Revista Chilena de Relaciones Internacionales. Vol. 3 No 1
Enero - Julio 2019. ISSN 0719-8256. www.rchri.cl
pp. 55-78

CIBERATAQUES: LA INFLUENCIA DEL INDIVIDUO COMO ACTOR NO ESTATAL EN EL RIESGO A LA SEGURIDAD NACIONAL

Cyberattacks: The influence of the individual as non-state actor at the risk to national security

Ataques cibernéticos: A influência do indivíduo como ator não estado no risco à segurança nacional

Maylena Dilia Azúa Vergara [1]

Para citar este artículo / To reference this article / Para citar este artigo:
Azúa Vergara, Maylena Dilia**.** Ciberataques: la influencia del individuo como actor no estatal en el riesgo a la seguridad nacional *Rev. chil. relac. Int*, vol 3 (1): 55-78**.**

Recibido el 17 de Enero de 2019
Aceptado el 29 de Junio de 2019

Resumen

Los ciberataques significan un importante foco de vulnerabilidad para la seguridad nacional, por lo que los gobiernos se han visto en la necesidad de incrementar planes de acción a fin de intensificar la protección a fuentes de infraestructura e información protegidas. El acceso a las redes es indiscriminado y universal, lo que convierte a cualquiera en un potencial actor difícilmente identificable. El presente estudio tuvo como propósito demostrar que los individuos, a través de sus acciones como hackers, son actores no estatales de las relaciones internacionales capaces de afectar la seguridad nacional de los Estados mediante ciberataques perpetrados contra la infraestructura crítica, analizando su incidencia sobre la seguridad nacional y las reacciones y estrategias que han adoptado los gobiernos para aminorar el impacto de sus intervenciones.

Palabras clave: actores no estatales; ciberataques; individuos; infraestructura crítica; relaciones internacionales; seguridad nacional

Abstract

Cyber-attacks represent an important source of vulnerability for national security, making the governments increase action plans in order to intensify the protection of infrastructure sources and confidential information. Access

[1] Magíster en Estudios Internacionales de la Universidad de Santiago de Chile. Ingeniero en Comercio Internacional de la Universidad Tecnológica Metropolitana del Estado de Chile. Docente de planta en el departamento de Administración y Negocios de la Universidad Tecnológica de Chile. Correo electrónico: maylena.azua@usach.cl

to network is indiscriminate and universal, which makes anyone a potential actor that is hard to identify. The purpose of this study was to demonstrate that individuals, through their actions as hackers, are non-state actors in international relations capable of affecting the national security of States through cyberattacks perpetrated against critical infrastructure, analyzing their impact on security and the reactions and strategies that governments have adopted to lessen the impact of their interventions.

Keywords: Critical infrastructure; cyberattacks; individuals; international relations; national security; non-state actors

Resumo

Os ataques cibernéticos representam um foco importante da vulnerabilidade de segurança nacional, os governos viram a necessidade de aumentar os planos de ação para intensificar a proteção de fontes protegidas de infraestrutura e informações. O acesso às redes é indiscriminado e universal, o que dificulta a identificação de qualquer ator em potencial. O objetivo deste estudo foi demonstrar que os indivíduos, através de suas ações como hackers, são atores não estatais nas relações internacionais capazes de afetar a segurança nacional dos estados por meio de ataques cibernéticos contra infraestrutura crítica, analisando seu impacto na segurança. nacional e as reações e estratégias que os governos adotaram para diminuir o impacto de suas intervenções.

Palavras chave: atores não estatais; ataques cibernéticos; indivíduos; infraestrutura crítica; relações Internacionais; segurança nacional

Introducción

La globalización ha conllevado una apertura en las relaciones que ha permeado las fronteras, tanto físicas como económicas, culturales, políticas y sociales. Rodríguez (1999) hace hincapié en este concepto realizando un vasto análisis acerca de cómo esta nueva revolución cultural y tecnológica ha permitido no solo la aparición y evolución de nuevos actores para las RRII, sino también su incidencia en asuntos que eran atribuidos solo a la interacción entre Estados. Asimismo, García (1993, p. 15),

señala que la introducción de otros participantes a la escena internacional "no se trata de cuestionar el protagonismo del Estado, sino de afirmar teóricamente la presencia de los llamados nuevos actores".

El mundo globalizado ha permitido a los individuos, no solo poder compartir experiencias diarias, sino también ser partícipe del acontecer, tanto nacional como internacional en tiempo real. Por otra parte, el uso de los computadores e Internet ha permitido grandes beneficios para la humanidad, pero su rápido crecimiento también ha contribuido a prácticas antiéticas por individuos que utilizan la red con otros propósitos (Uma y Padmavathi, 2011). En este sentido, el Consejo Estratégico de la OTAN (IEEE, 2010) indica que los ciberataques se consideran uno de los principales riesgos a la seguridad nacional. Sin embargo, hasta ahora para cualquier estudio o análisis sobre amenaza o riesgo internacional, los principales involucrados resultan ser los mismos Estados, que entre ellos han comenzado una nueva guerra basada en sistemas informáticos.

Pero, se ha podido observar el aumento de los ataques realizados por hackers individuales. A mediados de 2018 se hizo conocido el grupo "The Shadows Brokers", por haber liberado y ofrecido a la venta información acerca de los malware utilizados por "The Equation Group", el principal equipo de ciberinteligencia estadounidense. Este evento representa una situación de suma urgencia para diferentes gobiernos, quiénes sintieron que estos nuevos actores, ocultos bajo fuertes sistemas de camuflaje informático, han sido capaces de almacenar información confidencial, generando una reformulación de los sistemas de ciberseguridad.

De este modo, se observa que la vertiginosa expansión de las tecnologías, también ha permitido el ascenso de los individuos, a través de ataques directos a la seguridad nacional mediante el ciberespacio. Por lo que, lo que esta investigación buscó dar respuesta a variadas interrogantes como: ¿constituyen los individuos un factor de riesgo para los Estados mediante los ataques realizados a través Internet?; Con esto, ¿es posible indicar que los individuos ya no son participantes pasivos de las relaciones internacionales al alero de los Estados? Para ello, fue relevante plantear objetivos tales como la necesidad de distinguir los atributos propios de los actores no estatales que potencian al individuo como factor de riesgo para los Estados, describir los componentes del concepto actual de seguridad nacional y determinar cuáles de ellos se ven afectados por los ciberataques; de manera de analizar los riesgos para la seguridad nacional provenientes de los individuos como actores no estatales.

Ya que el acceso a la cibertecnología ha permitido que cada ciudadano tenga la oportunidad de intervenir tanto de manera indirecta como directa; la preocupación de la situación actual corresponde no solo a la alta dependencia de los sistemas informáticos para el funcionamiento de la infraestructura nacional, sino también a la oportunidad que tienen individuos anónimos de introducirse en sus sistemas sin ser percibidos. Esto ha llevado a los Estados a considerar estas nuevas formas de acceso dentro de sus programas de estrategia de seguridad nacional. Por lo que, esta investigación argumenta que el ciberespacio otorga a los individuos la posibilidad de incidir de manera directa en los riesgos y amenazas para la seguridad nacional, convirtiéndose por sí mismos en actores no estatales activos de las relaciones internacionales. Ante esto, el alcance de la presente investigación gravita en el análisis de la magnitud de los sucesos que han podido afectar a la población civil en general, de modo de presentar un análisis que contribuya en la consideración de los individuos como actores en las relaciones internacionales poniendo en riesgo los intereses del Estado.

1. Metodología de trabajo

Para poder analizar los sucesos y sus implicancias, se utilizó el análisis de varios de los acontecimientos de ciberataques más conocidos ocurridos en los últimos cinco años, los cuales fueron categorizados según distintos criterios que permitirán evaluar su nivel de riesgo y, posteriormente, su correlación con las medidas adoptadas por los Estados en el mismo periodo de tiempo. En este extracto no se detallarán todos los casos, sino los más importantes seleccionados para esta presentación. De este modo, se logró considerar a los individuos como actores no estatales en el sentido de transgredir la seguridad nacional a través de su intromisión directa en las vulnerabilidades de la infraestructura crítica. Para esto, este estudio tuvo como instrumento principal la construcción de un modelo tipo para categorizar y dimensionar cada una de las distintas unidades de observación y sus componentes respectivos. Derivados del análisis de la tabla, se elaboraron una serie de gráficos de construcción propia, los que pretenden demostrar un análisis estadístico sumario sobre los datos recolectados, interrelacionando la información con las opiniones que los expertos tienen acerca de la participación de los individuos particulares en estos ataques.

Ciberataques	Sector impactado	Objetivo del ataque	Alcance	Potencial consecuencia ataque	Nivel de riesgo
Suceso 1					
Suceso 2					
Suceso 3					
Suceso n					

Esta tabla se completó como anexo de acuerdo a las categorías descritas de acuerdo a las siguientes fuentes de clasificación de los ciberataques:

1. **En base al sector impactado:** La primera clasificación de ciberataques se ha tomado como referencia las categorías presentadas por ENISA en su reporte "Taxonomía de los incidentes en Ciberseguridad" (2018, p. 10).

2. **En base al objetivo del ataque:** Los objetivos del ataque fueron considerados desde el punto de vista del recuadro de consecuencias esperadas de la publicación del Departamento de Seguridad Nacional de EE.UU., en su Plan Nacional de Respuesta ante Ciber Incidentes de 2016.

3. **En base al rango del ataque:** El breve informe sobre "Evaluación de la Severidad" (de las amenazas), presentado por la empresa antivirus Symantec™ (2016, p.1), ha sido tomado como referencia para la clasificación de rango de alcance.

4. **En base a sus potenciales consecuencias:** La información de Goodman y Lyn (2007, p. 28-29), se ha tomado como referencia para la clasificación de las siguientes categorías para determinar las potenciales consecuencias de los ataques.

5. **En base a su nivel de riesgo:** El nivel de riesgo se determinó de acuerdo a la última categorización presentada por el Centro Nacional de Ciberseguridad del gobierno del Reino Unido (cf., 2018: web). A pesar de ser un plan trazado específicamente para establecer cursos de acción en Gran Bretaña, fue posible extrapolarlo y utilizarlo de manera generalizada a cualquier otra nación como método de análisis.

2. Individuos como actores no estatales en la escena internacional

El mundo se ha vuelto cada vez más interdependiente, por lo que las teorías basadas en la preponderancia del Estado-nación, ya no eran suficientes para describir y explicar la realidad nacional (Salomón, 2001). Frente a esto, Arenal (1989) indica que los cambios sociales, políticos, económicos y científico-técnicos, además del aumento significativo en cuanto a actores y sus interacciones, han influido ampliamente en la necesidad de revisión de las concepciones científicas de las RRII, así como de su paradigma.

En este sentido, se podría señalar que el incremento en el interés por los actores no estatales y los asuntos fuera de las fronteras de un Estado, han marcado una revolución dentro de las RRII, lo que ha sido interpretado como un vuelco desde lo inter-nacional (entre Estados) hacia lo transnacional (a través de los Estados y sus fronteras) (Gebhard, 2017).

En sí, como señalaría Risse-Kappen (1995), las relaciones transnacionales se producen a través de las fronteras nacionales y deben estar involucradas en ellas actores no estatales, es decir, que no operan con respaldo de un gobierno, por tanto, abarcan todas las interacciones mundiales, excepto las relaciones interestatales. Se entiende que el actor internacional produce funciones que deben tener un impacto en el sistema interestatal, a la vez que debe poseer cierto grado de autonomía y libertad a la hora de tomar decisiones (Barbé, 1995).

Dado lo anterior, Sotillo (2000) subraya el efecto del desarrollo de las comunicaciones y los avances científicos en que la vida internacional tenga alcance mundial. La revolución electrónica y los satélites brindan acercamiento a los acontecimientos dentro de los hogares, lo que implica que las personas se comprometan más con el curso de los eventos internacionales (Gül, 2009). De esta forma, "individuos aleatorios podrían potencialmente comenzar una revolución desde sus hogares, superando cualquier concepción de poder y trascender las fronteras espaciales y materiales hasta el punto donde la actividad política e incluso, la confrontación se etérea e inmaterial en conjunto" (Gebhard, 2017: p. 44).

Para Rodríguez (1999), la intervención del papel del individuo, impulsado por la globalización ha comenzado a ganar más incidencia como actor de las RRII, por lo que las acciones individuales tienen grandes consecuencias en las RRII. Como individuo, este actor ya no es un sujeto pasivo de las RRII, como miembro de la élite

política o como un actor estatal oficial, sino que ahora es un actor por derecho propio, o al menos está siendo contado por los investigadores más allá del análisis a nivel de Estado (Gebhard, 2017). Es decir, no se puede negar que la vida internacional depende de la participación activa de los individuos en los asuntos internacionales, por encima o en contra de los propios Estados (Calduch, 1991). Por lo que, los grandes fenómenos que se desarrollan en la esfera mundial están estrechamente relacionados con actuaciones individuales, que no están estas necesariamente vinculadas a acciones colectivas o grupales (Calduch, 1991).

En la actualidad, los individuos y grupos interactúan a través de las fronteras, por lo que relativizan el significado del espacio y territorio. La rápida expansión de las tecnologías de información ha incrementado la movilidad de las personas y la probabilidad de que las interacciones ocurran más allá de sus fronteras (Gebhard, 2017).

3. Riesgos a la Seguridad Nacional y actualización de sus atributos en el mundo virtualizado

El concepto de seguridad nacional ha estado en constante evolución, no obstante, una gran variedad de autores coincide en su definición abarcando todas las acciones que el Estado puede llevar a cabo para alcanzar y preservar sus metas, cuando estas son consideradas objetivos o intereses nacionales (Martí, 2018).

La visión realista de las RRII establecía en el contexto de la Guerra Fría, que la seguridad era un concepto que atañe exclusivamente a los Estados, admitiendo que la amenaza exterior se consideraba a partir de una invasión territorial por parte de otros Estados (Tisera, 2014). En este sentido, el término seguridad nacional se define por todas las políticas públicas a través de las cuales el Estado-nación asegura su supervivencia como comunidad soberana y, por lo tanto, la seguridad y prosperidad de sus ciudadanos (Jackson-Preece, 2011).

Apenas finalizada la Guerra Fría, la proliferación de nuevas amenazas ha sido la tónica de los estudios sobre seguridad internacional; ya sea por su naturaleza interestatal (cultural, étnica, religiosa, etc.), como por la aparición de actores no-estales que pueden afectar directamente al Estado, como es el caso del terrorismo (Tisera, 2014). Por otro lado, la fuente de nuevas amenazas es indeterminada y multidimensional, debido a que se pueden generar por diferentes asuntos y es,

además, multidireccional, ya que las amenazas pueden atentar contra la seguridad ya no solo de los actores estatales, sino también de los no estales (Cujabante, 2009).

El mayor vínculo con la tecnología ha obligado a los Estados a continuar generando mecanismos de seguridad (Gil, 2017). Ello ha conllevado a la inclusión de las ciberamenazas como un riesgo determinado y concretizado en la Estrategia de Seguridad Nacional (Amich y Velázquez 2014). En este sentido, la consideración del daño en el contexto de la ciberseguridad, será parte de la defensa y estrategia nacional, en cuanto se evalúen las condiciones de riesgo que harán actuar al aparato de defensa y cuáles serán sus objetivos estratégicos (Roberts et al, 2016).

Por lo que, los peligros en el ciberespacio se deben principalmente a la oportunidad que se da de afectar la economía y el funcionamiento del país, mediante ataques a sistemas bancarios, redes de comunicación, tráfico aéreo y terrestre y a la IC, como fuentes de energía o agua (Gil, 2017). Una infraestructura será considerada crítica cuando comprometa un área de importancia para el interés nacional; de manera que, cualquier interrupción en estas infraestructuras podría reducir el flujo de estos bienes y servicios esenciales e impedir las operaciones económicas y gubernamentales (Lewis, 2006).

Según Goodman y Lin, (2007), actualmente las amenazas más comunes emanan desde los hackers y criminales: se ha comenzado a tomar consciencia acerca de que el crimen organizado está creciendo y atacando en el ciberespacio, aunque estos ataques se encuentren en niveles muy inferiores. “Una de las características que aporta el ciberespacio es la posibilidad de que participen nuevos actores que antes no lo hacían en los conflictos convencionales” (Gil, 2017, p. 7).

La diversidad de actores no estatales en la esfera ciberespacial, incluidos los individuos preocupados por la libertad de internet o motivaciones políticas, incrementan los esfuerzos de los Estados por desarrollar estrategias nacionales para implementar infraestructuras digitales más seguras (Lewis y Neuneck, 2013). Esto preocupa cuando las redes interconectadas más críticas para la seguridad nacional -finanzas, telecomunicaciones, energía eléctrica- son mutuamente dependientes, ya que las vuelve inmediatamente más atractivas hacia los ciberataques (Lewis, 2006). En este sentido, los ciberataques han comenzado a ser considerados riesgos para la seguridad nacional tanto en países desarrollados, como en vías de desarrollo (Amigo, 2015). Como argumentan Amich y Velázquez (2014, p. 55). “Solo un conocimiento

suficiente y fundamentado de la verdadera falta de límites del ciberespacio y sus implicaciones en el mundo real, puede llevar a la efectiva aplicación de una estrategia de seguridad nacional".

4. El fenómeno de los ciberataques; hackers y el anonimato en la web

A partir de los años noventa, la expansión de los navegadores al público general produjo principalmente, la posibilidad de intercambiar información, convirtiendo al ciberespacio en un ámbito fundamental de la sociedad (Gil, 2017).

Los ciberataques representan un subconjunto de operaciones que emplean el uso hostil de las capacidades del ciberespacio, por parte de Estado-naciones o actores no estatales, que actúen en su nombre o de forma solitaria, causando daños, destrucción o víctimas a estructuras tanto militares, económicas y/o políticas de un país (Sigholm, 2018). Ghandi et al. (2011), definen los ciberataques como cualquier acto que comprometa las expectativas de seguridad de un individuo, organización o nación. Lo mencionado anteriormente ha alcanzado gran importancia debido a que, según Soriano (s.f.), los atacantes a una red de telecomunicación no necesitan estar en contacto físico con la víctima; los datos pueden ser fácilmente copiados, transmitidos, modificados o destruidos cuando son transmitidos por la red.

Es así que los ciberataques podrían ser lanzados contra cualquier infraestructura pública, como los sistemas de energía o tratamiento de aguas para detener el suministro de electricidad o agua a los habitantes de un determinado lugar (Abomhara y Koien, 2015). Los ataques cibernéticos resultan más precisos, en el sentido de que, a pesar de que no pueden socavar el monopolio estatal de la fuerza, pueden atacar compañías u organizaciones del sector público, lo que afecta de manera selectiva a los grupos de autoridad (Rid, 2013).

Tanto las denegaciones de servicio contra redes gubernamentales y sitios web privados para interrumpir o deshabilitar su funcionamiento normal, como los ataques destinados a eliminar, destruir o robar información de entidades públicas o privadas de sus sistemas de control industriales, son considerados actualmente como los ataques más significativos (Amigo, 2015). Este método pretende bloquear el acceso a información primordial de cualquier organización o gobierno cuando es requerida (Uma y Padmavathi, 2011).

Acontecimientos recientes han demostrado que los actores no estatales también podrían jugar un rol clave durante estos eventos (Sigholm, 2018). Asimismo, Lewis (2018) hace hincapié en que tantos Estados como actores no estatales tienen ambos la misma capacidad para atacar, es decir, los actores no estatales pueden ser igual de poderosos que los Estados cuando participan en el ciberespacio, indicando además, que la atribución de los ataques en muy difícil de determinar.

Respecto a lo anterior, Weissbrodt (2013), advierte que, debido a la variedad de actores, se complejiza el abordaje de las ciberoperaciones; así, una operación en la red podría ser perpetrada por un hacker solitario que es capaz de bloquear un sitio web gubernamental. Factores de su dificultad radican en el complicado rastreo de sus orígenes y responsables, la inversión en investigaciones, tanto en costo como en tiempo y la relación entre los Estados con los denominados hackers, ya que se han producido múltiples casos donde estos grupos no tiene relación ni están supeditados a los Estados, por lo que estos también pueden resultar siendo víctimas de los ataques (Gil, 2017).

De acuerdo a lo que señala Ablon (2018), la atribución de un ataque es complicada, debido a que es muy difícil tener evidencia suficiente para identificar a los atacantes o el país del cual proceden. Así como señalan Rid y Buchanan (2015), las atribuciones a nivel estratégico, es decir, de lo que para los Estados está en juego políticamente, contiene una cantidad significativa de suposiciones y juicios, donde estos procesos de atribución están en ocasiones guiados por fuentes de inteligencia no forenses (rastreo de llamados, intercepción de correos), o por el contexto geopolítico u otras motivaciones.

5. Resultados de la investigación

Las 19 unidades de observación que fueron seleccionadas para esta investigación se consideraron bajo el espectro de corresponder ataques cibernéticos significativos, que constituyeron una amenaza a la seguridad nacional. Para ello, se ha considerado un rango de cinco años hasta el presente, es decir, los sucesos analizados acaecieron en un periodo de tiempo desde 2013 a 2018.

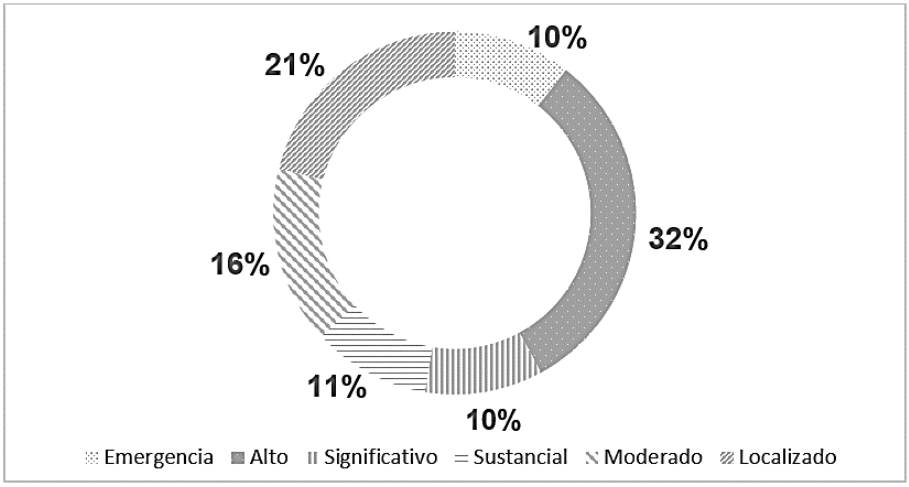
Los sucesos seleccionados incluyen ataques perpetrados por hackers descubiertos, otros anónimos o por grupos organizados bajo un seudónimo; todos estos sin que haya sido posible atribuir o relacionar el ataque a intereses de otro

Estado-nación, descartando de esta manera los presentados por FireEye (cf., s.f.: web) que han logrado reconocerse luego de múltiples seguimientos.

Los siguientes gráficos constituyen el análisis estadístico de las unidades de observación, donde cada uno de ellos presenta las estadísticas generadas a partir del cruce de la información extraída de la tabla de categorización de los ciberataques.

En el gráfico N° 1 se puede observar la categorización del nivel de riesgo de los eventos detallados, donde es posible vislumbrar que de las 19 unidades de análisis que se revisaron en este informe, un 32% corresponden a ataques de alto riesgo; ya que según dicha codificación, estos incidentes cumplen o con impactar seriamente al gobierno central o con afectar servicios esenciales para la población.

Gráfico 1: Nivel de riesgo de ciberataques observados

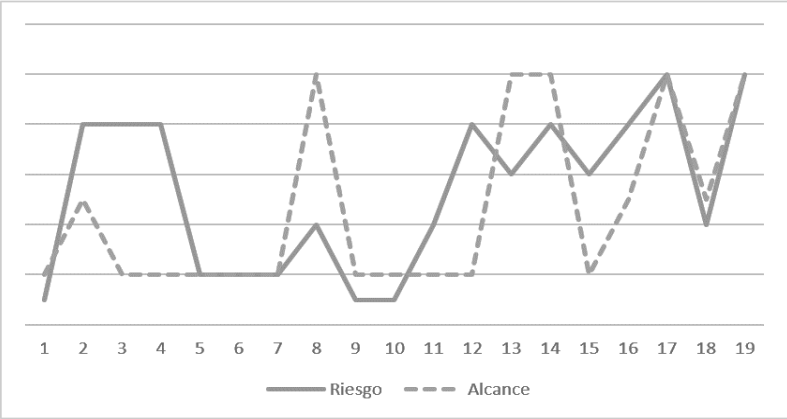


Fuente: Elaboración propia

Uno de los acontecimientos observados que levantó la alarma de emergencia, es el caso del ransomware NotPetya, que aunque comenzó siendo un ataque específico a Ucrania, logró expandirse rápidamente a sistemas de toda Europa y a otros sectores del mundo. Ejemplo de sus consecuencias fue el daño colateral a la compañía de transportes Maersk. El director del Centro Danés para la Ciberseguridad, Thomas Lund Sorensen (cf., Morbin, 2018: web) ha señalado que los ciberataques son hoy en día la amenaza más importante contra el país, incluso sobre la guerra física o los ataques terroristas.

Este ciberataque de grandes magnitudes fue atribuido por Gran Bretaña a Rusia, en una ofensiva por afectar a Ucrania. A pesar de esta denuncia iniciada, no hay pruebas públicas que demuestren la participación del Kremlin en este ataque, así lo señala al menos Dmitry Peskov, el vocero oficial de la Federación Rusa. Según Peskov (cf., 2018: web), estas acusaciones no tienen fundamentos, "lo cual mantiene la campaña rusofóbica (sic)" contra el Kremlin y que el ataque mencionado también afectó a una serie de compañías rusas. En el caso de un suceso de alto riesgo, se observó que el robo de información a la empresa australiana de buques militares Austal, demuestra la vulnerabilidad de la mensajería virtual, al exponer los planos de construcción de armamento que maneja la compañía, luego de la intrusión a través de los correos electrónicos. En esta situación, si bien los medios de comunicación australianos señalaron que los hackers fueron identificados como ciudadanos iraníes, el director del Centro de Ciberseguridad Australiano, Alastair McGibbon (cf., Packham, 2018: web), es disidente con esta información al indicar que es "fácil especular, pero la atribución puede tomar meses, incluso años". De la misma manera, un representante de la embajada iraní en Canberra alega que el ataque no tiene ninguna relación con su gobierno. En otro punto, en el gráfico N° 2, es posible observar que en los ataques de 2017 y 2018, se visualiza una mayor correlación respecto a la escala y el nivel de riesgo que ha dispuesto un malware, ya que los virus liberados no solo han logrado expandirse a través del globo, sino también causado un profundo impacto, afectando a diferentes países y tipos de objetivos, sean estos gobiernos, salud, universidades, negocios o individuos en particular.

Gráfico 2: Comparación de nivel de riesgo contra alcance de cada ciberataque



Fuente: Elaboración propia

Uno de los sucesos presentados en este informe, el ransomware WannaCry fue liberado a larga escala, lo que no se previó que podía causar serios daños a la seguridad nacional global. Para el Reino Unido, este fue el primer ciberataque donde se tomó conciencia de las consecuencias que un ataque cibernético podía tener en el espacio físico, debido a la postergación de operaciones o procedimientos médicos. El jefe de operaciones de la Unidad de Cibercrimen de Gran Bretaña, Mike Hulett (cf., 2018: web), confirma lo complejo que es determinar si una irrupción ha sido ocasionada por un Estado extranjero o por criminales especializados. De acuerdo a sus palabras, el nivel de sistema de ataque de un delincuente informático puede ser tan bueno como lo es el ataque proveniente de un Estado-nación, por lo que es difícil determinar si se está lidiando con un actor estatal o con un criminal.

Asimismo, a pesar de que EE.UU. apresó a un ciudadano norcoreano acusado de ser parte del equipo de hackers "The Lazarus Group", presuntamente por haber expandido el ransomware WannaCry auspiciado por el gobierno de su país natal, el Ministro de Relaciones Exteriores de dicha nación asiática ha alegado por la continuidad de las acusaciones que EE.UU. ha realizado acerca de los ciberataques, señalando que las acusaciones son irracionales mientras no se demuestre evidencia forense (cf., Parrish, 2017: web).

En el gráfico N° 3, la información recopilada indica que los sectores más atacados fueron gobierno, energía y agua.

Gráfico 3: Distribución de los ciberataques según sector impactado

Fuente: Elaboración propia

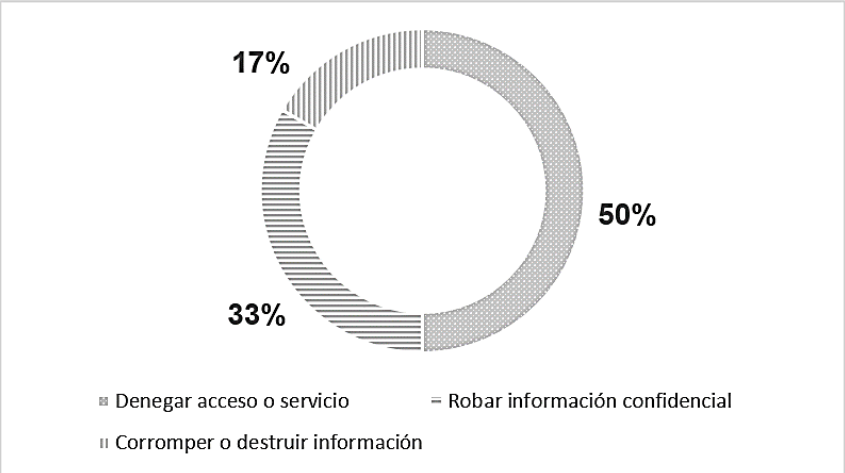
Un suceso de análisis sumamente importante resulta el robo de The Shadow Brokers al equipo Equation Group, el responsable de generar herramientas de hackeo para la Agencia de Seguridad Nacional (NSA por sus siglas en inglés) de EE.UU. De acuerdo a lo señalado por el ex agente de la CIA, Leon Panetta (cf., Pelroth, 2017: web), las filtraciones son increíblemente perjudiciales para la inteligencia y sus capacidades cibernéticas. Este ataque que liberó docenas de kits desarrollados por la Agencia, se presumió en primera instancia fue ocasionado por Rusia, sin embargo, Rusia también terminó siendo víctima de este ataque en múltiples empresas privadas y del sector estatal.

También se puede vislumbrar la importancia del robo de información confidencial de pacientes, como es el caso de Noruega. Luego de una enorme filtración de los datos de los pacientes del sistema de salud, el director de la Autoridad de Seguridad Nacional, Kjetil Nilsen, ha señalado que el ataque debe haber sido perpetrado por un "jugador avanzado" con las herramientas y el conocimiento necesario para llevar a cabo un ataque de esta naturaleza (cf., Shah, 2018: web). En otra entrevista realizada años atrás, Nilsen ya señalaba que el aumento del cibercrimen en diferentes niveles, se ha convertido en un asunto creciente de preocupación global, esto implica la participación desde hackers novatos, hacktivistas, crimen organizado y diferentes tipos de ataques patrocinados por Estados (cf., The Cyber Wire 2014: web).

Del mismo modo, el gobierno de Australia (cf, Blogle, 2018: web) se encuentra particularmente preocupado por el área de salud, ya que para mediados de julio de 2018 llevaban alrededor de 300 ataques al sistema médico y a mediados de julio recibieron una intrusión que bloqueó la red de acceso a "My Health Record" (cf., Whigham, 2018: web).

En el gráfico N° 4 se observa que, de la cantidad de sucesos clasificados según sector atacado, las potenciales consecuencias, aunque en su mayoría corresponden la interrupción de los servicios, incluyen también la posibilidad de causar compromiso de vidas humanas, debido no solamente al robo de las llamadas ciberarmas, sino también de información confidencial sobre armamento y herramientas militares convencionales, lo que provoca una grave vulnerabilidad de los Estados versus sus potenciales enemigos.

Gráfico 4: Potenciales consecuencias de los ciberataques según sector impactado

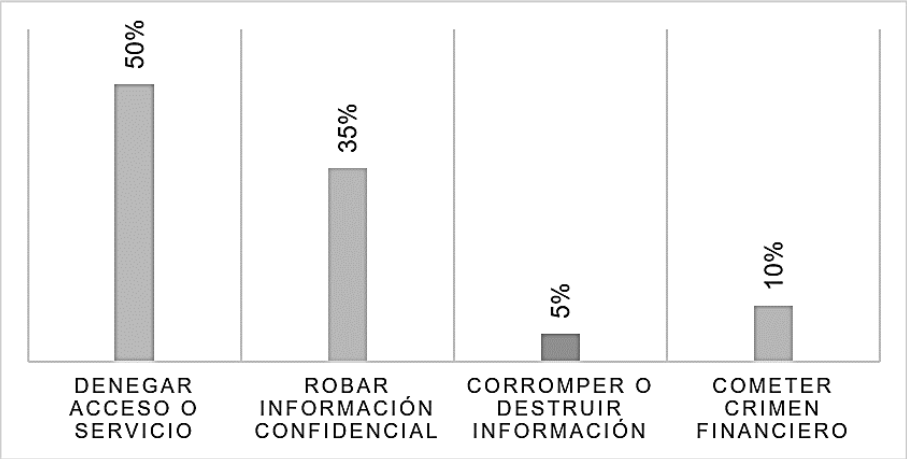


Fuente: Elaboración propia

Al caso de Austal analizado anteriormente, se le suman otros como el asalto a la industria naval italiana o el robo a la Fuerza Aérea de Chile. Este último suceso es un ejemplo de ataque que podría comprometer vidas humanas; la filtración de información militar de la Fuerza Aérea de Chile reveló una serie de documentos confidenciales respecto a la negociación de compras de armamento. El Gobierno de Chile no realizó una persecución de los atacantes, sin embargo el grupo peruano Lulz es reconocido como una de las bandas con gran participación en el ciberespacio y que no ha sido posible atribuir su participación a la colaboración de ningún país.

En el gráfico N° 5, se puede ver que el porcentaje más alto de ciberataques, independiente de su objetivo, buscaba como objetivo el denegar acceso o servicio, es decir, bloquear la posibilidad de ingresar o continuar con las operaciones del sistema.

Gráfico 5: Porcentajes de ciberataques de acuerdo a su objetivo



Fuente: Elaboración propia

Canadá declara que frecuentemente las actividades maliciosas en el ciberespacio están motivadas por ganancias monetarias, como ocurre en las campañas de phishing donde se ingresa a los dispositivos de las personas para obtener su información bancaria o a través de los ransomware que encriptan los archivos para luego solicitar una recompensa a cambio de su restauración (National Cyber Security Strategy, 2018).

Esto sucedió en el caso del bloqueo del sistema circuito cerrado de vigilancia de la policía de Washington días antes de la inauguración del mandato de Donald Trump. En un comienzo, el gobierno de Inglaterra detuvo a dos sospechosos de haber sido los causantes de la denegación de acceso y corte de las cámaras de seguridad, ambos apresados en Londres por la Agencia Nacional del Crimen (NCA por sus siglas en inglés) del Reino Unido (cf., Wei, 2017: web). Los capturados en aquella oportunidad fueron una ciudadana sueca y un ciudadano británico, quienes habían solicitado un pago a las víctimas por el desbloqueo de los archivos. No obstante, meses posteriores, el Departamento de Justicia de EE.UU. detuvo a dos sospechosos rumanos, luego de una investigación realizada por el agente James Graham (2017), quién señala que de acuerdo a la evidencia encontrada, se determinó que los acusados eran los culpables de participar en este acto de conspiración contra la policía de Washington.

El caso sucedido a la compañía petrolera Aramco en Arabia Saudita, denegó y destruyó del 85% de los archivos para el normal funcionamiento de la planta. Para

Arabia Saudita la necesidad de contar con herramientas de ciberseguridad se convirtió en una prioridad esencial de la seguridad nacional (cf., Badr Sallam, 2018: web), debido a que constituye al país más atacado del Medio Este, principalmente a la infraestructura, comunicaciones y petróleo.

Por otra parte, en el ámbito de las telecomunicaciones, uno de los ciberataques más conocidos el que se efectuó a la compañía española Telefónica. El subdirector de servicios del Incibe, Marcos Gómez, ha señalado que identificar a los hackers es sumamente complejo, debido a que el pago solicitado por estos a través de Bitcoins, no deja rastros de los atacantes (cf., Muñoz, 2017: web).

Tim Maurer (cf., 2018: web) afirma que otros actores además de los Estados pueden ser capaces de causar alto daño a través del hackeo. Según Maurer (ídem), actores menos sofisticados pueden provocar riesgos más grandes que los de los actores sofisticados (estatales), debido a su falta de precisión en los códigos, como fue el caso del ransomware WannaCry. Esta situación genera gran preocupación para James Christy (cf., s.f.: web), ex director de Investigaciones de Crímenes Computacionales de la Fuerza Aérea de EE.UU., ya que, según él, el anonimato es una de las grandes dificultades de los ataques cibernéticos; en sus propias palabras, señala que cualquier persona puede comprar un computador barato y tener conexión a Internet, lo que permite a cualquier individuo contar con un arma de destrucción masiva en el escritorio de su dormitorio. Pomerleau (cf., Pomerleau, 2015: web), indica que no está claro si los actores no estatales tienen las mismas capacidades de las naciones, sin embargo, la potencialidad de sus ofensivas levanta la preocupación sobre el daño que podrían producir los ataques solitarios.

En definitiva, tal como lo reconoce Rugge (cf, 2018: web), los asuntos en desarrollados en el ciberespacio están comenzando a tener un impacto en la estabilidad de las relaciones internacionales y que la ciberactividad está tomando un rol muy importante, lo que urge comprender cómo afecta a la seguridad para mitigar el riesgo que estas podrían provocar.

6. Conclusiones

En su carácter más esencial, un ciberataque es siempre para un Estado un factor de riesgo, debido a que en gran parte de los casos, como se evidencia en las unidades de observación seleccionadas y el reconocimiento de los Estados a través

de sus protocolos de seguridad, se atenta directamente contra las infraestructuras críticas afectando la seguridad nacional.

Es posible advertir que en las estrategias, tanto de seguridad nacional como aquellas dedicadas exclusivamente a la ciberseguridad, los Estados revisados especifican la importancia de un plan de protección ante los posibles ataques informáticos. Si bien los gobiernos reconocen que evitar un ciberataque es casi imposible, sus maniobras se basan principalmente en la preparación de cursos de acción una vez que estos han ocurrido.

Sin embargo, a pesar de que es posible demostrar que los ciberataques presentan un factor de riesgo para la seguridad nacional de los Estados y estos generan normativas y estrategias ante estas intrusiones cibernéticas; uno de los principales retos que tiene el fenómeno estudiado es que, tal como lo señalan los expertos, es sumamente difícil atribuir responsabilidades a un actor por sobre otro, debido al carácter anónimo derivado de las técnicas informáticas para ocultar la identidad que se utilizan en este tipo de ataques.

Ha sido posible distinguir a individuos comunes que no sostienen conexión alguna con gobiernos y que poseen diferentes motivaciones, principalmente la obtención de beneficios monetarios. Lo anterior es de suma relevancia, debido a que en gran parte de los ciberataques se carece de evidencia, lo que hace muy difícil descartar a los individuos como actores no estatales, como responsables de vulnerar y poner en riesgo la seguridad nacional de los Estados a través de las redes del ciberespacio.

Es por esto que, de acuerdo a dicho análisis, este estudio pudo confirmar la hipótesis que los individuos particulares, como actores no estatales constituyen un factor de riesgo para la seguridad nacional, ya que es posible afirmar que los ataques perpetrados por estos en el ciberespacio han provocado la instauración de medidas y estrategias para mitigar el daño a la infraestructura crítica. Además, ha sido posible demostrar que los Estados sí están contemplando a estos actores dentro de sus amenazas, considerando que estos individuos constituyen un actor no estatal cuando sus ofensivas no logran ser asociadas a ningún gobierno. En definitiva, de acuerdo a lo observado, aquellas naciones que se encuentran más actualizadas en cuanto a desarrollo de estrategias de ciberseguridad, debido principalmente por ser blanco de los ataques, han comenzado a reconocer que los individuos como actores

no estatales, bajo las ciberamenazas pueden llegar a tener las mismas capacidades y habilidades de ataque que un Estado.

7. Referencias

Abomhara, M, & Koien, G. (2015). Cyber Security and the Internet of Things: vulnerabilities, threats, intruders and attacks. *Journal of Cyber Security, 4,* 65 – 88. Disponible en: doi: 10.13052/jcsm2245-1439.414

Amich, C. y Velázquez, A. (2014). La ciberdefensa y sus dimensiones global y específica en la estrategia de seguridad nacional española. Revista Cuatrimestral de las Facultades de Derecho y Ciencias Económicas y Empresariales, 92, 49 – 76. Disponible en: https://revistas.upcomillas.es/index.php/revistaicade/article/viewFile/4094/3915

Amigo, A. (2015). Consideraciones sobre la ciberamenaza a la seguridad nacional. Política y Estrategia, 125, 39-51. Disponible en: https://doi.org/10.26797/rpye.voi125.44

Arenal, C. (1989). La teoría de las relaciones internacionales hoy: debates y paradigmas. Estudios Internacionales, 22(86), 153-182.

Badr, E. (2018). Cybersecurity has enhaced Saudi Arabia's national security. Saudi Gazette. Disponible en: http://saudigazette.com.sa/article/550030

Barbé, E. (1995). Relaciones Internacionales. Madrid: Tecnos S.A.

Blogle, A. (2018). Healthcare data a growing target for hackers, cybersecurity experts warn. ABC News. Disponible en: https://www.abc.net.au/news/science/2018-04-18/healthcare-target-for-hackers-experts-warn/9663304

Calduch, R. (1991). El Individuo como Actor Internacional. El Individuo como Actor de las Relaciones Internacionales. En R. Calduch (Ed.), Relaciones Internacionales (pp. 260 – 265). Madrid: Ediciones Ciencias Sociales.

Christy, J. (s.f.). Interview. Frontline, PBS. Disponible en: https://www.pbs.org/wgbh/pages/frontline/shows/hackers/interviews/christy.html

Cujabante, X. (2009). La seguridad internacional: evolución de un concepto. Relaciones Internacionales, Estrategia y Seguridad, 4(2), 93 – 106. Disponible en: https://www.redalyc.org/pdf/927/92712972007.pdf

ENISA (2018). Cybersecurity Incident Taxonomy. Disponible en: http://ec.europa.eu/information_society/newsroom/image/document/2018-30/cybersecurity_incident_taxonomy_00CD828C-F851-AFC4-0B1B416696B5F710_53646.pdf

Estados Unidos. Departamento de Seguridad Nacional. (2016). National Cyber Incident Response Plan. Disponible en: https://www.us-cert.gov/sites/default/files/ncirp/National_Cyber_Incident_Response_Plan.pdf

Estados Unidos. Departamento de Justicia (2017). Two Romanian suspects charged with hacking of Metropolitan Police Department surveillance cameras in connection with ransomware scheme. Disponible en: https://www.justice.gov/usao-dc/pr/two-romanian-suspects-charged-hacking-metropolitan-police-department-surveillance-cameras

Fireeye (s.f.). Advanced persistent threat. Disponible en: https://www.fireeye.com/current-threats/apt-groups.html

García, C. (1993). La Evolución del concepto de Actor en la Teoría de las Relaciones Internacionales. Sociología, 41, pp 13-31

Gebhard, C. (2017). One World, Many Actors. En McGlinchey, S. (Ed.) International Relations (pp. 32 – 45). Bristol: E-International Relations.

Ghandi, R., Sharma, A., Mahoney, W., Sousan, W., Zhu Q. & Laplante, P. (2011). Dimensions of cyber-attacks. Social, political, economic, and cultural. IEEE Technology and Society, 30. 28 – 38. Disponible en: doi: 10.1109/MTS.2011.940293

Gil, J. (2017). La integración del ciberespacio en el ámbito militar. Análisis GESI, 35. Disponible en: http://www.seguridadinternacional.es/?q=es/content/la-integración-del-ciberespacio-en-el-ámbito-militar

Goodman, S. & Lin, H. (2007). Toward a safer and more secure cyberspace. Washington: The National Academies Press.

Graham, J. (2017). Affidavit in support of a criminal complaint. United States District Court for the District of Columbia. Disponible en: http://cdn.cnn.com/cnn/2017/images/12/20/hackers.taking.over.dc.pd.cameras.affidavit.pdf

Gül, M. (2009). The concept of change and James N. Rosenau: Still international relations? African Journal of Political Science and International Relations, 3 (5), 199-207. Disponible en: http://www.academicjournals.org/app/webroot/article/article1379788149_Gul.pdf

Instituto Español de Estudios Estratégicos (IEEE) (2010). Los Actores no Estatales y la Seguridad Internacional: Su papel en la resolución de conflictos y crisis. Cuadernos de Estrategia, 147. Disponible en: http://www.ieee.es/Galerias/fichero/cuadernos/CE_147_ActoresNoEstatales.pdf

Jackson-Prece, J. (2011). Security in International Relations. London: University of London.

Lewis, J. (2006). Cybersecurity and Critical Infrastructure protection. Disponible en: https://csis-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/media/csis/pubs/0601_cscip_preliminary.pdf

Lewis, J. & Neuneck, G. (2013). The Cyber Index. International security trends and realities. Ginebra: UNIDIR.

Martí, L. (2018). La seguridad nacional y el acceso a la Información pública en México. Letras Jurídicas, 13. Disponible en: https://www.researchgate.net/publication/266498456_La_seguridad_nacional_y_el_acceso_a_la_Informacion_publica_en_Mexico

Maurer, T. (2018). Here's how hostile states are hiding behind "independent" hackers. The Washington Post. Disponible en: https://www.washingtonpost.com/news/monkey-cage/wp/2018/02/01/heres-how-hostile-states-are-hiding-behind-independent-hackers/?noredirect=on&utm_term=.4a549d0bd85a

Morbin, T. (2018). Maersk cyber-attack "best thing to happen in Denmark". SC Magazine UK. Disponible en:

https://www.scmagazineuk.com/maersk-cyber-attack-best-thing-happen-denmark/article/1493521

Muñoz, R. (2017). El gobierno confirma un ciberataque masivo a empresas españolas. El País. Disponible en: https://elpais.com/tecnologia/2017/05/12/actualidad/1494585889_857386.html

Packham, C. (2018). Australia's cyber security chief says Austal defense hack investigation may take years. Reuters. Disponible en: https://www.reuters.com/article/us-australia-iran-cybercrime/australias-cyber-security-chief-says-austal-defense-hack-investigation-may-take-years-idUSKCN1NI03X

Parrish, K. (2017). North Korea denies accusations of WannaCry attack involvement. Digital Trends. Disponible en: https://www.digitaltrends.com/web/north-korea-wannacry-attack/

Pelroth, N., Shane, S. & Sanger, D. (2017). Security breach and spilled secrets have shaken the NSA to its core. The New York Times. Disponible en: https://www.nytimes.com/2017/11/12/us/nsa-shadow-brokers.html

Pomerleau, M. (2015). State vs. non-state hackers: different tactics, equal threat?. Defense Systems. Disponible en: https://defensesystems.com/articles/2015/08/17/cyber-state-vs-non-state-haclers-tactics.aspx

Reino Unido. National Cyber Security Centre. (2018). New cyber attack categorization systems to improve UK response to incidents. Disponible en: https://www.ncsc.gov.uk/news/new-cyber-attack-categorisation-system-improve-uk-response-incidents

Rid, T. (2013, November/December). Cyberwar and peace. Hacking can reduce real-world violence. Foreing Affairs, 92(6), 77 – 87.

Rid, T. & Buchanan, B. (2014). Attributing Cyber Attacks. Journal of Strategic Studies, 38, 4 – 37. Disponible en: http://cs.brown.edu/courses/cs180/sources/Attributing_Cyber_Attacks.pdf

Risse-Kappen, T. (1995). Bringing Transnational Relations Back In Non-State Actors, Domestic Structures and International Institutions. Cambridge: Cambridge University Press.

Roberts, T., Agrafiotis, I., Bada, M., Cornish, P., Creese, S., Goldsmith, M., Ignatuschtschenko, e. & Upton, D. (2016). Cyber Harm: Concepts, Taxonomy and Measurement. SSRN Electronic Journal. Disponible en: doi:10.2139/ssrn.2828646

Rodríguez, I. (1999). Globalización y Actores Internacionales. El papel del individuo ante los conflictos armados. Investigaciones Políticas y Sociológicas, 1, 63 - 86. Disponible en: https://www.redalyc.org/pdf/380/38010104.pdf

Rugge, F. (2018). Cybercrime and International Relations. Instituto Per Gli Studi di Politica Internazionale. Disponible en: https://www.ispionline.it/it/pubblicazione/cybercrime-and-international-relations-20996

Salomón, M. (2001). La teoría de las Relaciones Internacionales en los albores del siglo XXI: diálogo, disidencia, aproximaciones. CIDOB D'Affers Internacionals, 56, 7 – 52. Disponible en: https://www.raco.cat/index.php/revistacidob/article/viewFile/28242/28076

Shah, S. (2018). Professional hack on Norwegian health authority compromises data of three million patients. The Inquirer. Disponible en: https://www.theinquirer.net/inquirer/news/3024692/norway-health-south-east-rhf-hacked

Sigholm, J. (2013/04/14). Non-state actors in cyberspace operations. Journal of Military Studies, 4(1). Disponible en: doi: 10.1515/jms-2016-0184

Soriano, M. (s.f.). Seguridad en redes y seguridad de la información. Disponible en: http://improvet.cvut.cz/project/download/C2ES/Seguridad_de_Red_e_Informacion.pdf

Sotillo, J. (2000). Actor internacional. Universidad Complutense de Madrid. Disponible en: https://webs.ucm.es/info/eurotheo/diccionario/A/actorinternacional.pdf

Symantec™ Security Response. (2006). Assessing the severity of threats, events, vulnerabilities, security risks. Disponible en: https://www.symantec.com/content/en/us/about/media/securityintelligence/SSR-Severity-Assesment.pdf

Tisera, J. (2014). El estudio de la Seguridad Internacional: ampliación y profundización del debate en torno a la nueva agenda de seguridad. Repositorio Institucional de la UNLP. Disponible en: http://hdl.handle.net/10915/44797

Uma, M, & Padmavathi G. (2011). A survey on various cyber-attacks and their classification. International Journal of Network Security, 15(5), 390 – 396. Disponible en: https://www.researchgate.net/publication/289802787_A_survey_on_various_cyber_attacks_and_their_classification

Wei, W. (2017). Two Arrested for Hacking Washington CCTV Cameras Before Trump Inauguration. The Hackers News. Disponible en: https://thehackernews.com/2017/02/cctv-camera-hacking.html

Weissbrodt, D. (2013). Cyber-conflict, cyber-crime, and cyber-espionage. Minnesota Journal of International Law, 22, 347 – 387. Disponible en: https://scholarship.law.umn.edu/cgi/viewcontent.cgi?article=1227&context=faculty_articles

Whigham, N. (2018). Health sector tops the list as Australians health data breaches since February. News. Disponible en: https://www.news.com.au/technology/online/hacking/health-sector-tops-the-list-as-australians-hit-by-300-data-breaches-since-february/news-story/5e95c47694418ad072bf34d872e22124