CENTRO DE INVESTIGACIONES Y ESTUDIOS ESTRATÉGICOS
ANEPE.CL

ISSN 0719-4110

CUADERNO DE TRABAJO N°9-2018

SEGURIDAD VERSUS LIBERTAD EN EL CIBERESPACIO

CUADERNOS DE TRABAJO es una publicación orientada a abordar temas vinculados a la Seguridad y Defensa a fin de contribuir a la formación de opinión en estas materias.

Los cuadernos están principalmente dirigidos a tomadores de decisiones y asesores del ámbito de la Defensa, altos oficiales de las Fuerzas Armadas, académicos y personas relacionadas con la comunidad de defensa en general.

Estos cuadernos son elaborados por investigadores del CIEE de la ANEPE, pero sus páginas se encuentran abiertas a todos quienes quieran contribuir al pensamiento y debate de estos temas.

CUADERNO DE TRABAJO DEL CENTRO DE INVESTIGACIONES Y ESTUDIOS ESTRATÉGICOS es una publicación electrónica del Centro de Investigaciones y Estudios Estratégicos de la Academia Nacional de Estudios Políticos y Estratégicos y está registrada bajo el **ISSN 0719-4110 Cuad. Trab., - Cent. Estud. Estratég.**
Dirección postal: Avda. Eliodoro Yáñez 2760, Providencia, Santiago, Chile.
Sitio Web www.anepe.cl. Teléfonos (+56 2) 2598 1000, correo electrónico ciee@anepe.cl

SEGURIDAD VERSUS LIBERTAD EN EL CIBERESPACIO

Agosto, 2018
Pía Martabit Tellechea*

RESUMEN

En el invierno de 2018 una institución financiera fue víctima de dos ataques informáticos, dando pie a un importante debate público sobre cómo estar a la altura de las amenazas globales en el ciberespacio. Las teorías clásicas de las relaciones internacionales aplicadas a la ciberseguridad permiten dilucidar diferentes problemáticas que conlleva la penetración digital en el mundo, y cuales son las formas de comprender el ciberespacio. En esta búsqueda de seguridad en el espacio cibernético, se presenta una dicotomía entre potenciar la libertad de los individuos y asegurar la red global contra amenazas reales y potenciales al Estado. Este cuaderno tiene por objetivo plantear consideraciones iniciales para dar pie a establecer un equilibrio entre seguridad y libertad, al que pronto Chile tendrá que afrontar.

PALABRAS CLAVE: Seguridad internacional, ciberseguridad, teoría de las Relaciones Internacionales.

Introducción

Una de las principales discusiones que se ha instalado a nivel nacional en los últimos meses trata sobre la seguridad en internet y sus consecuencias en la protección de datos personales y otra información privada de relevancia. A partir de los hechos ocurridos en Chile durante los meses de mayo y julio sobre ciberseguridad, resulta necesario encontrar un punto común entre la búsqueda de seguridad y la protección de la libertad en el ciberespacio, de acuerdo a las distintas visiones teóricas de las relaciones internacionales para el mantenimiento y protección de la red global, donde la seguridad y la autonomía entran en conflicto. Es fundamental, entonces, revisar qué elementos empujan: más seguridad a cambio de menos libertad o más libertad a cambio de menos seguridad.

Antes de los ataques contra el Banco de Chile, la discusión sobre la ciberseguridad se mantenía, a grandes rasgos, en círculos reducidos de expertos o, en casos específicos de carácter criminal, en los organismos de seguridad interna del país. Pero es necesario expandir el círculo de discusión, incorporando análisis multidisciplinarios de los distintos sectores y objetos de estudio que se encuentran en

* Cientista político de la Universidad del Desarrollo y Magíster en Periodismo Mención Prensa Escrita de la Pontificia Universidad Católica de Chile. Investigadora independiente en materias de ciberseguridad. piajomte@gmail.com

las sociedades complejas y globalizadas. El concepto "seguridad" apela a una idea compleja y extensa a lo que poco a poco, con mayor interés de la opinión pública, el debate público ha ido ampliando su espectro para estar a la altura del fenómeno en el contexto del siglo XXI.

De acuerdo a las opiniones e ideas desplegadas y a un análisis de dicha discusión, además de una revisión de los actores y su categoría o tipología dentro de la sociedad, se puede detectar una visión particular que domina la forma en que el país y sus autoridades están tratando de comprender el fenómeno: ese prisma es la teoría liberal de las relaciones internacionales. Más precisamente a una visión pragmática del enfoque liberal en este campo de estudio.

"El liberalismo y el realismo permiten entender las discrepancias que existen en formas y fondos de las relaciones humanas en el ciberespacio, precisamente porque son relaciones que traspasan las fronteras del Estado-Nación..."

Las teorías clásicas de las relaciones internacionales aplicadas a la ciberseguridad permiten dilucidar diferentes problemáticas que conlleva la penetración digital en el mundo, y cuales son las formas de comprender algo que "el hombre creó, pero no entiende"[1]. Más que no entender el fenómeno en su funcionamiento, la interpretación y los análisis sobre las consecuencias que se producen con el desarrollo de las tecnologías de la información no es libre de discrepancia, ni libre de ser muy acotada para visualizar la complejidad del fenómeno.

El liberalismo y el realismo[2] permiten entender las discrepancias que existen en formas y fondos de las relaciones humanas en el ciberespacio, precisamente porque son relaciones que traspasan las fronteras del Estado-Nación, y también permite revelar diferencias de resolución y decisión en estas interacciones.

Al plantear estas diferencias y dicotomías —que caracterizan los diferentes enfoques teóricos—, se puede revelar los sesgos que se encuentran presentes en la discusión actual chilena en materia de ciberseguridad. Al acotar la vulnerabilidad de las instituciones financieras y otros organismos productivos a solo seguridad e integridad del sistema económico y sus actores, el análisis podría presentar puntos ciegos que son necesarios reconocer y que a futuro deben comenzar a considerarse tanto el realismo como el constructivismo para poder visualizar el panorama completo, y en la complejidad de los actores y fenómenos de las relaciones internacionales.

Para eso, hay que visualizar el problema de la ciberseguridad a partir del enfoque más cercano a la realidad chilena y que es a través del enfoque teórico liberal, y cuáles podrían ser los desafíos tanto desde la misma mirada del enfoque señalado, como también su antagónico, el realismo. Esto, como se verá, construye posiciones contrapuestas en donde la dicotomía libertad versus seguridad toma forma.

Este trabajo tiene como objetivo general determinar las distintas perspectivas de cómo abordar la seguridad en el ciberespacio desde la perspectiva de la seguridad y defensa: es decir la realidad de Chile en el contexto de la globalización y multidimensionalidad de la amenaza, especialmente tras los ataques informáticos contra el Banco de Chile: esto más

[1] "The Internet is the first thing that humanity has built that humanity doesn't understand, the largest experiment in anarchy that we have ever had", Eric Schmidt. En: MURRAY, Andrew D. The Regulation of Cyberspace: Control in the Online Environment. New York: Routledge, 2007.

[2] N. del Autor: Hoy en día es más preciso hablar de neorealismo y neoliberalismo, entre otros conceptos, pero para simplificar la lectura se utilizará realismo y liberalismo, aun cuando en la teorización están incorporadas las actualizaciones "neo".

por un "despertar" en los actores nacionales ante las vulnerabilidades informáticas del país, que por las consecuencias materiales y sociales del ataque.

De esta manera, primero se hará una revisión de la cobertura y análisis de la opinión pública tras los ataques informáticos, haciendo énfasis en las declaraciones y los actores involucrados en el ataque como en la respuesta a este. En segundo lugar, se analizará la discusión académica internacional sobre la aplicación del enfoque liberal de las relaciones internacionales a los estudios de seguridad y específicamente a la ciberseguridad. En tercer término, se espera desplegar las distintas posibilidades de acción o escenarios que los diferentes actores podrían llegar a tomar o crear de acuerdo los enfoques teóricos. Finalmente se busca plantear la dicotomía seguridad versus libertad tensada por los intereses de los actores en juego.

"La disciplina de la Seguridad Internacional debe abordar esta consideración de una manera inclusiva en el análisis para enfrentarse a la futura discusión de normativas, compatibilizando tanto las libertades como la seguridad."

No se pretende dar respuesta única a todas las dudas surgidas en el camino a definir y comprender la ciberseguridad, o la construcción de esta, sino más bien visualizar las distintas formas de entender el fenómeno y cómo estas perspectivas en aspectos fundamentales entran en tensión. Adicionalmente, y producto de esto, presentar interrogantes que puedan ser en el futuro desarrolladas por la Academia.

Es de relevancia para ciertos actores de la sociedad civil la visión de la red global como un lugar de libertad, autonomía y descentralismo. Pero con la tendencia a digitalizar aspectos centrales de la vida humana, nuevos espacios de inseguridad crecen. La disciplina de la Seguridad Internacional debe abordar esta consideración de una manera inclusiva en el análisis para enfrentarse a la futura discusión de normativas, compatibilizando tanto las libertades como la seguridad.

Despliegue mediático de los ataques contra un banco en Chile

Desde el hackeo al Banco Chile entre los meses de mayo y julio, la prensa desplegó un importante debate de la opinión pública sobre las diferentes dudas que surgieron a partir de los ataques, sobre todo para evitar este tipo de agresiones en el futuro[3]. El *Diario Financiero*, que se especializa en prensa económica, desplegó una editorial el día 29 de junio en donde cuestiona el rol de Chile en la llamada "cuarta revolución industrial", que responde a la idea de "un tsunami de innovaciones tecnológicas y científicas que impondrá nuevos paradigmas a las sociedades del siglo XXI"[4]. El medio de comunicación mencionado define el panorama nacional de la siguiente manera:

> "Uno de los principales bancos del país es burlado por una banda de hackers asiáticos; el gobierno anuncia que aplicará impuestos a la economía digital; un estudio de abogados participa en un startup legal que operará con inteligencia artificial; una inmobiliaria planea instalar cargadores gratuitos para vehículos eléctricos en sus edificios;

[3] DIARIO FINANCIERO. Chile y la cuarta revolución industrial [En línea]. *Diario Financiero*, Editorial, 29 de junio, 2018. [Fecha de consulta: 2 de agosto 2018]. Disponible en: <https://www.df.cl/noticias/opinion/editorial/chile-y-la-cuarta-revolucion-industrial/2018-06-29/192558.html>.

[4] Ibíd.

> la gigante Amazon podría escoger a Chile como sede de un nuevo data center regional"[5].

A este panorama se le suma, sin duda, que el actual gobierno del presidente Sebastián Piñera busca acelerar un proyecto "que busca unir el territorio de Asia-Pacífico con el continente americano por medio de un nuevo cable submarino de fibra óptica de alta velocidad, que se sumaría a otros que ya pasan por Chile"[6]. Estos cables de fibra óptica son los que construyen la infraestructura que finalmente contiene y permite la conectividad chilena a la red informática mundial, o Internet. Ante dichos ataques también llegó a la agenda parlamentaria la preocupación de proteger la integridad de dicha infraestructura[7].

Casi un mes después de la editorial antes mencionada, el diario *La Segunda* también dedicó una editorial al tema, señalando que "los ciberataques son probablemente la principal amenaza de seguridad que enfrenta el país. (...) Lo que está en juego en episodios de este tipo es la confianza de las personas respecto de los sistemas digitales y, con ello, las posibilidades de avanzar en el uso de estas plataformas para el comercio y para otros servicios"[8].

En primera instancia, fueron los sectores económicos que se vieron mayormente alertados debido al rol social que tenía la víctima las vulnerabilidades: fue el Banco de Chile, una institución financiera que recibió, al parecer, tres tipos de agresiones informáticas. Es preciso señalar que las ofensivas fueron de diferentes naturaleza, y que incluso existe discrepancia entre distintos actores nacionales sobre "qué fue que".

Debido a una digitalización de las transacciones económicas, el primer ataque replica un robo de dinero, pero que no ocurre de manera material, es decir, no sustrajeron "billetes" de un banco, pero alteraron los registros de flujo para quitarle cifras de una "cuenta interna" (no de los clientes), y agregarlas a otra. En esta agresión, ocurrido el 24 de mayo de 2018, el banco determinó que "el origen de la falla detectada fue un virus, presumiblemente proveniente de redes internacionales(...)"[9], provocando inconvenientes en las sucursales físicas, y 10 millones de dólares extraídos[10].

Según el comunicado oficial del Banco se estableció que el virus fue dirigido directamente a la sus oficinas centrales, y no a sus clientes, como tampoco sus cuentas y productos[11].

---

[5] Ibíd.

[6] MORAGA, Efraín. La hoja de ruta del nuevo cable transoceánico que llegará a Chile [En línea]. *La Tercera*, Pulso, Empresas & Mercado, 30 de julio, 2018. [Fecha de consulta: 2 de agosto 2018]. Disponible en: <https://www.latercera.com/pulso/noticia/la-hoja-ruta-del-nuevo-cable-transoceanico-llegara-chile/261943/>

[7] SENADO DE CHILE. Desprotección frente a ciberataques: "el problema también está en la seguridad de las redes de fibra óptica". Noticias, 30 de julio, 2018. [Fecha de consulta: 2 de agosto 2018]. Disponible en:< http://www.senado.cl/desproteccion-frente-a-ciberataques-el-problema-tambien-esta-en-la/senado/2018-07-27/103248.html>.

[8] LA SEGUNDA [versión impresa]. La Segunda, Opinión, 26 de julio, 2018. pp. 36. [Fecha de consulta: 2 de agosto 2018]. Disponible en: <http://impresa.lasegunda.com/2018/07/26/A/JA3E88F1>.

[9] BANCO DE CHILE. Comunicado Oficial, Declaración Pública. 28 de mayo, 2018. [Fecha de consulta: 2 de agosto 2018]. Disponible en: <https://ww3.bancochile.cl/wps/wcm/connect/nuestro-banco/portal/sala-de-prensa/noticias-y-comunicados/declaracion-publica2>

[10] DÍAZ, Camila. Entendiendo el ataque al Banco de Chile: ¿Qué diferencia a un virus común de una vulnerabilidad en el sistema? EMOL.CL, 11 de junio, 2018. [Fecha de consulta: 2 de agosto 2018]. Disponible en:< http://www.emol.com/noticias/Tecnologia/2018/06/11/909452/Entendiendo-el-ataque-al-Banco-de-Chile-Que-diferencia-a-un-virus-comun-de-una-vulnerabilidad-en-el-sistema.html>.

[11] BANCO DE CHILE, Op. Cit.

En cuanto al concepto "virus", desde la organización de la sociedad civil "Derechos Digitales", discrepan que lo haya sido: sostuvieron en un medio de comunicación que lo ocurrido fue una "explotación de vulnerabilidad de los sistemas"[12] y que la diferencia está en que no se introdujo un programa malicioso que genera daño, si no que fue un defecto de los sistemas, una vulnerabilidad, que fue aprovechada[13].

Otra consideración de este caso apela a los actores y la procedencia del ataque. El dinero extraído fue llevado a Hong Kong, pero los hackers serían de Israel, propiamente de un equipo llamado *Lazarus Group*, que se adjudicó el hecho pero que no se puede asegurar que sean los mismos individuos detrás de otros ataques (el ataque contra Sony), adjudicados por un grupo del mismo nombre[14].

El segundo ataque, según indica el *Diario Financiero*, estaría vinculado al primero en donde un exempleado habría sustraído pequeños montos vía transferencias durante una década, siendo una estafa superior a $2 mil millones[15]. Sin embargo, a pesar de las sospechas levantadas por dicha publicación, la Superintendencia de Bancos e Instituciones Financieras (SBIF) señala que no estaría relacionado el primer caso con el segundo[16].

El tercer ataque tiene una naturaleza diferente. Datos de 14 mil tarjetas de crédito y débito fueron filtradas[17], y este ataque fue adjudicado por un grupo de hackers que no serían del grupo "criminal" que dijeron ser en redes sociales, según indican expertos[18]. Otro carácter distintivo de este tercer ataque fue que no sustrajeron el dinero de las cuentas filtradas, si no que solicitaron dinero a cambio para eliminar la información sustraída[19].

"Esta reacción de la opinión pública responde a un gran número de preguntas y dudas que surgieron a partir de un fenómeno de seguridad al cual pareciera que no están claras las respuestas"

A partir de estos ciberataques el despliegue de artículos periodísticos y de opinión aumentaron considerablemente, y a agosto de 2018, el tema "ciberseguridad" aparece en los medios de comunicación diariamente. Esta reacción de la opinión pública responde a un gran número de preguntas y dudas que surgieron a partir de un fenómeno de seguridad al cual pareciera que no están claras las respuestas. Así es como posterior a la cobertura de los ataques, diversas opiniones técnicas fueron consultadas, comenzando a divergir ponencias con respecto a qué se puede hacer para aumentar la seguridad.

[12] DÍAZ, Loc. cit.

[13] Ibíd.

[14] Ibíd

[15] DIARIO FINANCIERO [En línea]. SBIF: Robo a Banco de Chile no está vinculado al ciberataque. *Diario Financiero*, Mercados, Mercados en Acción, 19 de julio, 2018. [Fecha de consulta: 2 de agosto 2018]. Disponible en:<https://www.df.cl/noticias/mercados/mercados-en-accion/sbif-robo-a-banco-de-chile-no-esta-vinculado-al-ciberataque/2018-07-18/193411.html>.

[16] Ibíd.

[17] AGUIRRE, Francisco. Expertos informáticos analizan el ciberataque: "Se puede deducir fácilmente que no fue un ataque dirigido a los bancos". *La Tercera* [En línea], Tendencias, 27 de julio, 2018. [Fecha de consulta: 2 de agosto 2018]. Disponible en: <https://www.latercera.com/tendencias/noticia/expertos-informaticos-analizan-ciberataque-se-puede-deducir-facilmente-no-fue-ataque-los-bancos/258588/>.

[18] Ibíd.

[19] Ibíd.

Más allá de las dudas, diversos actores también salieron al debate. En primera instancia se encuentra la Superintendencia de Bancos e Instituciones Financieras (SBIF)[20], que como entidad fiscalizadora de instituciones privadas, fue la primera en ser consultada por su rol. También representantes del Fondo Monetario Internacional (FMI), junto al SBIF y el Banco Central sostuvieron una reunión con el ministro de Hacienda, a solicitud de este[21]. Se citó a reunión el Comité Interministerial de Ciberseguridad, creado en 2015, donde participaron los subsecretarios de la cartera de Interior, Defensa, Relaciones Exteriores, de la Presidencia, Justicia, Economía, Telecomunicaciones y la Agencia Nacional de Inteligencia, y de Hacienda como invitada[22].

Días antes, el senador Felipe Harboe lideró un conversatorio sobre ciberseguridad entre profesionales de distintas áreas públicas y privadas: "Carlos Landeros, Director del Programa Red Conectividad del Estado del Ministerio del Interior; Javiera Sepúlveda, abogada del equipo de Tecnologías y Protección de Datos Carey y Cía; Kenneth Pugh, Senador de la República; Alejandro Hevia, profesor del Departamento de Ciencias de la Computación de la Universidad de Chile y Daniel Álvarez, Fundador de la ONG Derechos Digitales"[23].

La Asociación de Bancos (ABIF) fue citada a la comisión de Hacienda en esta materia[24], además de realizar reuniones con trabajadores bancarios (asociados en la Confederación de Sindicatos Bancarios y Afines) para abordar las vulnerabilidades[25], entre otras reuniones en diversos organismos gremiales[26]. Los muy diversos actores que se sumaron al debate público parecieran tener poco en común en sus otras materias de incumbencia, pero en materia de ciberseguridad todos tienen perspectivas fundamentales para poder comprender el fenómeno en su totalidad.

Ya para fines de julio, La Segunda indicó que "según el estudio de 2017 *Latín América Cybersecurity Report,* desarrollado por la

[20] MINISTERIO DE HACIENDA DE CHILE. Equipo del FMI finaliza su evaluación sobre ciberseguridad con reuniones con el Ministro de Hacienda y autoridades financieras. Sala de Prensa, Noticias, Histórico, 25 de julio, 2018. [Fecha de consulta: 2 de agosto 2018]. Disponible en: <http://www.hacienda.cl/sala-de-prensa/noticias/historico/equipo-del-fmi-finaliza-su-evaluacion.html>.

[21] Ibíd.

[22] PULSO [En línea]. Mesa técnica de ciberseguridad e industria de tecnología realizó su primera sesión. *La Tercera*, Pulso, Empresas & Mercado, 30 de julio, 2018. [Fecha de consulta: 2 de agosto 2018]. Disponible en: <https://www.latercera.com/pulso/noticia/mesa-tecnica-ciberseguridad-e-industria-tecnologia-realizo-primera-sesion/263223/>.

[23] SUBTEL [En línea]. Desarrollar políticas en ciberseguridad será clave para la llegada del 5G. Subsecretaría de Telecomunicaciones (Subtel), Ministerio de Transportes y Telecomunicaciones, Sala de Prensa, Noticias, 11 de julio, 2018. [Fecha de consulta: 2 de agosto 2018]. Disponible en: <https://www.subtel.gob.cl/desarrollar-politicas-en-ciberseguridad-sera-clave-para-la-llegada-del-5g/>.

[24] LEIVA, M.; VILLENA, M. Ciberseguridad: Asociación de Bancos pide que transferencias electrónicas no sean instantáneas. *La Tercera,* El Pulso, Trader, 19 de junio, 2018. [Fecha de consulta: 2 de agosto 2018]. Disponible en: <https://www.latercera.com/pulso/noticia/ciberseguridad-asociacion-bancos-pide-transferencias-electronicas-no-sean-instantaneas/212913/>.

[25] PULSO. Abif se reúne con trabajadores bancarios por ciberseguridad. *La Tercera*, El Pulso, Trader, 2 de julio, 2018. [Fecha de consulta: 2 de agosto 2018]. Disponible en: <https://www.latercera.com/pulso/noticia/abif-se-reune-trabajadores-bancarios-ciberseguridad/227780/>.

[26] VILLAGRÁN, Juan Manuel. Ciberseguridad: protocolo incluye que reguladores compartan resultados de sus inspecciones. *La Tercera*, El Pulso, Empresas & Mercado, 28 de julio, 2018. [Fecha de consulta: 2 de agosto 2018]. Disponible en:<https://www.latercera.com/pulso/noticia/ciberseguridad-protocolo-incluye-reguladores-compartan-resultados-inspecciones/260166/>. ; PULSO [en línea]. Mesa técnica de ciberseguridad e industria de tecnología realizó su primera sesión. Loc. Cit.

consultora IDC, un 12% de las empresas chilenas invirtió sólo ocasionalmente en ciberseguridad durante el año pasado, y un 83% sólo usó un quinto de su presupuesto total de tecnología (TI) en defensa informática"[27]. Esto refleja, como la gran mayoría de los artículos, una visión económica de la seguridad en tanto concluyen que estamos "al debe" en ciberseguridad argumentado por el nivel de inversión en las empresas privadas para protegerse de ataques informáticos. Además el medio indica que "en 2021, los cibercriminales superarán tres a uno a los profesionales de seguridad, según cifras de la firma de investigación *Cybersecurity Ventures*"[28]. Estas estimaciones provocan alerta inmediata en el lector, independientemente de quién sea y cuánto sepa en la materia.

Otras estadísticas, de carácter regional, también aportan a visualizar el panorama nacional como que "en 2017 el número de vulneraciones en Latinoamérica se disparó y creció un 131% según el reporte de *Eset Latín American Security*"[29], también indican o provocan la idea de que no estamos seguros. Se suma a esta noción que el artículo cita a Nicolás Corrado, de la consultora Deloitte Chile, aseverando que "estudios internacionales de Ponemon Institute indican que en promedio las organizaciones tardan 241 días en detectar que fueron hackeadas. Lo ocurrido es algo que viene pasando hace tiempo y hoy nos demuestran el poder que tienen"[30]. En ambos casos estos discursos indican alerta. En el desarrollo del artículo, citan a Oliver Hartley, experto en seguridad de Soluciones Orión, donde asegura que "dentro de la región, Chile está altamente tecnologizado y tiene altos ingresos, lo que lo hace un blanco más atractivo"[31]. Detrás de esta aseveración tiene implícita dos fuerzas en tensión: más tecnologización y digitalización (o "*Internet of Things*") versus más vulnerabilidades, que será desarrollada más adelante.

Dos días después de la publicación de *La Segunda*, un extenso reportaje publicado en *La Tercera* buscó abarcar el panorama completo del país[32]. Ahí se menciona comparativamente nuestro episodio de ciber-"inseguridad" con los ataques ejecutados a nivel mundial, el desarrollo de la Política Nacional de Seguridad, nuestra adhesión al Convenio de Budapest sobre Cibercriminalidad, la apertura de una investigación formal en la Fiscalía de Alta Complejidad Oriente, ingresos de proyectos de ley con suma urgencia en esta materia, la desproporcionalidad en el país entre avances e innovación tecnológica versus inversión en seguridad tecnológica, creación pronta de un Equipo de Respuesta Computacional a la Emergencia (CERT), además de supuestas disputas entre el Ministerio de Defensa y el Ministerio del Interior sobre quién iba a liderar, en su momento, la política de ciberseguridad[33].

[27] O'RYAN, Felipe. Ataques informáticos se han disparado en la región: "Chile es fácil de vulnerar". *La Segunda*, Economía, 27 de julio, 2018. pp. 18-19. [Fecha de consulta: 2 de agosto 2018]. Disponible en: <http://impresa.lasegunda.com/2018/07/27/A/GK3E8TEC>.

[28] Ibíd.

[29] Ibíd.

[30] Ibíd.

[31] Ibíd.

[32] ARTAZA, Francisco; AHUMADA, María José; AYALA, Leslie. Actualizaciones pendientes: la carrera por poner al día los sistemas anticiberataques. *La Tercera*, Reportajes, 29 de julio, 2018. [Fecha de consulta: 2 de agosto 2018]. Disponible en: <https://www.latercera.com/reportajes/noticia/actualizaciones-pendientes-la-carrera-poner-al-dia-los-sistemas-anticiberataques/260662/>.

[33] Ibíd.

A la fecha de la construcción de este cuaderno, 1 de agosto, el exsubsecretario de Defensa y Secretario Ejecutivo del Comité Interministerial de Ciberseguridad, Marcos Robledo Hoecker, respondió a esta última declaración señalando de falsa esta rivalidad entre Interior y Defensa argumentando que "no hubo desacuerdo sobre ese tema"[34]:

> "Particular cuidado hubo de no militarizar lo que no corresponde, así como de definir la primera Política de Ciberdefensa (PCD), que norma y orienta el desarrollo y empleo de las capacidades de la defensa. Y especial coordinación al respecto hubo entre los ministerios del Interior y de Defensa. El gobierno de la Presidenta Bachelet puso en marcha una política comprehensiva sobre el desarrollo ciber: la PNCS [Política Nacional de Ciberseguridad]; una política vinculada a los sectores productivos (Agenda Digital); la PCD; y una de carácter internacional, la cual permitirá al país gestionar y superar los desafíos del área en los próximos años"[35].

Días antes, otra carta en el mismo medio fue publicada. El senador Felipe Harboe, quien había liderado ya una mesa de trabajo días después de los incidentes, escribía en *La Tercera* en respuesta a las declaraciones del ex Superintendente de Bancos e Instituciones Financieras (SBIF), Enrique Marshall, que señala que era "mejor dejar a la SBIF referirse a la filtración de datos, ya que es la institución "mejor preparada" para enfrentar ese fenómeno"[36]. El senador indicó que:

> "Al respecto, creo necesario señalar que en propias palabras del actual superintendente, dicha institución no posee las capacidades técnicas para enfrentar el tema de la ciberseguridad, ya que históricamente su recurso humano y misión no consideraron dicho flagelo. Así las cosas, resulta fundamental hacer entender a algunos actores que la cibercriminalidad no se circunscribe a las instituciones bancarias, sino a toda la denominada infraestructura crítica, donde se encuentran empresas financieras, telecomunicaciones, energía, minería y servicios públicos"[37].

"La mirada, principalmente económica, que se le ha dado al desarrollo de la noticia no solo se explica por la naturaleza del actor vulnerado, sino que también se refleja en las secciones donde se llevan los temas de ciberseguridad en prensa y, en general, las preocupaciones expuestas."

Entre las declaraciones expuestas, quienes se encuentra más cercano a la complejidad del dilema de la ciberseguridad, en su aspecto más multidisciplinario, son: el senador Felipe Harboe, en tanto sí se ha dado una tendencia en este caso chileno a focalizar el punto al sector económico del país, incluyendo el carácter técnico de las ciencias computacionales e informáticas; y Marcos Robledo Hoecker, exsubsecretario de Defensa y Secretario Ejecutivo del Comité Interministerial de Ciberseguridad, en cuanto a la consideración de las problemáticas detrás de militarizar y "segurizar"[38] de manera indiscriminada el ciberespacio.

---

[34] ROBLEDO H., Marcos. Ciberseguridad. *La Tercera*, Correos de los Lectores, 1 de agosto, 2018. [Fecha de consulta: 2 de agosto 2018]. Disponible en: <https://www.latercera.com/opinion/noticia/ciberseguridad-3/265109/>.

[35] Ibíd.

[36] HARBOE, Felipe. Ciberseguridad. *La Tercera* Correos de los Lectores, 30 de julio, 2018. [Fecha de consulta: 2 de agosto 2018]. Disponible en: <https://www.latercera.com/opinion/noticia/ciberseguridad-2/262509/>.

[37] Ibíd.

[38] N. del Autor: La palabra segurizar es un neologismo que significa hacer algo seguro en operaciones computacionales. En: FUNDÉUBBVA. Segurizar mejor que securizar. FundéuBBVA, Buscador urgente de dudas, 19 de febrero, 2015. [Fecha de consulta: 2 de agosto 2018]. Disponible en: <https://www.fundeu.es/recomendacion/segurizar-securizar-securitizar/>.

La mirada, principalmente económica, que se le ha dado al desarrollo de la noticia no solo se explica por la naturaleza del actor vulnerado, sino que también se refleja en las secciones donde se llevan los temas de ciberseguridad en prensa y, en general, las preocupaciones expuestas. Claramente, con excepciones, como la acotación del senador o el exsubsecretario, e incluso la presencia de la ONG Derechos Digitales, aportando con una mirada de sociedad civil en esta materia.

El panorama nacional actual entonces presenta un aumento considerable en la agenda pública, prensa y opinión del concepto de ciberseguridad: suplementos periodísticos completos dedicados a esta temática, principalmente en materias de gestión y administración de empresas, columnas de opinión de especialistas y autoridades, como también comisiones y reuniones especiales. Todo esto para aumentar la seguridad informática del sector empresarial, principalmente, con algunas excepciones que destacan tenuemente en la mitad de la contingencia.

¿Pero eso es todo lo que implica la ciberseguridad? ¿Es meramente una forma de protección de los bienes de una empresa, como es la información, o de una infraestructura que le permite funcionar correctamente, como es el registro de transacciones? ¿O es esta vulnerabilidad particular parte de una conversación más amplia, que cuestiona el rol, y por ende la conducta humana en las tecnologías de información?

Es comprensible que los actores que salieron al frente de la discusión pública fueran principalmente actores de la economía nacional, no solo porque la víctima y el blanco de ataque fue una institución financiera (o información financiera), sino que también porque lo que estaba en juego era la integridad del buen funcionamiento de una actividad económica, como también la confianza de los usuarios en la operatividad del servicio.

Sin embargo, hay un rol que jugar en la ciberseguridad para los actores de la seguridad y defensa del Estado y/o de la población de un Estado-nación. Si no fuera así, la cartera ministerial en esta materia no estaría en el Comité Interministerial sobre Ciberseguridad (CICS). A pesar de la positiva diversidad de ministerios en el CICS que abarca el aspecto multidisciplinario de la problemática, es necesario profundizar el debate de la ciberseguridad a aspectos políticos, internacionales y estudios de la seguridad para poder comprender el ciberespacio en lo que es y tomar mejores medidas y decisiones a la hora de proteger, lo que sea que se quiera proteger.

“Sin embargo, hay un rol que jugar en la ciberseguridad para los actores de la seguridad y defensa del Estado y/o de la población de un Estado-nación.”

La idea de este cuaderno no es hacer una evaluación normativa y positiva de si las acciones de los diversos actores y las estrategias desplegadas son las correctas o inadecuadas. Más que ofrecer una mirada alternativa, la idea es entregar una claridad “macro” o panorámica de cómo la ciberseguridad puede ser observada y estudiada desde los estudios de las relaciones internacionales aplicadas a la seguridad internacional. Es decir, ampliar la mirada a su punto máximo. La utilidad detrás de este cuaderno es reconocer qué preguntas aún no se han planteado para poder avanzar de manera integral en una estrategia de ciberseguridad completa, proactiva y no reactiva. Dicho esto, y de acuerdo al panorama expuesto, hay varias preguntas que hay que visualizar y categorizar.

La primera tiene que ver con los actores. La presencia de actores de opinión y decisión tan diversos en el debate público, habla de la naturaleza del espacio en la cual ocurre la inseguridad. Es decir, es un escenario complejo con una pluralidad de actores que difieren en intereses, conductas, capacidad y tamaño. ¿Cómo podemos analizar y hasta cierto punto prever la conducta de los actores en el ciberespacio de acuerdo a sus propias características particulares?

La segunda tiene que ver con estos mismos intereses, en cuanto determina qué es lo que se quiere proteger, con qué finalidad y si la protección prioritaria de un elemento puede dar espacio a la transgresión de otro elemento que también tiene valor social. Es decir, ¿cuál es el elemento a proteger?

Es necesario que en el desarrollo de "segurizarnos" de acuerdo a las inseguridades globales actuales y futuras, la toma de posiciones sea consecuente con las cosmovisiones y necesidades del país en su complejidad y pluralidad. Este último punto es esencial, en tanto Chile podría seguir el camino de China, Rusia, Estados Unidos, Europa o India en materia de ciberseguridad, Estados que tienen formas propias de abordar la ciberseguridad. Sin embargo, todos estos caminos responden a políticas exteriores e internas diferentes, además de otras necesidades regionales.

Preguntas como la expuesta en la editorial del Diario Financiero sobre la cuarta revolución industrial[39] (si estamos preparados o no), empujan a buscar formas de estarlo. El desafío no solo está en diagnosticar lo antes posible en qué áreas Chile está atrasado pero también está en cómo abordar los distintos desafíos: ¿A qué costo vamos a desarrollar mayor ciberseguridad? ¿La inseguridad es con un foco económico? ¿Un foco ciudadano? ¿Un foco de criminalidad o un foco de áreas de la defensa? ¿Aplica la importancia de la idea y la defensa de la Nación y la soberanía o el camino será hacia potenciar una inserción chilena a una aldea global y cosechar los beneficios de esta decisión? ¿Consideraremos la información como propiedad privada o como un bien común? ¿Qué se quiere proteger? Estas preguntas deben de responderse, pero particularmente este cuaderno busca responder cómo los enfoques clásicos de las relaciones internacionales se aplican a ciberseguridad y cómo esto afecta la percepción del fenómeno.

"Es innegable y hasta cierto punto obvio, pero es necesario argumentar que en ambos casos, se desconoce de dónde provienen tanto los ataques como aquellos que los ejecutaron. Es entonces un campo que supera las fronteras nacionales..."

Enfoques clásicos y la seguridad en el ciberespacio

A partir del panorama nacional, es necesario responder las preguntas clásicas de los enfoques teóricos de las RR.II. aplicadas al ciberespacio. Antes de determinar estas preguntas, hay que aclarar que estas pertenecen al espectro más macro de dicha teoría. La necesidad de retrotraer la ciberseguridad a su visión más extensa, que es el escenario internacional, se condice por la globalidad que tiene la red mundial informática. Es innegable y hasta cierto punto obvio, pero es necesario argumentar que en ambos casos, se desconoce de dónde provienen tanto los ataques como aquellos que los ejecutaron.

[39] DIARIO FINANCIERO. Chile y la cuarta revolución industrial. Loc. Cit.

Es entonces un campo que supera las fronteras nacionales y ahí es donde se encuentra la primera pregunta: ¿qué pasa con los paradigmas tradicionales de la soberanía y las fronteras? Esta se encuentra directamente relacionada con nuestro entendimiento sobre la naturaleza del espacio cibernético, altamente homologado con espacios materiales físicos y las analogías que se utilizan para poder comprender y estudiar el ciberespacio como campo de las relaciones internacionales.

La segunda pregunta, como ya se planteó inicialmente, tiene que ver con la naturaleza y la relevancia de los actores en juego, que poseen intereses y campos de acción diferentes. Los que participan de la red global de información también se observan y analizan a sí mismos de distintas perspectivas según enfoques teóricos variados. Además, tienen diferentes necesidades y, por ende, disímiles elementos a proteger de acuerdo a sus intereses. Es entonces relevante considerar que no todos quieren asegurar los mismos elementos.

A continuación se desarrollarán los dos enfoques clásicos de las relaciones internacionales, centrado en las características base del enfoque liberal, aplicados a la seguridad internacional e ir reduciendo el espacio de estudio hasta la ciberseguridad. Estas dos preguntas no se encuentran independientes en el análisis, ya que las tres se superponen constantemente a la hora de ir aplicando los enfoques al espacio cibernético.

El enfoque teórico liberal del estudio de las RR.II., y con un énfasis en los estudios de seguridad, es decir en su aspecto más general, presenta características desplegadas en los siguientes puntos[40]:

(1) En primer lugar, "(...), no es una teoría. Es un enfoque analítico amplio con una familia de ideas relacionadas y prácticas preferidas. (...) Queda un poco corto de explicaciones teóricas bien desarrolladas de porqué esas cosas (lineamientos, consejos, conclusiones, orientaciones de conducta) funcionan. Es la concepción dominante en la práctica actual de las RR.II. y es influyente en el estudio de las políticas internacionales también"[41]. Además, es un enfoque clásico y se superpone con el realismo, descartando disputas realistas centrales[42].

(2) Es fundamentalmente optimista sobre política, economía y RR.II., es decir, no existe un dilema de seguridad inherente al escenario. Sugiere prácticas preferidas: el liberalismo empuja hacia la cooperación y la democracia; defiende el libre mercado y la propiedad privada; y la defensa de los derechos humanos basados en la importancia del individuo[43]. La idea detrás de defender un sistema económico liberal, se basa en la teoría de la interdependencia creada entre Estados cuando existe y se mantienen enormes flujos comerciales, tornándose más costoso el romper relaciones y la paz[44]. En tanto, "el liberalismo no puede ser entendido sin su compromiso normativo al individuo" .

[40] MORGAN, Patrick. Liberalism. En: COLLINS, Allan. Contemporary Security Studies. Oxford University Press, 2010, pp 338 - 358.

[41] Ibíd.

[42] Ibíd.

[43] Ibíd.

[44] Ibíd.

[45] OWEN IV, John M. "Liberalism and Security." Oxford Research Encyclopedia of International Studies. 30 de noviembre, 2017. Oxford University Press. [Fecha de consulta: 2 de agosto 2018]. Disponible en: <http://internationalstudies.oxfordre.com/view/10.1093/acrefore/9780190846626.001.0001/acrefore-9780190846626-e-33>.

(3) "Las políticas internacionales también son configuradas por las decisiones políticas, económicas y sociales que toma la población de un Estado, decisiones que no necesariamente están determinadas por el sistema internacional"[46]. Se enfatiza el rol de la política interna, como también los actores dentro de las fronteras, como influyentes y jugadores en el escenario internacional: "la política exterior son las preferencias domésticas proyectadas hacia afuera"[47]. Es decir, reconoce como actores internacionales a grupos, agencias, y organismos de toma de decisión, dentro y fuera de las fronteras estatales.

Apartir de estas características, ¿cómo se aplican estas al ciberespacio? Esquematizar estas temáticas por separado no es preciso ni útil, porque se superponen y relacionan en todo momento. Es por esto que se presentarán en un orden relativo, pero continuamente estas materias se irán engranando unas con otras durante el desarrollo del análisis.

Liberalismo occidental y propiedad privada

En la primera característica, que es una perspectiva dominante en las prácticas internacionales, es importante precisar que dicho dominio del enfoque liberal en la práctica internacional es más bien una práctica occidental, y es dominante por consecuencia del fin de la Guerra Fría. Se señaló en la recapitulación del caso chileno la adhesión de Chile al Convenio de Budapest: este Convenio tiene una pretensión universal, pero gestada en la Unión Europea. El Acuerdo entonces no está libre de un sesgo occidental y liberal en tanto pretende la creación de una institucionalidad internacional global de cooperación[48]. Lo que entonces requiere para que el Convenio de Budapest funcione es que, por lo menos en esta materia, todos los Estados soberanos, independientemente de si son occidentales, liberales o no, se suscriban al tratado de cooperación y confianza. ¿Por qué todos? Porque el ciberespacio traspasa las fronteras estatales, por ende necesario que la regulación cubra todos los espacios de la red.

"Lo que entonces requiere para que el Convenio de Budapest funcione es que, por lo menos en esta materia, todos los Estados soberanos, independientemente de si son occidentales, liberales o no, se suscriban al tratado de cooperación y confianza."

Una de las críticas más interesantes al Convenio de Budapest, es aquella de Anja Kovacs, que analiza el Acuerdo en el marco de los beneficios y costos que puede generar para India. En esto, plantea: "¿Qué valor tiene realmente la Convención contra el Cibercrimen si algunos de los países de cuyo territorio se cree que emana una cantidad considerable de esos delitos, como Rusia y China, nunca se inscribirán?[49]".

Esta crítica es fundamental en tanto plantea un problema de la occidentalidad de las formas liberales de cooperación e institucionalización en el escenario internacional, por un lado, de la naturaleza transfronteriza del ciberespacio en el centro, y por otro, de la paradoja que presenta la libertad de elegir y tolerar formas iliberales: si los Estados tienen la soberanía necesaria para la autodeterminación, que el liberalismo

[46] Ibíd.

[47] Ibíd.

[48] KOVACS, Anja. India and the Budapest Convention: To sign or not? Considerations for Indian stakeholders. International Democracy Project, 2016. [Fecha de consulta: 2 de agosto 2018] Disponible en: <https://internetdemocracy.in/reports/india-and-the-budapest-convention-to-sign-or-not-considerations-for-indian-stakeholders/>.

[49] Ibíd.

reconoce, hay Estados que no necesariamente juegan a la cooperación, de poco sirve tener marcos legales entre países que sí juegan a la cooperación en un ciberespacio donde tiene fronteras profundamente más permeables que las fronteras del territorio y deben interactuar con Estados no dispuestos a cooperar.

A partir de lo que dice Kovacs sobre la reticencia de China a firmar el Convenio de Budapest, existe por lo menos un antecedente de un convenio en el cual se encuentra suscrito China pero que no cumplió: la Convención de las Naciones Unidas sobre el Derecho del Mar durante la disputa de territorio marítimo con los países miembros de Asean y Japón.

Además, en la práctica, la independencia y autonomía de internet ante formas de regulación presenta un desafío: la libertad absoluta de los flujos de información permitiría acciones que van en contra del liberalismo económico ya que existe una discrepancia en torno a si la información es un bien privado, un bien común o incluso un bien libre.

Trevor McDougal realizó un análisis de la "cultura hacker" en Rusia para aportar al entendimiento de su comportamiento tras casos de ciberataques que son rastreados hasta territorio ruso[50]. En este estudio se plantea la existencia de una cultura hacker rusa: desarrollada tras la caída de la Unión Soviética, y a partir de trabajadores calificados sin puestos de trabajo y salarios sintonizados a sus capacidades, estos hackers buscaron mejores oportunidades laborales "informales", es decir, al margen de la ley[51]. Aun cuando existe una normativa que penaliza el "hackeo", no se observa como algo moralmente malo sino que aceptable, siempre y cuando no sea en contra de las instituciones e intereses rusos[52].

"...se puede establecer que para los actores económicos la información tiene un valor de mercado y es privatizable. Pero para los Estados pueden existir múltiples preocupaciones que incentivan a acercarse a este interés, o a alejarse, determinado específicamente por el contenido de la información. "

En términos genéricos, se puede establecer que para los actores económicos la información tiene un valor de mercado y es privatizable. Pero para los Estados pueden existir múltiples preocupaciones que incentivan a acercarse a este interés, o a alejarse, determinado específicamente por el contenido de la información.

Para los Estados la información tiene un valor estratégico. Como lo plantea David D. Clark, hay una visión tendiente al realismo, ligada a la retórica de Washington y a la seguridad nacional, mientras que hay otra que está unida a la actividad económica y globalización[53]: "esta captura el crimen internacional y el espionaje industrial"[54]. Clark incorpora no solo los intereses de la "seguridad nacional" de los Estados y los del grupos económicos, sino que también el de la "persona común":

[50] MCDOUGAL, Trevor. Establishing Russia's Responsibility for Cyber- Crime Based on Its Hacker Culture. Int'l L. & Mgmt. Rev., 2015, vol. 11, p. 55. [Fecha de consulta: 2 de agosto 2018] Disponible en: <https://digitalcommons.law.byu.edu/ilmr/vol11/iss2/4>.

[51] Ibíd.

[52] Ibíd.

[53] CLARK, David D. Protecting the Internet as a Public Commons. Bulletin of the American Academy of Arts and Sciences, Vol. 64, No. 2, pp. 62-63. American Academy of Arts & Sciences. [Fecha de consulta: 2 de agosto 2018] Disponible en: <http://www.jstor.org/stable/41149356>.

[54] Ibíd.

> "Muchos de estos temas, aparte de la delincuencia internacional, no nos conciernen a diario como individuos mientras usamos Internet. Varios de nosotros instamos a la Academia a adoptar una visión diferente y centrada en la persona de la ciberseguridad, una visión positiva centrada en Internet como un bien común global. (...) Para el individuo, los problemas de seguridad no se centran en conceptos como la ciberguerra. En cambio, se centran en el miedo al fraude y el robo de identidad, la pérdida de información personal y otros tipos de temores personales. (...) El objetivo es recuperar el "discurso de seguridad" que hoy se centra en el lenguaje y la postura de la guerra, la defensa y la disuasión, para enfocarlo en aquellos asuntos que se relacionan con la forma en que Internet puede empoderar al individuo y puede proporcionar una suficiente "costumbre que el usuario está dispuesto a participar de esa experiencia"[55].

Como ya se ha señalado, el liberalismo reconoce la importancia de actores más allá de los Estados en el escenario internacional. La tensión que existe entre el liberalismo y realismo es reflejo de que el primero reconoce grupos de decisión intraestatales que participan de la configuración del escenario internacional, mientras que el segundo insiste en la relevancia y preponderancia de los Estados como actores principales y determinantes. Es decir, el enfoque liberal tiende a la seguridad considerando y validando una multiplicidad de actores, mientras que para el realismo la búsqueda de la seguridad es, a fin de cuentas, la del Estado.

El ciberespacio presenta un desafío a estos dos enfoques, en cuanto reconoce que los individuos por sí solos podrían generar ataques, llevando el individuo como actor al juego internacional. Independiente de que se reconozca la capacidad destructiva de un hacker, es preciso aclarar cuál es el interés del individuo como categoría de actor y Clark hace una interesante aproximación. El individuo común y corriente, sin ser líder de un grupo de poder, sin capacidad de decisión colectiva, se integraría como un actor internacional. Sin embargo, no es interés de todos los individuos participar de la misma forma que los otros tipos de actores organizados y con una cuota mínima de poder y capacidad de acción internacional. No necesariamente son agentes racionales impulsados por intereses y obtención de poder, o beneficios económicos personales: eso habla de los bienes comunes.

Aquí hay que considerar la composición del ciberespacio. La información es replicable: un dato puede ser sustraído de su propietario, pero el propietario sigue teniendo el dato, solo que después del "robo", hay dos individuos con el mismo dato y, según la característica del dato y las reglas del juego, con los beneficios de este. Detrás de esto está la idea de "*creative commons*", "*open source*", entre otros. Dependiendo del contenido de la información esto puede ser considerado como un delito de robo o plagio, e incluso no queda tan claro ya que la información podría considerarse como un recurso renovable. Incluso, aún dentro de normativas razonables y modernas como el Convenio de Budapest, donde se enmarca casos como el de *Cambridge Analytica*[56], en donde no fue por medio de hackeo que se realizaron dudosas acciones con información que los usuarios entregaron voluntariamente.

Una consideración importante es necesaria revelar: el ciberespacio no fue concebido libre

[55] Ibíd.

[56] BBCMUNDO. 5 claves para entender el escándalo de Cambridge Analytica que hizo que Facebook perdiera US 37.000 millones en un día. *BBC News*, Mundo, 21 de marzo, 2018. [Fecha de consulta: 2 de agosto 2018] Disponible en: <https://www.bbc.com/mundo/noticias-43472797>.

[57] MCEVOY M., Mary. From Global Village to Virtual Battlespace: The Colonizing of the Internet and the Extension of Realpolitik. International Studies Quarterly, Vol. 54, No. 2, junio de 2010, pp. 381-401. Wiley Publications. [Fecha de consulta: 2 de agosto 2018] Disponible en: <http://www.jstor.org/stable/40664172>.

de una ideología económica: "el ciberespacio era capitalista, no socialista, no se basaba en el trueque o en algún otro sistema, y, por extensión, se podría argumentar que el ciberespacio también se interpretó como "occidental"[57]. Mary McEvoy señala que existen discrepancias entre los enfoques. Las posiciones liberales, una más pragmática y otra más utópica, y la realista poseen ideas contrapuestas sobre el significado de la información en sí misma[58]. Los utopistas ven la información como un bien gratuito que se conserva colectivamente, mientras que los realistas la consideran como una sustancia que podría ser propiedad, blanco o arma[59].

Inicialmente, esta pregunta se planteó de acuerdo a la naturaleza y relevancia de los actores en juego, que poseen interés y campos de acción diferentes. Entonces, de acuerdo al enfoque liberal, —que respalda el proceso de la globalización y que ésta a su vez incorpora la hiperconectividad más allá de la fronteras–, existen Estados, organismos, instituciones nacionales e internacionales, e individuos que todos participan en la red global.

Esto hace que bajo el prisma liberal, todos los individuos son potenciales actores internacionales en cuanto concurren, y son incentivados a participar, de las redes de información. Se enmarcan en la aldea global como actores sociales pero pueden configurarse como actores políticos una vez que tengan capacidad de ejecutar una cuota de poder. Aquellos individuos con capacidad técnica suficiente, eventualmente podrían tener suficiente cuota de poder para desestabilizar el normal funcionamiento del ciberespacio. Aquí el individuo pasa a ser una amenaza en potencia en cuanto tenga la capacidad para llevar un ataque.

El siguiente paso sería, entonces, empujar a generar mecanismos de supervisión, o supervigilancia de los individuos para asegurarnos entonces de agentes solitarios. Pero esto, dentro del mismo enfoque liberal que prioriza al individuo, se encuentran dos formas pujantes. El individuo y sus intereses particulares es al mismo tiempo lo que se busca proteger como de lo que hay que protegerse si esos intereses van en contra de otros intereses, y se manifiesta como amenaza. Es decir, el sistema siempre está en una constante alerta de amenazas porque todos los individuos tienen intereses que chocan, es parte de la noción pluralista del individuo globalizado. La noción detrás de esta situación es que para conservar la privacidad y libertad del individuo en Internet, pero a su vez evitar que este se transforme en una amenaza, es donde la seguridad y la libertad debe encontrar un equilibrio.

"Esto hace que bajo el prisma liberal, todos los individuos son potenciales actores internacionales en cuanto concurren, y son incentivados a participar, de las redes de información. "

En segundo lugar, el individuo puede tener intereses contrapuestos con grupos con mayor cuota de poder, como por ejemplo los económicos. La idea detrás del bien público o bien libre es contrario a la idea de un bien privado. Esto se materializa, por ejemplo, en las discusiones en torno a la propiedad intelectual y al espionaje industrial, e incluso en la mencionada "cultura hacker" rusa. La ONG Derechos Digitales durante la discusión del

[58] Ibíd.

[59] Ibíd.

[60] GARAY, Vladimir. TPP-11: ¿En qué consiste la nueva versión del Tratado Transpacífico?. Derechos Digitales, 27 de noviembre, 2017. [Fecha de consulta: 2 de agosto 2018] Disponible en: <https://www.derechosdigitales.org/11738/tpp-11-en-que-consiste-la-nueva-version-del-tratado-transpacifico/>.

Tratado Transpacífico (TPP) sostuvo, junto a otros organismos internacionales, de medidas draconianas en relación a la protección de la propiedad intelectual contra incluso derechos fundamentales de los individuos[60]. Como se señaló, una institucionalización de la información como propiedad privada a nivel global reduce los espacios de libertad de los individuos para poder quizás transar información bajo otras formas que responden a los intereses individuales que el liberalismo pretende proteger.

Esta complejidad es necesario tenerla presente a la hora de institucionalizar normativas de protección de la información y su valor diferido entre los distintos y numerosos actores que interactúan en el ciberespacio. Esto toma cada vez más importancia cuando, de acuerdo al sociólogo Manuel Castells, la información se ha transformado en el primer y mayor recurso de productividad material en la emergente "economía del conocimiento"[61].

"Esta complejidad es necesario tenerla presente a la hora de institucionalizar normativas de protección de la información y su valor diferido entre los distintos y numerosos actores que interactúan en el ciberespacio. "

Tierra, mar, aire, ¿Internet?

La información tiene un valor, pero ese valor no es fijo. Y esa diferencia de valor, también afectará la necesidad de protegerla. La necesidad de resguardo de la información entonces tampoco sería fija. Pero esto no sería nada nuevo: "la noción básica de atacar y defender información y sistemas de información es tan antigua como la guerra misma"[62], es decir, anterior a la masificación de Internet. Eriksson y Giacomello indican que:

"Ya en la década de 1970, se pensaba que las nuevas tecnologías de la información aumentarían la vulnerabilidad de los Estados. (...) Actualmente, la mayoría de los gobiernos son conscientes de que, a través de Internet, individuos y grupos de todo el mundo pueden comunicar información sobre la cual un solo gobierno tiene poco o ningún control. Esta información puede afectar la actitud de su ciudadanía frente a las estructuras políticas y económicas de sus países. Este no es un fenómeno nuevo, ya que los Estados Nación han tenido una experiencia similar con la radio y la televisión. Lo que es diferente es la magnitud de la información y los múltiples puntos de entrada que han agotado aún más las capacidades estatales y sus recursos para bloquear la penetración de esa información"[63].

Los autores indican que Internet tiene una característica distintiva que la separa de los otros medios de comunicación masivo que han preocupado a los Estados. Esta particularidad representa al mismo tiempo una infraestructura y un medio de comunicación[64]. Este presenta una dimensión que se separa de la radio y la televisión como tal, ya que es también un flujo de información que tiene un valor económico considerable para la economía global. Los ataques contra el Banco de Chile sostiene esta idea.

A fin de cuentas, entonces, el ciberespacio, Internet, o la red global es a la vez un medio de comunicación social, un flujo de información con un valor económico, y también un infraestructura crítica "material" (que va desde los cables

[61] ERIKSSON, Johan y GIACOMELLO, Giampiero. The Information Revolution, Security, and International Relations: (IR) Relevant theory?. International Political Science Review, Vol. 27, No. 3 (Jul., 2006), pp. 221-244. Sage Publications, Ltd. [Fecha de consulta: 2 de agosto 2018] Disponible en: <http://www.jstor.org/stable/20445053>.

[62] Ibid.

[63] Ibid.

[64] Ibid.

de fibra óptica submarino, como también los protocolos que permiten las corrientes de información). Además, cada vez nos hacemos más dependientes de este espacio para el desarrollo de la vida social (resumido en la tendencia "Internet de las Cosas" de hacer todo digital y conectado a la red global). Esto lo hace un escenario complejo donde las relaciones humanas operan bajo reglas espacio-temporales-materiales, diferentes a las del escenario global de carácter terrenal-material-natural. Es por esto que la acción, hasta cierto punto casi inconsciente, de trasladar los paradigmas de un espacio al otro, esperando los mismos resultados, es un error.

"...los desarrolladores técnicos de Internet y sus colegas académicos cuentan una historia neoliberal mientras que la comunidad de estudios militares y estratégicos cuentan una historia neorrealista. Ambas historias reconocen al ciberespacio como un nuevo tipo de territorio, con desafíos únicos y ventajas para los participantes."

La información, y los protocolos que ordenan y estructuran esa información, como su infraestructura material, es la consistencia única del ciberespacio. Pero, al parecer, en la práctica, según el comportamiento humano que ocurre en estos flujos de información, suceden fenómenos que nos hacen plantear el ciberespacio como eso: un espacio que opera paralelamente al territorio material.

La aseveración liberal de que el realismo coexiste en el escenario internacional con el liberalismo indica que el liberalismo y el realismo, además de ser enfoques teóricos que compiten, también provocan en los actores competencia de intereses al adoptar estas perspectivas para tomar decisiones sobre las acciones en el escenario internacional.

Sin embargo, al llevarlo al ámbito "ciber" nos encontramos con una problemática: a partir de que Collins no precisa a que se refiere con lugares (¿se refiere a lugar de seguridad y defensa como el mar, la tierra, o el aire sometido a una soberanía?, o ¿se refiere más bien a ser liberal en lo económico pero no necesariamente en política exterior, o no necesariamente liberal con todos los actores?).

Una respuesta breve es que el Estado puede ser realista o no, de manera relativamente independiente, entre su territorio, su política exterior, su política comercial, su política interna y su política informática.

Ejemplo de esto es China que logra exitosamente desarrollar, de manera relativa, una política económica liberal, con políticas internas no liberales y una exterior cambiante. Esto también puede ser unitario al actor, como ya se precisó que no. Pero abre el análisis a la naturaleza del ciberespacio: ¿qué es concretamente el ciberespacio? ¿es un espacio, un escenario, un campo nuevo de acción? ¿o es más bien una hiperconexión que sobrepasa los límites temporales y espaciales al aumentar la velocidad?

Como ya se mencionó, el ciberespacio es una infraestructura material que genera una red de conexión por donde circulan a alta velocidad vastas cantidades de información de un lado del mundo a otro. Según señala McEvoy, "los desarrolladores técnicos de Internet y sus colegas

académicos cuentan una historia neoliberal mientras que la comunidad de estudios militares y estratégicos cuentan una historia neorrealista. Ambas historias reconocen al ciberespacio como un nuevo tipo de territorio, con desafíos únicos y ventajas para los participantes"[65].

La autora señala que desde la perspectiva realista, el ciberespacio es un "terreno estratégico" por lo que no es nada especialmente distinto de otros tipos de terrenos[66]. Al otro extremo, la versión más utópica del liberalismo entiende que el Internet es un "espacio"; donde los actores se reúnen en una variedad de formatos estructurados y no estructurados para intercambiar información, creando una sociedad civil sin fronteras que forma parte del "mundo en el que vivimos" y que la meta del sistema es proveer de información como un bien libre que puede ser abiertamente compartido[67].

La versión más pragmática del liberalismo describe el ciberespacio como: un universo alterno; creado reflexivamente por la acción humana, donde las estructuras del antiguo mundo físico, con sus énfasis en poder, identidad y riqueza, son menos relevantes, y que la información y su seguridad es un bien colectivo que todos los actores del sistema deben respetar mediante el desarrollo de normas de Internet[68].

En ambas percepciones se concibe la información como bienes, unos de libre consumo y otros de consumo más restringido, y por ende propenso a la creación de reglas del juego y marcos normativos. Para los utópicos, según comprende la autora, la aldea global que conforma el ciberespacio es un bien común, sin dueño, que debe ser preservado de esa forma para el bien de todos, como los casquetes polares[69].

"En ambas percepciones se concibe la información como bienes, unos de libre consumo y otros de consumo más restringido, y por ende propenso a la creación de reglas del juego y marcos normativos."

Esto principalmente por la noción que el ciberespacio en su libre flujo de información democratiza esta última. Recordemos que el enfoque liberal promueve la idea de democracia, aun cuando se puede argumentar que la promueve solo como un régimen y sistema político, no necesariamente para cada aspecto humano.

La autora pone el marco histórico la idea del ciberespacio como algo que obtener y defender:

> "(...) tenía poco sentido hablar de "interés nacional" en el ciberespacio, ya que inicialmente no había nada que defender. (...) Y si un virus, ya sea accidental o intencionalmente, destruye algo, era solo el hardware propio de uno o el software que reside en la propia computadora personal. No tenía sentido que algo tangible y de valor residiera en Internet, o que requiriera defensa y preservación. (...) A medida que el ciberespacio adquirió el estatus de propiedad privada, también adquirió estatus como propiedad inmobiliaria. (...) La capacidad de los sitios de Internet para generar ingresos en función del número de visitantes significaba que una dirección ahora tenía un precio debido a su clasificación general en los motores de búsqueda. El ciberespacio tenía así una geografía,

[65] MCEVOY. Loc. Cit.[66] Ibíd.
[67] Ibíd.
[68] Ibíd.

con territorios que podían ser propiedad, valorados y comercializados en el mercado"[70].

El ciberespacio, en para la autora, un espacio construido para ambos enfoques: es a la vez un espacio de liberación, cooperación, participación y movilización, como lo visualizan los utópicos, pero a la vez un lugar oscuro y siniestro como las partes peligrosas y sin gobernabilidad del mundo físico, un nuevo tipo de espacio fallido, con el potencial de cultivar amenazas reales que rápidamente se derramarán en el mundo real[71].

Es probable entonces que los realistas intenten defender, armar y/o dominar el ciberespacio en nombre de la seguridad, mientras que los liberales destinarán sus esfuerzos a regular el ciberespacio como también sus productos físicos e intelectuales por medio de cooperación internacional[72].

Es también importante señalar la problemática de las fronteras. El mercado global, el desarrollo de organizaciones no gubernamentales con influencia y campo de acción internacional, y los movimientos sociales globales son parte de los fenómenos propios del proceso de globalización, ya sea impulsado por las tecnologías de la información, o estas últimas fueron impulsadas por la necesidad de conectividad de las primeras. Independientemente de que vino primero, y más allá del ciberespacio, el proceso de globalización sostiene una permeabilidad de las fronteras nacionales.

Sin embargo, "la globalización es un poderoso símbolo contemporáneo de la visión liberal, sobre todo de las actividades económicas"[73]. Este fenómeno implica la rápida erosión de la soberanía y la autonomía de muchos países en muchos niveles[74], que conduce el escenario internacional en dirección contraria según declara el realismo que es. En el aspecto ciber "los límites se disuelven entre lo internacional y lo doméstico, entre las esferas civil y militar, entre lo privado y lo público, y entre la paz y la guerra"[75]. No solo las fronteras se disuelven, si no que la interdependencia entre las mismas clasificaciones y categorización de la conducta humana se superponen.

Esto "sugiere que no solo se desafía la seguridad de los sistemas de información, sino también, y más fundamentalmente, la soberanía de los Estados (...). Las amenazas cibernéticas desafían principalmente la soberanía interna (control efectivo del territorio nacional y de las personas que viven dentro de ella), pero no necesariamente la soberanía externa (el reconocimiento formal de la independencia por otros Estados (...)"[76].

Este desafío de la soberanía interna responde a que el Estado pierde capacidad de poder de control de las amenazas contra su población, en tanto estos se encuentran conectados casi sin regulación alguna, con individuos y actores a nivel global. Además, la categorización y separación a la hora de tratar con ellas pierde valor, razón por la cual resulta necesario que las agencias de seguridad de los Estados mantengan un diálogo permanente y colaborativo.

Libertad versus seguridad

Por último, hay que retrotraerse a la segunda característica del liberalismo, en tanto indica que la característica fundamental de este enfoque

[69] Ibíd.

[70] Ibíd.

[71] Ibíd.

[72] Ibíd.

[73] Collins. Loc. Cit.

[74] Ibíd.

[75] Eriksson, Giacomello, Loc. Cit.

es la importancia del individuo. “Un liberalismo consistente no se preocupa por la “seguridad del Estado” o la “seguridad nacional”, excepto en la medida en que sean decisivos para la seguridad de las personas dentro de esos Estados”[77]. En este sentido el liberalismo en el ciberespacio se debería guiar por la protección del individuo, y de su seguridad, más que del resguardo e integridad de la información como valor estratégico.

“En este sentido el liberalismo en el ciberespacio se debería guiar por la protección del individuo, y de su seguridad, más que del resguardo e integridad de la información como valor estratégico. ”

En sentido estricto, y por la naturaleza de las amenazas, el individuo como unidad de cuidado se observa desde la protección de su privacidad y de sus antecedentes, como también de los intereses materiales que existen detrás de los datos. Esto le da un carácter primordial aunque no exclusivo de criminalidad.

El individuo se ve más amenazado directamente por la cibercriminalidad que por el espionaje internacional. Pero, a su vez, la construcción de la amenaza a otros actores o referentes de protección, como la infraestructura crítica, el orden, el régimen, el Estado, las empresas privadas propietarias de las infraestructuras o incluso de los datos, afectan por su relación con el individuo. Pero cuando se habla de aspecto más complejos como hacktivismo, el individuo se encuentra en una situación de protegido secundario: “el Estado es instrumental para los propósitos de las personas. (...) Las personas pueden crear, mantener y destruir instituciones y así mejorar o degradar la seguridad nacional e internacional”[78].

De acuerdo a las declaraciones del exsubsecretario, Marcos Robledo, en cuanto a no militarizar lo que no corresponde, responde entonces al equilibrio que hay que definir en su máxima complejidad cuando el individuo y su multiplicidad de intereses tiene la capacidad de ser un criminal o una amenaza a las estructuras de poder político o económico como también el objetivo fundamental a proteger. Cuando este equilibro dentro de las fronteras no se cumple, los individuos gracias a la hiperconectividad pueden encontrar respaldo y cooperación más allá de los Estados. Internet “permite a los estados separar a individuos y grupos de manera profunda, permite a individuos y grupos cooperar en todos los estados para el beneficio mutuo”[79].

Es por esta razón que los gobiernos, siguiendo enfoques liberales, buscarán centrar sus visiones de ciberseguridad en la criminalidad, más que en visiones realistas donde el actor principal es el Estado, y los individuos son todos amenazas en potencia, si es que tienen las capacidades técnicas necesarias para efectuar ataques de gran escala.

El valor que tiene la información, la única sustancia que existe en la red global, variará de actor “A” a actor “B”, de interés “a” a interés “b”, de contenido “x” a contenido “y”, y de enfoque liberal a enfoque realista. La protección y su valor estratégico dependerá de caso a caso. Además, de acuerdo a la tendencia global de impulsar la tecnología y las interacciones humanas hacia más y mayor digitalización y conectividad global en línea, en ningún sentido los intereses de los diversos actores serán fijos.

[76] Ibíd

[77] Owen. Op. Cit.

[78] Ibid.

Dicho esto, habrá casos donde un mismo enfoque se verá contrapuesto por sí mismo y con otros, mientras que la aplicación de ambos podría mejor aclarar el panorama. Por ejemplo, el caso de *Cambridge Analytica* puso en contraposición la visión más pragmática del liberalismo cibernético con una eminentemente moral, en cuanto utilizó información entregada voluntariamente para otros fines, dentro de las mismas políticas de seguridad de los canales aceptadas por los usuarios, pero que posteriormente fue utilizado para empujar a los individuos a una determinada acción, no elegida libremente por estos.

"Tras este caso, todas las plataformas digitales cambiaron sus términos y condiciones de privacidad y seguridad, además de una visualización de la necesidad de proteger los datos personales."

Lo que ocurrió no se concibe como una amenaza a la seguridad nacional proveniente de un agente externo a las fronteras del Estado-Nación, aun cuando la mala praxis de datos vino de instituciones y actores fuera de las fronteras. Por ende, no es asunto del ciberseguridad de los estudios de la defensa, sino más bien un acto contra principios liberales, de protección de los intereses y valores de seguridad del individuo. Estos casos no responden ni a la cibercriminalidad ni a la ciberseguridad, pero tras este hecho la aseveración resulta dudosa. Tras este caso, todas las plataformas digitales cambiaron sus términos y condiciones de privacidad y seguridad, además de una visualización de la necesidad de proteger los datos personales. Posterior al suceso, se ha generado entonces un nuevo elemento a proteger.

Por otro lado, la divulgación de mensajes de odio contra grupos de una sociedad, o en contra de un régimen, pueden considerarse como amenazas a la seguridad. Son formas en donde la libertad de expresión compite con otras libertades en el primer caso, o en contra de la seguridad realista de un Estado.

De acuerdo entonces con el liberalismo, la protección de la información debe constituir la segunda categoría de la seguridad del individuo, de esta manera se genera inmediatamente una jerarquía de acciones en el ciberespacio que permiten distintos niveles de represalias.

Por ejemplo, un hackeo de corte de luz, si bien es contra una empresa, pertenece a una infraestructura crítica y puede generar daños materiales. No tanto como si las torres de control de un aeropuerto fuera hackeada. Sin embargo, el tráfico de música ilegal no debería posesionarse con el mismo nivel de sanción, o el boicot por ejemplo contra una página web.

Se puede deducir, de acuerdo a lo revisado, que las tendencias realistas promueven la sanción a cualquier forma de alteración de la información, mientras que un enfoque liberal debería tender a consideraciones más específicas. Con todo, tras la guerra contra el terrorismo, los países más liberales han empujado sus perspectivas hacia el realismo para poder luchar con dicha amenaza.

Tras los argumentos desplegados en este cuaderno, el escenario global hiperconectado por el ciberespacio presenta una dicotomía entre seguridad y libertad. Si realmente la seguridad, en su sentido más realista y pragmático, fuera el objetivo central de un Estado, sencillamente

[79] Ibíd.

[80] GOLDSMITH, Jack. The Failure of Internet Freedom. Emerging Threats, Knight First Amendment Institute, Columbia

la supervigilancia y el control del tránsito de la información se implementaría en un instante.

China es un ejemplo de esto[80]. Si bajo la idea de proteger el sistema económico (liberal o no) y el sistema (democrático o no) se quisiera sancionar las voces que, al hacer uso de su libertad de expresión, van y empujan en contra del *statu quo*, nos encontramos con una contradicción que solo se resuelve por medio del mismo enfoque liberal: "las intervenciones de la red para promover la libertad y la democracia no están en el mismo plano moral que las intervenciones de la red para interrumpir o socavar la democracia"[81]. Entre el caso de China, y la defensa de un hacktivismo liberal, hay un espectro amplio de acciones en donde la libertad y la seguridad entran en juego.

Conclusión

Retomando las preguntas planteadas podemos hacer algunas aproximaciones. ¿Qué pasa con los paradigmas tradicionales de la soberanía y las fronteras? Estas se ven replanteadas, no reemplazadas o borradas. El individuo en su materialidad sigue existiendo en un territorio soberano, dentro de un Estado con el monopolio exclusivo de la fuerza. Sin embargo, el acceso a información es universal, y eso modifica las percepciones y valores de los individuos.

¿Cuál es el elemento que se busca proteger? Si el rol del Estado es estar al servicio del individuo y sociedad y otorgarles protección, replanteará entonces sus nociones a asegurar de acuerdo a las necesidades y demandas de su población. Esto claramente, y según lo expuesto, no estaría libre de posiciones contrapuestas y contradictorias. Tendrá que buscar equilibrios entre la "tecnologización" y digitalizacion de las acciones humanas tanto productivas como sociales, entre fuerzas externas como internas, y considerando el respeto hacia el individuo, si se espera en tanto mantenerse en un enfoque de práctica liberal.

"Si el rol del Estado es estar al servicio del individuo y sociedad y otorgarles protección, replanteará entonces sus nociones a asegurar de acuerdo a las necesidades y demandas de su población. Esto claramente, y según lo expuesto, no estaría libre de posiciones contrapuestas y contradictorias."

Para esto, Chile en este vasto escenario altamente complejo, de múltiples variables y profundas consideraciones, la mejor forma para empezar a precisar las políticas y toma de decisión, frente a problemas de ciberseguridad, es plantear y definir el valor económico, moral, y estratégico de la multiplicidad de actores nacionales y extranjeros que interactúan en el ciberespacio, y contrastarlos con los paradigmas pasados y presentes en materia de seguridad interna y externa.

University, 2018.

[81] Ibíd.

Bibliografía.

AGUIRRE, Francisco. Expertos informáticos analizan el ciberataque: “Se puede deducir fácilmente que no fue un ataque dirigido a los bancos”. La Tercera [En línea], Tendencias, 27 de julio, 2018. [Fecha de consulta: 2 de agosto 2018]. Disponible en: <https://www.latercera.com/tendencias/noticia/expertos-informaticos-analizan-ciberataque-se-puede-deducir-facilmente-no-fue-ataque-los-bancos/258588/>.

ARTAZA, Francisco, AHUMADA, María José y AYALA, Leslie. Actualizaciones pendientes: la carrera por poner al día los sistemas anticiberataques. La Tercera, Reportajes, 29 de julio, 2018. [Fecha de consulta: 2 de agosto 2018]. Disponible en: <https://www.latercera.com/reportajes/noticia/actualizaciones-pendientes-la-carrera-poner-al-dia-los-sistemas-anticiberataques/260662/>.

BANCO DE CHILE. Comunicado Oficial, Declaración Pública. 28 de mayo, 2018. [Fecha de consulta: 2 de agosto 2018]. Disponible en: <https://ww3.bancochile.cl/wps/wcm/connect/nuestro-banco/portal/sala-de-prensa/noticias-y-comunicados/declaracion-publica2>.

BBCMUNDO. 5 claves para entender el escándalo de Cambridge Analytica que hizo que Facebook perdiera US 37.000 millones en un día. BBC News, Mundo, 21 de marzo, 2018. [Fecha de consulta: 2 de agosto 2018] Disponible en: <https://www.bbc.com/mundo/noticias-43472797>.

CLARK, David D. Protecting the Internet as a Public Commons. Bulletin of the American Academy of Arts and Sciences, Vol. 64, No. 2, pp. 62-63. American Academy of Arts & Sciences. [Fecha de consulta: 2 de agosto 2018] Disponible en:<http://www.jstor.org/stable/41149356>

DIARIO FINANCIERO. Chile y la cuarta revolución industrial [En línea]. Diario Financiero, Editorial, 29 de junio, 2018. [Fecha de consulta: 2 de agosto 2018]. Disponible en: <https://www.df.cl/noticias/opinion/editorial/chile-y-la-cuarta-revolucion-industrial/2018-06-29/192558.html>.

DIARIO FINANCIERO [En línea]. SBIF: Robo a Banco de Chile no está vinculado al ciberataque. Diario Financiero, Mercados, Mercados en Acción, 19 de julio, 2018. [Fecha de consulta: 2 de agosto 2018]. Disponible en: <https://www.df.cl/noticias/mercados/mercados-en-accion/sbif-robo-a-banco-de-chile-no-esta-vinculado-al-ciberataque/2018-07-18/193411.html>.

DÍAZ, Camila. Entendiendo el ataque al Banco de Chile: ¿Qué diferencia a un virus común de una vulnerabilidad en el sistema? EMOL.CL, 11 de junio, 2018. [Fecha de consulta: 2 de agosto 2018]. Disponible en: <http://www.emol.com/noticias/Tecnologia/2018/06/11/909452/Entendiendo-el-ataque-al-Banco-de-Chile-Que-diferencia-a-un-virus-comun-de-una-vulnerabilidad-en-el-sistema.html>.

ERIKSSON, Johan y GIACOMELLO, Giampiero. The Information Revolution, Security, and International Relations: (IR) Relevant theory?. International Political Science Review, Vol. 27, No. 3 (Jul., 2006), pp. 221-244. Sage Publications, Ltd. [Fecha de consulta: 2 de agosto 2018] Disponible en: <http://www.jstor.org/stable/20445053>.

FUNDÉUBBVA. Segurizar mejor que securizar. FundéuBBVA, Buscador urgente de dudas, 19 de febrero, 2015. [Fecha de consulta: 2 de agosto 2018]. Disponible en: <https://www.fundeu.es/recomendacion/segurizar-securizar-securitizar/>.

GARAY, Vladimir. TPP-11: ¿En qué consiste la nueva versión del Tratado Transpacífico?. Derechos Digitales, 27 de noviembre, 2017. [Fecha de consulta: 2 de agosto 2018] Disponible en: <https://www.derechosdigitales.org/11738/tpp-11-en-que-consiste-la-nueva-version-del-tratado-transpacifico/>.

GOLDSMITH, Jack. The Failure of Internet Freedom. Emerging Threats, Knight First Amendment Institute, Columbia University, 2018.

HARBOE, Felipe. Ciberseguridad. La Tercera Correos de los Lectores, 30 de julio, 2018. [Fecha de consulta: 2 de agosto 2018]. Disponible en: <https://www.latercera.com/opinion/noticia/ciberseguridad-2/262509/>.

KOVACS, Anja. India and the Budapest Convention: To sign or not? Considerations for Indian stakeholders. International Democracy Project, 2016. [Fecha de consulta: 2 de agosto 2018] Disponible en: <https://internetdemocracy.in/reports/india-and-the-budapest-convention-to-sign-or-not-considerations-for-indian-stakeholders/>.

LA SEGUNDA [versión impresa]. La Segunda, Opinión, 26 de julio, 2018. pp. 36. [Fecha de consulta: 2 de agosto 2018]. Disponible en: <http://impresa.lasegunda.com/2018/07/26/A/JA3E88F1>.

LEIVA, M. y VILLENA, M. Ciberseguridad: Asociación de Bancos pide que transferencias electrónicas no sean instantáneas. La Tercera, El Pulso, Trader, 19 de junio, 2018. [Fecha de consulta: 2 de agosto 2018]. Disponible en: <https://www.latercera.com/pulso/noticia/ciberseguridad-asociacion-bancos-pide-transferencias-electronicas-no-sean-instantaneas/212913/>.

MCDOUGAL, Trevor. Establishing Russia's Responsibility for Cyber- Crime Based on Its Hacker Culture. Int'l L. & Mgmt. Rev., 2015, vol. 11, pp. 55. [Fecha de consulta: 2 de agosto 2018] Disponible en: <https://digitalcommons.law.byu.edu/ilmr/vol11/iss2/4>.

MCEVOY M., Mary. From Global Village to Virtual Battlespace: The Colonizing of the Internet and the Extension of Realpolitik. International Studies Quarterly, Vol. 54, No. 2, junio de 2010, pp. 381-401. Wiley Publications. [Fecha de consulta: 2 de agosto 2018] Disponible en: <http://www.jstor.org/stable/40664172>.

MINISTERIO DE HACIENDA DE CHILE. Equipo del FMI finaliza su evaluación sobre ciberseguridad con reuniones con el Ministro de Hacienda y autoridades financieras. Sala de Prensa, Noticias, Histórico, 25 de julio, 2018. [Fecha de consulta: 2 de agosto 2018]. Disponible en: <http://www.hacienda.cl/sala-de-prensa/noticias/historico/equipo-del-fmi-finaliza-su-evaluacion.html>.

MORAGA, Efraín. La hoja de ruta del nuevo cable transoceánico que llegará a Chile [En línea]. La Tercera, Pulso, Empresas & Mercado, 30 de julio, 2018. [Fecha de consulta: 2 de agosto 2018]. Disponible en:<https://www.latercera.com/pulso/noticia/la-hoja-ruta-del-nuevo-cable-transoceanico-llegara-chile/261943/>

MORGAN, Patrick. Liberalism. En: COLLINS, Allan. Contemporary Security Studies. Oxford University Press, 2010, pp 338 - 358.

MURRAY, Andrew D. The Regulation of Cyberspace: Control in the Online Environment. New York: Routledge, 2007.

O'RYAN, Felipe. Ataques informáticos se han disparado en la región: "Chile es fácil de vulnerar". La Segunda, Economía, 27 de julio, 2018. pp. 18 - 19. [Fecha de consulta: 2 de agosto 2018]. Disponible en: <http://impresa.lasegunda.com/2018/07/27/A/GK3E8TEC>.

OWEN IV, John M. "Liberalism and Security." Oxford Research Encyclopedia of International Studies. 30 de noviembre, 2017. Oxford University Press. [Fecha de consulta: 2 de agosto 2018]. Disponible en: <http://internationalstudies.oxfordre.com/view/10.1093/acrefore/9780190846626.001.0001/acrefore-9780190846626-e-33>.

PULSO [En línea]. Abif se reúne con trabajadores bancarios por ciberseguridad. La Tercera, El Pulso, Trader, 2 de julio, 2018. [Fecha de consulta: 2 de agosto 2018]. Disponible en: <https://www.latercera.com/pulso/noticia/abif-se-reune-trabajadores-bancarios-ciberseguridad/227780/>.

PULSO [En línea]. Mesa técnica de ciberseguridad e industria de tecnología realizó su primera sesión. La Tercera, Pulso, Empresas & Mercado, 30 de julio, 2018. [Fecha de consulta: 2 de agosto 2018]. Disponible en: <https://www.latercera.com/pulso/noticia/mesa-tecnica-ciberseguridad-e-industria-tecnologia-realizo-primera-sesion/263223/>.

ROBLEDO H., Marcos. Ciberseguridad. La Tercera, Correos de los Lectores, 1 de agosto, 2018. [Fecha de consulta: 2 de agosto 2018]. Disponible en: <https://www.latercera.com/opinion/noticia/ciberseguridad-3/265109/>.

SENADO DE CHILE. Desprotección frente a ciberataques: "el problema también está en la seguridad de las redes de fibra óptica". Noticias, 30 de julio, 2018. [Fecha de consulta: 2 de agosto 2018]. Disponible en: <http://www.senado.cl/desproteccion-frente-a-ciberataques-el-problema-tambien-esta-en-la/senado/2018-07-27/103248.html>.

SUBTEL [En línea]. Desarrollar políticas en ciberseguridad será clave para la llegada del 5G. Subsecretaría de Telecomunicaciones (Subtel), Ministerio de Transportes y Telecomunicaciones, Sala de Prensa, Noticias, 11 de julio, 2018. [Fecha de consulta: 2 de agosto 2018]. Disponible en: <https://www.subtel.gob.cl/desarrollar-politicas-en-ciberseguridad-sera-clave-para-la-llegada-del-5g/>.

VILLAGRÁN, Juan Manuel. Ciberseguridad: protocolo incluye que reguladores compartan resultados de sus inspecciones. La Tercera, El Pulso, Empresas & Mercado, 28 de julio, 2018. [Fecha de consulta: 2 de agosto 2018]. Disponible en: <https://www.latercera.com/pulso/noticia/ciberseguridad-protocolo-incluye-reguladores-compartan-resultados-inspecciones/260166/>.

DIRECCIÓN DE LA REVISTA

DIRECTOR

CONSEJO EDITORIAL


CENTRO DE INVESTIGACIONES Y ESTUDIOS ESTRATÉGICOS
ANEPE.CL