Recebido: 15/10/2021
Aceito: 10/11/2021
Disponível: 29/11/2021

sapienza International Journal of Interdisciplinary Studies
ISSN: 2675-9780

https://doi.org/10.51798/sijis.v2i4.145

El ciber-espionaje como herramienta estratégica de los actores internacionales en la era digital: una revisión desde la literatura

Cyber-espionagem como ferramenta estratégica para atores internacionais na era digital: uma revisão da literatura

Cyberespionage as a strategic tool for international actors in the digital age: a review from the literature

David Horacio García Waldman
david.garciaw@uanl.mx
Universidad Autónoma de Nuevo León – México
ORCID: 0000-0002-0623-4874

Gustavo Daniel Ortiz Téllez
gustavo.ortiz.tellez@gmail.com
Universidad Autónoma de Nuevo León – México
ORCID: 0000-0002-4340-2232

Paola Giselle Santos Sánchez
paola95.santos@gmail.com
Universidad Autónoma de Nuevo León – México

RESUMEN

El presente estudio tiene como objetivo analizar y establecer la tipificación del uso del ciber espionaje como herramienta que permite alcanzar objetivos de los actores en el sistema internacional. Este estudio estriba en tipo cualitativo, siendo no experimental, enfocándose en la recolección de documentos históricos y científicos para su análisis y descripción. La primera fase es utilizada como un medio de revisión de literatura sobre el ciber espionaje y el comportamiento de los actores internacionales a través del tiempo para recolectar y analizar las investigaciones existentes sobre dicha problemática, la segunda fase se enfoca principalmente en establecer a los principales actores internacionales que recurren al ciber espionaje como medio para alcanzar sus objetivos. Se pretende que lo expuesto en el presente documento tenga la trascendencia suficiente para abrir paso a nuevos estudios enfocados en el tema.

Palabras clave: Ciber-Espionaje, Era digital, Diplomacia, Globalización, Relaciones Internacionales.

RESUMO

O presente estudo tem como objetivo analisar e estabelecer a tipificação do uso da cyber-espionagem como ferramenta que permite atingir os objetivos dos atores do sistema internacional. Este estudo é qualitativo, sendo não experimental, com foco no acervo de documentos históricos e científicos para análise e descrição. A primeira fase é utilizada como meio de revisar a literatura sobre cyber-espionagem e o comportamento dos atores internacionais ao longo do tempo para coletar e analisar as pesquisas existentes sobre o referido problema, a segunda fase se concentra principalmente em estabelecer os principais atores internacionais que recorrem à cyber-espionagem como um meio para atingir seus objetivos. Pretende-se que o exposto neste documento seja de suficiente importância para abrir caminho a novos estudos voltados para o assunto.

Palavras-chave: Cyber-espionagem, Era Digital, Diplomacia, Globalização, Relações Internacionais.

ABSTRACT

The present study aims to analyze and establish the typification of the use of cyber espionage as a tool that allows reaching the objectives of the actors in the international system. This study is qualitative, being non-experimental, focusing on the collection of historical and scientific documents for analysis and description. The first phase is used as a means of reviewing the literature on cyber espionage and the behavior of international actors over time to collect and analyze existing research on said problem, the second phase focuses mainly on establishing the main actors internationals who resort to cyber espionage to achieve their objectives. It is intended that what is stated in this document is of sufficient importance to open the way to new studies focused on the subject.

Recebido: 15/10/2021
Aceito: 10/11/2021
Disponível: 29/11/2021

sapienza International Journal of Interdisciplinary Studies
ISSN: 2675-9780

https://doi.org/10.51798/sijis.v2i4.145

Keywords: Cyber-Espionage, Digital Age, Diplomacy, Globalization, Foreign Affairs.

1. INTRODUCCION

La presente investigación tiene como objetivo la identificación del uso del ciber espionaje como herramienta que permite alcanzar objetivos de los actores internacionales. Esta investigación se enfocó en investigaciones previas como la de Sánchez Madero (2013), Konakalla & Veeranki (2013) Alfonso Beltrán (2015), Alfonso Hirare (2017), Mejías Alonso (2016) y Amaral (2014). Donde se analizaron factores económicos, sociales y políticos que determinaron el uso del ciber espionaje como herramienta de seguridad por parte de los actores internacionales. Este trabajo de disertación conduce una investigación teórica de tipo exploratoria, no experimental y descriptiva, estableciendo como pregunta de investigación: ¿Los Estados, las empresas y los grupos terroristas son actores internacionales que recurren al ciberespionaje como medio para alcanzar sus objetivos? En la fase exploratoria se revisaron documentos científicos de forma exhaustiva con la finalidad de recopilar, analizar y correlacionar información de diferentes fuentes. La metodología de este estudio permitió exponer el vacío que existe en investigaciones pasadas que se enfocaron de manera específica al uso del ciber espionaje por parte de actores internacionales. Concluyendo que:

Resultado 1: Los Estados, las empresas privadas globales y los grupos terroristas utilizan el ciber espionaje como herramienta para alcanzar sus objetivos.

Resultado 2: Los principales objetivos de un Estado para utilizar ciber espionaje son la Seguridad y Defensa de un país, así como también el control sobre la sociedad.

Resultado 3: Los principales objetivos de los grupos terroristas para utilizar ciber espionaje son la identificación de blancos y la obtención de información confidencial.

Resultado 4: Los principales objetivos de las empresas privadas globales para utilizar ciber espionaje son el adecuarse a las necesidades de los consumidores y la obtención de información de la competencia, proveedores y grupos de interés.

2. PROCEDIMIENTO METODOLÓGICO

El presente estudio es de carácter documental y exploratorio abarcando principalmente la recolección de literatura científica para la realización de este. El diseño de este estudio documental y exploratorio es: no experimental y descriptivo, debido a que se pretende analizar, observar y describir la información sin algún tipo de práctica o técnica que altere los resultados dados de manera natural y exploratoria, según Hernandez et al. (2014) realizar dicha acción nos puede ayudar a entender el fenómeno central de estudio, y le sirve al investigador para conocer los antecedentes de un ambiente, así como las vivencias o situaciones que se producen en él y su funcionamiento cotidiano y anormal debido a que los resultados pretenden ser generales para que en el futuro puedan ser utilizados como punto de partida para futuras investigaciones con objetivos más concretos, se tomaron como base tres variables (categorías analíticas) para la estructura del estudio, dichas variables son: . Estados Nación, grupos terroristas y empresas privadas globales.

3. FUNDAMENTO TEORICO

3.1 Antecedentes

Recebido: 15/10/2021
Aceito: 10/11/2021
Disponível: 29/11/2021

sapienza International Journal of Interdisciplinary Studies
ISSN: 2675-9780

https://doi.org/10.51798/sijis.v2i4.145

El desarrollo de la investigación inició con una revisión exhaustiva de documentos electrónicos sobre el tema en cuestión, de entre los que destacan artículos de investigación y tesis de nivel maestría y doctorales a través de bases de datos. Dicha búsqueda arrojó como resultado el trabajo de Sánchez Madero (2013) que expone al ciber espionaje como una de las actividades delictivas que más se ha presentado desde el surgimiento de las Tecnologías de Información y Comunicación (de ahora en adelante TICs). A su vez, plantea como a consecuencia de esto, los Estados incorporan a sus agendas de política exterior estrategias de ciberseguridad que, de la misma manera, rayan en lo ilícito al transgredir la soberanía de otros Estados, así como en la violación de tratados internacionales en materia de derechos humanos. Esto, con el objetivo de estudiar actividades de ciber espionaje, así como también de las soluciones que han brindado sobre el tema y las nuevas propuestas que han surgido a partir del crecimiento de esta actividad.

De manera similar Konakalla & Veeranki (2013), en su artículo sobre ataques de seguridad y seguridad tecnológica, presenta como han evolucionado los ataques cibernéticos a lo largo de la historia. Además, hace una relación entre los métodos que se utilizan, las ventajas de cada uno y los programas que facilitan su desmantelamiento. De entre los principales sistemas de ataque, contabiliza el ciberespionaje y expone a la confidencialidad y disponibilidad como algunas de las ventajas que se le asocian a este acto. Los autores también hacen hincapié en que el ciber espionaje es un conjunto de acciones que implican la intercepción o acceso a comunicaciones no autorizadas, la inserción de métodos para distorsionar comunicaciones o crear mensajes falsos, borrar o modificar contenido, entre otros.

Algo similar plantea Alfonso Beltrán (2015), en su investigación llevada a cabo en Valencia, España. En ella recopila casos y análisis de técnicas de ataque mediante internet, con la diferencia de que su objetivo, es evidenciar de manera específica los realizados por los Estados contra otros actores internacionales. Además, dentro de su planteamiento analiza al ciber espionaje como un instrumento estratégico para la ciberseguridad con la finalidad de obtener información que no solo proporcione una ventaja en caso de una confrontación, sino que también permita conocer las intenciones de sus adversarios para evitar el conflicto. Lo anterior, en favor de causas políticas o conflictos bélicos o prebélicos. De igual forma realiza una revisión histórica de la evolución y desarrollo de los métodos de espionaje.

Por su parte Sancho Hirare (2017) realiza un estudio enfocado en la ciberseguridad, en el cual, de manera semejante, expone como uno de los factores de riesgo más frecuentes en el ciberespacio es el espionaje y hace hincapié en que las amenazas cibernéticas, pueden tener diversos orígenes (estatal o no estatal), pero el mismo efecto de perjudicar a las personas, dañar a las organizaciones e impedir el funcionamiento normal de las instituciones. Por este motivo, el autor dedica un apartado para explicar cómo la existencia de ciberdelitos como el ciber espionaje, obligan a reconocer la importancia de la seguridad en el ciberespacio y el de asumir su complejidad.

En lo que toca a Mejías Alonso (2016) reflexiona sobre los sistemas y tecnologías que intervienen en la recopilación, gestión, conservación y análisis de datos masivos y las consecuencias que ello supone en la privacidad; reflejando cómo la gestión documental puede ser, en este caso, una potente herramienta de vigilancia masiva. De manera similar Amaral (2014) en su artículo, plantea de manera general, como existe un alto grado de dependencia en los sistemas informáticos que s Sancho e encargan del procesamiento de datos, por parte los diferentes actores internacionales. De entre los que menciona se encuentran los grupos sociales, organizaciones públicas y privadas, así como las esferas de gobierno que tienen bajo su cargo la seguridad y la defensa de un país.

Cabe destacar que para efectos de este trabajo se tomará como referencia lo descrito por Velázquez Flores, et al. (2019) para definir los conceptos de Sistema Internacional, así como de actor

Recebido: 15/10/2021
Aceito: 10/11/2021
Disponível: 29/11/2021

Sapienza International Journal of Interdisciplinary Studies
ISSN: 2675-9780

https://doi.org/10.51798/sijis.v2i4.145

internacional. Tomando en cuenta lo anterior; un Sistema Internacional se entiende como el conjunto de actores, factores, procesos y patrones que interactúan de manera constante en un espacio y un tiempo determinado, bajo ciertas reglas y en función de un eje rector. En cuanto al termino actor/es se hace referencia a todos aquellos que interactúan dentro del sistema internacional; llámese Estados, organizaciones internacionales, las empresas trasnacionales, los medios de comunicación de impacto internacional, la opinión pública internacional, los grupos de terrorismo trasnacionales, el crimen internacional organizado y los distintos individuos que pueden tener influencia en el sistema internacional.

Retomando el planteamiento inicial si bien, es un hecho el papel positivo que ha desempeñado las TIC 's para la difusión de información y empoderamiento en materia de derechos humanos como resultado de la globalización y el surgimiento de la era digital. Por otra parte, el ciber espionaje se ha ido presentando desde el surgimiento de estas nuevas tecnologías de la información y comunicación, por lo que no es completamente nuevo. Tampoco lo es la discusión sobre las repercusiones a los derechos humanos que resultan del uso de las TIC 's. En distintos contextos, se han desarrollado estudios diversos sobre los beneficios y las consecuencias que las nuevas tecnologías de información y comunicación han implicado para los derechos humanos. Sobre esto, podemos concluir que, en definitiva, las plataformas virtuales y los dispositivos móviles actuales han permitido un avance considerable para la comunicación y el conocimiento, transformándose en fenómeno global irreversible; de ahí la importancia de considerar las implicaciones negativas de los avances en la tecnología como efecto de la globalización sin las debidas regulaciones.

3.2 Planteamiento del problema

La globalización ha interconectado de manera cibernética a muchos actores internacionales y más allá de eso también a la propia sociedad, sin embargo, estos beneficios de la cercanía a través de la web también han provocado ataques cibernéticos por parte de los mismos actores quienes la utilizan día a día, atacándose unos a otros. La reincidencia de estos acontecimientos refleja una realidad en la que el espionaje se mantiene como uno de los medios favoritos para alcanzar objetivos dentro de las estrategias de cualquier actor. A pesar del surgimiento de métodos para recolectar y procesar información de maneras cada vez más eficientes e innovadoras; el espionaje se ha reinventado para adaptarse a las plataformas virtuales. Algo en lo que concuerda Candau (2019) quien lo cataloga como un método relativamente económico, rápido y que implica menos riesgos que el espionaje tradicional, porque dada la dificultad de atribución de la autoría, siempre cabe la posibilidad de negar su uso. Por ello, es importante reconocer al ciberespionaje como parte de las implicaciones negativas que trajo consigo la globalización tecnológica; y entender de qué manera su uso, repercute a los derechos humanos en materia de seguridad y privacidad, así como también en el derecho a la no intervención y en la soberanía de los Estados

Sancho Hirare (2017) nos menciona que la ciberseguridad constituye una condición para permitir que los ciudadanos, las organizaciones e instituciones puedan beneficiarse del uso del ciberespacio. En este contexto, se reconoce que el empleo de métodos ilegales como parte de las estrategias de seguridad dentro del ciberespacio se ha normalizado. Partiendo de esta base, el espionaje toma protagonismo, al contabilizarse dentro de las principales tácticas de abuso informático. Al respecto Martínez Jiménez (2015), aclara como el ciber espionaje es un ciberataque, pero un ciberataque no es ciber espionaje, ya que el primero conlleva acciones que infligen daños a la parte que los recibe y el ciber espionaje es el paso previo, el de obtención de información.

3.3 Revisión de literatura sobre el ciber espionaje y el comportamiento de los actores internacionales a través del tiempo

Recebido: 15/10/2021
Aceito: 10/11/2021
Disponível: 29/11/2021

sapienza International Journal of Interdisciplinary Studies
ISSN: 2675-9780

https://doi.org/10.51798/sijis.v2i4.145

3.3.1 La evolución del concepto

El espionaje ha estado presente desde el inicio de los tiempos. Se ha presentado en la antigüedad a través de situaciones sencillas como la búsqueda de planes de un pueblo vecino para obtener ventajas sociales, Pume Maroto (2009), así como en otras más complejas, como el uso de métodos de codificación de mensajes; las grandes civilizaciones griega, romana y persa, fueron pioneras en este último, Arreola García (2015).".

Según la Real Academia Español (2019) el espionaje, es aquella actividad dedicada a obtener, de modo oculto o fraudulento, información reservada o secreta.

Algo similar propone Alfonso Beltrán (2015), para definir el concepto. En su obra afirma que el espionaje es el robo organizado de información. Sin embargo, hace hincapié en que este acto se ve "legalizado" por las condiciones imperantes de competitividad y/o conflicto y que, además, es aceptado e inclusive alentando por los Estados, organismos e individuos como una actividad cotidiana de interacción en el mundo de hoy.

Por otro lado, la Escuela de las Américas explica en su manual de contrainteligencia que el espionaje es el acto de obtener, dar, transmitir, comunicar o recibir información en relación con la defensa nacional con la intención o el propósito creíble de que ésta será utilizada para dañar al gobierno nacional y en beneficio o ventaja del país extranjero.

Como se ha dicho, la industria del espionaje es una de las profesiones más antiguas de este mundo, y como antecedente se tiene conocimiento de todos los métodos para encriptar información escrita que utilizaban las antiguas culturas. Hay que recordar que, desde el fin de la guerra fría, vivimos en un mundo enfrascado en una guerra económica, que necesariamente requiere de inteligencia o espionaje para su desarrollo Arreola García (2015). Algo en lo que concuerda (Ramos, 2014), quien plantea como la tecnología presente se está convirtiendo en pieza de museo, nuestra comprensión de lo que puede ser una guerra.

En definitiva, el espionaje es una actividad de la que nos hemos valido durante mucho tiempo y es un hecho que no va a desaparecer. Es fácil considerar este planteamiento cuando desde el surgimiento de las TIC con la Globalización; todos los procesos se han ido digitalizando poco a poco y con ellos han surgido los métodos para transgredirlos. Algo similar menciona Rid (2013), quien afirma que, en comparación con el ciberdelito, todos los ciberataques políticos anteriores y actuales son versiones complejas de actividades, tan antiguas como el propio conflicto humano, de entre esas actividades podemos encontrar el espionaje.

Avanzado en este razonamiento; Llamas Covarrubias & Llamas Covarrubias (2018) en su obra, afirman que existen tres tipos principales de ciberataques: cibercrimen, ciberterrorismo y ciberguerra. A su vez menciona, como estas pueden representarse a través de diferentes acciones que se catalogan como ciberdelitos; de entre ellos hace referencia a la adquisición ilícita de datos o lo que él denomina espionaje de datos. Partiendo de este planteamiento, el ciberespionaje pasaría a catalogarse como ciberataque. Martínez Jiménez (2015) menciona como un ciberataque, conlleva acciones que infligen daños a la parte que los recibe y el ciberespionaje es el paso previo, el de obtención de información. En la actualidad, uno de los métodos más eficaz para conseguir datos es a través del uso de programas como spyware. Spyware o programa espía, es un código malicioso, que se dedica a extraer información de los usuarios de forma no autorizada, Baretto (2017).

A lo largo de la historia, el impacto del espionaje ha tenido éxitos relativamente menores o mayores que, en general pueden atribuirse a errores por parte de la persona que ha sido el objetivo en vez de la habilidad del propio agresor. Sin embargo, existen acontecimientos que, de manera intencional, han contribuido a este fenómeno.

3.3.2 Seguridad, globalización y ciber espionaje

Recebido: 15/10/2021
Aceito: 10/11/2021
Disponível: 29/11/2021

sapienza International Journal of Interdisciplinary Studies
ISSN: 2675-9780

https://doi.org/10.51798/sijis.v2i4.145

Parte de los cambios que dejó el fin de la Segunda Guerra Mundial y el desarrollo de las economías, fue el surgimiento de una nueva era de globalización algo en lo que concuerdan Brunet & Böcker (2008) y Frieden (2009). Lo que más adelante resultó en la aparición de las TIC así como también en "la intensificación de las comunicaciones físicas y la expansión mundial de los mercados de bienes y, sobre todo, de capitales, favorecidos por un nuevo clima político" Cabello Martín (2013).

Es así como con el nacimiento de las Tecnologías de Información y Comunicación y su extensión durante las décadas posteriores; que se consolidó en 1989 la creación del WWW (World Wide Web) así como también el libre acceso a internet al año siguiente. Lo que marcaría un hito en la historia. Algo similar sucede en 1993 con el desarrollo de otro de los inventos más prominentes de las TIC; La red de posicionamiento global (GPS) que inicialmente fue para uso único militar, para después pasar a ser dominio público. Cabello Martín (2013). "La privatización y la popularización de Internet, a mediados de la década de 1990, permitió concretar una lógica de interconexión a escala global sustentada en un flujo continuo de información" Osaba (2015). En otras palabras, consolidó lo que hoy es la red; el intercambio constante de información a través de conductos digitales.

El sistema ha logrado adaptarse a este nuevo panorama, "tanto el capitalismo como la administración burocrática se acomodaron fácilmente al nuevo régimen digital; ambos prosperan muy bien con los flujos de información" Morozov (2013), Algo que se ha declarado desde los primeros años de su desarrollo. Sin embargo, con el internet también surgieron nuevas tensiones y problemáticas, destacando la idea de cobro para el acceso a la información contenida y la de las posibles regulaciones que se le debían aplicar a esta nueva herramienta. Si bien, la historia ha registrado sucesos importantes con resultados positivos y negativos para ambas cuestiones, dichas problemáticas siguen presentes y en constante evolución. Cabe destacar que, en el caso de las regulaciones, la idea abarca un amplio espectro que gira en torno a la libertad. Uno de los focos rojos de las libertades en la red se centra en la manera particular en la que permite la circulación de información. Internet es una red sin centro, sin embargo, su columna vertebral se encuentra en los Estados Unidos, aquí se encuentran las sedes de las instituciones internacionales especializadas en su regulación y organización. Así también y desde el atentado de las torres gemelas dicho país se encargó de limitar los derechos de sus ciudadanos y del extranjero, disfrazando dichas restricciones de discursos y políticas de seguridad.

Bajo este supuesto, Pérez Luño (1992) donde la tecnología forma parte de la sociedad contemporánea suscita que los ciudadanos, desde su nacimiento, están expuestos a violaciones a su intimidad, al ser perpetradas por determinados abusos en informática y telemática. La injerencia del ordenador en las diversas esferas y en el tejido de relaciones que conforman la vida cotidiana se hace cada vez más extendida, más difusa, más implacable.

Por esta razón es que la sociedad debe de aceptar que nos enfrentamos a una realidad en la que las legislaciones internacionales aún no están a la par con las capacidades del internet y los dispositivos tecnológicos que están en constante evolución. Ramos (2014) nos menciona que el Internet nació en el siglo pasado con un diseño que no estaba pensado para todos los usos que ahora se aplican (…) como en el gobierno, educación y comercio electrónico, todas las capacidades que tienen ahora los dispositivos electrónicos, propiciaron el escenario perfecto para la escalada del espionaje virtual.

Recebido: 15/10/2021
Aceito: 10/11/2021
Disponível: 29/11/2021

sapienza International Journal of Interdisciplinary Studies
ISSN: 2675-9780

Tabla I. Características de los Sistemas de espionaje digital

Secretos Intrusivos	Intrusivo	Implantes físicos/virtuales	Gran capacidad de almacenamiento	Transmisores remotos de información
Llaves maestras de programas sistemas operativos	Ponen en riesgo la soberanía y seguridad de Estados, organismos e individuos	Requieren de equipos multidisciplinarios para su diseño y operación	Tecnología de punta	Empleo de los grandes servidores hackers y hackers para saltear las medidas de seguridad digital
Multisciplinarios	Especializados	Son herramientas de manipulación	Transgreden los derechos humanos	Buscan el control y el poder de la información
No tienen una regulación internacional	Promovidos por agencias estatales	Cuentan con la participación de las empresas privadas globales de fabricación de componentes	Furtivos	Con disfraz de servicios gratuitos
En coalición internacional	Emplean organismos internacionales como fuentes	Con capacidad para mutar	De un diseño general personalizado	Usan las redes de internet como su medio de conexión
Flexibles	Justifican acciones de seguridad	Persistentes	-	-

Nota: Elaboración propia. Datos tomados de "Ciber espionaje: La puerta al mundo virtual de los Estados e individuos", por A. Arreola García (2015).

3.3.3 El ciber espionaje dentro del Sistema Internacional

Vigilar y castigar se convierten en mecanismos inherentes al funcionamiento de cualquier sistema y el modus operandi del poder, supuesto que apoyan Ricaurte Quijano, et al. (2014). Además, el daño causado por los ataques dirigidos al ciberespacio genera confusión social debido a los avances que se han ido generando con el paso del tiempo. Algo similar sucede con los atacantes, que han enfocado esfuerzos en el desarrollo de su organización tanto económica como política, asegura Chai, Min, & Han (2015)

"Estados Unidos es uno de los pioneros de las estrategias de ciberespionaje y utilizará cualquier otro medio con fines políticos. Además, se cree que es uno de los países que más indaga sobre la información de las personas" (Yancey, 2017). La denominada "lista negra" de Bill Clinton es

Recebido: 15/10/2021
Aceito: 10/11/2021
Disponível: 29/11/2021

sapienza International Journal of Interdisciplinary Studies
ISSN: 2675-9780

un buen ejemplo, en ella el expresidente incluye los nombres de personas y empresas que, según el gobierno norteamericano, se encuentran relacionados conel narcotráfico López Torres (2014).

Por otro lado, la ONU, utiliza drones espías para presionar a las milicias rebeldes en República Democrática del Congo y para observar los movimientos de los civiles que están siendo desplazados. (Lara, 2014)

Yancey (2017) también menciona el caso del mayor ataque de espionaje cibernético que tuvo lugar cuando China se infiltró en el Pentágono. Así como el establecimiento militar de la India y robó documentos confidenciales, o el incidente de espionaje de China para robar el avión Lockheed Martin F-35. Aunque China aún no ha producido tecnología militar estadounidense o india, se hace de las herramientas y de sus habilidades en el ciberespacio para hostigar su rivalidad regional con Estados Unidos y la India

Otro buen ejemplo son los ciberataques que sufrió Estonia en el incidente de Tallin del 2007, o los ciberataques descubiertos en el parlamento alemán en 2015 que llevaron a gobiernos de diferentes países del mundo a contratar expertos en seguridad de la información para proteger sus sistemas del espionaje y sabotaje extranjero, a manera que puedan responder rápido a incidentes de tales características (Estrada Aravena, 2017). Así como estos, los ataques cibernéticos a través del ciber espionaje suceden de manera constante alrededor del mundo. Tomando en cuenta lo anterior, a continuación, se muestra una tabla en donde se ilustra algunos de los ciberataques relacionados con ciber espionaje que se llevaron a cabo en los últimos tres años.

Recebido: 15/10/2021
Aceito: 10/11/2021
Disponível: 29/11/2021

sapienza International Journal of Interdisciplinary Studies
ISSN: 2675-9780

4. ACTORES INTERNACIONALES QUE RECURREN AL CIBER ESPIONAJE COMO MEDIO PARA ALCANZAR SUS OBJETIVOS

4.1 Estados Nación

La variable de Estado Nación destacó en las investigaciones de: Amaral (2014), Ricaurte Quijano, et al. (2014) Alfonso Beltrán (2015), Arreola García (2015), Sánchez Cañestro (2015), Mejias Alonso (2016), Machín Nieva, (2016), Ramírez Castaño (2017), Yancey (2017) y Chávez & Velázquez Tovar (2017).

El estudio de Amaral (2014), argumenta que "existe un alto grado de dependencia por parte de estructuras críticas para la gobernabilidad, la seguridad y la defensa de un país, con los sistemas informáticos interconectados por medio de complejas redes de procesamiento de datos". Algo similar plantean Torres & Vila Viñas (2015) en la medida en que avanzan las tecnologías que facilitan la vigilancia de las comunicaciones por parte del Estado, ésta falla en garantizar que las leyes y regulaciones relacionadas con la vigilancia de las comunicaciones estén en consonancia con el derecho internacional de los derechos humanos y protejan adecuadamente los derechos a la intimidad y a la libertad de expresión. Así mismo, Ricaurte Quijano, et al. (2014) afirman como la seguridad es el argumento que sostienen los estados para justificar la vigilancia: un paradigma que se sitúa por encima del derecho a la privacidad.

El gobierno de un país busca ejercer control sobre la sociedad que reside en el mismo; Los actores externos de manera similar han buscado extender su control. Es el caso de aquellos que, mediante la infiltración a los sistemas operativos de gobiernos extranjeros, han intentado expandir sus influencias y poder no solo a otros países si no a otros continentes, "(…) una gran parte de los Estados interceptan las comunicaciones militares y diplomáticas de otros países" Alfonso Beltrán (2015). Además, el autor declara que, con este escenario, no es difícil imaginarse una situación similar para las comunicaciones entre sus propios ciudadanos y agrega, que los Estados están en constante búsqueda de nuevos métodos para acceder a la información secreta de sus contrapartes. Un ejemplo de esto es la intervención de comunicaciones que se lleva a cabo a través de mensajes o mediante los nuevos sistemas operativos que han resultado de la globalización. Aquellos que forman parte de las nuevas tecnologías de información y comunicación.

Arreola García (2015) menciona que la seguridad nacional justifica gran parte de, por no decir todas, las acciones menos transparentes de los Estados, que ponen en riesgo los derechos humanos. Incluso si esta afirmación justifica dichos actos, existe información suficiente que comprueba como ésta, no es la única razón por la que el espionaje ha permanecido como herramienta de los países. Mejias Alonso (2016) hace mención del informe Moraes, el cual reconoce la existencia de programas confidenciales de vigilancia que no solo se relacionan con cuestiones de seguridad nacional y que además atentan contra los derechos humanos socavando la seguridad y la fiabilidad de la red de comunicaciones. Del mismo modo, reconoce el uso de tecnología de invasión avanzada que pueden recopilar y analizar datos de comunicación de todo el mundo en Estados Unidos y otros países.

Bajo esta misma línea, el estudio de Sánchez Cañestro (2015) describe el estado actual del espionaje y vigilancia masiva. Menciona como los Estados hacen uso de esta herramienta amparándose en intereses legítimos (crimen organizado, pedofilia, tráfico de drogas, terrorismo), sin embargo, intuye otros usos ilegítimos y a ejemplo menciona los intereses comerciales, ante países rivales o incluso

Recebido: 15/10/2021
Aceito: 10/11/2021
Disponível: 29/11/2021

sapienza International Journal of Interdisciplinary Studies
ISSN: 2675-9780

aliados y los intereses de control de la disidencia. A su vez repasa información relevante a modo de resumen sobre las revelaciones de Snowden en las que utiliza el término de espionaje político para referirse a la vigilancia que se llevó a cabo y tuvo como objetivo la presidencia de Dilma Rouseff en Brasil y en aquel entonces candidato a la presidencia de México, Enrique Peña Nieto.

Dicho de otro modo, los Estados siendo los actores primarios dentro del Sistema Internacional y en su disputa constante por el poder; han optado por ser partidarios del uso de las herramientas que nos ha proporcionado la nueva era tecnológica para sus fines de política exterior y seguridad. "es por ello por lo que la vigilancia como práctica conduce a un control de información que a su vez generará mayor sed de controlarlo todo, no sólo en sus límites, sino que también fuera de ellos", Ramírez Castaño (2017).

Es así como el objetivo principal del ciberespionaje, es la búsqueda de un balance entre las partes que integran un escenario. Yancey (2017) refiere que dicho equilibrio no es ni pacífico ni beneficioso (…) y en ocasiones es el objetivo de los Estados que tienen rivalidad con otros. (…) La idea es lograr ganancias a través de medios no convencionales porque el Estado rival no puede aspirar a alcanzar a sus competidores a través de tácticas convencionales. Algo en lo que concuerdan Chávez & Velázquez Tovar (2017), en su estudio mencionan los métodos que utilizan los Estados para obtener información entre las que destaca el espionaje y asegura que dichas tácticas no son propias únicamente de los Estados sino de cualquier actor.

Tomando en cuenta lo anterior, es fácil entender por qué los Estados son parte del problema. Esto, al estar conscientes de la ventaja comparativa que representa delante de otros actores. En relación, Machín Nieva (2016) menciona que países como China, Rusia, Estados Unidos o Israel, al conocer la situación, han optado por el desarrollo de armas cibernéticas, por lo que podemos predecir que el aumento exponencial de la complejidad de los ciberataques se va a ver aún más potenciado a consecuencia de la inversión procedente de los Estados. Por consiguiente, se puede afirmar que los departamentos de seguridad y defensa de los países son usuarios y objetos de ataques cibernéticos mediante actividades como el ciber espionaje.

4.3 Grupos terroristas

Cabe señalar que existen muy pocos estudios disponibles que mencionen el uso del ciber espionaje como herramienta por parte de grupos terroristas. Sin embargo, es un actor que ha tomado relevancia durante la última década. Por esta razón se decidió que merece la pena otorgar un espacio dentro del estudio.

Recebido: 15/10/2021
Aceito: 10/11/2021
Disponível: 29/11/2021

sapienza International Journal of Interdisciplinary Studies
ISSN: 2675-9780

La variable de grupos terroristas destacó en las investigaciones de: Pume Maroto (2009), Ruíz Díaz (2011), Candau Romero, (2011), Emmerson (2014), Botta (2014), Alfonso Beltrán (2015), Yancey (2017), Pons Gamón (2017), Crespo Pazmiño (2017), Corella (2018).

Es así como se expone la obra de Pume Maroto (2009) quien menciona como el uso de las tecnologías de información y comunicación se han convertido en una de las herramientas favoritas para los terroristas. Gracias a la facilidad con la que se propaga información dentro de las plataformas digitales. “Los terroristas emplean Internet por la sencilla razón de que es fácil y barato diseminar información de forma instantánea, por todoel mundo, y relativamente sin censura”. Como ejemplo en su investigación propone a los sitios web de organizaciones terroristas, en los que, de manera frecuente, aparecen preguntascomo «¿Qué puedes hacer?» o «¿Cómo puedo ayudar?» que te vinculan a otros apartados de la misma página. Es en esta acción en la que los cibernautas son monitorizados e investigados con la finalidad de conseguir candidatos aptos para sus misiones. Otro ejemplode este último es el que presenta Pastor Acosta (2009) quien menciona como en octubre de 2007 la Guardia Civil de España desarticuló, en la provincia de Burgos, una red depresuntos islamistas que, desde Internet, se dedicaban a adoctrinar para la Yihad en escenarios internacionales. Adicionalmente, Botta (2014) hace alusión a esta idea, mencionado en su artículo como los grupos terroristas hacen uso del internet como medio de reclutamiento movilización, así como también como medio por el cual obtienen información para sus actividades.

Siguiendo esta misma línea, el estudio de Alfonso Beltrán (2015) plantea como el ciberterrorismo juega con la idea de rebelión justificando actos barbáricos como el tiranicidio. Utilizando de esta manera el terror, para incitar a las masas a derrocar el estado derecho como método para sus fines políticos.

Sin embargo, existe otra teoría que plantea como hay una diferencia entre el espionaje, el terror y el crimen en un contexto cibernético. La guerra cibernética está basadaen operaciones para sustraer información, cortar o destruir sus sistemas de comunicación, alterar sus bases de datos, es decir, lo que habitualmente hemos entendido como guerra, pero con la diferencia de que el medio empleado no sería la violencia física sino un ataque

Recebido: 15/10/2021
Aceito: 10/11/2021
Disponível: 29/11/2021

sapienza International Journal of Interdisciplinary Studies
ISSN: 2675-9780

informático Sánchez Medero (2012) dicho ataque va desde la infiltración en los sistemas informáticos enemigos para obtener información hasta el control de proyectiles mediante computadores, pasando por la planificación de las operaciones y la gestión del abastecimiento (Colle, 2000).

Por su parte Taqwadin, (2014). Afirma que el ciberterrorismo y el cibercrimen son muy diferentes a la guerra cibernética. Plantea que el ciberterrorismo tiene como objetivo causar estragos, bajas y destrucciones a través del ciberespacio, lo que permite a los atacantes permanecer lejos del objetivo mientras inflige despojo excesivo. Dichas operaciones podrían reducir los problemas logísticos de transferencia de explosivos y otros equipos. En contraste, los ciberdelincuentes o "piratas informáticos" buscan ganancias, en lugar de espectáculo. Se centran en el robo de identidad, la transferencia ilegal de fondos, blanqueo de dinero, fraude en Internet, evasión fiscal y comunicaciones entre delincuentes organizaciones. Algunas otras teorías de terrorismo sugieren que la táctica se puede utilizar para afectar los patrones de voto o ser un atajo para una revolución. En términos de espionaje cibernético, el objetivo sería entonces provocar reacciones internas a través del miedo a la amenaza cibernética Yancey (2017).

Artículos de revistas científicas desde años atrás, han apartado un espacio para argumentar sobre las amenazas cibernéticas que se han desarrollado. A partir de la existencia de las TICS, los actores internacionales han sido autores y protagonistas, destacando los grupos terroristas por su relativamente reciente adición dentro del escenario internacional. "Si para la preparación y ejecución de la mayoría de las acciones terroristas, en la actualidad se interviene cibernéticamente, quiere decir que en algún momento han utilizado medios cibernéticos para ejecutarlas para la comunicación o la acción" Pons Gamón (2017).

Esta situación hace visible como la destrucción provocada por los grupos terroristas (especialmente los grupos radicales), tiene un mayor impacto en términos de daños personales y materiales que los atentados de hace unos años (11-S). Considerando que ahora, a través de Internet y las redes de datos privadas de empresas y gobiernos, el flujo de información es muy sensible a la seguridad nacional de la mayoría de los países occidentales. Avanzando en este razonamiento el autor Ruíz Díaz (2011), sugiere el ciberespionaje y robo de datos como acciones asociadas a los grupos terroristas con la finalidad de ocasionar agravios a empresas privadas globales y Estados. De manera similar Candau Romero (2011), quien expone cómo los grupos terroristas emplean el ciberespacio para actividades delictivas, entre ellas, el obtener información de sus posibles objetivos sin su consentimiento, especialmente centrada en organizaciones y personas susceptibles de ser atacadas por estos grupos.

Recebido: 15/10/2021
Aceito: 10/11/2021
Disponível: 29/11/2021

sapienza International Journal of Interdisciplinary Studies
ISSN: 2675-9780

Otro de los artículos que relaciona a los grupos terroristas con actividades de ciberespionaje es el de Emmerson (2014). En su informe para la ONU reconoce la importancia de la actuación contra el terrorismo "la lucha contra [este actor] es tan crucial que, en principio, puede formar la base de una justificación discutible para la vigilancia masiva de Internet".

Así también, el caso que presenta Corella (2018) de cómo la web puede convertirse en una herramienta para los grupos terroristas es el de la desfiguración de páginas web, que "consiste en deformar una página web hackeada con un nuevo contenido insertado por el hacker resultando en una suplantación o identidad falsa del original". Miles de hackers están dispuestos a utilizar programas maliciosos, tener activas las opciones de geolocalización, enviar cookies a terceros o cualquier otro medio que les permita vigilar y/o obtener información para llevar a cabo sus objetivos. Según Crespo Pazmiño (2017) intentan explotar cualquier debilidad en los medios de almacenamiento de información, sin ningún lineamiento ético y con fines personales, criminales o inclusive terroristas.

4.4 Empresas Privadas globales

La variable de Empresas destacó en las investigaciones de: Montsuchi (2005), Rojas Mesa (2006), Pastor Acosta; et, al. (2009), Ruíz Díaz (2011), Aldasoro Alustiza, et. Al, (2012), Amaral (2014), Ricaurte Quijano (2014) Alfonso Beltrán (2015), Machín Nieva, (2016), Roman Soltero (2019).

En relación con el ciberespionaje y las empresas privadas globales, podemos encontrar una situación similar. Amaral (2014), hace énfasis en que, de los numerosos ataques cibernéticos que se dan a lo largo del mundo, una parte van dirigidos a las empresas. Aunque identificar la procedencia resulta un trabajo complicado, se sabe que de entre los posibles responsables se pueden encontrar empresas de espionaje industrial, grupos terroristas para fines políticos e incluso por agentes estatales. Si bien, no especifica el tipo de ciberataques, puntualiza que estos, son solo una evolución de tres actividades humanas: el sabotaje, el espionaje y la subversión. Así también Alfonso Beltrán (2015), quien menciona como el tiempo es testigo de cómo los avances tecnológicos también facilitan el hacerse de conocimiento de manera malintencionada de las capacidades y vulnerabilidades de los sistemas de información no solo de los Estados, sino también de las empresas y expone de ejemplo las redes de infraestructuras críticas como las de energía, servicios básicos, banca, etc.

A lo largo del tiempo, las empresas han implementado estrategias para la protección de aquella información que, en manos equivocadas podría resultar en una amenaza. Cabe destacar que, en gran medida, son las mismas empresas las que buscan hacerse de esta información para desprestigiar a la competencia.

La transición de todo tipo de documentos y datos de valor estratégico a un plano digital nos obliga a tomar acción para una adecuada implementación de la tecnología en el área empresarial. Esto, considerando las desventajas que conlleva el uso de las herramientas que nos presenta la era tecnológica en la que vivimos. Algo en lo que concuerda Roman Soltero (2019) "la facilidad de realizar espionaje casero y/o laboral, e irrumpir con los derechos humanos (…) están al alcance público digital, como se puede hacer al acceder sitios web como http://www.keylogger.org el cual nos brinda hasta 27 opciones de Spyware". Con este planteamiento, surge la necesidad de la creación de regulaciones.

Sin embargo, la existencia de violaciones a la intimidad fomentadas por las empresas privadas globales va más allá de la obtención de información de las compañías. En la actualidad, es fácil

Recebido: 15/10/2021
Aceito: 10/11/2021
Disponível: 29/11/2021

sapienza International Journal of Interdisciplinary Studies
ISSN: 2675-9780

encontrarse con teorías conspirativas sobre cómo las compañías que se encargan de la producción de bienes y servicios espían a sus consumidores para adecuarse a sus necesidades. La idea no suena tan descabellada, si tomamos en cuenta el hecho de que una gran parte de la población mundial ha proporcionado datos personales en más de una ocasión dentro de las plataformas virtuales que abundan en internet. Esta situación resulta en una oportunidad para las compañías, por el hecho de que dichos datos pueden ser obtenidos con facilidad y sin el consentimiento previo de las personas. De hecho, la relación de las empresas con el espionaje industrial no es nueva, Pastor Acosta; et, al. (2009) menciona como en España, a nivel nacional, la empresa Recovery Labs afirma que en 2007 el 20% de sus clientes sufrieron casos de ciberespionaje, un 18% más que el año anterior.

Machín Nieva, (2016) Cataloga los tipos de espionaje que realizan las empresas, como espionaje industrial y espionaje comercial. A la vez, menciona cómo las empresas como agentes económicos son de los principales en generar ciberataques. Sobre esto Montsuchi, (2005) menciona a título de ejemplo las prácticas ilegítimas dentro de organizaciones e instituciones con el "control y monitoreo en los lugares de trabajo que (…) proporcionan sin conocimiento de los afectados".

Por otro lado, Rojas Mesa (2006) afirma que Una organización que aspire a competir con éxito en el entorno actual (…) debe saber que ofrecen, en primer término, sus propios integrantes, sus proveedores, los grupos de interés y los clientes, es decir, la sociedad en su conjunto y más específicamente aquellos sectores en los que dicha organización actúa. Avanzando en este razonamiento, Ruíz Díaz (2011) menciona como en un entorno altamente globalizado y competitivo, las empresas multinacionales también son hostigadas por espías electrónicos para buscar información sobre nuevos proyectos dedesarrollo.

Por esta razón se justifica el uso de herramientas de vigilancia tecnología, algo en lo que concuerda Aldasoro Alustiza, et. Al, (2012) quienes mencionan como los cambios y avances en la tecnología obligan a las organizaciones y empresas a contar con información anticipada de los competidores, convertirla en conocimiento, elaborar un conocimiento que sea relevante para el negocio y utilizarlo para alcanzar sus objetivos.

Además, está el caso del espionaje que las empresas realizan en convenio con los Estados. Ricaurte Quijano (2014) menciona como el Estado, a través de empresas de telecomunicaciones, transgrede la esfera privada de los sujetos que han incorporado la tecnología a su vida cotidiana. La recolección de datos personales (dataveillance) se haconvertido en la principal forma de vigilancia en la actualidad.

Recebido: 15/10/2021
Aceito: 10/11/2021
Disponível: 29/11/2021

sapienza International Journal of Interdisciplinary Studies
ISSN: 2675-9780

La finalidad de este escrito radicó en el identificar qué actores internacionales recurren al ciber espionaje como medio para alcanzar sus objetivos. A su vez, exponer con qué objetivos recurren al uso del ciber espionaje. Así también, el examinar los casos de ciber espionaje presentes a lo largo de la historia. Además, exponer las legislaciones internacionales que reconocen el impacto que tiene este fenómeno en los derechos humanos y la soberanía de los actores

El paso siguiente consistió en la definición de los tres actores que se delimitaron a partir de la literatura científica recolectada, como los principales actores internacionales que recurren al ciber espionaje como medio para alcanzar sus objetivos. Cabe destacar que la información recabada para la identificación de las variables/ actores estudiados, también sirvió como base para la formulación de la herramienta de comprobación de esta investigación.

5. CONCLUSIONES Y PROPUESTAS

A lo largo de esta investigación, se estudiaron a los actores internacionales que recurren al ciber espionaje como herramienta para alcanzar sus objetivos. Para esto, se realizó una compilación de notas periodísticas sobre casos de ciber espionaje llevado a cabo por Estados, empresa y grupos terroristas dentro del periodo 2016-2018 alrededor del mundo. Cabe destacar que, en primera instancia, se abordó la problemática a través de un análisis exhaustivo. Además, se utilizó como referencia información de artículos de investigación y tesis de nivel posgrado con la intención de recabar las variables identificadas para este estudio.

5.1 De la comprobación cualitativa

Lo siguiente en el proceso fue delimitar los parámetros a través del modelo de investigación exploratorio /experimental/ descriptivo basado en la recopilación de literatura científica empleando bases de datos para la búsqueda de las variables seleccionadas como objeto de estudio de otros autores Esto con la intención de sostener la veracidad de la teoría que presenta el planteamiento de investigación.

5.2 De la comprobación de la hipótesis

Una vez que se llevó a cabo el recabo de información proveniente de documentos científicos y que se utilizó como referencia durante todo el marco teórico del escrito, lo siguiente fue realizar la comprobación de la hipótesis. El resultado se tradujo en dos fenómenos: el primero de ellos, la aprobación de las variables expuestas.

5.2 De las limitaciones del estudio

Para finalizar con las aclaraciones de esta investigación, es menester puntualizar las limitaciones que se presentaron a lo largo de su desarrollo. Comenzando por mencionar la falta de literatura científica reciente en materia de ciber espionaje. Si bien, es una conclusión contundente, la realidad es que la mayoría de los recursos encontrados son de años anteriores al 2010, muchos otros

Recebido: 15/10/2021
Aceito: 10/11/2021
Disponível: 29/11/2021

sapienza International Journal of Interdisciplinary Studies
ISSN: 2675-9780

incluso del milenio pasado. Lo que termina por dejar a estos documentos, más como medio de consulta para una mejor comprensión del tema, que como parte de las referencias literarias. Hay que mencionar además que lo anterior no puede tomarse como un indicador de la disminución del fenómeno que se estudia, por otro lado, solo refleja una reducción en el interés de ser estudiado.

Ligado al punto anterior, la segunda limitación que se logró identificar durante la realización del escrito fue la escasez de documentos de investigación orientados al estudio del uso del ciber espionaje como herramienta de reclutamiento por parte de grupos terroristas. Incluso el encontrar estudios con apartados dedicados de manera específica al uso del ciber espionaje por grupos terroristas simbolizó un reto significativo.

5.3 De las recomendaciones

A pesar de las limitaciones, el estudio cuenta con una estructura sólida y un modelo de investigación que puede utilizarse como base para la creación de nuevos estudios que tengan como objetivo indagar sobre este fenómeno desde diferentes ángulos, recomendando aplicar instrumentos mas elaborados como la entrevista a profundidad por parte de lado cualitativo o método cuantitativos para resultados más sólidos y concretos se recomienda de ser posible, ampliar el alcance de la comprobación de las variables a través de la aplicación de encuestas a aquellos que representen el sujeto de estudio. En este caso en particular, representantes, colaboradores o sujetos expuestos directamente a los actores internacionales estudiados en la investigación.

REFERENCIAS

Aldasoro Alustiza, J. C., Cantonnet Jordi, M. L., & Cilleruelo Carrasco, E. (2012). La Vigilancia tecnológica y la inteligencia competitiva en los estándares de gestión de calidad en I+D+i. 6th International Conference on Industrial Engineering and Industrial Managment, (págs. 1162-1168). España. Obtenido de http://adingor.es/congresos/web/uploads/cio/cio2012/SP_04_Gestion_Innovacion_Tecnol ogica_y_Organizativa//1162-1168.pdf

Amaral, A. C. (2014). La Amenaza Cibernética para la Seguridad y Defensa de Brasil. Visión Conjunta (10), 19-22. Obtenido de http://cefadigital.edu.ar/bitstream/1847939/32/3/VC%2010-2014%20AMARAL.pdf

Arreola García, A. (2015). Ciberespionaje: La puerta al mundo virtual de los Estados e individuos.

Ciudad de México, México: Siglo veintiuno.

Baretto, J. F. (2017). La Defensa Nacional y la Estrategia Militar de Seguridad Cibernética. Escuela Superior de Guerra Conjunta de las Fuerzas Armadas, Ministerio de Defensa. Repositorio Digital del Centro Educativo de las Fuerzas Armadas. Obtenido de http://190.12.101.91/bitstream/1847939/1061/1/TFM%2004-2018%20BARETTO.pdf

Botta, P. J. (2014). El uso de Internet por parte de los grupos yihadistas. Researchgate, 2-11. Obtenido de https://www.researchgate.net/profile/Paulo_Botta/publication/5005007_El_uso_de_Inter net_por_parte_de_los_grupos_terroristas_yihadistas/links/09e41505aab231832d000000/ El-uso-de-Internet-por-parte-de-los-grupos-terroristas-yihadistas.pdf

Brunet, I., & Böcker, R. (2008). Desarrollo, industria y empresa. Revista Internacional de Organizaciones (8), 151-154. Obtenido de Sociales, 235-260.

Candau, J. (2019). Ciberespionaje, una amenaza al desarrollo económico y la defensa. Seguritecnia 460. Revista decana independiente de seguridad (460), 70-72. Obtenido de https://www.seguritecnia.es/revistas/seg/460/index.html

Chai, S. W., Min, K. S., & Han, M. (2015). Un estudio comparativo internacional sobre estrategia de cibernética. International Journal of Security and Its Applications, 9(2), 13-20.

Chávez, L. E., & Velázquez Tovar, S. (2017). Ejercicio del Ciberpoder en el ciberespacio. Tecnología e innovación, 236-

Recebido: 15/10/2021
Aceito: 10/11/2021
Disponível: 29/11/2021

sapienza International Journal of Interdisciplinary Studies
ISSN: 2675-9780

244.

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

Corella, M. (2018). Defacement o Desfiguración: Táctica del activismo político. Obtenido de https://riunet.upv.es/bitstream/handle/10251/110074/VASSEUR%20-%20El%20defacement%20o%20desfiguraci%c3%b3n%3a%20t%c3%a1ctica%20para%20el%20activismo%20pol%c3%adtico.pdf?sequence=1&isAllowed=y

Crespo Pazmiño, D. F. (2017). El TLC entre EE. UU. y la UE: Incidencias en el poder de negociación estadounidense a partir de las declaraciones de Edward Snowden Sobre el espionaje en el periodo entre febrero 2013 y marzo 2014. Tesis, Universidad Católica del Ecuador, Facultad de Comunicación, Linguística y Literatura Escuela Multilingue de Negocios y Relaciones Internacionales.

Estrada Aravena, E. (2017). Conflictos de Soberanía en la implementación del convenio de budapest: Análisis crítico de la conservación y acceso transfronterizo de datos personales para la persecución internacional de ciberdelitos. 5° Simposio Internacional LAVITS Vigilancia, Democracia y Privacidad en América Latina: Vulnerabilidades y resistencias. (págs. 322-336). Santiago, Chile: lavits: Red latinoamericana de estudios en vigilancia, tecnología y sociedad.

Fernández López, O., Jiménez Hernández, B., Alfonso Almirall, R., Sabina Molin, D., & Cruz Navarro, Frieden, J. A. (2009). Capitalismo Global. El trasfondo económico de la historia del siglo XX. Economic History Research, 5(14), 179-219. Obtenido de https://recyt.fecyt.es/index.php/IHE/article/view/70199/42432

Hernandez Sampieri , R., Fernández Collado, C., & Baptista Lucio, M. d. (2014). Metodologia de la investigación. Ciudad de México: Mc Graw Hill.

Konakalla, A., & Veeranki, B. (2013). Evolution of Security Attacks and Security Technolgy. International Journal of Computer Science and Mobile Computing, 2, 270-276. Obtenido de https://ijcsmc.com/docs/papers/November2013/V2I11201366.pdf

Lara, B. (2014). ¿Amenazan los "drones" el derecho internacional? Política Exterior. 28(159), 94-101. Obtenido de http://www.jstor.org/stable/43594956

Llamas Covarrubias, J. Z., & Llamas Covarrubias, I. N. (2018). Internet ¿Arma o Herramienta ?

(Primera Edición ed.). Jalisco: Universidad de Guadalaja.

López Torres, J. (2014). Antecedentes Internacionales en materia de privacidad y protección de datos personales. Obtenido de http://publicaciones.eafit.edu.co/index.php/ejil/article/view/2849/2616

Machín Nieva, G. (2016). La Ciberseguridad como factor crítico en la seguridad de la Unión Europea. Revista UNISCI(42), 47-68.

Martínez Jiménez, C. (2015). El uso de ciberataques como herramienta de relaciones internacionales por parte de actores estatales: Los casos de Estados Unidos y Rusia. Universidad Pontificia de Comillas, Ciencias Humanas y Sociales. Madrid: Repositorio Universidad Pontificia de Comillas.

Mejias Alonso, E. (2016). La vigilancia y el control de la población a través de la gestión, la conservación y la explotación de datos masivos. Obtenido de Trabajo de investigación del Máster de Archivística y Gestión de Documentos de l'Escola Superior d'Arxivística i Gestió de Documents. ((Trabajos fin de Máster y de postgrado

Montsuchi, L. (2005). Aspectos Éticos de las tecnologías de la información y de la comunicación: la ética de la computación, internet y la World Wide Web . Obtenido de Documentos de trabajo de CEMA: Serie Documentos de Trabajo. 298, Universidad del CEMA.:

Morozov, E. (22 de Noviembre-Diciembre de 2013). The Real Privacy Problem. MIT Technology Review (06), 32-43. Obtenido de https://www.technologyreview.com/s/520426/the-real-privacy-problem/

Pastor Acosta, Ó., Peréz Rodríguez, J. A., de la Torre, A. D., & Taboso Ballesteros, P. (2009).

Pons Gamón, V. (2017). Internet, la nueva era del delito: ciberdelito, ciberterrorismo, legislación y ciberseguridad. URVIO, Revista Latinoamericana de Estudios de Seguridad (20).

Pume Maroto, J. (2009). El Ciberespionaje y la Ciberseguridad. La violencia del siglo XXI. Nuevas dimensiones de guerra, 45-76. Obtenido de https://dialnet.unirioja.es/servlet/articulo?codigo=4549946

Ramírez Paniagua, A. (2014). Ciberseguridad para la Administración Pública Federal en México: Propuesta de Política Pública para la protección de los Sistemas de la información como activos estratégicos de las instituciones. Instituto Tecnológico y de Estudios Superiores de Monterrey. Obtenido de https://www.academia.edu/17017569/Ciberseguridad_para_la_Administraci%C3%B3n_P%C3%BAblica_Federal_en_M%C3%A9xico?email_work_card=view-paper

Recebido: 15/10/2021
Aceito: 10/11/2021
Disponível: 29/11/2021

sapienza International Journal of Interdisciplinary Studies
ISSN: 2675-9780

Ramos, M. (2014). Acerca de la soberanía del Ecuador en el ciberespacio.

ALAI. Obtenido de La Agencia Latinoamericana de Información ALAI: https://www.alainet.org/images/Acerca%20soberania%20Ecuador%20en%20ciberespacio. pdf

Real Academia Española. (2019). Diccionario de la lengua española. Recuperado el 2019, de https://dle.rae.es/espionaje?m=30_2

Ricaurte Quijano, P., Nájera, J., & Robles Maloof, J. (2014). Sociedades de control: tecnovigilancia de Estado y resistencia civil en México. TeknoKultura, revista de Cultura Digital y Movimientos Sociales, 259-282.

Rid, T. (2013). Cyber War Will Not Take Place. Madison Ave. Nueva York: Oxford University Press, Inc.

Roman Soltero, A. R. (2019). Análisis ético de la información en el escándalo Pegasus. Revista de Investigación en Tecnologías de la Información, 7(14), 22-37. doi:SSN: 2387-0893

Ruíz Díaz, J. (2011). Ciberamenazas: ¿El terrorismo del Futuro? Revista del Instituto Español de Estudios Estratégicos (149), 257-322. Obtenido de https://dialnet.unirioja.es/servlet/articulo?codigo=3837524

Sánchez Cañestro, A. (2015). Programas de vigilancia masiva y contramedidas aplicables. Universitat Oberta de Catalunya. Obtenido de http://openaccess.uoc.edu/webapps/o2/bitstream/10609/43061/7/as_canestroTFM0615 memoria.pdf

Sánchez Madero, G. (2013). El Ciberespionaje. derecom(13), 115-124. Obtenido de https://www.academia.edu/7414397/El_ciberespionaje

Sánchez Madero, G. (2013). El Ciberespionaje. Derecho de la Comunicación (13), 115-124.

Sancho Hirare, C. (2017). Ciberseguridad. Presentación del dossier. Revista Lationamericana de Estudios de Seguridad, 8-15. Obtenido de https://www.researchgate.net/publication/318031894_Ciberseguridad_Presentacion_del_ dossierCybersecurity_Introduction_to_Dossier

Taqwadin, D. A. (2014). Ciberterrorismo: dinámica contemporánea y respuesta legal. Revista Internacional de Ciencia y Tecnología Aceh. Obtenido de https://www.academia.edu/5839030/CyberTerrorism_Contemporary_Dynamics_and_Lega l_Response

Torres, J., & Vila Viñas, D. (2015). Conectividad: Accesibilidad, soberanía y autogestión de las infraestructuras de comunicación. Buen conocer, 2.0, 703-738. Obtenido de https://book.floksociety.org/wp-content/uploads/2015/05/4_3_-_Conectividad.pdf

Yancey, J. (Abril de 2017). Los ataques cibernéticos y sus repercusiones políticos globales. Obtenido de https://repositorio.utdt.edu/bitstream/handle/utdt/6596/MEI_2017_Yancey.pdf?sequenc e=1