methaodos.revista de ciencias sociales, 2022, *10*(2): 243-258

La seguridad en el ciberespacio desde una perspectiva sociocultural

Security in cyberspace from a sociocultural perspective

Fulgencio Sánchez Vera | fsanchev@ull.edu.es
Universidad de la Laguna, España

Javier Eloy Martínez Guirao | j.eloymartinez@um.es | Autor de correspondencia
Universidad de Murcia, España

Anastasia Téllez Infantes | atellez@umh.es
Universidad Miguel Hernández, España

10.17502/mrcs.v10i2.577

Recibido: 30-07-2022
Aceptado: 30-09-2022

Resumen

En este artículo presentamos una aproximación al problema de la seguridad en el ciberespacio desde una perspectiva sociocultural. Comenzamos caracterizando el nuevo espacio a través de un modelo estratificado que da relevancia a las personas como agentes que utilizan y dan sentido a la infraestructura tecnológica. Mostramos cómo la expansión del ciberespacio ha generado de manera paralela un aumento de la cibercriminalidad, en sus distintas formas –ciberdelito, ciberterrorismo, ciberguerra, entre otros. Sin obviar la importancia de la tecnología subyacente, nos centramos en el papel del factor humano analizando las principales ciberamenazas a las que estamos expuestos y los actores que intervienen. Finalmente, apuntamos cómo el rápido avance del ciberespacio en extensión y profundidad dará soluciones asombrosas a ciertas necesidades humanas, pero a la vez aumentará la vulnerabilidad abriendo un escenario de alto riesgo que la sociedad tendrá que enfrentar para establecer la confianza necesaria que garantice la seguridad y la libertad en el nuevo entorno. Concluimos defendiendo que las ciencias sociales tienen un papel esencial pues los problemas que atañen a la seguridad y los derechos no pueden abordarse como una cuestión meramente técnica.

Palabras clave: ciberseguridad, ciberespacio, ingeniería social, ciberdelincuencia, educación.

Abstract

In this article we present an approach to the problem of security in cyberspace from a sociocultural perspective. We begin by characterizing the new space through a stratified model that gives relevance to people as agents who use and give meaning to the technological infrastructure. We show how the expansion of cyberspace has generated in parallel an increase in cybercrime, in its different forms –cybercrime, cyber terrorism, cyber war, among others. Without ignoring the importance of the underlying technology, we focus on the role of the human factor by analysing the main cyber threats to which we are exposed and the actors involved. Finally, we point out how the rapid advance of cyberspace in scope and depth will provide astonishing solutions to certain human needs, but at the same time will increase our vulnerability by opening up a high-risk scenario that society will have to face in order to establish the necessary trust to guarantee security and the freedom of people in the new environment. In this scenario, the social sciences have an essential role to play since the problems that concern our security and our rights cannot be addressed as a merely technical question.

Keywords: *cyber security, cyberspace, social engineering, cybercrime, education*

Sumario

Cómo citar este artículo

Sánchez Vera, F., Martínez Guirao, J.E., y Téllez Infantes, A. (2022). La seguridad en el ciberespacio desde una perspectiva sociocultural. *methaodos.revista de ciencias sociales, 10*(2): 243-258. http://dx.doi.org/10.17502/mrcs.v10i2.577

methaodos.revista de ciencias sociales, 2022, *10*(2): 243-258

1. Introducción

Es evidente que la seguridad en el ciberespacio se vincula con la seguridad de la información que circula por las redes y es almacenada en los dispositivos interconectados. En consecuencia, la información es vista como el bien más preciado, el bien a proteger y preservar. Los expertos en seguridad consideran que la seguridad de la información se consigue con actuaciones que garanticen tres propiedades: confidencialidad, integridad y disponibilidad[1]; entendiendo la información en sus diversas formas, tanto digitales: almacenada electrónicamente y transmitida por medios electrónicos, como no digitales: impresa o escrita en papel (ISO, 2004). Las tecnologías para el tratamiento de la información digital son el objeto de estudio de la seguridad informática, subcampo de la seguridad de la información, que se encarga de la protección de los sistemas sobre los que la información se almacena y transmite, convirtiendo la infraestructura tecnológica en otro activo a proteger[2]. Así, tradicionalmente, el enfoque de la seguridad ha consistido en proteger la información y sistemas informáticos ante las amenazas para las que son vulnerables, seleccionando e implementando controles o contramedidas que ayuden a reducir el riesgo que representan dichas vulnerabilidades (Gerber y Solms, 2005; ISO, 2005).

Esta visión, centrada en la información y los sistemas, ha guiado a los expertos en seguridad durante mucho tiempo. Sin embargo, se trata de una orientación con un sesgo tecnocéntrico importante. Otra visión de la seguridad es la que considera como activos a proteger: las personas y los intereses de la sociedad, además de la información y la infraestructura tecnológica (Von Solms y Van Niekerk, 2013). En este caso hablaríamos de seguridad en el ciberespacio o ciberseguridad.

Por tanto, si para la seguridad informática el activo a proteger son los sistemas tecnológicos y para la seguridad de la información es la información junto con la tecnología subyacente; para la ciberseguridad el objetivo principal claramente no es proteger el ciberespacio, sino más bien proteger a aquellos que funcionan en el ciberespacio, ya sean personas, organizaciones o naciones (Von Solms y Van Niekerk, 2013).

Aunque esta definición de ciberseguridad es mucho más completa y fértil aún nos parece insuficiente. No podemos ver a las personas exclusivamente como un elemento pasivo a proteger, ya que además de potenciales víctimas también pueden ser manipuladas y utilizadas como medios para iniciar un ataque. Este hecho es bien conocido por los expertos en seguridad entre los que se repite el mantra de que "las personas son el eslabón más débil de la cadena de la seguridad". Sin embargo, tradicionalmente, tanto el abordaje analítico de la problemática como el diseño de soluciones ha estado orientado fundamentalmente hacia las infraestructuras de comunicación, los dispositivos y las aplicaciones, olvidando el factor humano como un elemento activo para garantizar la seguridad.

Sobre esta situación, podemos apuntar, a modo de explicación tentativa, dos hechos: primero, que la infraestructura tecnológica es fácil de visualizar, identificar sus componentes y someterlos a prueba o control; además, como está definida técnicamente de forma determinista, su funcionamiento puede ser probado, mejorado y reparado. Sin embargo, la actividad social no es determinista, al contrario, el comportamiento humano es extremadamente variable e incluso impredecible y, por tanto, mucho más difícil de anticipar y controlar. A esta situación, y como segunda causa explicativa, hay que sumar que los equipos y expertos encargados de la ciberseguridad tienen un perfil técnico, con una alta preparación en informática, pero no sobre el comportamiento humano, la incidencia de la cultura y la formación. En la actualidad con el incremento de la actividad en el ciberespacio se requieren también expertos de otras disciplinas capaces de analizar el comportamiento de los usuarios y colaborar en el análisis y diseño de soluciones a los problemas de la ciberseguridad.

Nuestra hipótesis es que el ciberespacio está penetrando toda la experiencia humana y esto obliga a la ciberseguridad a ir más allá de los aspectos técnicos, para convertirse en una disciplina multidisciplinar donde participen expertos en comportamiento que aporten una perspectiva sociocultural, y educadores que

[1] La confidencialidad, integridad y disponibilidad, conocidas por las siglas CIA (del inglés: *Confidenciality, Integrity and Availabiliaty*), son las dimensiones básicas que han guiado las actuaciones en seguridad de la información. Progresivamente otros autores han añadido otros aspectos; así, Whitman y Mattord (2009) consideran la exactitud, autenticidad, utilidad y posesión como elementos de la información que deben protegerse.

[2] La seguridad informática se refiere a todos aquellos aspectos relacionados con definir, archivar y mantener la confidencialidad, integridad, disponibilidad, no-repudio, responsabilidad, autenticidad y fiabilidad de los recursos de información (ISO, 2004, p. 3).

methaodos.revista de ciencias sociales, 2022, *10*(2): 243-258

ayuden a las personas a convertirse en agentes activos, trascendiendo la visión de usuarios pasivos a proteger.

Para validar nuestra hipótesis, exponemos una caracterización del ciberespacio desde una perspectiva antropológica que da relevancia a las personas, pues son ellas quienes utilizan y dan sentido a la infraestructura tecnológica. En definitiva proponemos un modelo capaz de representar la complejidad del nuevo espacio en relación con las personas. Mostramos cómo la expansión del ciberespacio conlleva de manera paralela un aumento del ciberdelito, el ciberterrorismo y la ciberguerra. Revisamos el perfil de los actores -agentes y víctimas-, centrándonos en determinar una caracterización de agentes en función de los objetivos que orientan sus actuaciones, así como los métodos y técnicas que se orientan a explotar la vulnerabilidad humana. Analizamos las ciberamenazas más importantes apoyándonos en indicadores de ciberdelincuencia y en el estudio de casos de ataques reales. Finalmente, apuntamos como el rápido avance del IoT (del inglés: *Internet of Things*) podrá dar soluciones a ciertas necesidades humanas, pero a la vez aumentará las vulnerabilidades abriendo un escenario de alto riesgo y un nuevo reto para la seguridad cuyas soluciones trascienden lo tecnológico.

2. Metodología

Aunque este trabajo tiene una orientación fundamentalmente descriptiva, para la recopilación de la información en la que se basa, se aplicaron diferentes técnicas de investigación en un periodo que abarca desde los años 2018 a 2021. Por un lado, se realizó una búsqueda documental en bases de datos académicas, así como seguimiento de publicaciones y foros especializados en la temática. Por otro lado, se entrevistó a expertos en ciberseguridad que trabajan en empresas e instituciones educativas del sureste español, fundamentalmente del sur de la Comunidad Valenciana y de la Comunidad Autónoma de la Región de Murcia. Estos expertos diariamente exploran amenazas y vulnerabilidades para tomar acciones que reduzcan los riesgos de los ataques; por tanto, están en la primera línea de acción y son los grandes conocedores de los retos a los que nos enfrentamos.

3. Expansión del ciberespacio y de la ciberdelincuencia

El concepto de red de computadores se fraguó a lo largo de la década de los sesenta y se concretó en el proyecto ARPANET, una red de computadoras ideada y desarrollada por científicos y académicos de universidades americanas por encargo del Departamento de Defensa de los Estados Unidos. El primer nodo se creó en la Universidad de California y el primer mensaje se envió en 1969. En pocos años, esta tecnología se extiende por EE.UU., llega a Europa y finalmente al resto del mundo, convirtiéndose en una red de comunicación de alcance global. En 1990 desaparece ARPANET y se finaliza la transición al modelo de protocolos comunes TCP/IP capaces de conectar redes físicas heterogéneas integrándolas en una gran red lógica: Internet.

Internet saltó del mundo universitario para proveer nuevos servicios a las empresas y a la ciudadanía. A partir del año 2000, tras la explosión de la burbuja de las *puntocom*, llega la Web 2.0 o web social. Se trata de una nueva filosofía de la Web que gracias a su plasticidad se redefine permitiendo que los usuarios finales dejen de ser consumidores de información y se conviertan en participantes activos. Aparecen aplicaciones que permiten a los usuarios no sólo interactuar y comunicarse con otros, sino crear servicios y contenidos de forma autónoma. Esta explosión de la actividad social acompañada de la mejora de las comunicaciones, el abaratamiento de los dispositivos y una lenta pero cada vez mayor competencia digital de la población ha conseguido que el número de usuarios crezca de manera espectacular. Si a finales de 1995 había 16 millones de usuarios conectados a la Red, un 0,4% de la población mundial (IWS, 2020); en diciembre de 2021 llegamos a 5,251 millones de usuarios, el 66,2% de la población mundial. Esta evolución puede observarse de manera global y por regiones en la Tabla 1.

Como se puede observar, más de la mitad de los usuarios de Internet (53,1%) están en Asia. Mientras que el mayor porcentaje de usuarios se da en Europa (88,4%) y en Norte América (93,4%). En cualquier caso, más allá del grado de penetración de Internet, es incuestionable que todos los ciudadanos, incluso aquellos

methaodos.revista de ciencias sociales, 2022, *10*(2): 243-258

que no son usuarios directos, dependen de los sistemas informáticos, pues son estos los que soportan la economía y la administración de las sociedades complejas actuales.

Tabla 1. Uso de Internet en el mundo

Regiones	Población (2022 Est.)	Población (% Pob.)	Usuarios de Internet 31-dic-21	Penetración (% Pob.)	Crecimiento 2000-2022	Internet (% Mundo)
África	1.394.588,55	17,60%	601.327,46	43,10%	0,1322	11,50%
Asia	4.350.826,90	54,80%	2.790.150,53	64,10%	0,02341	53,10%
Europa	841.319,70	10,60%	743.602,64	88,40%	6,08	14,20%
América Latina/Caribe	663.520,32	8,40%	533.171,73	80,40%	0,02851	10,10%
América del Norte	372.555,59	4,70%	347.916,69	93,40%	2,22	6,60%
Oriente Medio	268.302,80	3,40%	205.019,13	76,40%	0,06141	3,90%
Oceanía/Australia	43.602,96	0,50%	30.549,19	70,10%	3,01	0,60%
Total	7.934.716,82	100,00%	5.251.737,36	66,20%	0,01355	100,00%

Fuente. Internetworldstats.

Desde el origen de Internet, la tendencia ha sido que cada vez más actividades sociales se asienten en el ciberespacio o estén mediadas por las tecnologías digitales. La pandemia de COVID-19 ha sido sin duda un punto de inflexión en esta migración de servicios, actividades y relaciones que antes no imaginábamos posibles a través de una pantalla. La realidad de la actual cibersociedad es que pocas actividades escapan al interminable flujo de información digital –negocios, transacciones bancarias, educación, compras, relaciones personales, etc.

Se ha llegado aquí en una acelerada expansión que ha fascinado por las posibilidades y servicios desplegados, y aunque es indudable que, en numerosos aspectos, el ciberespacio está permitiendo mejorar la vida de muchas personas, también está generando nuevos riesgos y amenazas. La seguridad de la actividad en el ciberespacio está lejos de estar garantizada. De hecho, la expansión de la actividad en el nuevo entorno ha sido directamente proporcional al incremento del ciberdelito y el cibercrimen. Sobre este hecho, cabe preguntarse por las diferencias del ciberdelito y el delito tradicional, si existe una nueva criminalidad y, en tal caso, cómo es y cómo actúa.

Podemos entender "ciberdelito" o "cibercrimen" como "cualquier infracción punible, ya sea delito o falta, en el que se involucra un equipo informático o Internet y en el que el ordenador, teléfono, televisión, reproductor de audio o vídeo o dispositivo electrónico, en general, puede ser usado para la comisión del delito o puede ser objeto del mismo delito" (Rayón-Ballesteros y Gómez-Hernández, 2014). Aunque pudiera parecer una simple migración de los delitos tradicionales al nuevo espacio, lo cierto es que el ciberdelito supone una remodelación de los papeles de autor y víctima, además de una adaptación e incluso innovación en las formas de actuar. Podemos afirmar que el ciberespacio ha creado una nueva criminalidad, pues el ciberdelincuente, individualmente u organizado en grupos, puede realizar sus ataques desde cualquier lugar, con pocos medios y con un alto impacto sobre sus víctimas, sean estas personas, empresas, entidades públicas e incluso países.

El ciberdelito ocurre por las características de la propia infraestructura tecnológica y por otras razones socioculturales. Es decir, porque existen fallos en el diseño de la infraestructura tecnológica que es aprovechada por los cibercriminales. Pero también, por los vacíos de legislación, que no es capaz de adaptarse con suficiente celeridad a este nuevo espacio cambiante y transnacional. Por la facilidad de acceso, cada vez mayor, que se hace presente en diferentes grupos humanos con sus propias características sociales y culturales. Por el "anonimato" con el que, al menos en un primer momento, es posible actuar evitando que entren en acción los mecanismos de control social. Por la distancia física que permite este lugar descorporeizado, sobre el que se puede actuar desde cualquier lugar del planeta. Y, sobre todo, por la complejidad y dificultad de acceso a un conocimiento que no llega a todos de la misma manera, donde se

methaodos.revista de ciencias sociales, 2022, *10*(2): 243-258

hacen presentes las diferentes "brechas": generacional, entre países, de género, etc. De este modo, la falta de pericia y las actuaciones descuidadas de los usuarios que conlleva, configuran vulnerabilidades que son explotadas por los ciberdelincuentes.

Evidentemente, cualquier solución pasa por comprender las amenazas potenciales, quiénes son los actores principales y qué les motiva a actuar, cuáles son sus vulnerabilidades y qué riesgos reales se asumen con la actividad en el ciberespacio. En los siguientes apartados intentaremos clarificar estas y otras cuestiones. Pero antes conviene caracterizar de una manera adecuada el ciberespacio, necesitamos un modelo capaz de representar este espacio y la complejidad de las relaciones entre los dispositivos, las infraestructuras tecnológicas, las aplicaciones de usuario y los propios usuarios.

4. Un modelo del ciberespacio

El término ciberespacio como ya apuntaba Pierre Lévy (2007) "designa no solamente la infraestructura material de la comunicación numérica, sino también el oceánico universo de informaciones que contiene, así como los seres humanos que navegan por él y lo alimentan" (p. 1). Pero ¿cómo se conectan estos elementos –personas, redes de comunicación e información? y ¿cómo se explican sus propiedades y características –apertura, neutralidad, no distancialidad, anonimato, etc.? En nuestra opinión, el modelo más fértil para comprender el ciberespacio se basa en un enfoque estratigráfico, basado en capas o niveles. En la literatura científica se pueden encontrar diversas propuestas, concretamente David Clark (2010) y Dunn Cavelty (2013) han desarrollado modelos del ciberespacio estructurándolo en tres capas: física, lógica y social.

Para Clark (2010) la capa física "es la base del ciberespacio, los dispositivos físicos con los que está construido. El ciberespacio es un espacio de dispositivos informáticos interconectados, por lo que sus cimientos son PC y servidores, supercomputadoras y redes, sensores y transductores e Internet y otros tipos de redes y canales de comunicación" (p. 2). La función de esta capa es la transferencia y almacenamiento de la información. Además, como sus componentes resultan visibles, tangibles y tienen una localización geográfica precisa, se pueden trazar mapas en los que localizar cada componente —infraestructuras de suministro de energía, circuitos electrónicos, servidores de almacenamiento y enrutamiento de datos, etc. (Sánchez-Vera, 2018).

Por el contrario, la capa lógica no es visible ni tangible, pues se basa en *software* y datos. Parte del *software* proporciona servicios de bajo nivel –sistemas operativos y protocolos para el transporte de datos– sobre ellos se despliegan aplicaciones, bases de datos, servidores web, etc. En la cima de esta jerarquía se encuentran las plataformas y aplicaciones de usuario final que permiten interactuar a las personas, como el correo electrónico, las redes sociales, blogs y otras (Clark, 2010, p. 3).

A diferencia de la capa física, la geolocalización de los componentes lógicos no está tan definida y puede no ser estable en el tiempo. En un determinado momento, podemos identificar el servidor o dispositivo que aloja un sitio web o una plataforma, pero este *software* puede reinstalarse en otro servidor cruzando fronteras para evitar ciertas jurisdicciones. En el caso de la comunicación de datos, no es una tarea simple geolocalizar con precisión la ruta utilizada, esto es así debido a que la información viaja a través de la infraestructura física dividida en pequeños paquetes de datos que pueden atravesar diferentes rutas, ya que la Red, aprovechando la redundancia de caminos y que no existen nodos esenciales, es capaz de reorganizar de manera dinámica las rutas por donde se envían los datos (Sánchez-Vera, 2018).

Hay que destacar que la infraestructura tecnológica que define las capas física y lógica se sustenta en su apertura, redundancia y anonimato; esto implica que todo el mundo puede acceder sin necesidad de identificarse, que ningún nodo es central y la información puede moverse por diferentes rutas alternativas, y que la Red puede albergar e intercambiar todo tipo de información sin consideraciones sobre su significado. Estas características son inherentes al diseño de Internet y dificultan la implantación de mecanismos de control. Sin embargo, esta neutralidad sobre los contenidos que circulan y la identidad de las personas que interactúan puede ser comprometida, por ejemplo, consiguiendo el control de ambas capas como ocurre en ciertos países como China o Corea del Norte, o a través de sofisticados sistemas de *malware* para vigilancia, como lo demuestran las revelaciones de Snowden sobre el alcance de la vigilancia masiva realizada por las agencias de inteligencia (Greenwald, MacAskill, y Poitras, 2013). O las estrategias de

methaodos.revista de ciencias sociales, 2022, *10*(2): 243-258

recopilación de datos por parte de empresas privadas para crear perfiles personales sobre gustos y comportamientos.

La última capa sería la social y estaría formada por las personas que a través de distintos avatares o perfiles personales o como miembros de organizaciones públicas o privadas generan el flujo de información y la actividad que da sentido al ciberespacio. No puede existir un ciberespacio sin personas. Un ciberespacio vacío, desprovisto de interacciones sociales y de contenido original, carecería de fundamento, habría que llenarlo y darle vida. En definitiva, el ciberespacio existe en cuanto las personas crean e intercambian información a través de los dispositivos y plataformas.

Este modelo de tres capas —física, lógica y social— nos da una primera aproximación a la organización de sus componentes y relaciones básicas, pero faltaría preguntarse por el grado de interdependencia entre ellas. Para observar este factor conviene volver la mirada hacia atrás y recordar cómo en los inicios de Internet los usuarios se conectaban y desconectaban a la Red a voluntad, de manera consciente se entraba y salía del ciberespacio. La interconexión era temporal y controlada. Sin embargo, hoy no se conecta o se desconecta, se está constantemente en el ciberespacio, puede que no se esté interactuando personalmente pero los *smartphones* ya lo están haciendo: comparten la geolocalización, informan de mensajes en las redes sociales, monitorizan la actividad, la comparten, etc. Esta presencia constante implica una integración permanente de la capa social con la lógica y física, cuya interconexión se intensifica con el desarrollo de las tecnologías asociadas a los llamados objetos "inteligentes", elementos clave del IoT[3].

El uso y aplicación de estos objetos inteligentes se inició hace dos décadas. Pero, en la actualidad, su prevalencia y conectividad crece de manera significativa. La consultora Gartner pronosticó que para el año 2021 habrá unos 25 mil millones de dispositivos IoT conectados (Gartner, 2018), paralelamente la tecnología de telecomunicaciones que los interconecta evoluciona del 4G a 5G.

El IoT está creciendo en sectores como la domótica, la salud, la industria, el transporte o la vigilancia. Pero, sin duda, uno de los usos más evidentes es el de los dispositivos *wearables* o portables, es decir que se pueden llevar sobre el cuerpo —como relojes inteligentes, pulseras, dispositivos para escuchar, entre otros— y que de manera constante miden a través de potentes microchips y sensores ciertos datos del usuario que se envían mediante Bluetooth, Wi-Fi o una red celular a otros dispositivos (Tankovska, 2020). Las aplicaciones son enormes, por ejemplo, en el campo de la salud se puede monitorear el estado general del usuario, los hábitos alimenticios, ejercicio físico realizado, pulso, sueño, etc. La nueva frontera donde está penetrando el IoT son las prótesis e implantes biónicos que se conectan a la Red para enviar datos a servidores donde se procesan y monitorizan. Estas funciones suponen grandes ventajas para los usuarios, pero también los convierte en objetivo de los piratas informáticos, pues los ciberdelincuentes pueden alterar el funcionamiento de estos dispositivos, acceder a los datos personales almacenados o incluso manipularlos (Kaspersky, 2018).

El riesgo de sufrir un ciberataque contra el cuerpo se hace extremadamente crítico en personas que cuentan con implantes inteligentes para la administración de insulina o marcapasos. Y dado que son tecnologías emergentes, muchos dispositivos IoT "presentan vulnerabilidades técnicas en los mecanismos de autenticación y limitaciones de cálculo, que dificultan la implantación de cifrado tanto en la información en tránsito como en la almacenada" (INCIBE, 2020).

Lo que enseña la Historia es que si existe una vulnerabilidad siempre existirá alguien que intentará sacar provecho de su existencia. En este sentido, el ciberespacio está creando nuevos riesgos y la ciberseguridad se enfrenta a retos importantes. En los siguientes apartados analizaremos estos riesgos adentrándonos en el carácter de las amenazas, los actores involucrados y sus objetivos.

5. Ciberamenazas y ciberdelincuencia

Las amenazas son circunstancias que pueden ocurrir y que conllevarían consecuencias negativas para las personas, las empresas u organizaciones e incluso para ciudades o países. Una ciberamenaza puede provocar que los servicios no funcionen o lo hagan de manera incorrecta o incluso que dejen de tener valor. Las causas pueden ser accidentales o intencionadas; y pueden dirigirse a la capa física, lógica o social.

[3] IoT (*Internet of Things*) hace referencia a la red de objetos físicos que incorporan tecnología para detectar e interactuar con sus estados internos, con el entorno externo y comunicarse con otros; su función es recopilar datos, analizarlos y realizar acciones de manera autónoma.

methaodos.revista de ciencias sociales, 2022, *10*(2): 243-258

Nos centraremos en aquellas inducidas por actores interesados en causar algún tipo de daño de manera intencional; por tanto, estamos adentrándonos en el ámbito de la delincuencia, el crimen y el delito adaptado al nuevo entorno. Podemos decir que las actividades de esta nueva criminalidad se diferencian de las tradicionales en cuatro aspectos fundamentales: "se cometen fácilmente; requieren escasos recursos en relación al perjuicio que causan; pueden cometerse en una jurisdicción sin estar físicamente presente en el territorio sometido a la misma; y se benefician de lagunas de punibilidad que pueden existir en determinados Estados, los cuales han sido denominados paraísos cibernéticos, debido a su nula voluntad política de tipificar y sancionar estas conductas" (Subijana Zunzunegui, 2008).

Estas ventajas generan un alto grado de impunidad que la ciberdelincuencia está aprovechando. No es fácil cuantificar la cantidad de ataques y tampoco su virulencia, pues muchos no se denuncian bien porque supondría un desprestigio o pérdida de credibilidad para la persona o empresa que recibió el ataque, o bien por ser parte de acciones de la ciberguerra latente y oculta que se está produciendo entre algunos estados.

Centrándonos en España, la parte de la actividad criminal que sí es reportada a los servicios de seguridad del estado y que queda recogida en los informes oficiales nos puede ayudar a entrever la envergadura del problema. En la siguiente tabla se muestra la serie temporal de datos entre los años 2016 a 2019, que corresponden a la actividad registrada por las Fuerzas y Cuerpos de Seguridad del Estado Español (Cuerpo Nacional de Policía, Guardia Civil, Policía Foral de Navarra, Ertzaintza, Mossos d' Esquadra y distintos Cuerpos de Policía Local)[4] (Tabla 2).

En el periodo mostrado, se constata una tendencia al alza de los delitos, aumentando más del doble en tan sólo cuatro años. En 2019, se dieron un total de 218.302 hechos, lo que supone un 35,8% más con respecto al año anterior. De las tipologías de delitos es remarcable como el fraude informático (estafas) es el principal delito cometido, suponiendo el 88,1% del total, seguido de amenazas y coacciones (5,9%), falsificación informática (1,95%) y acceso e interceptación ilícita (1,83%).

Según la Europol (2020), el ciberdelito se está volviendo más agresivo y conflictivo. En los países de la Unión Europea donde Internet está ampliamente implantado y el comercio electrónico y el pago online es una actividad cotidiana, la ciberdelincuencia es un problema creciente. El interés no es sólo por los datos financieros sino por todos los datos. El número y la frecuencia de las violaciones de datos van en aumento, lo que a su vez genera más casos de fraude y extorsión.

6. Ciberarmas: la ingeniería social

Según la Europol (2020), la creatividad de los ciberdelicuentes y la enorme variedad de acciones que realizan es impresionante, incluyendo: uso de *botnets*[5] para transmitir virus, SPAM, ataques DDoS[6]; crear "puertas traseras" en los dispositivos comprometidos para permitir el robo de dinero y datos, o el acceso remoto a los dispositivos para crear *botnets;* crear mercados en línea para comerciar con conocimientos o herramientas para piratería, venta de armas, pasaportes falsos, tarjetas de crédito falsificadas y clonadas, drogas y servicios de piratería; blanquear dinero, tanto tradicional como virtual; realizar fraude en línea, por ejemplo, a través sistemas de pago en línea, tarjetas e ingeniería social; y diversas formas de explotación sexual infantil, como la distribución en línea de materiales sobre abuso sexual infantil e incluso su transmisión en vivo.

La lista de métodos de ataque es enorme, pero si nos centramos en los más utilizados en 2019, según el Centro Criptológico Nacional (2020) destacan: actividades de *ransonware*[7], *botnets,* código dañino avanzado, ataques a sistemas de acceso remoto, ataques web, ingeniería social, ataques contra la cadena de suministro y ataques contra sistemas ciberfísicos. Cada uno de estos ataques se inicia explotando una vulnerabilidad

[4] La tabla sigue la clasificación adoptada por el Convenio sobre cibercriminalidad o Convenio de Budapest y otras infracciones penales reguladas en la legislación española.

[5] Un *botnet* es una red de ordenadores infectados sin el conocimiento del usuario que se comunican entre sí y con el equipo del atacante que se convierte en el centro de control de toda ellos. El atacante puede manejarlos a su merced cuando desee lanzar un ataque masivo.

[6] DDoS (del inglés, *Distributed Denial of Service*) es un ataque que aprovecha que los recursos de red, como son los servidores Web, tienen unos límites de capacidad de respuesta, de manera que enviando múltiples solicitudes al recurso se puede desbordar la capacidad del mismo y evitar que este funcione correctamente.

[7] *El ransomware* consiste en impedir que los usuarios puedan acceder a sus dispositivos, normalmente a través de un *malware* que cifra el disco duro, exigiendo un rescate para recuperar el acceso.

que puede localizarse en la capa física, lógica o social. Aquellos que se inician o dirigen a la capa social se referencian bajo el término "ingeniería social" y es uno de los más usados según el Centro Criptológico Nacional.

Tabla 2. Evolución de hechos conocidos por categorías delictivas

Hechos conocidos	**2016**	**2017**	**2018**	**2019**
Acceso e interceptación ilícita	3.243	3.150	3.384	4.004
Amenazas y coacciones	12.036	11.812	12.800	12.782
Contra el honor	1.546	1.561	1.448	1.422
Contra propiedad indust./intelec.	129	121	232	197
Delitos sexuales(*)	1.231	1.392	1.581	1.774
Falsificación informática	3.017	3.280	3.436	4.275
Fraude informático	70.178	94.792	136.656	192.375
Interferencia datos y en sistema	1.336	1.291	1.192	1.473
Total	92.716	117.399	160.729	218.302

Fuente. Sistema Estadístico de Criminalidad (Ministerio del Interior, 2019).

Si bien "ingeniería social" es un término moderno, el procedimiento es muy antiguo, pues se basa en identificar y aprovechar las diferentes vulnerabilidades que pueden existir en las potenciales víctimas debido a su posición sociocultural y a las limitaciones y condicionantes que esta conlleva. Se basa también en explotar la psicología humana para manipular a las personas y que entreguen información confidencial o personal que se utilizará con fines fraudulentos. Para conseguirlo, los ciberdelincuentes tratarán de ofrecer algo que capte el interés de la víctima y que no levante sospechas. Según la consultora Verizon (2020), el 96% de los ataques de ingeniería social en las organizaciones se realiza a través del correo electrónico. El tipo más común es el *phishing,* una modalidad en la que el atacante se hace pasar por un usuario o institución legítima y utilizando el miedo, la urgencia o la curiosidad, engaña a su víctima para que haga clic en enlaces maliciosos, abra archivos adjuntos cargados de *malware* o le entregue sus credenciales de inicio de sesión. Los ataques de *phishing* representaron el 22% de todas las infracciones en 2019 (Verizon, 2020).

El *phishing* se puede realizar a través de campañas masivas o personalizadas. Las masivas se lanzan de manera indiscriminada intentando alcanzar al mayor número posible de personas. Evidentemente los métodos de suplantación de identidad serán genéricos e incluso poco sofisticados, de manera que un usuario vigilante lo detectará con facilidad; sin embargo, el cibercrimen la sigue utilizando pues dado el gran número de receptores un porcentaje de éxito bajo sigue siendo muy lucrativo.

En el caso de ataques de *phishing* dirigidos (*spear-phishing*), se elige a la víctima, persona u organización, y se prepara la fórmula de contacto de manera personalizada. Por ejemplo, suplantando servicios o personas en los que la víctima confía. Este tipo de ataques pueden ser extremadamente sofisticados, con un profundo estudio previo de la víctima, a través de fuentes abiertas[8] o de técnicas de acercamiento por redes sociales mediante perfiles falsos (CCN-CERT, 2020).

Otras variantes de la ingeniería social que ha resonado en los últimos años son las dirigidas a montar campañas de desinformación, desarrollando noticias falsas y manipulando a los usuarios para que las difundan a través de sus redes sociales. En estos casos, la ingeniería social aprovecha dos sesgos cognitivos de las personas: el sesgo de confirmación y el de pertenencia al grupo (CCN-CERT, 2020). Apoyándose en ellos, se difunden rumores y datos falsos con la intención de condicionar resultados electorales, promover revueltas o desestabilizar sociedades. El impacto de estas campañas pone sobre la mesa cuestiones de gran

[8] OSINT (acrónimo del inglés, Open-Source Intelligence, en español: Inteligencia de Fuentes Abiertas) es una metodología que se basa en métodos cualitativos y cuantitativos para recopilar datos accesibles en fuentes disponibles públicamente, analizarlos y tomar decisiones.

methaodos.revista de ciencias sociales, 2022, *10*(2): 243-258

calado y complejidad como la neutralidad o el control de la Red, pues enfrentan valores que hay que conciliar como la libertad de expresión y la seguridad.

Aunque resulta evidente, debemos remarcar que la ingeniería social no es una técnica secundaria; de hecho, es una de las principales tácticas de ataque, ratificando la idea que apuntan los expertos al afirmar que "el usuario es el eslabón más débil en la cadena de la seguridad". Sin embargo, esta debilidad se puede resolver reconociendo la centralidad del factor humano en la seguridad, analizando su comportamiento y aportando soluciones en dos ámbitos: el primero, la formación, haciendo a los usuarios más conscientes de los riesgos y más competentes en sus actividades con los dispositivos, aplicaciones y servicios del ciberespacio; y, segundo en el diseño de la tecnología, que se debería fundar en principios éticos y adaptados a la cognición y al comportamiento humano. En ambos casos, se requiere una presencia de expertos en estas áreas que colaboren con ingenieros y programadores de dispositivos.

Llegados aquí, tras revisar las ciberamenazas, los ciberdelitos y cómo el cibercrimen hace uso de la ingeniería social para atacar la cognición humana, para completar nuestro mapa de contexto vamos a mostrar quiénes son los agentes inductores de las amenazas de seguridad, cuáles son sus objetivos y a quién dirigen sus ataques.

7. Agentes, objetivos y víctimas

El Centro Criptológico Nacional (2020) ofrece una clasificación de las víctimas, agrupándolas en cuatro categorías: sector público, infraestructuras críticas, empresas y ciudadanos. El mismo organismo, atendiendo al grado de actividad en los últimos años, considera como agentes inductores fundamentales: los Estados y grupos patrocinados, ciberdelincuentes, ciberterroristas y hacktivistas. Por su parte, Quintana (2016) aporta otra clasificación de los agentes fundamentalmente, que serían: los Estados, los grupos terroristas, grupos de hackers(crackers), delincuentes y mercenarios ocasionales, hacktivistas, cibervándalos y empresas. En nuestra opinión, en estas clasificaciones el término delincuente o ciberdelincuente es demasiado genérico y, por tanto, poco informativo; lo mismo ocurre con el de hackers (crackers).

Partiendo de estas categorías, proponemos una clasificación que tenga en cuenta tanto los objetivos, como la posición sociopolítica de los agentes. Aunque los objetivos y las funciones son dinámicos y en muchas ocasiones confluyen, el móvil principal puede estar enfocado en el concepto de poder o basarse en una motivación más estrictamente económica. A su vez, en el primero de los casos, la ciberdelincuencia puede ejercerse desde los propios grupos hegemónicos y de poder o desde grupos subalternos o minoritarios a modo de resistencia.

Igualmente existen diferentes niveles que van desde lo macro a lo micro, desde las propias relaciones internacionales entre países y compañías multinacionales, pasando por grupos dentro de países y comunidades, y llegando hasta los propios sujetos sociales en sus procesos de identificación a grupos, creencias, valores e ideologías determinadas. La ciberdelincuencia, a su vez, puede ejercerse de manera más horizontal o vertical en cuanto la jerarquía política y económica, de manera unidireccional o establecerse relaciones de reciprocidad negativa (Sahlins, 1963), que no son reconocidas abiertamente.

7.1. Ciberdelincuencia y economía

Una de las principales motivaciones para la ciberdelicuencia pone su foco en los beneficios económicos que se pueden obtener haciendo uso de estos medios. A veces se ejerce de una manera más horizontal desde unos sujetos o pequeños grupos a otros por medio de "ciberestafas". Otras, vienen de manera vertical, desde determinadas empresas que tratan de conocer y controlar el comportamiento de sus clientes de hecho o potenciales con el fin de incrementar sus beneficios económicos. Estas empresas, en ocasiones, entran en confrontación entre ellas, de una manera más horizontal, o incluso traspasan fronteras estatales y buscan una posición de poder en el ámbito internacional que les permita, además, alcanzar una situación económica más ventajosa.

methaodos.revista de ciencias sociales, 2022, *10*(2): 243-258

7.1.1. Ciberestafadores

Como hemos señalado, la ciberestafa se refiere a acciones guiadas por un fin de ganancia económica. Puede llevarse a cabo por ciberdelincuentes individuales o por grupos organizados. Las empresas y cualquier ciudadano son las víctimas principales, y entre estos aquellos que descuidan la seguridad de sus equipos.

El perfil del ciberestafador viene marcado por su objetivo que es fundamentalmente económico, sin fines políticos o militares. La actividad de estos ciberdelincuentes es de las más relevantes; de hecho, las denuncias sobre estafas son las más altas entre las tipologías de delitos reportadas, resultando un 88,1% del total en 2019 (véase Tabla 2).

Como señala Gil (2017) su peligrosidad puede ir más allá de la estafa, pues al tener capacidades para realizar ciberataques puedan ser contratados por grupos de ciberterrorismo o cibercrimen.

7.1.2. Empresas

Las empresas son frecuentemente víctimas de ataques, pero también algunas son agentes inductores de los mismos. Las empresas privadas desarrollan su actividad en un duro sistema de competencia donde el éxito y el fracaso, el crecimiento o la desaparición, no depende sólo de ellas mismas sino de los desarrollos de sus competidores. Desde siempre, algunas empresas han conseguido acceder a información crítica de la competencia —nuevos productos, prototipos o estrategias— a través de medios ilegales, como pagar a empleados corruptos o contratando espías. En la actualidad el ciberespionaje industrial está en manos de hackers que intentan acceder a los servidores de las compañías para recolectar toda la información que sea provechosa: datos personales, secretos industriales o bienes protegidos por la propiedad intelectual, como patentes o productos emergentes; pero también para desarrollar ataques de sabotaje contra sus competidores. Estos ataques no siempre salen a la luz, pues las empresas intentan resolver estas cuestiones fuera del alcance del público para evitar efectos negativos sobre su imagen y reputación.

Otra forma de ciberespionaje es la recolección de datos personales de los usuarios. Se trata de una actividad generalizada a la que todo el mundo está expuesto. Todo lo que se hace a través de Internet es rastreado, almacenado y procesado, para crear perfiles sobre gustos y comportamiento. Estos perfiles se venden y utilizan para realizar campañas de publicidad dirigida.

7.2. Ciberdelincuencia y poder

La ciberdelincuencia se ha erigido como una herramienta de control social y para el ejercicio del poder, pues las nuevas herramientas tecnológicas permite monitorizar en tiempo real el comportamiento de sujetos sociales y adoptar medidas, a veces coercitivas para reprimir conductas, y otras no coercitivas para influir, promulgar ideologías, construir lo deseable, o en definitiva, establecer pensamientos hegemónicos (Gramsci, 1999).

7.2.1. Estados y grupos patrocinados

Como afirma Quintana (2018, parr. 1), "el mayor riesgo para la seguridad en Internet no son los delincuentes informáticos, sino los Estados que han encontrado en la tecnología una herramienta de control casi absoluto". Los actores Estado son el principal impulsor de ciberataques y el que dispone de mayores capacidades. Las acciones que realizan tienen por objetivo la ciberguerra, cibervigilancia, ciberespionaje y de influencia. Como indica el Consejo Nacional de Seguridad (2019):

> Las mayores capacidades corresponden principalmente a actores estatales (organismos de inteligencia o militares), que fundamentalmente operan a través de las denominadas Amenazas Persistentes Avanzadas (APT). Un tipo de amenaza en la que el adversario posee sofisticados niveles de conocimiento y de recursos e infraestructuras para, mediante múltiples tipos de ataques, interactuar sobre sus objetivos por un extenso periodo de tiempo, adaptarse a los esfuerzos del defensor para resistir, así como mantener el nivel de interacción para ejecutar sus objetivos (p. 7).

methaodos.revista de ciencias sociales, 2022, *10*(2): 243-258

Los ataques pueden dirigirse al sector público, infraestructuras críticas, empresas y ciudadanos. En definitiva, nada escapa a sus objetivos, que se concretarían en:

1. El ciberespionaje sobre otros estados, empresas y ciudadanos[9].
2. La cibervigilancia, monitorizando la actividad de los ciudadanos para el control social. De este modo la tecnología ha permitido el máximo desarrollo del panoptismo (Bentham, 1979; Foucault, 2008) que se ha expandido a niveles estatales e incluso globales. El objetivo es conocer y controlar a la disidencia o generar miedo para que las personas no utilicen el ciberespacio de manera libre. En estos casos, la libertad de expresión está conculcada y conectaría con el siguiente objetivo: la cibercensura.
3. La cibercensura es otro de los objetivos, pues las nuevas capacidades de las personas para publicar, organizarse y promover acciones en el ciberespacio ponen en riesgo la estabilidad de ciertos regímenes. Así, algunos gobiernos han comenzado a tomar medidas para preservar sus intereses. Las acciones consisten en restringir acceso a determinados sitios web y redes sociales, penalizar comentarios en foros, sancionar con multas o incluso cárcel a aquellos que publican informaciones que puedan comprometer a las élites. Según Reporteros Sin Fronteras, en los primeros lugares de la lista de los principales enemigos de Internet están: China, Irán, Siria e Uzbekistán, entre otros (RSF, 2017). Todos ellos un amplio historial en violación de los Derechos Humanos.
4. La ciberguerra, esto es, actuaciones o confrontaciones en el ciberespacio entre organizaciones militares cuyo objetivo es la dominación militar o política. La diferenciación con el ciberterrorismo a veces no está clara, ya que las acciones siguen pautas similares.
5. La influencia es otro de los objetivos de los Estados. Se trata de ataques dirigidos a las personas en general con la intención de desinformar, generar alarma, miedo, inestabilidad social, manipular el voto o promocionar movimientos desestabilizadores dentro de otros países.

Estos cincos objetivos se utilizan con frecuencia simultáneamente en el diseño de acciones híbridas. La tendencia es que cada vez más estados son capaces de realizar ciberataques bien a través de sus propios medios militares y técnicos o bien a través de grupos patrocinados. Entre los países más activos estarían: Estados Unidos, China, Rusia y Corea del Norte (Quintana, 2018). Aunque como apunta Yolanda Quintana más de 100 países tienen capacidades militares en el ciberespacio y el número sigue creciendo.

En respuesta a esta nueva situación, en la Cumbre de Varsovia de la OTAN de 2016, los jefes de Estado y de Gobierno reconocieron el ciberespacio como un nuevo dominio de operaciones militares (NATO, 2016). El ciberespacio se convierte así en el quinto dominio de guerra, uniéndose a los tradicionales: aire, tierra, mar y espacio. Un dominio artificial, creado por el ser humano, pero desde el que se puede afectar a los otros cuatro.

Como ya apuntaba Álvarez Munárriz (2013) ciertos estados "hace tiempo que están librando la batalla de la denominada ciberguerra: el uso de las tecnologías digitales para conocer y así poder atacar y destruir los centros vitales del otro y de sus de los aliados. Las superpotencias están obsesionadas por la ciberseguridad. De momento esta guerra solamente se está librando en el ciberespacio y su impacto real es muy limitado y además conocido y consensuado entre ellas. Pero no podemos en manera alguna descartar el peligro de un enfrentamiento militar si lo que por el momento es solamente virtual se convierte en real" (p. 22). Para ilustrar el potencial destructivo y desestabilizador de las acciones de ciberguerra revisaremos dos casos: el primero, el virus Stuxnet descubierto en 2010, una ciberarma diseñada para dañar las plantas de enriquecimiento nuclear de Natanz (Irán), con el objetivo de ralentizar los avances del país en esta área. El virus alcanzó los ordenadores que controlaban las centrifugadoras alterando el funcionamiento de estas. Se sospecha que detrás puedo estar EEUU o Israel, pues ambos se oponían firmemente al desarrollo nuclear iraní. El éxito de la operación dejó claro el poder de un ciberataque y es un aviso sobre los efectos terribles que se pueden producir.

El segundo caso es la injerencia en las elecciones presidenciales de 2016 en EEUU, en las que el candidato republicano Donald J. Trump alcanzó la presidencia. Un informe del Departamento de Seguridad Nacional estadounidense (NSA, por sus siglas en inglés) y del FBI, apuntaban a Rusia como responsable de los ciberataques y difusión de correos electrónicos sensibles del Partido Demócrata (Fernández, 2016). Al menos

[9] Algunos casos documentados de ciberespionaje gubernamental son: GhostNet, Red Shadow, Titan Rain y Moonlight Maze.

methaodos.revista de ciencias sociales, 2022, *10*(2): 243-258

60.000 correos electrónicos fueron robados y posteriormente publicados por Wikileaks, lo que provocó la dimisión de altos funcionarios y una gran vergüenza para el Partido Demócrata y la campaña Hillary Clinton. Incluso existen sospechas de que se intentó *hackear* al propio sistema electoral (Smith y Swaine, 2017).

Estos dos ejemplos son suficientemente ilustrativos para reconocer la situación. Estamos asistiendo a continuos ataques de unos países sobre otros, algunos expertos en seguridad hablan de ciberguerra fría, donde "las grandes potencias están midiendo las fuerzas del contrario a través de ciberataques, a la vez que intentan conseguir algún tipo de ventaja sobre el adversario" (Sánchez-Vera, 2018). Como indica Sanjay Goel (2020) "las ramificaciones de los ataques son cada vez más peligrosas y el aventurismo de los países sigue aumentando. Los países están recurriendo a ataques cibernéticos en lugar de ataques convencionales debido a la atribución nebulosa y al menor temor a la condena". Esta situación obliga a que los países que se incorporan y crecen en el ciberespacio desarrollen capacidades defensivas que permitan repeler los ataques (Gil, 2017).

7.3. Ciberdelincuencia y resistencia

Del mismo modo que la ciberdelicuencia puede tener como fin alcanzar, mantener o incrementar el poder, también puede constituir un modo de resistencia a ese poder establecido.

7.3.1. Cibervándalos

La extrapolación del vandalismo del espacio físico al ciberespacio obedece en cierto modo a motivaciones similares. Éstas pueden ser variadas y constituir desde una manifestación de lo que Scott (1985) denominara "armas de los débiles", es decir, una forma a pequeña escala de resistencia a los poderes y normas establecidas, hasta retos para demostrar el conocimiento entre iguales o como forma de "autosuperación". El relativo anonimato del ciberespacio permitiría el ocultamiento necesario.

La sutil diferencia es que el vandalismo callejero puede ser espontáneo y requiere poco esfuerzo, pero en el ciberespacio es necesaria la premeditación y preparación para ejecutarlo. Algunos cibervándalos dedican una cantidad colosal de tiempo y esfuerzo para conseguir dañar equipos, aplicaciones y datos de sus víctimas.

El perfil tradicional es el de un programador; de hecho, la mayoría de los primeros virus informáticos fueron creados por jóvenes programadores. Actualmente, sigue predominando este perfil de estudiante de programación que quiere poner a prueba sus habilidades y mostrarlas a sus pares. A estos se suman cada vez más jóvenes que sin ser programadores disponen de mucho tiempo para aprender nociones básicas a través de páginas y blogs de *hacking*, recopilan *malware* y lo lanzan contra sus víctimas. Aunque cualquiera puede ser víctima, el impacto del cibervandalismo es de baja intensidad.

7.3.2. Hacktivistas

La configuración de Internet como espacio para la resistencia se ve manifestada explícitamente en su versión más radical mediante el ciberactivismo o hacktivismo.

El objetivo básico de los hacktivistas son la denuncia y la transformación social. Los movimientos hacktivistas son de todas las ideologías y tendencias políticas. Entre los grupos más famosos y prolíficos de la última década destacan Anonymous y Wikileaks. Pero, en la actualidad, están debilitados y han aparecido otros como OpGreenRights, OpChile o OpCalunia, muy activos en los últimos años.

Para trazar el perfil del hacktivista o de los movimientos hacktivistas debemos partir de que no es una cualidad estable en las personas, el hacktivista aparece cuando se dan las circunstancias. Partiendo de aquí, podemos apuntar que con frecuencia actúan individualmente y cuando se agrupan no existen jerarquías ni estructuras estables, los liderazgos son puntuales, están orientados a una acción concreta y vinculados a una capacidad específica que le atribuye al sujeto el liderazgo para ejecutarla. El adherente de los miembros de un grupo es una ideología y unos objetivos compartidos sobre los que se deciden las acciones. De manera general las acciones van dirigidas a promover un cambio político, bien para defender y dar a conocer una causa bien para castigar a una persona, organización o gobierno que consideran no ético según sus

methaodos.revista de ciencias sociales, 2022, *10*(2): 243-258

principios e ideario. Causas comunes de los hacktivistas son, por ejemplo, defender los derechos laborales, el medioambiente, las libertades, denunciar la corrupción, el feminismo[10], etc.

Las acciones que llevan a cabo son variables, pero suelen interesarse por ataques DoS sobre un servicio online, recopilación de información confidencial para su difusión, acceso ilícito a un sitio web para desfigurarlo y publicar sus mensajes sobre objetivos políticos. Creación y distribución de *software* malicioso para realizar sus ataques, así como formación y asesoramiento para el ciberactivismo. En general, se puede afirmar que el hacktivismo no es peligroso en el sentido material, pues los daños son reversibles, otra cuestión son los daños morales, de credibilidad y de imagen que pueden sufrir las víctimas.

Según el Centro Criptológico Nacional, en su informe Anual 2019 Hackitivismo y Ciberyihadismo, el escenario hacktivista sigue una tendencia de degeneración, desideologización y atomización de identidades individuales desorganizadas movidas por el afán de notoriedad y sin una conciencia colectiva. Tampoco, los efectos de las acciones registradas han sido de relevancia. Respecto al ciberyihadismo, indica que aparenta una total desestructuración y sólo se dan acciones individuales de baja visibilidad sobre webs, desfigurándolas y publicando mensajes de contenidos islamistas.

7.3.3. Ciberterroristas

No cabe duda de que una de las formas más destructiva de ciberdelincuencia es el ciberterrorismo, esto es, el uso del ciberespacio con fines terroristas. Un ciberterrorista es aquel que aplica violencia por medio de ciberataques "para producir un daño directo contra un objetivo y un efecto indirecto contra una audiencia más amplia (generación del terror en la sociedad, advertencia a las instituciones estatales)" (CCN-CERT, 2020). Los objetivos pueden ser cambios políticos, reclutar seguidores, financiación para su organización o dar notoriedad a su causa. Las acciones del ciberterrorismo responden a una motivación ideológica y las consecuencias son más graves que la ciberdelincuencia común, pues causa alarma social y pánico colectivo.

Los grupos ciberterroristas conectan, a través del ciberespacio, no sólo con sus miembros sino con otras organizaciones. Es común encontrar publicaciones de apoyo entre grupos de todo el mundo que intercambian información sobre la logística, planificación y ejecución de atentados —como construir bombas, crear y organizar una célula terrorista, perpetrar ataques— (Subijana Zunzunegui 2008).

Aunque cualquier usuario puede ser víctima, el ciberterrorismo se focaliza en el ámbito de economía nacional y también a menor nivel en sectores empresariales, que pueden terminar afectando a las pequeñas empresas. Las consecuencias más significativas de este tipo de delitos son económicas y de imagen. Pero, sin duda, la gran aspiración de los grupos terroristas son las infraestructuras críticas del país, pues saben que estas pueden ser accedidas y manipuladas a través de un ataque digital con consecuencias catastróficas, tanto a nivel económico como vital.

El Centro Criptológico Nacional distingue el concepto de ciberterrorismo y ciberyihadismo e indica que durante 2019 no se identificaron operaciones de ciberyihadismo y sigue sin haber evidencias de capacidades ofensivas de estos grupos (CNN, 2020). Sin embargo, se debe estar alerta, pues cada vez las infraestructuras críticas tienen mayor dependencia de Internet, haciéndolas más vulnerables; en consecuencia, el ciberterrorismo no puede verse como un problema con impacto puntual o individual sino como un problema de seguridad nacional.

8. Conclusión

El ciberespacio se expande en dos dimensiones: la primera y más evidente en extensión, la capa física se está desplegando por todo el planeta a través de cables y satélites; la capa lógica se perfecciona, multiplicando sus funciones y servicios; y la capa social crece en número de personas, actividades e interacciones.

La segunda dimensión tiene que ver con la profundidad. El ciberespacio ha dejado de ser un espacio aparte o superpuesto para penetrar en los objetos. Los objetos inteligentes que conforman el IoT son capaces de analizar sus estados internos y externos, tomar decisiones y comunicarse con otros objetos o

[10] Sobre el Ciberfeminismo y hackfeminismo recomendamos consultar mujeresenred.net (España), apcwomen.org (EEUU), https://escuelafeminista.red/ (Centroamérica), rimaweb.com.ar (Argentina) o famafrique.org (África). Y para quien desee profundizar aún más: https://www.pikaramagazine.com/2018/02/hackers-ciberfeminismo-y-revolucion/

methaodos.revista de ciencias sociales, 2022, *10*(2): 243-258

personas. Cualquier objeto cotidiano puede convertirse en inteligente. Este avance del ciberespacio en profundidad genera una mayor interdependencia entre lo físico y lo virtual con implicaciones para la seguridad. Entre los ámbitos donde estos objetos se aplican, quizás el más inquietante es el del cuerpo. Los objetos inteligentes, como los *smartphones* y *smartwatch,* son ya elementos cotidianos que se portan sobre los propios cuerpos. El *smartphone* se puede separar, el *smartwatch* se lleva atado. La siguiente generación de objetos inteligentes salta la barrera de la piel para integrarse en el cuerpo. Los desarrollos han empezado en el campo de la salud, con implantes biónicos conectados a la Red, por ejemplo, las bombas de insulina que se conectan con una aplicación para monitorizar y regular su funcionamiento, al mismo tiempo que envía datos a servidores lejanos para usos diagnósticos y terapéuticos.

Pero, como hemos visto, este proceso de expansión está empañado por las ciberamenazas y los riesgos que se originan. No cabe duda de que la cibercriminalidad puede suponer un freno e incluso el cuestionamiento de ciertas actividades; pero no hay renuncia posible, el ciberespacio se ha integrado en la realidad y, en cierto modo, se ha puesto al servicio del desarrollo humano. En este sentido, aumenta la consideración del ciberespacio e Internet como bien público, con dos implicaciones para los Estados: garantizar las condiciones necesarias para que los ciudadanos puedan hacer un uso seguro y ofrecer acceso a Internet a toda la población.

La confianza en un ciberespacio seguro resulta básica. Pero para ello el Estado debe favorecer y trabajar por unas condiciones de seguridad que garanticen la confidencialidad, integridad y disponibilidad de los datos y las comunicaciones. Las ciberestafas, cibervigilancia, ciberespionaje, ciberterrorismo y la ciberguerra obliga implementar políticas que protejan las infraestructuras críticas del país y que garanticen los derechos de los ciudadanos (Sancho, 2017).

Por su parte, el acceso a la Red exige a las autoridades el desarrollo de políticas que aborden las desigualdades socioeconómicas que afectan al acceso equitativo, así como la formación para desarrollar las competencias y destrezas que el ciudadano necesita para hacer un uso pleno del nuevo espacio. La competencia en ciberseguridad de las personas se tiene que reforzar. Un uso incorrecto por parte del usuario, por accidente, desidia o por el engaño de un ciberdelincuente puede suponer una oportunidad para un atacante. Actualmente, los ciberataques más comunes utilizan como arma la ingeniería social, pues todavía es más fácil manejar a las personas que a las máquinas.

Nadie cuestiona que la solución para prevenir ataques pasa por la formación y concienciación de los ciudadanos. Sin embargo, esta labor va a remolque de las circunstancias pues, tradicionalmente, los estudios sobre seguridad de los nuevos entornos tecnológicos se han focalizado en los aspectos técnicos y se han dirigido a la capa física y lógica, olvidando a las personas. El ciberespacio está avanzando más rápido que la capacidad global para adaptarse, comprenderlo y contribuir críticamente en su desarrollo. Esto es algo que debemos revertir.

Por supuesto, no cabe duda de que la ciberseguridad requiere de la participación de programadores y administradores de redes, pero también de otros expertos, especialmente del mundo de las ciencias sociales que estudien el comportamiento humano en el ciberespacio y ayuden a crear mejores soluciones tanto técnicas como de concienciación y formación. En consecuencia, debemos estudiar tanto la ciberdelincuencia como las víctimas potenciales dentro del contexto sociocultural en el que se desarrollan. Y, desde esta perspectiva, entendemos que las personas no pueden tratarse como un agente pasivo o como el elemento más débil de la cadena de la seguridad, debemos reorientar esa mirada y verlas como el mayor activo para protegerse en el ciberespacio. Consideramos necesario un enfoque antropológico del ciberespacio, donde confluyan ciberdelitos, ciberarmas, ciberdelicuentes y posibles víctimas. Lo que obliga como ha quedado patente a incluir una perspectiva sociocultural y educativa en las actuaciones para garantizar la seguridad, sólo así podremos abordar los retos actuales y futuros vinculados a los avances en la relación-hombre máquina, la actividad inmersiva virtual y las experiencias mediadas por la inteligencia artificial y los algoritmos, así como una caracterización de las víctimas potenciales que permitan acciones más precisas. Líneas de investigación emergentes que requieren de un abordaje sistémico y multidisciplinar, pues en ningún caso, los problemas que atañen a la seguridad y los derechos pueden resolverse como una cuestión meramente técnica.

Referencias

Álvarez Munárriz, L. (2013). Foreword: anthropological approach to security. En F. Antón, G. Ercolani, y (Edts.), *Anthropology and Security Studies*. Universidad de Murcia, Nottingham Trent University y College of William and Mary (USA).

Bentham, J. (1979). *El panóptico.* La Piqueta.

CCN-CERT. (2020). *Ciberamenazas y tendencias. Edición 2020*. Centro Criptológico Nacional, CCN-CERT. Centro Criptológico Nacional. https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos.html?limit=100

Clark, D. D. (2010). Characterizing cyberspace: Past, present and future (ECIR Working Paper No. 2010-3). MIT Political Science Department.Version: Author's final manuscript. https://hdl.handle.net/1721.1/141692

CNN. (2020). *Hacktivismo y ciberyihadismo. Informe anual 2019*. Centro Criptológico Nacional.

Consejo Nacional de Seguridad. (2019). Orden PCI/487/2019, de 26 de abril, por la que se publica la Estrategia Nacional de Ciberseguridad 2019, aprobada por el Consejo de Seguridad Nacional. Boletín Oficial del Estado. https://www.boe.es/eli/es/o/2019/04/26/pci487

Dunn Cavelty, M. (2013). From Cyber-Bombs to Political Fallout: Threat Representations with an Impact in the Cyber-Security Discourse. *International Studies Review, 15*(1), 105-122. https://doi.org/10.1111/misr.12023

Europol. (3 de enero de 2020). *Europol*. https://www.europol.europa.eu/crime-areas-and-trends/crime-areas/cybercrime

Fernández, C. (30 de diciembre de 2016). Así se produjo el ciberataque ruso en la campaña electoral de EE UU, según el FBI. *El País.* https://bit.ly/3y53OH2

Foucault, M. (2008). *Vigilar y castigar. Nacimiento de la prisión.* Siglo XXI.

Gartner. (7-11-2018). *Gartner.* Gartner Identifies Top 10 Strategic IoT Technologies and Trends. https://gtnr.it/2JLiEbA

Gerber, M., y Solms, V.R. (2005). Management of risk in the information age. *Computers y Security, 24*(1).

Gil, J.M. (11-10-2017). La integración del ciberespacio en el ámbito militar. *Grupo de estudios en seguridad internacional.* https://bit.ly/3C0T918

Goel, S. (2020). National Cyber Security Strategy and the Emergence of Strong Digital Borders. *Connections: The Quarterly Journal, 19*(1), 73-86.

Gramsci, A. (1999) *Antología.* Selección, traducción y notas de M. Sacristán. Siglo XXI.

Greenwald, G., MacAskill, E., y Poitras, L. (11 de junio de 2013). Edward Snowden: the whistleblower behind the NSA surveillance revelations. *The Guardian.* https://bit.ly/3fyY4PC

INCIBE. (2020). *Seguridad en la instalación y uso de dispositivos IoT*. (I. N. CIBERSEGURIDAD, Ed.). https://bit.ly/3SpP5yx

ISO. (2004). ISO/IEC 13335-1:2004. Information technology - Security techniques - Management of information and communications technology security - Part 1: Concepts and models for information and communications technology security management. https://bit.ly/3y2dpP6

ISO. (2005). ISO/IEC 27002: code of practice for information security management. https://bit.ly/3C1oAsx

IWS. (2020). *Internet Growth Statistics.* https://www.internetworldstats.com/emarketing.htm

Kaspersky. (26 de febrero de 2018). Las prótesis e implantes inteligentes abren la puerta a nuevas ciberamenazas en el cuerpo. *Europapress.* https://bit.ly/3y4CdpC

Lévy, P. (2007). *Cibercultura. Informe al Consejo de Europa.* Anthropos.

Ministerio del Interior. (2019). *Estudio sobre la cibercriminalidad en España.* https://bit.ly/3Rk4PC0

NATO. (8-9 Julio, 2016). *NATO.* Obtenido de Warsaw Summit Communiqué: https://bit.ly/3UTAehu

Quintana, Y. (2016). *Ciberguerra. Todo lo que no sabes sobre las nuevas amenazas y las guerras que ya se libran en la red.* Los libros de la Catarata.

Quintana, Y. (2018). Ciberseguridad, una cuestión de Estados. *Política exterior,* (185). https://bit.ly/3UVf0QC

Rayón-Ballesteros, M.C., y Gómez-Hernández, J.A. (2014). Cibercrimen: particularidades en su investigación y enjuiciamiento. *Anuario Jurídico y Económico Escurialense*, 209-234.

RSF. (2017). *Censura y vigilancia de periodistas: un negocio sin escrúpulos.* Reporteros Sin Fronteras. https://bit.ly/3riF8ab

Sahlins, M. (1963). "On the Sociology of Primite Exchange". En M. Gluckman y F. Eggan (Eds.), *The Relevance of Models for Social Anthropology* (pp.139-236). F. Praeger.

Sánchez-Vera, F. (2018). The dissolution of Cyberspace. En I. Mack, y R. Payne, *Cyberspace. Trends, Perspectives and Opportunities* (pp. 19-38). Nova Science Publishers.

Sancho, C. (2017). Ciberseguridad. Presentación del dossier/Cybersecurity. Introduction to Dossier. *URVIO. Revista Latinoamericana De Estudios De Seguridad,* (20), 8-15. https://doi.org/10.17141/urvio.20.2017.2859

Scott, J.C. (1985). *Weapons of the Weak: Everyday Forms of Peasant Resistance*. Yale University Press.

Smith, D., y Swaine, J. (5 junio, 2017). Russian agents hacked US voting system manufacturer before US election – report. *The Guardian*. https://bit.ly/3dXA0W6

Subijana Zunzunegui, I. J. (2008). El ciberterrorismo: Una perspectiva legal y judicial. *Eguzkilore,* 169-187. https://www.ehu.eus/documents/1736829/2176658/08+Subijana.indd.pdf

Tankovska, H. (23 septiembre, 2020). *Statista*. Obtenido de Connected wearable devices worldwide 2016-2022: https://www.statista.com/statistics/487291/global-connected-wearable-devices/

Verizon. (2020). *Data breach investigation report. 2020.* https://vz.to/2USiMeb

Von Solms, R., y van Niekerk, J. (2013). From information security to cyber security. *Computer y security, 38,* 97-102. https://doi.org/10.1016/j.cose.2013.04.004

Whitman, M., y Mattord, H. (2009). *Principles of Information Security*. Thompson Course Technology.

Breve CV de los autores/as

Fulgencio Sánchez Vera es doctor en Antropología Social y Cultural. Durante veinte años ha sido docente en enseñanza secundaria y ha impartido numerosos cursos de formación al profesorado de secundaria a través de los Centros de Formación del Profesorado. Actualmente es docente de la Universidad Internacional de la Rioja y de la Universidad de la Laguna. Entre sus líneas de investigación destacan la convivencia escolar y la transformación de los modelos de relación socioeducativa,la escuela y la educación en valores,los recursos educativos, el ciberespacio y la ciberseguridad, los efectos de la tecnología digital sobre la atención y la formación en mindfulness.

Javier Eloy Martínez Guirao es doctor en Antropología Social por la UNED y doctor en Sociología por la Universidad de Alicante. Es Profesor Titular del área de Antropología Social de la Universidad de Murcia. Forma parte de los grupos de investigación "Cultura y sociedad" de la Universidad de Murcia y "Economía, cultura y género" (ECULGE) de la Universidad Miguel Hernández de Elche. Ha realizado diferentes investigaciones desde una perspectiva socioantropológica en líneas como el cuerpo, las artes marciales, la economía, el trabajo, las masculinidades, el turismo, la educación, la salud, el ciberespacio, entre otras. Director de la Revista *Nuevas Tendencias en Antropología* (desde 2010). Vicedecano de Calidad e Investigación de la Facultad de Trabajo Social de la Universidad de Murcia (desde 2019).

Anastasia Téllez infantes es doctora en Antropología Social y Profesora Titular de Antropología Social y Cultural del Departamento de Ciencias Sociales y Humanas de la Universidad Miguel Hernández de Elche (Alicante, España). Desde hace 28 años investiga sobre la construcción sociocultural de las identidades masculinas y femeninas con perspectiva de género. Asimismo, es Directora del Grupo de Investigación ECULGE (Economía, Cultura y Género) y del Título propio de postgrado de "Especialista universitario en masculinidades, género e igualdad" (2020-2021) (UMH). También es fundadora y directora (2002-2012) del Seminario Interdisciplinar de Estudios de Género (SIEG) e integrante del Centro Interdisciplinar de Estudios de Género (CIEG).

Declaración de autoría CRediT

Conceptualización: F.S.V, J.E.M.G, A.T.I.; Metodología: F.S.V, J.E.M.G, A.T.I.; Validación: F.S.V, J.E.M.G, A.T.I.; Investigación: FSV, JEMG, AT; Redacción (borrador original): F.S.V, J.E.M.G, A.T.I.;Redacción (revisión y edición): F.S.V, J.E.M.G, A.T.I.