les resulta más complejo actuar. De esa forma, emplean la Red para financiarse, reclutar a otras personas, entrenarse, comunicarse, coordinarse, adoctrinarse, conseguir notoriedad, etc.

En este contexto, el ciberespacio se ha vuelto un campo de batalla con nuevas posibilidades para los delincuentes, ya que este tipo de agresiones se suelen caracterizar, a diferencia de los conflictos bélicos tradicionales, por su gran asimetría, corta duración,

reacción rápida, bajos costes económicos y menores daños físicos para los soldados. La ciberguerra, por tanto, es una manera de luchar de forma intensa no para doblegar físicamente al adversario, sino para dominar los sistemas rivales desde casi cualquier lugar y casi de forma indetectable. Esto significa que para la ciberguerra no se necesita tener un armamento sofisticado, un ejército numeroso y estar situado cerca del enemigo, pues solo basta con poseer un ordenador y determinados conocimientos informáticos para conseguir efectos tan devastadores como los alcanzados con la guerra tradicional. Sin embargo, y a pesar de estas posibilidades para generar daño en el rival, cabe destacar que por el momento tanto los países como los grupos terroristas parecen estar haciendo un uso pasivo de la Red, a excepción de los recursos propagandísticos que emplea Estado Islámico, otros grupos afines o los ciberdelincuentes.

En medio de estas circunstancias, resulta alarmante el informe anual de la empresa de seguridad McAfee, en el cual se ha vislumbrado la posibilidad de tener que enfrentar una "guerra fría cibernética". Esto quiere decir que la ciberguerra, la ciberdelincuencia y el ciberterrorismo son amenazas reales a las que se debe prestar atención a lo largo de este siglo XXI.

Para ello, es indispensable que cada usuario de la Red procure que la información que quiere transmitir llegue al destino elegido y sea usada de manera correcta o para el fin deseado. Esto implica adoptar mejores prácticas en el ciberespacio, así como emplear antivirus más potentes y mantener actualizado el *software* que se usa en Internet. Por ello, se debe ser consciente de que los ciberdelincuentes se pueden encontrar al acecho de cualquier víctima, sea una persona, una organización o un Estado.

Referencias

Arteaga, M., Ballesteros, M., Cerpa, O., Cervantes, D. y Díaz, H. (2019). *El pensamiento estratégico: una habilidad para anticiparse al futuro.* Chile: Centro de Estudios Estratégicos CEEAG. Recuperado de http://www.ceeag.cl/wp-content/uploads/2019/03/40603-TICA-3-EL-PENS-EST.pdf#page=88.

Colle, R. (2000). Internet: un cuerpo enfermo y un campo de batalla. *Revista Latina de Comunicación Social, 30.* Recuperado de http://www.revistalatinacs.org/aa2000qjn/91colle.htm.

De La Cuesta, J. L. y Pérez Machío, A. I. (2010). Ciberdelincuentes y cibervíctimas. En De La Cuesta, J. L. y De la Mata, N. J. (eds.), *Derecho penal informático* (pp.99-120). Navarra: Civitas Ediciones-Thomson Reuters.

Di Piero, C. (2012). *El cibercrimen. Fenomenología y criminología de la delincuencia en el ciberespacio*. Recuperado de http://www.indret.com/pdf/984.pdf.

Dinca, C. F. (2016). *Fraudes en internet* (trabajo final de grado). Universidad Jaime I de Castellón (España). Recuperado de http://repositori.uji.es/xmlui/bitstream/handle/10234/161252/TFG_2016_DincaClaudia.pdf?sequence=1.

Fernández-Rodríguez, J. C. and Miralles, F. (2016). The terrorist suicide woman in Jihadism. In Martín Ramírez, J. and Fernández-Rodríguez, J. C. (eds.), *Security in Infraestructures* (pp. 186-202). Newcastle: Cambridge Scholars Publishing.

Gallego, A. (2012). *Delitos informáticos: malware, fraudes y estafas a través de la Red y cómo prevenirlos* (proyecto fin de carrera). Universidad Carlos III de Madrid. Recuperado de http://e-archivo.uc3m.es/bitstream/handle/10016/16868/pfc_alberto_gallego_yuste.pdf?sequence=1.

Gallo, T. (3 de mayo de 2016). Conozca el perfil de un ciberdelincuente, según Digiware. *El Heraldo.* Recuperado de http://www.elheraldo.co/tecnologia/conozca-el-perfil-del-ciberdelincuente-258538.

Garrido, V., Stangeland, P. y Redondo, S. (2006). *Principios de criminología*. Valencia: Tirant lo Blanch.

González, A. y Campoy, P. (2018). Ciberacoso y cyberbullying: diferenciación en función de los precipitadores situacionales. *Revista Española de Investigación Criminológica*, *16*, 1-31.

Guilabert, N. G. (2016). Actividades cotidianas de los jóvenes en Internet y victimización por malware. *Revista de Internet, Derecho y Política*, (22), 59-72.

Gutiérrez, M. L. (2005). Reflexiones sobre la ciberdelincuencia hoy (en torno a la ley penal en el espacio virtual). *Revista Electrónica del Departamento de Derecho de la Universidad de La Rioja, REDUR, 3*(4). Recuperado de https://dialnet.unirioja.es/revista/2206/A/2005.

Leetaru, K. (2016). *What The Bangladesh SWIFT Hack Teaches About The Future Of Cybersecurity And Cyberwar*. Retrieved from http://www.forbes.com/sites/kalevleetaru/2016/04/30/what-the-bangladesh-swift-hack-teaches-about-the-future-of-cybersecurity-and-cyberwar/.

Mateos, I. (2013). *Ciberdelincuencia, desarrollo y persecución tecnológica* (trabajo final de grado). Universidad Politécnica de Madrid. Recuperado de http://oa.upm.es/22176/1/PFC_IVAN_MATEOS_PASCUAL.pdf.

McAfee (2016). *Informe de McAfee Labs sobre amenazas. Septiembre de 2016*. Recuperado de http://www.mcafee.com/es/resources/reports/rp-quarterly-threats-sep-2016.pdf.

Meseguer, J. (2013). Los nuevos modi operandi de los ciberdelincuentes durante la crisis económica. *Revista de Derecho UNED*, (12), 495-523. Doi: https://doi.org/10.5944/rduned.12.2013.11704

Ministerio del Interior (2017). *Estudio sobre la cibercriminalidad en España*. Recuperado de http://www.interior.gob.es/documents/10180/8859844/Informe+2017+sobre+Cibercriminalidad+en+Espa%C3%B1a.pdf/a9f61ddb-3fcf-4722-b9d8-802a424a1a70.

Miró, F. (2012). *El cibercrimen. Fenomenología y criminología de la delincuencia en el ciberespacio*. Madrid: Marcial Pons.

Pantano, A. (2014). *Ciberguerra.* Recuperado de https://dspace.palermo.edu:8443/dspace/bitstream/handle/10226/1448/Ciberguerra-Pantano%2068586.pdf?sequence=1&isAllowed=y.

Patrón, P. (2013). *Drogas informáticas y terrorismo informático. ¿Nuevos métodos de delito o mitos digitales?* Recuperado de http://www.derecho.usmp.edu.pe/cedetec/articulos.html.

Portafolio (2013). *Así es el perfil del ciberdelincuente en las empresas*. Recuperado de http://www.portafolio.co/tendencias/perfil-ciberdelincuente-empresas-67906.

Roca, J. (2014). *Cibercrimen y ciberterrorismo. ¿Exageración mediática o realidad?* (trabajo final de grado). Universidad Politécnica de Madrid. Recuperado de http://www.criptored.upm.es/guiateoria/gt_m078a.htm.

Sánchez, G. (2008). Ciberterrorismo: La guerra del siglo XXI. *El Viejo Topo*, (242), 15-24

Sánchez Medero, G. (2012). Cibercrimen, ciberterrorismo y ciberguerra: los nuevos desafíos del s. XXI. *Revista CENIPEC*, (31), 241-267. Recuperado de http://www.saber.ula.ve/handle/123456789/36770.

Sutherland, E. (1943). Juvenile Delinquency and Urban Areas: A Study of Rates of Delinquents in Relation to Differential Characteristics of Local Communities in American Cities. *American Journal of Sociology*, *49*, 100-101.

Rol de Contribución	**Autor (es)**
Conceptualización	Juan Carlos Fernández: principal, Fernando Miralles: principal Luis Millana: principal
Metodología	Juan Carlos Fernández: principal, Fernando Miralles: apoya Luis Millana: apoya
Software	Juan Carlos Fernández: principal, Fernando Miralles: principal Luis Millana: principal
Validación	Juan Carlos Fernández: principal, Fernando Miralles: principal Luis Millana: principal
Análisis Formal	Juan Carlos Fernández: principal, Fernando Miralles: principal Luis Millana: apoya
Investigación	Juan Carlos Fernández: principal, Fernando Miralles: principal Luis Millana: principal
Recursos	Juan Carlos Fernández: principal, Fernando Miralles: principal Luis Millana: principal
Curación de datos	Juan Carlos Fernández: principal, Fernando Miralles: principal Luis Millana: principal
Escritura - Preparación del borrador original	Juan Carlos Fernández: principal, Fernando Miralles: principal Luis Millana: principal
Escritura - Revisión y edición	Juan Carlos Fernández: principal, Fernando Miralles: principal Luis Millana: principal
Visualización	Juan Carlos Fernández: principal, Fernando Miralles: apoya Luis Millana: apoya
Supervisión	Juan Carlos Fernández: principal, Fernando Miralles: principal Luis Millana: principal
Administración de Proyectos	Juan Carlos Fernández: principal, Fernando Miralles: principal Luis Millana: principal
Adquisición de fondos	Juan Carlos Fernández: principal, Fernando Miralles: principal Luis Millana: principal