INTERNATIONAL E-JOURNAL OF CRIMINAL SCIENCES
Supported by DMS International Research Centre

¿Nos parecen más inseguros los ciberlugares después de un ciberataque?[1]

Francisco Javier Castro Toledo[2]
Investigador del Centro CRÍMINA para el estudio y prevención de la delincuencia, Universidad Miguel Hernández de Elche

Fernando Miró Llinares
Catedrático de Derecho Penal y Criminología de la Universidad Miguel Hernández de Elche y director del Centro CRÍMINA para el estudio y prevención de la delincuencia

Resumen

En la literatura sobre miedo al crimen en espacio físico existe una relación bien establecida entre las experiencias directas de victimización, las características ambientales del lugar de victimización y su impacto sobre el riesgo percibido de victimización futura. No obstante, en la actualidad son muy limitadas las evidencias sobre esta relación en el ciberespacio. Por ello, aquí vamos a presentar un innovador diseño de investigación experimental basado en la simulación de un ciberataque mediante *malware*. Los resultados apuntan en una doble dirección. Por un lado, que tanto el riesgo percibido de cibervictimización futuro como las medidas de autoprotección adoptadas no se distribuyen aleatoriamente en diferentes ciberlugares y, en segundo lugar, que la

[1] Este estudio ha recibido el apoyo del Instituto Nacional de Ciberseguridad (INCIBE) en el marco de las "Ayudas para la excelencia de los equipos de investigación avanzada en ciberseguridad" (ref. INCIBEI-2015-02480). Desarrollado en el marco del proyecto *Criminología, evidencias empíricas y Política criminal. Sobre la incorporación de datos científicos para la toma de decisiones en relación con la criminalización de conductas* (ref. DER2017-86204-R) financiado por el Mtª de Economía, Industria y Competitividad. Queremos agradecer a Miriam Esteve el diseño y programación del ciberataque simulado.
[2] Autor de correspondencia: Universidad Miguel Hernández de Elche. Avda. de la Universidad s/n. Edif. Hélike (CRIMINA), 03202, Elche (España). (+34) 966 65 84 06, fj.castro@crimina.es

INTERNATIONAL E-JOURNAL OF CRIMINAL SCIENCES
Supported by DMS International Research Centre

experiencia con el ataque en un ciberlugar específico parece extender tanto el riesgo percibido como el nivel de autoprotección a otros ciberlugares diferentes.

Palabras Clave: malware, riesgo percibido de cibervictimización, miedo al cibercrimen, ciberataques simulados, medidas de autoprotección

Abstract

In the literature on fear of crime in physical space, there is a well-established relationship between direct experiences of victimization, the environmental characteristics of the place of victimization and its impact on the perceived risk of future victimization. However, nowadays there is very limited evidence about this relationship in cyberspace. Therefore, here we present an innovative experimental research design based on the simulation of a malware cyberattack. The results point in a double direction. On the one hand, both the perceived risk of future cybervictimization and the self-protection measures adopted are not distributed randomly in different cyber-places and, secondly, the experience with the attack in a specific cyber-place seems to extend both the perceived risk and the level of self-protection to other different cyber-places.

Keywords: malware, perceived risk of cybervictimization, fear of cybercrime, simulated cyber-attacks, self-protection measures

Introducción

El riesgo percibido de victimización ha tenido un papel fundamental en la comprensión de los niveles de miedo al crimen de las personas. Tal es su relevancia que, frente al interés por la evaluación de la reacción emocional (Ferraro, 1995; Ferraro & LaGrange, 2000; Garofalo, 1981; Maguire, Johnson, Kuhns & Apostolos, 2017), y que configura el paradigma afectivista de aproximación al estudio del miedo al crimen, la introducción en la arena científica del riesgo percibido de victimización inauguró una comprensión de este fenómeno emocional en términos de evaluación cognitiva. Su principal consecuencia es que el miedo al crimen es definido como un estado mental

específico basado en una estructura evaluativa de eventos delictivos (Hale, 1996; Jackson, 2006; Lavenda, McLeigh & Katz, 2017; Rountree & Land, 1996). Ciertamente, este no es lugar para dirimir la interesante cuestión sobre las ventajas y desventajas en la elección de un paradigma de investigación u otro. Un hecho que, sin duda alguna, van a tener un impacto fundamental en la ontología del fenómeno (Castro-Toledo, Perea-García, Bautista-Ortuño, Mitkidis, 2017). Más bien, aquí vamos a adoptar una posición más aplicada, poniendo de relieve el interés existente por la relación entre las experiencias directas de victimización, las características ambientales del lugar de victimización y su impacto sobre el riesgo percibido de victimización futura. En virtud de ello, podemos afirmar que mientras esta relación ha sido bien establecida en la literatura criminológica cuando de espacio físico tradicional se trata, apenas ha recibido atención en el ciberespacio. Dicho esto, veamos antes de manera sucinta lo que ya sabemos respecto del espacio físico.

En primer lugar, las experiencias directas de victimización son desde los años 60 una de las primeras hipótesis propuestas más utilizadas en la explicación de los niveles de miedo al crimen. Son numerosas las investigaciones que han subrayado que la victimización directa modula el riesgo percibido de victimización futuro, ya que inician un proceso de redefinición del marco interpretativo de la peligrosidad de determinas situaciones (Akers, Greca, Sellers & Cochran, 1987; Cates, Dian & Schnepf, 2003; Ferraro, 1995; Hale, 1996; Katz, Webb & Amstrong, 2003; Smith and Hill, 1991; Skogan, 1990). Con mayor alcance teórico, Clark (2003) se inspira en el modelo de las tres realidades y explica que el impacto emocional derivado de un proceso de victimización responde a una triple fase: el derrumbe de la creencia de invulnerabilidad, la pérdida de confianza tanto en el orden social como hacia otras personas y, por último, la pérdida de autoestima causada por la autoestigmatización. Por el contrario, más allá de la evaluación de características intrínsecas al individuo particular, la investigación criminológica se ha interesado igualmente por otro tipo de elementos "no individuales" para la explicación de los niveles del miedo al crimen (Castro-Toledo y Miró-Llinares, en prensa), y que emergen de la interacción del sujeto con elementos de su entorno, ya sean ambientales o sociales. Respecto de los primeros, de modo muy sintético, podemos decir que los enfoques ambientales se han interesado en responder a la pregunta sobre por qué determinados espacios o lugares generan y/o concentran mayores experiencias de miedo al crimen. En otras palabras, qué constituye un *hot spot of fear* (Maltz, Gordon y Friedman, 1990), *hot spot of fear of crime* (Fisher & Nasar, 1995) o un enclave del miedo

(Buil-Gil, 2017). Para entender la distribución espacial del riesgo percibido de victimización y, por tanto, del miedo al crimen se han desarrollado, principalmente, dos tipos de explicaciones. La primera de ellas refiere a los desórdenes o incivilidades del lugar, poniendo de relieve la relación entre los niveles de miedo al crimen y la toma de contacto o la evaluación de las características físicas del ambiente, en especial, de aquellos signos físicos asociados a la actividad delictiva o a símbolos de ella (Hinkle, 2015; Kellings & Coles, 1997; Ross & Mirowsky, 1999; Salem & Lewis, 2016; Skogan & Maxfield, 1981). Asimismo, se han encontrado numerosas evidencias sobre otros elementos del espacio físico, dependientes del diseño urbanístico (ej. zonas verdes, iluminación, espacios abiertos, etc.) y que no están conectados directamente con la actividad criminal, pero sí despliegan capacidades para modular la experiencia emocional de los ciudadanos y su evaluación de la inseguridad de los espacios (Nasar & Fisher, 1993; Painter, 1996; Vozmediano y San Juan, 2010)

Pero, ¿sucede del mismo modo en el ciberespacio? Empecemos diciendo que si aceptamos que el ciberespacio es un nuevo ámbito de oportunidad criminal (Miró Llinares, 2011, 2012), parece que, en consecuencia, lo es también para elicitar experiencias de miedo al cibercrimen. Y, pese a que podría parecer una obviedad, aún son muy limitados los datos sobre si las explicaciones tradicionales propias del espacio físico mantienen su funcionalidad en contextos digitales, o si bien se dan elementos diferenciales para su estudio específico. Es más, si efectuásemos una búsqueda de "*fear of cybercrime*" en *Google Scholar* obtendríamos menos de un centenar de resultados, lo que hace tremendamente llamativo que un área como la cibercriminología, con una trayectoria tan importante, haya recibido tan poca atención en esta materia. De hecho, en la actualidad, las investigaciones han pivotado casi en exclusiva en torno a las explicaciones basadas en las experiencias previas de victimización, las vulnerabilidad sociales y económicas y las actividades cotidianas. Por ejemplo, desde la perspectiva de la cibercriminalidad social, los primeros trabajos de Alshalan (2006), así como con posterioridad Henson, Reyns & Fisher (2013) o Randa (2013), encontraron que las experiencias previas de interacción *online* en los que hayan mediado conductas de acoso, solicitudes sexuales, intimidación o amenazas de violencia son buenos predictores de los niveles de riesgo percibido de cibervictimización social futura. Más allá va el trabajo de Pereira, Spitzberg & Matos (2016), quienes además de hallar datos convergentes con las investigaciones anteriores, encontraron que la participación doble, como víctima y agresor, también aparece asociada a un mayor riesgo percibido de cibervictimización. Por

su parte, en lo que respecta a la cibercriminalidad económica, Virtanen (2017) ha mostrado recientemente cómo aquellas personas que han sido víctimas de infección de malware, suplantación de identidad digital, robo de datos personales o por fraude presentan mayores índices de riesgo percibido de cibervictimización futura. Unos años antes, Roberts, Indermaur & Spiranovic (2013) mostraron la misma tendencia en lo relativo a experiencias previas de robo de identidad digital.

En definitiva, mientras que la hipótesis de las experiencias directas o previas de victimización parece tener buen encaje en el estudio del miedo al cibercrimen, los enfoques ambientales parecen no haber tenido el mismo éxito. En realidad, podría resultar razonable pensar que este tipo de aproximaciones no tienen capacidad explicativa alguna para fenómenos de ocurrencia en el ciberespacio, ya que su punto de partida es la noción "lugar" físico. Sin embargo, recientes investigaciones (Miró-Llinares & Johnson, 2018) han señalado los enormes beneficios tanto fenoménicos como metodológicos que supone la adaptación del concepto "lugar" al ciberespacio para el análisis tanto de las conductas delictivas como de los procesos de cibervictimización. Como explican los autores, los rasgos arquitectónicos del ciberespacio son diferentes en su núcleo más esencial al del tradicional espacio físico, de ahí que la noción de lugar no tenga aplicabilidad en términos espaciales, pero sí como convergencia e interacción. Esto es lo genera las oportunidades para la ocurrencia y la comprensión de nuevas tipologías delictivas y de otras viejas ahora digitalizadas que, además, no se distribuyen aleatoriamente entre los diferentes ciberlugares, sino que responden a patrones específicos. Como resultado, al igual que sucede con la distribución espacial no aleatorizada del riesgo percibido de victimización, sospechamos que en el ciberespacio sucede algo similar. No obstante, aún no disponemos de suficiente información sobre esto.

Tomando en consideración esto último, el presente estudio piloto pretende responder a un doble objetivo. El primero de ellos recupera el debate antes señalado acerca de la relación entre las experiencias directas de victimización, las características ambientales del lugar de victimización y su impacto sobre el riesgo percibido de victimización futura, y si este impacto se limita a experiencias ambientalmente equivalentes o, por el contrario, amplia su alcance a otras. Se trata de un debate que, pese al enorme interés y atención que suscita la cibercriminología en la actualidad, aún no ha tenido suficiente cobertura en su homólogo digital. Es por ello que, en primer lugar, queremos comprobar si esta relación también se da en el ciberespacio. De ahí que con nuestra primera hipótesis (H1a)

pronostiquemos que aquellos participantes de la condición experimental presentarán un mayor incremento en sus niveles de riesgo percibido de cibervictimización tras la experiencia con el ciberataque por infección de *malware* simulado. Pero, al mismo tiempo, con nuestra hipótesis (H1b) sospechamos que no sólo van a verse incrementados los niveles de riesgo percibido de cibervictimización en el mismo lugar del ciberataque simulado, sino que la tendencia se va extender a otros entornos ambientalmente diferentes.

Como consecuencia de hipótesis similares a las anteriores, no son pocas las investigaciones que han explorado también si existe una relación entre las experiencias directas de victimización y la adopción de medidas de autoprotección en espacio físico (McConnel, 1997; Ortega & Myles, 1987). Trasladando esta idea al ciberespacio, nuestra hipótesis (H2a) predice que aquellos participantes de la condición experimental presentarán un mayor incremento en sus niveles de autoprotección futura tras la experiencia con el ciberataque por infección de *malware* simulado. Por otra parte, planteamos una segunda hipótesis (H2b) con la que, por coherencia con el enfoque de los ciberlugares propuesto con (H1b), sospechamos que en el grupo experimental la adopción de medidas de autoprotección frente a futuros ciberataques equivalentes se extenderá a entornos ambientalmente diferentes.

Método

Variables e instrumento

Para la consecución de los objetivos propuestos, se ha considerado que el ciberataque por infección de *malware* simulado sea la variable independiente en el presente estudio (véase *Procedimiento*). Dicho esto, para responder a las hipótesis (H1a) y (H1b) se ha hecho una evaluación pre-pos del riesgo percibido de cibervictimización por infección de malware en diferentes ciberlugares a partir de la pregunta "en las siguientes plataformas digitales, ¿cuánto riesgo dirías que hay de infectarse por un virus informático?" con una escala de hasta 10 puntos (0= riesgo muy bajo; 10= riesgo muy alto). De igual forma, para las hipótesis (H2a) y (H2b) se han analizado los niveles de autoprotección frente a esta modalidad de ciberataques en diferentes ciberlugares por medio de la pregunta "en las siguientes plataformas digitales, ¿con que frecuencia dirías que tomas precauciones para

evitar ser infectado por un virus informático?", utilizando una escala de hasta 10 puntos (0= nunca tomo precauciones; 10= siempre tomo precauciones). Cabe indicar que, para la evaluación posterior a la prueba presencial, la formulación de este ítem varía a "en las siguientes plataformas digitales, ¿con que frecuencia dirías que tomarás en adelante precauciones para evitar ser infectado por un virus informático?", con una escala equivalente (0= nunca tomaré precauciones; 10= siempre tomaré precauciones).

En ambos casos, se contextualizaron las preguntas a partir de la adaptación del concepto "lugar" al ciberespacio para el análisis tanto de las conductas delictivas como de los procesos de cibervictimización de Miró-Llinares & Johnson (2018), lo que nos permitió distinguir entre los siguientes ciberlugares:

a) Redes sociales como *Whatsapp, Telegram, Snapchat, Skype*, foros, etc., que permiten la comunicación en tiempo real.
b) Redes sociales como *Facebook, Twitter, Instragram, Youtube,* etc., que permiten, en mayor medida que las anteriores, el almacenaje de información.
c) Correos electrónicos enviados por contactos conocidos.
d) Correos electrónicos enviados por contactos desconocidos.
e) Páginas web de enlaces de descarga directa como *Mega, Pirate Bay, Ciudad Gamer, Taringa, Filiserve*, etc.
f) Páginas web de series o películas *online*.
g) Páginas web de juegos *online*
h) Programa de descarga como *Jdownloader, Torrent, Ares, aTube, Catcher*, etc.

Por último, y con objeto de controlar algunas variables del máximo interés para garantizar la equivalencia entre condiciones experimentales, se decidió incluir tres variables de actividades cotidianas en el ciberespacio de acuerdo con las propuestas de algunos recientes estudios en materia de miedo al cibercrimen (Virtanen, 2017). En este sentido, se preguntó "habitualmente, ¿con qué frecuencia dirías que has ACCEDIDO a las siguientes plataformas digitales?"; a continuación, "habitualmente, ¿con qué frecuencia dirías que has ABIERTO ENLACES de las siguientes plataformas digitales?; y, por último, "habitualmente ¿con qué frecuencia dirías que has DESCARGADO ARCHIVOS de las siguientes plataformas digitales? En todos los casos, fueron evaluadas con una escala Likert de 4 niveles (0= Nunca; 1= Rara vez; 2= Frecuentemente; 3= Siempre).

Igualmente, se consideró adecuado controlar el nivel de conocimiento en informática de los participantes debido a la relación entre la posesión de conocimientos especiales, el control de la situación y el riesgo percibido de cibervictimización (Roberts et al., 2013). Para ello, se operativizó con una escala de hasta 10 puntos (0= no tengo ningún conocimiento en informática; 10= soy un experto en informática) a partir de la pregunta "¿Cuál diría que es su grado de conocimiento en materia de informática?".

Participantes

La muestra final de este estudio piloto (n= 14) estuvo compuesta por 11 mujeres (78,6%) y 3 hombres (21,4%) con una edad media de 24,86 (*DT*= 5,93; *Min*= 19; *Max*= 42), quienes fueron reclutados a través de una entrada del blog de la web oficial del centro CRÍMINA[3] y participaron a cambio de formar parte en un sorteo de dos paquetes de experiencias. Además, con el propósito de naturalizar lo máximo posible la experiencia de cibervictimización, se exigió como criterio de elegibilidad para poder formar parte del estudio tener un ordenador portátil personal con sistema operativo *Windows* que pudiesen traer a la prueba presencial.

Diseño

Nuestra propuesta responde a un diseño experimental de investigación en el que los participantes fueron asignados de manera aleatoria a dos condiciones experimentales. Respecto al grupo experimental, estos realizaron la tarea presencial bajo la influencia temporal de un ciberataque por infección de *malware* simulado. Por otra parte, dada la importancia de la equivalencia entre grupos, fue con la realización del pretest *online* cuando se pudo recoger información acerca de las variables de actividades cotidianas en el ciberespacio y de conocimientos especiales en informática. Sobre las primeras respecto del ciberlugar seleccionado para la prueba presencial (i.e. webs de enlaces, véase

[3] http://crimina.es/blog/2017/05/11/crimina-necesita-participantes-para-un-estudio-en-persona-sobre-uso-seguro-de-las-tic/

Procedimiento), podemos afirmar que no existen diferencias estadísticamente significativas entre grupos en ninguna de las tres variables. En orden de mayor a menor diferencia, sólo descriptiva, la frecuencia de descargas ocupa la primera posición (U= 19,500; p= 0,475), la frecuencia de abrir enlaces la segunda (U= 23,000; p= 0,830) y, en tercera posición, la frecuencia de acceso (U= 24,500; p= 1,000). Más aún, por lo que respecta a los conocimientos especiales, ambos grupos han mostrado la misma media de 5,86, aunque desviaciones típicas diferenciales (DT_{Con}= 2,673; DT_{Exp}= 1,574).

Procedimiento

El primer paso fue la construcción de una herramienta informática con una función triple: 1) hacer creer al participante que era un *software* de monitorización de la actividad del ratón y de grabación de la prueba; 2) instalar subrepticiamente el ciberataque para que se manifestase a partir del momento temporal 2:30, abriendo durante 30 segundos, a pantalla completa, una pantalla de MS-DOS cada 10 milisegundos que incluía mensajes de error en color verde, consumiendo la RAM del dispositivo e inhabilitándolo para su uso durante el ataque; y 3) limitar la duración de la prueba a 5 minutos.

En segundo lugar, con la distribución del pretest *online* una semana antes de la prueba presencial, y desde la toma en consideración de nuestras anteriores experiencias respecto a la selección del lugar que presenta mayor tasa de riesgo percibido de victimización (Castro-Toledo et al., 2017) (véase *Tabla 1*), el presente experimento se desarrolló en el portal ruso de enlaces de descarga directa de libros *Library Genesis*[4], y que consideramos perteneciente a la categoría E, correspondiente a las páginas web de enlaces de descarga directa (M= 8,50; DT= 2,103). Cabe subrayar, incluso, que ambas condiciones experimentales puntuaron de manera muy similar en esta variable, pero más concretamente a la referida al ciberlugar de nuestro interés (M_{Con}=8,86 y DT=0,459; M_{Exp}=8,14 y DT= 1,056). Todo ello contribuye a enfatizar aún más la equivalencia entre grupos.

[4] http://gen.lib.rus.ec/

INTERNATIONAL E-JOURNAL OF CRIMINAL SCIENCES
Supported by DMS International Research Centre

Tabla 1. *Resumen del riesgo percibido de cibervictimización por infección de malware en cada ciberlugar (ordenado de menor a mayor media)*

Ciberlugar	M	DT	Mín	Máx
C	5,00	3,374	0	9
B	5,71	2,730	0	9
A	5,86	2,742	0	9
D	8,14	1,748	5	10
G	8,21	1,718	4	10
F	8,29	1,637	5	10
H	8,36	2,590	0	10
E	8,50	2,103	2	10

Una semana después se recibió a los participantes en las instalaciones del centro CRÍMINA para el estudio y prevención de la delincuencia. Tratando de ocultar los objetivos reales de la investigación, se les explicó que el propósito del estudio era evaluar rutinas de uso seguro de las Tecnologías de la Información y la Comunicación a partir de la realización de una búsqueda de los contenidos que quisieran en la web *Library Genesis*. Como tarea confundidora, se les pidió que recogieran en una hoja de registro su impresión acerca de la seguridad de los diferentes enlaces que arrojaba su búsqueda. El objetivo era ocupar el tiempo suficiente para que el ciberataque se pudiese manifestar en el grupo experimental. Finalmente, tras finalizar la prueba presencial, se les administró un segundo cuestionario para evaluar las variables de interés de la investigación (véase *Variables e instrumento*).

Resultados

Nuestra primera hipótesis (H1a) predecía que los participantes de la condición experimental presentarán un mayor incremento en sus niveles de riesgo percibido de

cibervictimización tras la experiencia con el ciberataque por infección de *malware* simulado. En efecto, tras aplicar la prueba de rangos con signos de Wilcoxon, podemos decir que mientras que en el grupo control no se observan diferencias estadísticamente significativas en el riesgo percibido de cibervictimización en las webs de enlaces entre los datos recogidos una semana antes de la prueba presencial y una vez finalizada (Z= -,687; p= 0,492), sí que existe en el grupo experimental con 6 rangos positivos y un empate (Z= -2,333; p= 0,20). Cabe decir, pues, que podemos aceptar nuestra hipótesis (H1a).

Por su parte, con respecto a nuestra hipótesis (H1b), esta pronosticaba que no sólo van a verse incrementados los niveles de riesgo percibido de cibervictimización en el mismo lugar del ciberataque simulado (i.e. webs de enlaces), sino que la tendencia extendería a otros entornos ambientalmente diferentes. En este sentido, ya desde una perspectiva meramente exploratoria, o incluso atendiendo a los descriptivos, podemos percatarnos sobre cómo los polígonos que se han dibujado en los *Gráficos 1* y *Gráfico 2* son diferentes: mientras que en el grupo control la línea correspondiente al riesgo percibido de cibervictimización tras la prueba presencial cae siempre por debajo de la línea del pretest, en el grupo experimental sucede más bien lo contrario. Dicho de otro modo, mientras que en el grupo control parece incluso que mejora esta variable de manera casi general tras la experiencia, y en especial respecto de los videos *streaming* (Z= -2,014; p= 0,044) *y* los juegos *online* (Z= -2,414; p= 0,016), en el grupo experimental la tendencia descriptiva es la opuesta y en el sentido de nuestra hipótesis, pese a no poder ser aceptada. Así, los análisis de contraste nos indican que en el grupo experimental sólo hay un incremento casi estadísticamente significativo de esta variable respecto de los programas de descarga (Z= -1,857; p= 0,63).

Todos los datos relativos a ambas hipótesis (H1a) y (H1b) se resumen a continuación para el grupo control en el *Gráfico 1* y la *Tabla 2*, y para el grupo experimental en el *Gráfico 2* y la *Tabla 3*.

INTERNATIONAL E-JOURNAL OF CRIMINAL SCIENCES
Supported by DMS International Research Centre

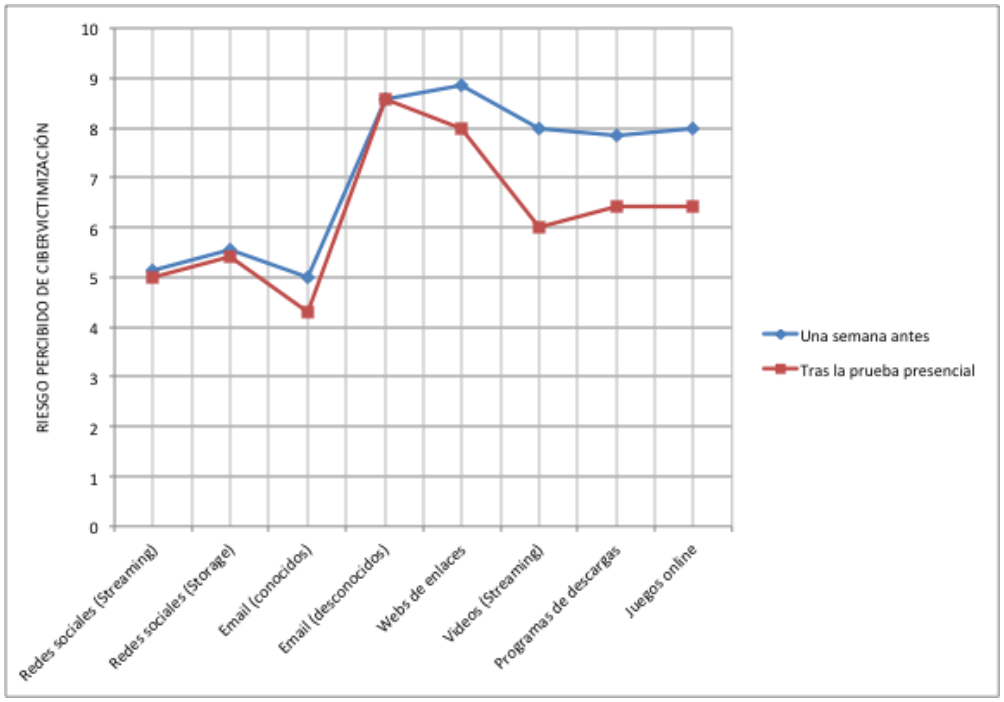

Gráfico 1. Medias del riesgo percibido de cibervictimización por infección de *malware* en cada ciberlugar (Grupo control)

Tabla 2. *Resumen del riesgo percibido de cibervictimización por infección de malware en cada ciberlugar (Grupo control)*

Ciberlugar	Fase del diseño	M	DT	Min	Max
Redes sociales (*Streaming*)	Una semana antes	5,14	3,132	0	9
	Tras la prueba presencial	5	2,449	3	9
Redes sociales (*Storage*)	Una semana antes	5,57	2,573	0	7
	Tras la prueba presencial	5,43	3,259	0	10
Email (conocidos)	Una semana antes	5	3,559	0	9
	Tras la prueba presencial	4,29	1,976	2	7
Email (desconocidos)	Una semana antes	8,57	1,988	5	10
	Tras la prueba presencial	8,57	1,512	6	10
Webs de enlaces	Una semana antes	8,14	2,795	2	10
	Tras la prueba presencial	8	1,528	6	10
Videos (*Streaming*)	Una semana antes	8	1,826	5	10
	Tras la prueba presencial	6	0,816	5	7
Programas de descargas	Una semana antes	7,86	3,579	0	10
	Tras la prueba presencial	6,43	0,976	5	8
Juegos online	Una semana antes	8	1,291	6	10
	Tras la prueba presencial	6,43	0,976	5	8

INTERNATIONAL E-JOURNAL OF CRIMINAL SCIENCES
Supported by DMS International Research Centre

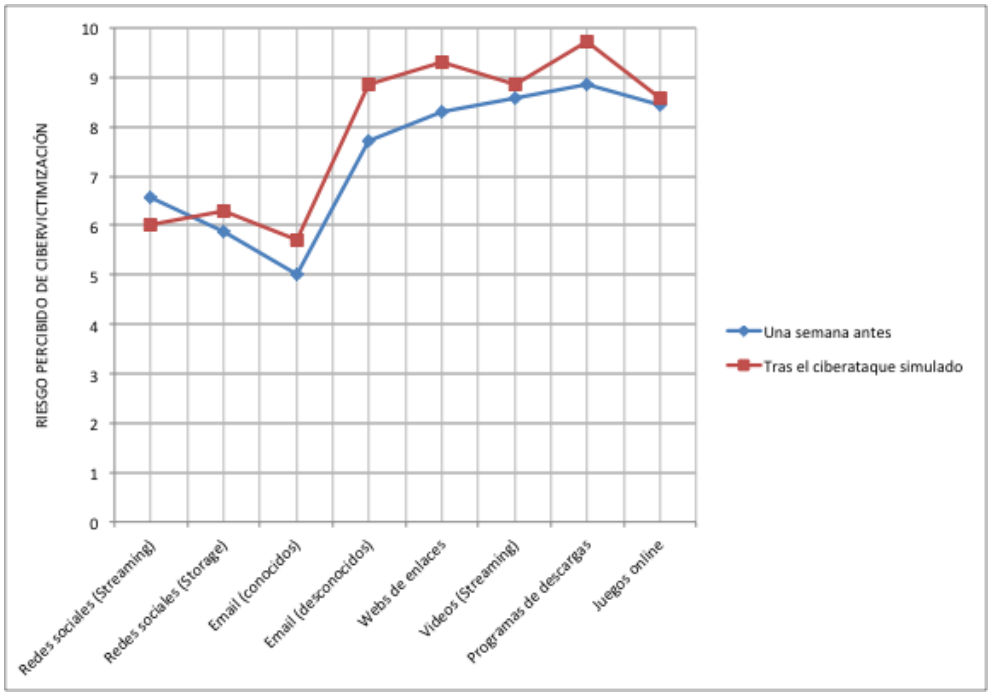

Gráfico 2. Medias del riesgo percibido de cibervictimización por infección de *malware* en cada ciberlugar (Grupo experimental)

Tabla 3. *Resumen del riesgo percibido de cibervictimización por infección de malware en cada ciberlugar (Grupo experimental)*

Ciberlugar	Fase del diseño	M	DT	Min	Max
Redes sociales (*Streaming*)	Una semana antes	6,57	2,299	2	8
	Tras el ciberataque simulado	6	1,826	3	8
Redes sociales (*Storage*)	Una semana antes	5,86	3,078	0	9
	Tras el ciberataque simulado	6,29	1,799	4	9
Email (conocidos)	Una semana antes	5	3,464	0	9
	Tras el ciberataque simulado	5,71	2,36	2	9
Email (desconocidos)	Una semana antes	7,71	1,496	6	10
	Tras el ciberataque simulado	8,86	1,069	7	10
Webs de enlaces	Una semana antes	8,29	0,756	7	9
	Tras el ciberataque simulado	9,29	0,756	8	10
Videos (*Streaming*)	Una semana antes	8,57	1,512	6	10
	Tras el ciberataque simulado	8,86	0,9	8	10
Programas de descargas	Una semana antes	8,86	1,069	8	10
	Tras el ciberataque simulado	9,71	0,488	9	10
Juegos online	Una semana antes	8,43	2,149	4	10
	Tras el ciberataque simulado	8,57	2,149	4	10

Una vez vistas las hipótesis relativas al riesgo percibido de cibervictimización, en lo que sigue analizaremos el segundo conjunto de hipótesis. Si recordamos, nuestra hipótesis (H2a) predecía que aquellos participantes de la condición experimental presentarán un mayor incremento en sus niveles de autoprotección futura tras la experiencia con el ciberataque por infección de *malware* simulado. Siguiendo la misma estrategia de análisis de datos con la prueba de rangos con signos de Wilcoxon, los resultandos nos indican que mientras el grupo control no muestra diferencias estadísticamente significativas respecto del nivel de autoprotección frente a ciberataques por *malware* una semana antes y tras la prueba presencial en un entorno de webs de enlaces (Z= -1,023; p= 0,141), sí que esta diferencia es enorme en el grupo experimental con 7 rangos positivos (Z= -2,384; p= 0,017), lo que nos permite aceptar, en consecuencia, nuestra hipótesis (H2a).

Por otra parte, también se planteó otra segunda hipótesis (H2b) con la que, por coherencia con (H1b), extendíamos nuestra sospecha de que en el grupo experimental la adopción de medidas de autoprotección frente a futuros ciberataques equivalentes se extendería a entornos ambientalmente diferentes. Algo similar ha sucedido en esta ocasión, ya que, desde una perspectiva descriptiva, observamos que tanto en el grupo

control como en el grupo experimental la línea correspondiente a los valores posteriores a la prueba presencial son en todos los ciberlugares más altos. No obstante, cabe subrayar que mientras no existe significancia estadística alguna en el grupo control, en el grupo experimental el incremento de los valores de medidas de autoprotección a otros ciberlugares es muy pronunciada. Más concretamente, los resultados aprecian diferencias relevantes en los siguientes ciberlugares: email enviado por desconocidos (Z= -2,214; p= 0,027), vídeos en *streaming* (Z= -2,214; p= 0,027), programas de descargas (Z= -2,371; p= 0,018) y juegos *online* (Z= -2,214; p= 0,027). De acuerdo con estos contrastes, podemos aceptar parcialmente nuestra hipótesis (H2b).

Asimismo, todos los datos descriptos relativos a las hipótesis (H2a) y (H2b) se resumen a continuación para el grupo control en el *Gráfico 3* y la *Tabla 4*, y para el grupo experimental en el *Gráfico 4* y la *Tabla 5*.

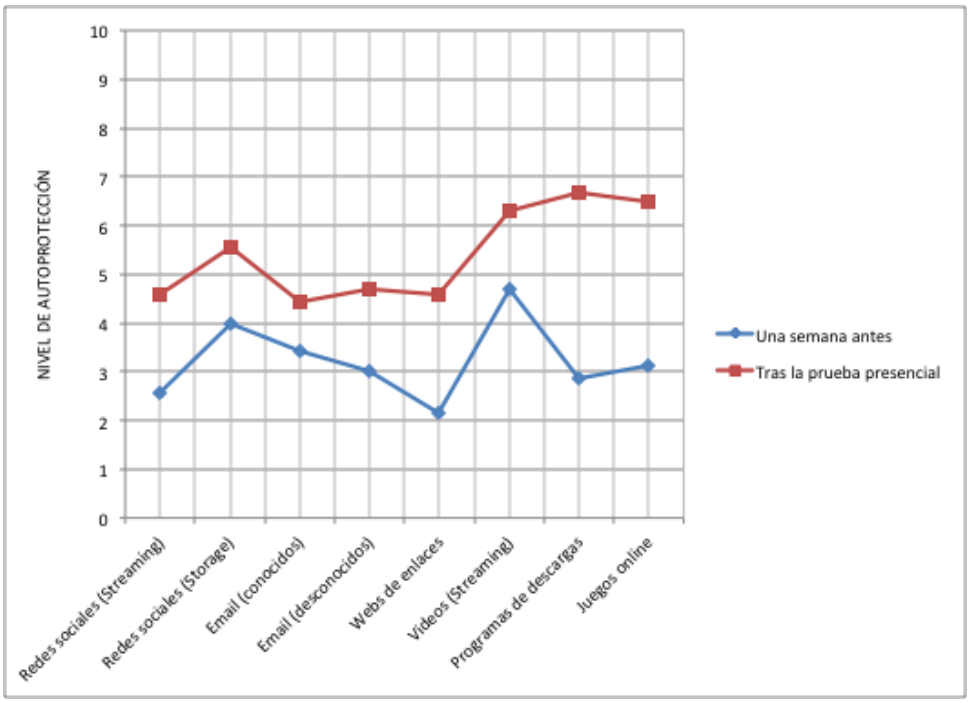

Gráfico 3. Medias del nivel de medida de autoprotección frente a ciberataques por infección de *malware* en cada ciberlugar (Grupo control)

INTERNATIONAL E-JOURNAL OF CRIMINAL SCIENCES
Supported by DMS International Research Centre

Tabla 4. *Resumen del nivel de medida de autoprotección frente a ciberataques por infección de malware en cada ciberlugar (Grupo control)*

Ciberlugar	Fase del diseño	M	DT	Min	Max
Redes sociales (Streaming)	Una semana antes	2,57	2,44	0	6
	Tras la prueba presencial	4,57	3,359	0	9
Redes sociales (Storage)	Una semana antes	4	3,512	0	9
	Tras la prueba presencial	5,57	3,867	0	10
Email (conocidos)	Una semana antes	3,43	2,82	0	9
	Tras la prueba presencial	4,43	3,409	0	9
Email (desconocidos)	Una semana antes	3	3,416	1	8
	Tras la prueba presencial	4,71	2,563	3	10
Webs de enlaces	Una semana antes	2,14	3,338	0	7
	Tras la prueba presencial	4,57	2,936	2	10
Videos (Streaming)	Una semana antes	4,71	3,904	0	9
	Tras la prueba presencial	6,29	1,38	4	8
Programas de descargas	Una semana antes	2,86	2,795	0	7
	Tras la prueba presencial	6,67	1,966	4	10
Juegos online	Una semana antes	3,14	4,018	0	9
	Tras la prueba presencial	6,5	1,378	4	8

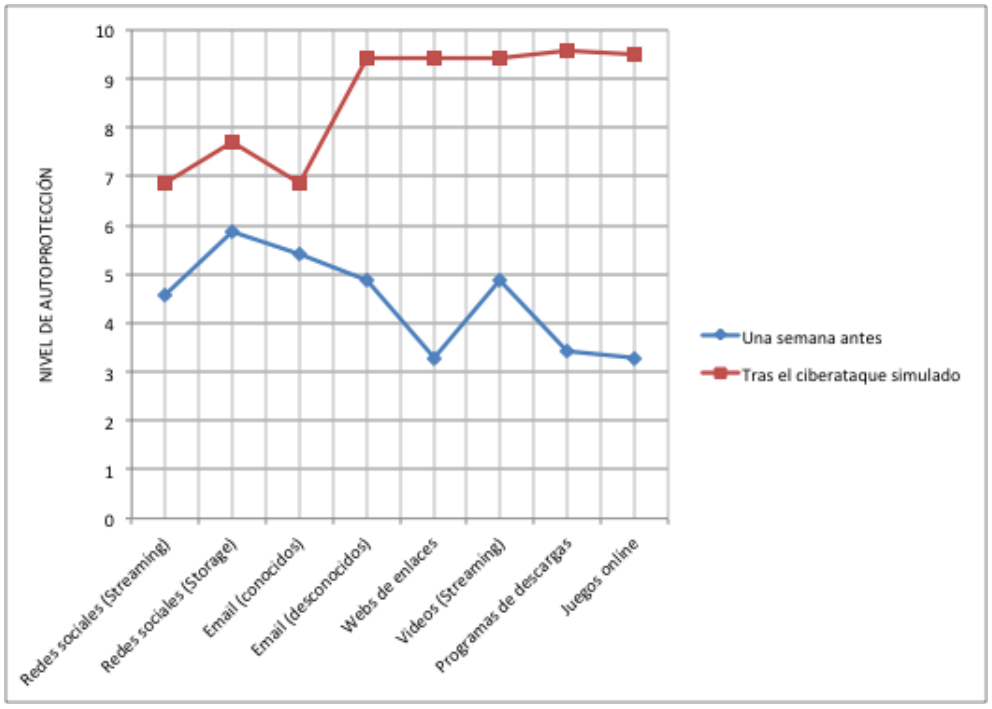

Gráfico 4. Medias del nivel de medida de autoprotección frente a ciberataques por infección de *malware* en cada ciberlugar (Grupo experimental)

INTERNATIONAL E-JOURNAL OF CRIMINAL SCIENCES
Supported by DMS International Research Centre

Tabla 5. *Resumen del nivel de medida de autoprotección frente a ciberataques por infección de malware en cada ciberlugar (Grupo experimental)*

Ciberlugar	Fase del diseño	M	DT	Min	Max
Redes sociales (Streaming)	Una semana antes	4,57	3,309	1	9
	Tras el ciberataque simulado	6,86	1,952	4	10
Redes sociales (Storage)	Una semana antes	5,86	3,132	1	9
	Tras el ciberataque simulado	7,71	1,604	5	10
Email (conocidos)	Una semana antes	5,43	3,409	1	9
	Tras el ciberataque simulado	6,86	3,436	1	10
Email (desconocidos)	Una semana antes	4,86	4,018	1	9
	Tras el ciberataque simulado	9,43	0,787	8	10
Webs de enlaces	Una semana antes	3,29	3,302	1	9
	Tras el ciberataque simulado	9,43	0,787	8	10
Videos (Streaming)	Una semana antes	4,86	4,018	1	9
	Tras el ciberataque simulado	9,43	0,787	8	10
Programas de descargas	Una semana antes	3,43	3,69	0	9
	Tras el ciberataque simulado	9,57	0,787	8	10
Juegos online	Una semana antes	3,29	4,152	0	9
	Tras el ciberataque simulado	9,5	0,837	8	10

Discusión

Con el presente estudio, hemos tenido la oportunidad de comprobar, desde una propuesta de diseño de investigación experimental, cómo la hipótesis tradicional de la victimización directa sigue siendo funcional en la explicación de los niveles del riesgo percibido de victimización futura en el ciberespacio. En nuestro caso, la literatura en materia de cibervictimización por infección de *malware* apunta, de manera general, en el sentido de nuestros resultados. Así, Mesko & Bernik (2011), con un enfoque que combina experiencias previas de victimización y actividades cotidianas en el ciberespacio, encontraron que el 57,8% de su muestra había sufrido un ciberataque por virus informático y, en consecuencia, era la modalidad que concentraba mayores tasas de riesgo percibido de cibervictimización futura. En la misma línea, Riek, Böhme & Moore (2014) encontraron datos convergentes sobre la relación entre estas variables, aunque cabe señalar que para los autores el miedo al cibercrimen y el riesgo percibido de cibervictimización son fenómenos diferentes, pero estrechamente conectados. Más recientemente, Brunton-Smith (2017) analizaron diferentes experiencias previas de cibervictimización en Gales e Inglaterra y hallaron que la infección por *malware* es, aparte de ser uno de los ciberataques más prevalentes, una de las principales fuentes de preocupación por el cibercrimen. Por su parte, desde las primeras propuestas prácticas para el desarrollo de políticas de prevención del cibercrimen de Moitra (2005) o de Henson (2011), la literatura científica es aún escasa respecto del segundo conjunto de hipótesis sobre medidas de autoprotección en el ciberespacio. Cabe mencionar en nuestro país una de las primeras investigaciones, sino la primera, sobre el miedo al crimen en entornos digitales, y fue la desarrollada por San Juan, Vozmediano, Vergara & Lenneis (2013). De acuerdo con sus resultados, existe una mayor percepción de invulnerabilidad en contextos digitales en comparación al espacio físico, y esto modula las diferentes medidas de autoprotección que pone en funcionamiento el sujeto para afrontar las consecuencias de una potencial cibervictimización.

No obstante, lo interesante de nuestra propuesta, más allá de ofrecer resultados consistentes con la literatura, reside en un doble aspecto. En primer lugar, el diseño responde a una comprensión del ciberespacio desde la adaptación del concepto de lugar, lo que permite hablar de la existencia de diferentes tipos de ciberlugares (Miro-Llinares & Johnson, 2018). De ahí que, en el ciberespacio, tal y como sucede en el espacio físico (véase *Introducción*), no se da una distribución aleatoria de los niveles de riesgo percibido

de cibervictimización en diferentes ciberlugares. O lo que es lo mismo, los participantes perciben que las probabilidades de ser víctimas de un ciberataque por infección de *malware,* y en consecuencia el nivel de autoprotección que van a adoptar, no son las mismas a causa de un email enviado por un contacto conocido que en una web de enlaces o en un programa de descarga, sólo por utilizar aquellos ciberlugares que presentan mayor polarización en esta variable. Esto es del máximo interés por sí mismo, pero es que, además, hemos observado, aun siendo de modo muy exploratorio por el momento, pero constituyendo unos resultados muy prometedores, cómo una experiencia de ciberataque en un ciberlugar específico parece contagiar su efecto en ambas variables sobre otros ciberlugares diferentes, o al menos en algunos de ellos. Aquí cabría preguntarse por las razones que motivan esta expansión, y pese a no disponer aún de datos suficientes, podemos sospechar que, en cierto sentido, existe una equivalencia ambiental que, tras ser enfrentada por los participantes, elicita reacciones emocionales y cognitivas similares. Esto, sin duda alguna, debe ser explorado con mayor detenimiento en futuras investigaciones.

El segundo de los elementos de interés de nuestra propuesta lo constituye la utilización de entornos de ciberataques simulados para la evaluación de fenómenos de interés criminológico. Ciertamente, esta estrategia metodológica está inexplorada en ciencias del crimen, y ello pese a tener una mayor saliencia en otros campos de la ciberseguridad. Sólo por mencionar algunos ejemplos de investigaciones que han trabajado directamente sobre la simulación de ciberataques por *malware,* Lesczyna, Fovino & Masera (2010) desarrollaron el *MAlSim-Mobile Agent* para reproducir el comportamiento de diferentes tipos de *malware* con objeto de hacer evaluaciones de seguridad de los sistemas de información. En una línea similar, aunque centrada en el ámbito de la ciberdefensa, Aybar, Singh & Shaffer (2018) presentan varios prototipos para la prueba de ciberataques. En su caso, parten de una revisión de las diferentes herramientas evaluadoras de vulnerabilidades en redes de estructuras críticas, integrándolas en el *Malicious Activity Simulation Tool* (MAST) que fue posteriormente utilizado para simular una red de ciberataques de este tipo.

Finalmente, también somos conscientes que el alcance de los resultados de nuestra propuesta podría incomodar a aquellos lectores preocupados por los tamaños muestrales. Es razonable pensar que, en la actualidad, la representatividad de los datos se haya convertido en un mantra entre los investigadores, pese a las enormes dificultades prácticas

que ello implica. No obstante, es importante poner de relieve que en los diseños experimentales la mayor o menor calidad de la investigación no radica únicamente el número de participantes que finalmente conforman la muestra. Nos referimos más específicamente a elementos que como la equivalencia entre grupos, el control de variables extrañas, la replicabilidad, la validez externa u otros que, de ser inobservados, van a poner en riesgo el alcance del trabajo, y que ningún incremento del tamaño muestral va a solucionar. En este sentido, mientras que debemos seguir trabajando por mejorar lo segundo, respecto de todo lo demás hemos sido especialmente concienzudos y cautelosos. En definitiva, podemos aseverar que, más de medio siglo después, y con la introducción del ciberespacio y sus peculiaridades, el miedo al crimen y sus fenómenos asociados, como el riesgo percibido de victimización, necesitan ser repensandos a la luz de su relación con las nuevas tecnologías, situándolos como uno de los tópicos criminológicos con mayor vigencia.

Referencias

Akers, R. L., Greca, A. J., Sellers, C., & Cochran, J. (1987). Fear of crime and victimization among the elderly in different types of communities. *Criminology, 25*(3), 487-506.

Alshalan, A. (2006). *Cyber-crime fear and victimization: An analysis of a national survey*. Mississippi: Mississippi University

Aybar, L., Singh, G., & Shaffer, A. (2018, March). Developing Simulated Cyber-Attack Scenarios Against Virtualized Adversary Networks. In *ICCWS 2018 13th International Conference on Cyber Warfare and Security* (p. 1).

Bernik, I., & Mesko, G. (2012, January). Study of the Perception of Cyber Threats and the Fear of Cybercrime. In *Proceedings of the 7th International Conference on Information Warfare and Security: ICIW* (p. 27). Academic Conferences Limited

Brunton-Smith, I. (2017). Worry about cybercrime in England and Wales. *The Routledge International Handbook on Fear of Crime*.

Buil-Gil, D. (2017). Un enfoque para el estudio ambiental del miedo al crimen: Aproximación Integradora al Enclave del Miedo (AIEM).*Revista electrónica de ciencia penal y criminología, 19*, 4.

Castro-Toledo, F. J., Perea-García, J. O., Bautista-Ortuño, R., & Mitkidis, P. (2017). Influence of environmental variables on fear of crime: Comparing self-report data with physiological measures in an experimental design. *Journal of Experimental Criminology, 13*(4), 537-545.

Castro-Toledo, F. J. y Miró Llinares, F. (en prensa). El miedo al crimen cincuenta años después. Vigencia y alcance de uno de los constructos criminológicos más analizados. *Cuadernos de Política Criminal.*

Cates, J. A., Dian, D. A., & Schnepf, G. W. (2003). Use of protection motivation theory to assess fear of crime in rural areas. *Psychology, Crime and Law, 9*(3), 225-236.

Clark, J. (2003). Fear in fear-of-crime. Psychiatry, *Psychology and Law, 102*, 267–282.

Ferraro, K. F. (1995). *Fear of crime: interpreting victimisation risk*. Albany, NY: State University of New York Press

Ferraro, K. F. & R. LaGrange (2000). The measurement of fear of crime. In J. Ditton and S. Farrall (Eds.), *The fear of crime*. (pp. 277-308). Ashgate, Aldershot.

Fisher, B., & Nasar, J. L. (1995). Fear spots in relation to microlevel physical cues: Exploring the overlooked. *Journal of Research in Crime and Delinquency, 32*(2), 214-239.

Garofalo, J. (1981). The fear of crime: causes and consequences. *Journal of Criminal Law and Criminology, 72*(2), 839.

Hale, C. (1996). Fear of crime: a review of the literature. International Review of *Victimology 4*, 79–150.

Henson, B., Reyns, B. W., & Fisher, B. S. (2013). Fear of crime online? Examining the effect of risk, previous victimization, and exposure on fear of online interpersonal victimization. *Journal of Contemporary Criminal Justice*, *29*(4), 475-497

Hinkle, J. C. (2015). Emotional fear of crime vs. perceived safety and risk: Implications for measuring "fear" and testing the broken windows thesis. *American Journal of Criminal Justice*, *40*(1), 147-168.

Katz, C. M., Webb, V. J., & Armstrong, T. A. (2003). Fear of gangs: A test of alternative theoretical models. *Justice Quarterly*, *20*(1), 95-130.

Kelling, G. L., & Coles, C. M. (1997). *Fixing broken windows: Restoring order and reducing crime in our communities*. London: Simon and Schuster.

Lavenda, O., McLeigh, J. D., & Katz, C. (2017). Measuring collective efficacy in the context of community-based child maltreatment prevention. *Child indicators research*, *10*(2), 489-504.

Leszczyna, R., Fovino, I. N., & Masera, M. (2010). Simulating malware with MAlSim. *Journal in computer virology*, *6*(1), 65-75.

Maguire, E. R., Johnson, D., Kuhns, J. B., & Apostolos, R. (2017). The effects of community policing on fear of crime and perceived safety: findings from a pilot project in Trinidad and Tobago. *Policing and Society*, 1-20.

Maltz, M.D., Gordon, A.C. & Friedman, W. (1990). *Mapping Crime and Its Community Setting: Event Geography Analysis*. Nueva York: Springer-Verlag

McConnell, E. H. (1997). Fear of crime on campus: A study of a southern university. *Journal of Security Administration*, *20*(2), 22-46.

Miró Llinares & Johnson, S. (2018). Cybercrime and Place: Applying Enviromental Criminology to Crimes in Cyberspace. En Bruisna, G. & Johnson, S. (eds), *The Oxford Handbook of Environmental Criminology*. Oxford: Oxford University Press.

Miró Llinares, F. (2011). La oportunidad criminal en el ciberespacio: Aplicación y desarrollo de la teoría de las actividades cotidianas para la prevención del cibercrimen. *Revista Electrónica de Ciencia Penal y Criminología, 13*(7).

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

Moitra, S. D. (2005). Developing policies for cybercrime. *European Journal of Crime Criminal Law and Criminal Justice*, *13*(3), 435.

Nasar, J. L., & Fisher, B. (1993). 'Hot spots' of fear and crime: A multi-method investigation. *Journal of environmental psychology*, *13(*3), 187-206.

Ortega, S. T., & Myles, J. L. (1987). Race and gender effects on fear of crime: An interactive model with age. *Criminology*, *25*(1), 133-152.

Painter, K. (1996). The influence of street lighting improvements on crime, fear and pedestrian street use, after dark. *Landscape and Urban Planning 35*(2–3), 193–201.

Pereira, F., Spitzberg, B. H., & Matos, M. (2016). Cyber-harassment victimization in Portugal: Prevalence, fear and help-seeking among adolescents. *Computers in Human Behavior, 62*, 136-146.

Randa, R. (2013). The influence of the cyber-social environment on fear of victimization: Cyber bullying and school. *Security Journal, 26*, 331-348.

Riek, M., Böhme, R., & Moore, T. (2014, June). Understanding the influence of cybercrime risk on the e-service adoption of European Internet users. In *13th Workshop on the Economics of Information Security*.

Roberts, L. D., Indermaur, D., & Spiranovic, C. (2013). Fear of cyber-identity theft and related fraudulent activity. *Psychiatry, Psychology and Law*, *20*(3), 315-328.

Ross, C. E., & Mirowsky, J. (1999). Disorder and decay: The concept and measurement of perceived neighborhood disorder. *Urban Affairs Review, 34*(3), 412-432.

Rountree, P. W., & Land, K. C. (1996). Perceived risk versus fear of crime: Empirical evidence of conceptually distinct reactions in survey data. *Social forces*, *74*(4), 1353-1376.

Salem, G. W., & Lewis, D. A. (2016). *Fear of crime: Incivility and the production of a social problem*. New Jersey, NY: Transaction Publishers.

Skogan, W. G. (1990). *Disorder and decline: crime and the spiral decay in American neighbourhoods*. Los Angeles, CA, University of California Press.

Skogan, W. G. & Maxfield, M. G. (1981). *Coping with crime: individual and neighborhood reactions*. Beverly Hills, CA, Sage Publications.

Smith, L. N. and G. D. Hill (1991). Victimisation and fear of crime. *Criminal Justice and Behaviour 18*(2), 217–239.

Virtanen, S. M. (2017). Fear of Cybercrime in Europe: Examining the Effects of Victimization and Vulnerabilities. *Psychiatry, Psychology and Law*, 1-16.

Vozmediano, L. y San Juan, C. (2010). *Criminología ambiental. Ecología del delito y de la seguridad*. Barcelon: Editorial UOC.

Vozmediano, L., San-Juan, C., Vergara, A. I., & Lenneis, A. (2013). Risk perception in digital contexts: questionnaire and pilot study. *International E-journal of Criminal Sciences*, (7).