CIEE

CENTRO DE INVESTIGACIONES Y ESTUDIOS ESTRATÉGICOS
ANEPE.CL

ISSN 0719-4110

CUADERNO DE TRABAJO N°1-2018


# CIBERINTELIGENCIA: CONTEXTUALIZACIÓN, APROXIMACIÓN CONCEPTUAL, CARACTERÍSTICAS Y DESAFÍOS


**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

# CIBERINTELIGENCIA: CONTEXTUALIZACIÓN, APROXIMACIÓN CONCEPTUAL, CARACTERÍSTICAS Y DESAFÍOS

Marzo, 2018
**Dra. Carolina Sancho Hirane***

"Hasta la fecha, la principal amenaza contra los datos masivos han sido su robo y filtración. Sin embargo, eso no era más que el principio. A medida que avancemos, toparemos con nuevos riesgos que podrían demostrar ser incluso más peligrosos, como la modificación sin autorización de la información de la cual depende el mundo para llevar a término sus actividades diarias. Aunque hemos depositado una confianza tremenda en los datos que guardamos febrilmente en ubicaciones externas, la precisión subyacente de esta información, tal como descubriremos, puede subvertirse con suma facilidad, con consecuencias relevantes para todos. Y es que, de la misma manera que los malos pueden hurtar nuestros datos, también pueden modificarlos. Esta tempestad que se avecina nos volverá vulnerables y sacudirá los cimientos de nuestra fe en un mundo que depende de los datos de modos que aún no somos completamente capaces de entender"**

## RESUMEN:

Este documento aborda la noción de "ciberinteligencia" como término que emerge en el marco de la existencia de una nueva dimensión en la que se efectúan las relaciones entre las personas, organizaciones e instituciones: el ciberespacio. En este contexto, es efectuada una aproximación teórica al término, identificándose el fenómeno al cual hace referencia, como también, describiendo algunas de las características que presenta y desafíos a abordar para el desarrollo de la ciberinteligencia.

**PALABRAS CLAVE:** Ciberespacio – ciberseguridad – ciberinteligencia

## Introducción

Este trabajo se estructura en tres partes. La primera, contextualiza el ambiente desde el que emerge el término ciberinteligencia. La segunda, explica la noción de ciberinteligencia y son descritas algunas de las características que presenta. Finalmente, en la tercera parte, son descritos algunos desafíos asociados a la ciberinteligencia. En forma transversal a lo largo del texto es revisada la situación chilena en la materia. Para el desarrollo de este trabajo se ha utilizado material bibliográfico especializado y actualizado proveniente de artículos, revistas y presentaciones efectuadas en conferencias donde han participado expertos en el tema.

* Doctora en Conflictos, Seguridad y Solidaridad, Universidad de Zaragoza en España. Magíster en Ciencia Política, Universidad de Chile. Licenciada en Gobierno y Gestión Pública y Administradora Pública, Universidad de Chile. Ha sido profesora en diferentes cátedras, entre ellas, la Escuela de Gobierno y Gestión Pública de Universidad de Chile; en la Universidad de Santiago de Chile la cátedra "Construcción de Procesos de Paz". Ha sido profesora titular y de Inteligencia y Jefa de Diplomados en ANEPE. También ha sido profesora en la Academia de Guerra Aérea de Chile. Se ha desempeñado en la Contraloría General de la República y como Jefa del Departamento de Crimen Organizado en el Ministerio del Interior y Seguridad Pública de Chile.

** GOODMAN, Marc. Los delitos del futuro. España, Ariel, 2015. pp. 192–193.

## Desarrollo[1]:

1.Contexto en el cual emerge la ciberinteligencia: Ciberespacio y ciberseguridad

La noción de ciberinteligencia es resultado de la existencia del ciberespacio el cual, como nueva dimensión o dominio, facilita las interacciones sociales pero además presenta peligros que requieren ser abordados desde una perspectiva de seguridad en el ciberespacio, como condición necesaria mas no suficiente. A continuación será descrita la noción de ciberseguridad y revisadas algunas de sus implicancias como nuevo ambiente en el cual se relacionan personas e instituciones.

1.1. Ciberespacio: Último dominio para la interacción entre personas

El ciberespacio es actualmente la última dimensión o dominio reconocido en la cual las personas, organizaciones e instituciones a nivel nacional, internacional y transnacional interactúan con la finalidad de comunicarse, intercambiar bienes o servicios, generar valor agregado a productos, entre otros. Las otras dimensiones "tradicionales" son tierra, aire y mar, considerándose además, en algunos casos, el espacio.

El ciberespacio como dominio presenta cualidades que lo distinguen de los otros, tal como indica Borg "el ciberespacio no es un ámbito análogo al de la tierra, mar, aire o estratósfera, no tiene distancias, posiciones ni territorios que puedan ocuparse; el ciberespacio no puede ser conquistado"[2]. Aunque las características y juventud de este ámbito pueden darle la cualidad de novedosa, ello no ha impedido un desarrollo teórico y práctico tanto del significado de su existencia como de las implicancias de contar con éste, siendo posible identificar entre otros temas, sus ventajas y desventajas.

**"El ciberespacio es actualmente la última dimensión o dominio reconocido en la cual las personas, organizaciones e instituciones a nivel nacional, internacional y transnacional interactúan con la finalidad de comunicarse, intercambiar bienes o servicios, generar valor agregado a productos, entre otros. "**

Siendo reciente este desarrollo teórico, producto de la existencia del ambiente digital o virtual[3], presenta un creciente consenso respecto a aproximaciones conceptuales como ciberespacio y ciberseguridad, términos que extrapolados de conceptos tradicionales como espacio y seguridad, dan cuenta de que se trata de nociones aplicadas a un fenómeno de naturaleza diferente. No obstante, es una actividad que está en sus etapas iniciales, existiendo términos asociados como el de ciberinteligencia donde es necesario generar algunos elementos de convergencia, pues dada la naturaleza del fenómeno a abordar, son diversos los actores de diferentes organizaciones, instituciones y países que podrían participar en ella y una aproximación compartida al fenómeno podría facilitar un buen comienzo.

[1] Algunas ideas planteadas en este cuaderno de trabajo han sido presentadas anteriormente en otros escritos de la autora publicados en ANEPE. Al respecto ver especialmente SANCHO, Carolina. "Ciberespacio bien público mundial en tiempos de globalización: Política pública de ciberseguridad una necesidad imperiosa y la ciberdefensa como desafíos en el siglo XXI", en Ciberdefesa e cibersegurança: Novas ameaças a segurança nacional. Brasil, XVII Conferencia de Directores de Colegios de Defesa Ibero-americanos, 2016.

[2] BORG, Scott. No es una guerra fría. En: Vanguardia Dossier Nº 54. España, 2015. pp. 65.

[3] Se reconoce que en sentido estricto los conceptos "ciberespacio", "digital" "cibernético" y "virtual" pueden ser diferentes. No obstante, en sentido amplio pueden ser considerados como sinónimos y es en este último sentido que son referenciados en el marco de este documento.

En este sentido, por ejemplo, la Unión Internacional de Telecomunicaciones (UIT), el organismo especializado de la Organización de Naciones Unidas (ONU) para la tecnología de la información y las comunicaciones (TIC), entiende el ciberentorno[4] como "usuarios, redes, dispositivos, todo el software, procesos, información almacenada o que circula, aplicaciones, servicios y sistemas que están conectados directa o indirectamente a las redes"[5]. En el caso chileno, dos documentos oficiales abordan conceptualmente esta concepción en forma similar. En efecto, el texto "Bases para una Política Nacional de Ciberseguridad", publicado en 2015, explica el concepto de ciberespacio como "un ambiente compuesto por las infraestructuras tecnológicas, los componentes lógicos de la información y las interacciones sociales que se verifican en su interior"[6] y en la Política Nacional de Ciberseguridad (PNCS), publicada en 2017, el mismo término es entendido como "el conjunto de infraestructuras físicas, lógicas y las interacciones humanas que allí ocurren"[7], constatándose una aproximación coincidente en todas ellas.

En la práctica, el uso del ciberespacio presenta un crecimiento sostenido, tal como queda reflejado en tanto en el Informe Medición de la Sociedad de la Información 2017 (ver gráfico N° 1), como en las diferentes versiones de estos informes publicados por la UIT desde 2007. En efecto, de acuerdo a cifras proporcionadas por UIT en 2016, más de 3.500 millones de personas en el mundo tenían acceso a internet, cifra que correspondería a "81% en los países desarrollados, 40% en los países en desarrollo y 15% en los Países Menos Adelantados"[8].

En el caso chileno se corrobora esta tendencia, debido a que los "accesos a internet han crecido en un 45,3%, en el último bienio, pasando de 52,2 accesos por cada 100 habitantes a inicios de 2014, a 73,8 accesos por cada 100 habitantes en marzo de 2016. La economía digital nacional, en tanto, creció en torno al 11% en el último bienio, pasando de 34.127 millones de dólares en 2014 a 39.485 millones de dólares en 2015"[9], de manera tal que "Chile ostenta la mayor tasa de penetración de internet en América Latina, con más de un 70% de su población conectada"[10].

[4] En este trabajo son considerados como sinónimos "ciberentorno" y "ciberespacio".

[5] UIT. Recomendación UIT-T X.1205 (04/2008). p. 2.

[6] CHILE. Bases para una Política Nacional de Ciberseguridad. Chile, Ministerio del Interior y Seguridad Pública y Ministerio de Defensa Nacional, 2015. p. 13. [Fecha de consulta: 10 de julio de 2017]. Disponible en http://ciberseguridad.interior.gob.cl/media/2015/12/Documento-Bases-Pol%C3%ADtica-Nacional-sobre-Ciberseguridad.pdf

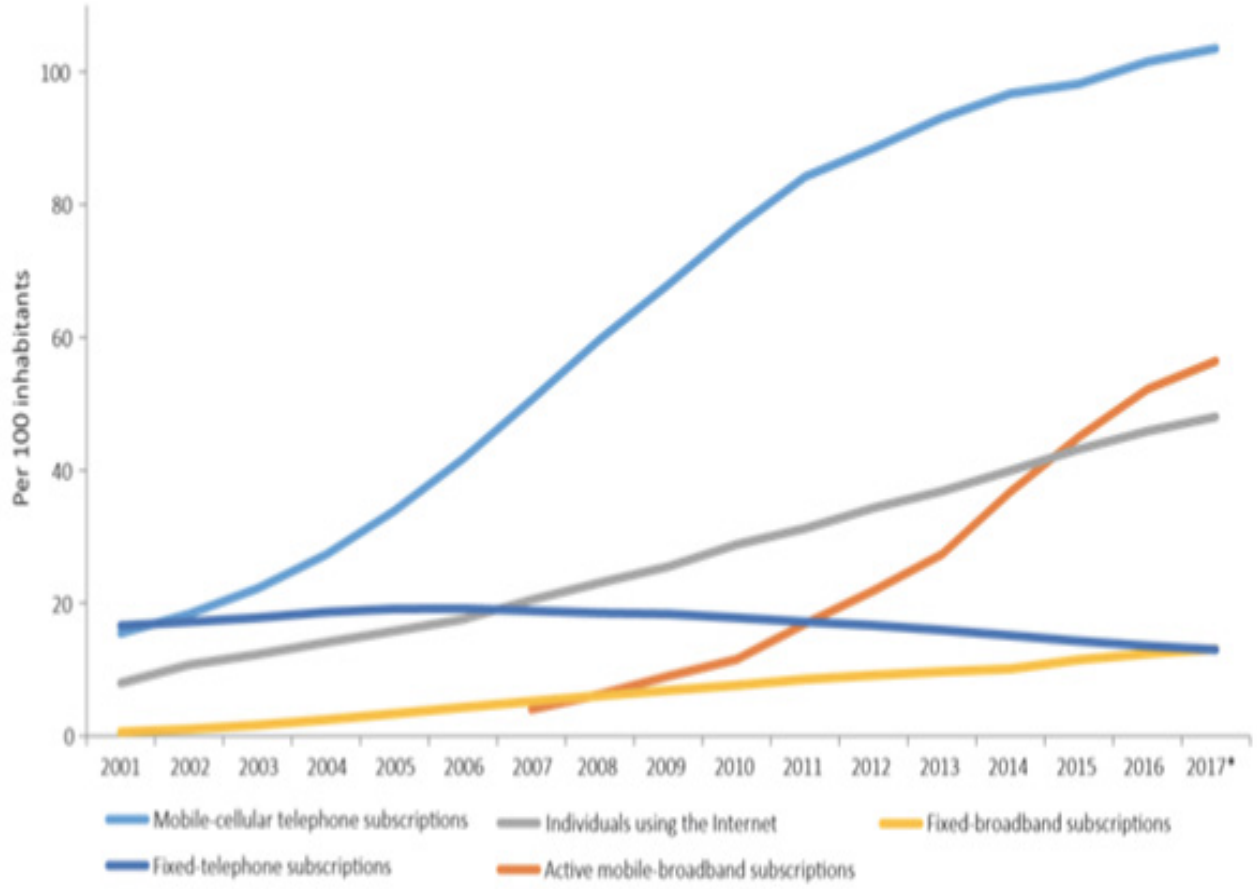
[7] CHILE. Política Nacional de Ciberseguridad. Chile, Gobierno de Chile, 2017. p. 16. [Fecha de consulta: 15 de julio de 2017].Disponible en http://www.ciberseguridad.gob.cl/media/2017/05/PNCS-ES-FEA.pdf

[8] "La UIT publica las cifras de 2016 de las TIC". Suiza, UIT, 2017. [Fecha de consulta: 10 de julio de 2017].Disponible en http://www.itu.int/es/mediacentre/Pages/2016-PR30.aspx

[9] BACHELET, Michelle. "Una política de Ciberseguridad para Chile". En: Política Nacional de Ciberseguridad. Chile, Gobierno de Chile, 2017. p. 5. [Fecha de consulta: 15 de julio de 2017].Disponible en http://www.ciberseguridad.gob.cl/media/2017/05/PNCS-ES-FEA.pdf

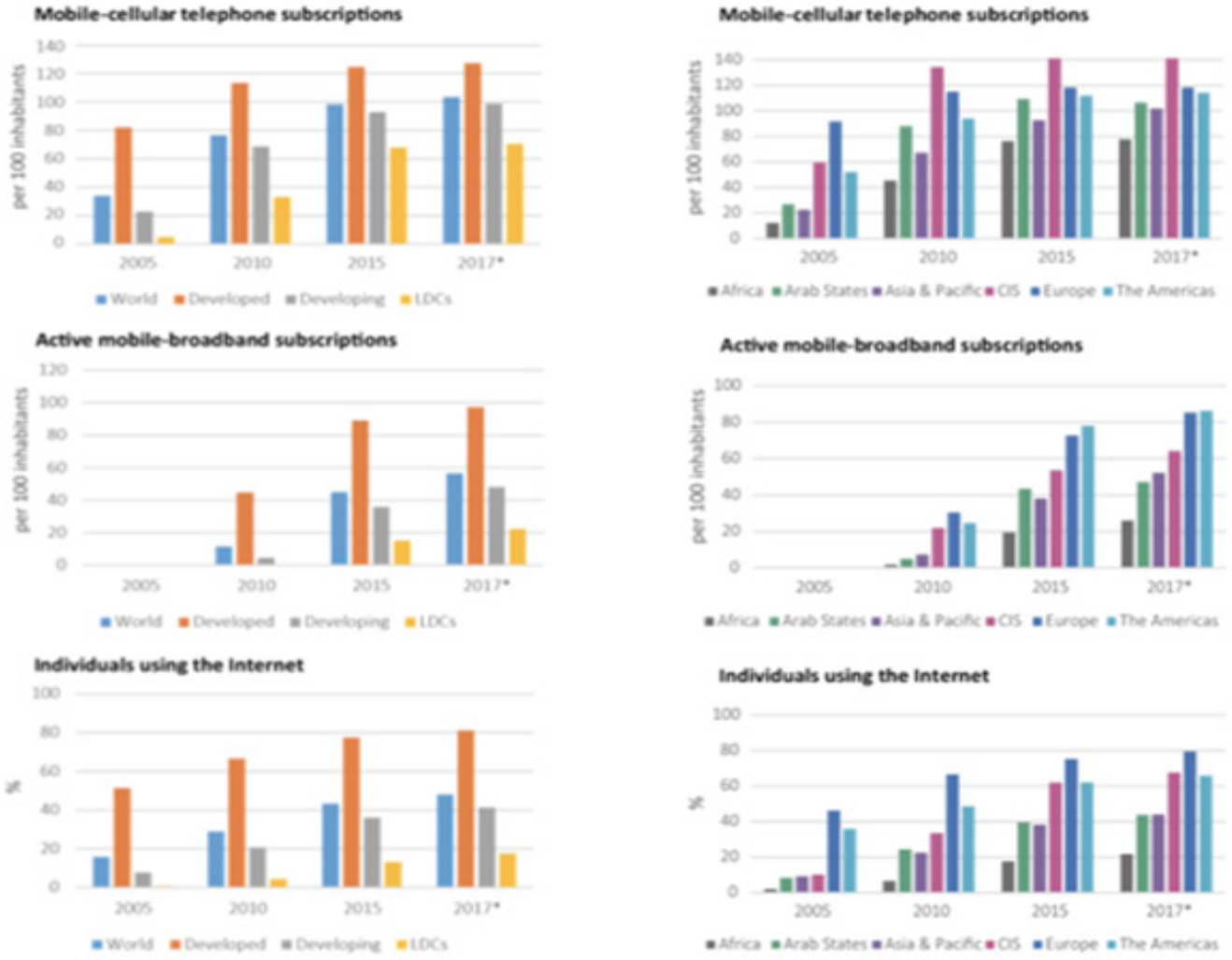
[10] ROBLEDO, Marcos. "Una política de Ciberseguridad para Chile". En: Política Nacional de Ciberseguridad. Chile, Gobierno de Chile, 2017. p. 9. [Fecha de consulta: 15 de julio de 2017].Disponible en http://www.ciberseguridad.gob.cl/media/2017/05/PNCS-ES-FEA.pdf

**Gráfico N°1: "Desarrollo Global de las TIC entre 2011-2017"**




Este crecimiento permanente en los diferentes tipos de mediciones con relación a las TIC, tal como se ilustra en la figura N°1, se relaciona con las ventajas que ofrece el uso del ciberespacio en términos de: facilidad de acceso para acceder a quien se desea contactar; rapidez en la transmisión de comunicaciones; y bajos costos asociados a la generación, almacenamiento y transmisión de información, en comparación con otras alternativas.

**Figura N°1: "Acceso u uso de las TIC según período, desarrollo del país y geográfico"**




De estamanera,losdiversosbeneficiosasociados a la utilización de ciberespacio, que van más allá de las personas que lo usan favoreciendo inclusive a la democracia, tal como se indica en un informe publicado por la UIT, el cual señala que

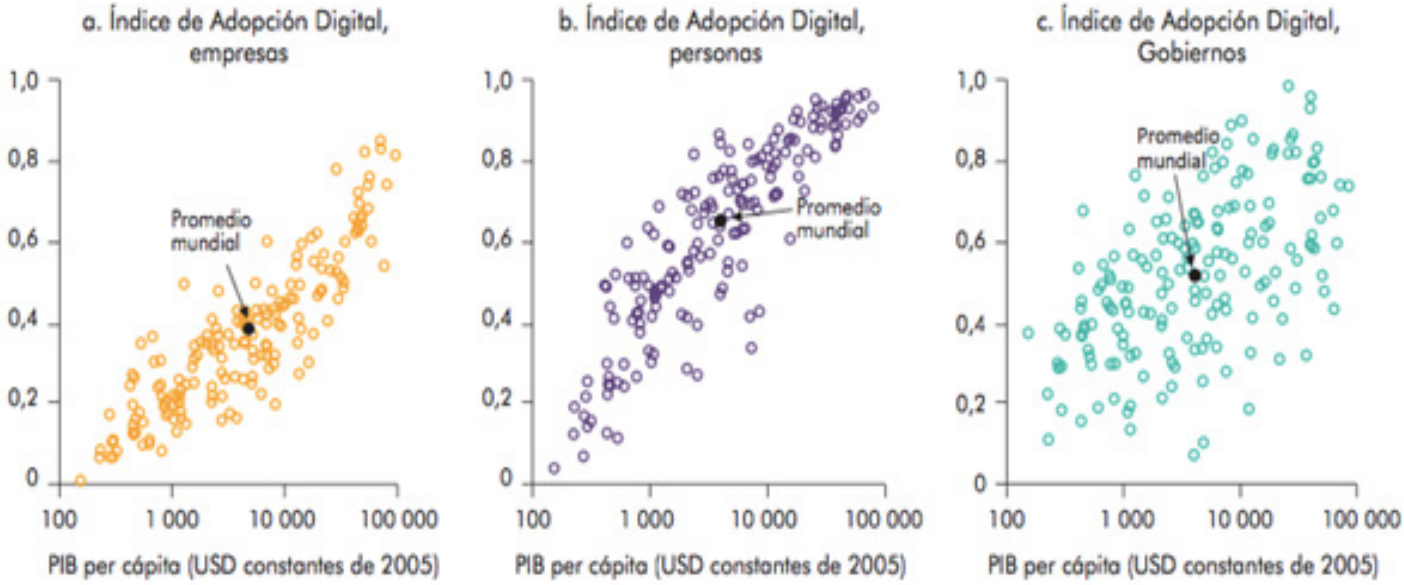
> "el acceso sin obstáculos a la información puede fomentar la democracia, pues el flujo de información queda fuera del control de las autoridades estatales (como ha ocurrido, por ejemplo, en Europa Oriental y África del Norte). Los adelantos técnicos han mejorado la vida diaria; la banca y la compra en línea, el uso de servicios móviles de datos y de transmisión vocal por el Protocolo Internet (VoIP) sólo son algunos ejemplos del grado de integración de las TIC en nuestra vida diaria"[11].

Muchas veces promoviendo cambios en organizaciones privadas e instituciones políticas[12]. Ello ha incentivado que empresas, personas y gobiernos incorporen en forma creciente esta herramienta para la comunicación y gestión de la información, tal como se indica en la figura N°2

[11] GERCKE, Marco. Informe "Comprensión del Ciberdelito: Fenómeno, Dificultades y Respuesta Jurídica". Suiza, UIT, 2014. p. 2. [Fecha de consulta: 10 de julio de 2017]. Disponible en www.itu.int/ITU-D/cyb/cybersecurity/legislation.html

[12] Al respecto ver NAÍM, Moisés. El fin del poder. España, Debate, 2013 y OBERMAIER, Frederick y OBERMAYER, Bastián. Panamá Papers. Colombia, Planeta, 2016.

**Figura N°2: "Extensión en uso de tecnologías digitales en el mundo".**




*Fuente:* Equipo a cargo del *Informe sobre el desarrollo mundial 2016*. Datos en http://bit.do/WDR2016-FigO_1.

*Nota:* En estos gráficos se representa la difusión de las tecnologías digitales en los países según el Índice de Adopción Digital (IAD), que fue compilado para el presente informe y se describe detalladamente en el capítulo 5 del informe completo. PIB = producto interno bruto.

La penetración de las TIC ha generado profundos cambios en la sociedad contemporánea[13], planteándose la existencia de una "Cuarta Revolución Industrial"[14] que se estaría desarrollando actualmente, la cual

> "no solo consiste en máquinas y sistemas inteligentes y conectados. Su alcance es más amplio. Al mismo tiempo, se producen oleadas de más avances en ámbitos que van desde la secuenciación genética hasta la nanotecnología, y de las energías renovables a la computación cuántica. Es la fusión de estas tecnologías y su interacción a través de los dominios físicos, digitales y biológicos lo que hace que la cuarta revolución industrial sea fundamentalmente diferente a las anteriores"[15].

En efecto, se trataría de cambios "tan profundos que, desde la perspectiva de la historia humana, nunca ha habido una época de mayor potencial o peligro"[16]. En esta perspectiva, tres motivos que permitirían argumentar la magnitud del cambio detectado, que justificaría darle la cualidad de revolucionario:

> "Velocidad: Al contrario que las anteriores revoluciones industriales, ésta está evolucionando a un ritmo exponencial, más que lineal. Este es el resultado del mundo polifacético y profundamente interconectado en que vivimos, y del hecho de que la nueva tecnología engendra, a su vez, tecnología más nueva y más poderosa"[17].
>
> "Amplitud y profundidad: Se basa en la revolución digital y combina múltiples tecnologías que están llevando a cambios de paradigma sin precedentes en la economía, los negocios, la sociedad y las personas. No sólo está cambiando el "qué" y el "cómo" hacer las cosas, sino el "quienes somos"[18].

[13] Al respecto ver VILLAMEDIANA, Miriam. "Los datos son el nuevo petróleo del siglo XXI". En: Euroexpress, publicado el 1 de julio de 2015. Disponible en http://www.euroxpress.es/noticias/los-datos-son-el-nuevo-petroleo-del-siglo-xxi

[14] SCHWAB, Klaus. La cuarta revolución industrial. Argentina, Debate, 2017.

[15] Ibíd. p. 21.

[16] Ibíd. p. 15.

[17] Ibíd.

[18] Ibíd.

> "Impacto de los sistemas: Se trata de la transformación de sistemas complejos entre (y dentro de) los países, las empresas, las industrias y la sociedad en su conjunto"[19].

En síntesis, el ciberespacio como concepto da cuenta de la existencia de un nuevo dominio, dimensión o ambiente que es usado en forma creciente por personas, organizaciones, empresas, gobiernos e instituciones las cuales se ven transformadas al incorporarlo en su gestión. Se constata coincidencias tanto en su conceptualización entre diferentes instituciones que lo han definido, como su incorporación incremental en las interacciones sociales ya sea con la finalidad de comunicarse como para gestionar información. Beneficios que serán sostenibles en el tiempo si el uso de este ambiente no presenta peligros que afecten la seguridad en el uso de los datos e información cibernéticos o virtuales. Junto a lo indicado, los cambios que está generando el uso de de las TIC ha llevado a plantear que estamos frente a la cuarta revolución que podría implicar un nuevo paradigma para la sociedad contemporánea.

En síntesis, el ciberespacio como concepto da cuenta de la existencia de un nuevo dominio, dimensión o ambiente que es usado en forma creciente por personas, organizaciones, empresas, gobiernos e instituciones las cuales se ven transformadas al incorporarlo en su gestión. Se constata coincidencias tanto en su conceptualización entre diferentes instituciones que lo han definido, como su incorporación incremental en las interacciones sociales ya sea con la finalidad de comunicarse como para gestionar información. Beneficios que serán sostenibles en el tiempo si el uso de este ambiente no presenta peligros que afecten la seguridad en el uso de los datos e información cibernéticos o virtuales. Junto a lo indicado, los cambios que está generando el uso de de las TIC ha llevado a plantear que estamos frente a la cuarta revolución que podría implicar un nuevo paradigma para la sociedad contemporánea.

1.2. Ciberseguridad: Condición necesaria más no suficiente en el ciberespacio.

Un creciente uso del ciberespacio y constante aumento en su cobertura, puede verse limitado por amenazas y vulnerabilidades. En efecto, los peligros que pueden impedir la adecuada utilización de este ambiente ha alertado respecto a las desventajas que presenta. De esta manera, adquiere relevancia la seguridad en el ciberespacio, constatándose coincidentes aproximaciones conceptuales a la noción en diferentes instancias multilaterales y nacionales. En efecto, la UIT plantea que la ciberseguridad es

**"Un creciente uso del ciberespacio y constante aumento en su cobertura, puede verse limitado por amenazas y vulnerabilidades."**

> "el conjunto de herramientas, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de gestión de riesgos, acciones, formación, prácticas idóneas, seguros y tecnologías que pueden utilizarse para proteger los activos de la organización y los usuarios en el ciberentorno. Los activos de la organización y los usuarios son los dispositivos informáticos conectados, los usuarios, los servicios/aplicaciones, los sistemas de comunicaciones, las comunicaciones multimedios, y la totalidad de la información transmitida y/o almacenada en el ciberentorno. La ciberseguridad garantiza que se alcancen y mantengan las propiedades de seguridad de los activos de la organización y los usuarios contra los riesgos de seguridad correspondientes en el ciberentorno. Las propiedades de seguridad incluyen una o más de las siguientes: disponibilidad; integridad, que puede incluir la autenticidad y el no repudio; confidencialidad"[20].

[19] Ibíd.

[20] UIT. Op cit. p. 3.

En el caso chileno, hay documentos oficiales que hacen referencia a este término en forma similar. Por ejemplo, en el texto "Bases para una Política Nacional de Ciberseguridad", es entendido "tanto una condición caracterizada por un mínimo de riesgos y amenazas a las infraestructuras tecnológicas, los componentes lógicos de la información y las interacciones que se verifican en el ciberespacio, como el conjunto de políticas y técnicas destinadas a lograr dicha condición"[21].

El Decreto 533, en su artículo séptimo, lo entiende de modo prácticamente igual señalando que "se entenderá por ciberseguridad aquella condición caracterizada por un mínimo de riesgos y amenazas a las infraestructuras tecnológicas, los componentes lógicos de la información y las interacciones que se verifican en el ciberespacio, como también el conjunto de políticas y técnicas destinadas a lograr dicha condición"[22]. Asimismo, en la PNCS se explica que la "ciberseguridad es una condición caracterizada por un mínimo de riesgos para el ciberespacio"[23]. De esta manera es posible constatar que, con mayor o menor extensión, la noción de ciberseguridad presenta un lineamiento consistente a nivel internacional y nacional, observándose en esta última coherencia entre las diferentes aproximaciones al término en documentos oficiales publicados durante los últimos años.

Sin embargo, coincidencias semánticas solo son una parte del tema. En este sentido, una aproximación compartida respecto a lo que es necesario proteger resulta clave en el marco de una política de ciberseguridad. Tal como se expresa en la definición de la UIT, se trata de proteger la información, específicamente su integridad, disponibilidad y confidencialidad. En el caso chileno, en la PNCS se explicita que "los atributos claves a proteger son la confidencialidad, integridad y disponibilidad de la información"[24], de acuerdo a estándares internacionales, lo que permitiría contar con un "ciberespacio robusto y resiliente"[25], existiendo coincidencia en la aproximación nacional e internacional del tema. La protección de estos atributos claves de la información digital implica contar con políticas, instituciones, recursos humanos expertos y tecnologías nuevas si el objetivo es ofrecer niveles mínimos de seguridad según estándares internacionales en el uso del ciberespacio. Ello implica una especialización en el tratamiento de estos elementos de política pública. La tabla N° 1 permite ilustrar la especificidad que contempla la aplicación de tecnologías en ciberseguridad en los diferentes ámbitos que ésta contempla.

[21] CHILE. Bases para una Política Nacional de Ciberseguridad. Loc. Cit.

[22] Decreto 533/2015, Ministerio del Interior y Seguridad Pública. CREA COMITÉ INTERMINISTERIAL SOBRE CIBERSEGURIDAD. Chile.

[23] CHILE. Política Nacional de Ciberseguridad. Chile. Loc. Cit.

[24] Ibíd.

[25] Ibíd.

**Tabla N°1: "Tecnologías de Ciberseguridad".**

| Técnicas | Categoría | Tecnología | Objetivo |
|---|---|---|---|
| Criptografía | Certificado y arquitectura de clave pública | Firma digital | Se utiliza para permitir la expedición y mantenimineto de certificadps que se utilizarán en las comunicaciones digitales. |
| | | Criptación | Criptación de los datos durante la transmición o el almacenamiento |
| | | Intercambio de claves | Determinar si se va a utilizar una clave de sesión o una clave de transacción para asegurar una conexión. |
| | Seguro | Criptación | Garantizar la autenticidad de los datos. |
| Control de acceso | Protección del perimetro | Cortafuegos | Controla el acceso desde y hacia una red. |
| | | Gestión de Contenido | Supervisa el tráfico de información no conforme. |
| | Autentificación | Factor unico | Un sistema que utiliza combinaciones de ID de usuario/contraseña para verificar el identificador. |
| | | Doble factor | Un sistema que requiere dos componentes para otorgar a un usuario acceso al sistema, como la posesión de un testigo físico además del conocimiento de un secreto. |
| | | Triple factor | Añade otro factor de identificación como características biométricas o la medición de una característica corporal. |
| | | Testigos inteligentes | Establece identificadores fiables de los usuarios mediante un circuitoespecífico de un diapositivo, como una tarjeta inteligente. |
| | Autorización | Por función | Mecanismos de autorización que controlan el acceso de los usuarios a los recursos del sistema adecuados, de acuerdo con su función asignada, |
| | | Por regla | Mecanismos de autorización que controlan el acceso de los usuarios a los recusos del sistema acedaudos, de acuerdo con reglas específicas asociadas a cada usuario, independientemente de su función dentro de la organización |
| Integridad del sistema | Antivirus | Métodos de firma | Protege contra los códigos informáticos maliciosos, como los virus, gusanos y caballos de Troya Antivirus utilizando sus firmas de código. |
| | | Métodos de comportamiento | Verifica que los programas que se ejecuten no tengan un comportamiento no autorizado |
| | Integridad | Detección de intrusión | Puede utilizarse para advertir a los administradores de red de la posibilidad de que ocurra un incediente de seguridad, como la puesta en peligro de archivos en un servidor |

Fuente: UIT, 2008.

En efecto, los atributos de la información pueden verse afectados por

> "… amenazas a los sistemas de comunicaciones de datos incluyen las siguientes: a) destrucción de información y/u otros recursos; b) corrupción o modificación de información; c) robo, eliminación o pérdida de información y/u otros recursos; d) divulgación de información confidencial; e e) interrupción de servicios"[26],

lo cual puede generar importantes daños a las personas, organizaciones, instituciones y países. En efecto, a partir de incidentes en el ciberespacio se han hecho algunas estimaciones de los costos involucrados, de esta manera, un informe publicado en 2014 por la UIT indica que

> "en 2003, los software dañinos causaron pérdidas de hasta 17.000 millones USD. De conformidad con algunas estimaciones, en 2007 los ingresos del ciberdelito superaron los 100.000 millones de USD, rebasando así a los correspondientes al comercio ilegal de drogas por primera vez. Teniendo en cuenta un estudio publicado en 2014, las pérdidas anuales causadas por el ciberdelito en el mundo entero podrían ascender a 400.000 millones USD. Casi el 60% de las empresas de los Estados Unidos estiman que el ciberdelito les resulta más costoso que el delito físico"[27].

Complementa lo indicado, un informe publicado por el BID y la OEA en 2016, el cual indica que

> "el cibercrimen le cuesta al mundo hasta US$575.000 millones al año, lo que representa 0,5% del PIB global. Eso es casi cuatro veces más que el monto anual de las donaciones para el desarrollo internacional. En América Latina y el Caribe, este tipo de delitos nos cuestan alrededor de US$90.000 millones al año"[28].

Para una mejor comprensión de la diversidad de amenazas en el ciberespacio, se presenta en la tabla N° 2 una relación entre amenaza y modo en que puede manifestarse.

**Tabla N°2: "Amenazas en el ciberespacio y modo en que pueden manifestarse".**

| Modelo de amenazas de la X.800 | Método de ataque |
|---|---|
| Destrucción de la información y/o otros recursos | Intrusión de AP |
| Corrupción o modificación de la información | Pirateo de la clave, intromisión. |
| Hurto, supresión o pérdida de la información y/o recursos | Intrusión de AP, pirateo de la clave WEP, intromisión, falsificación de la dirección MAC, diapositivos maliciosos, el "war driving", apropiación de la capa 3, redes con fines específicos. |
| Revelación de la información | Intrusión de AP, pirateo de la clave WEP, intromisión, falsificación de la dirección MAC, diapositivos maliciosos, el "war driving", apropiación de la capa 3, redes con fines específicos. |
| Interrupción del servicio | Interderencia radioeléctrica, inundación de datos, apropiación de la capa 2, AP falso, trama de desautentificación falsificada, denegación del servicio FATA-Jack. |

Fuente: UIT, 2008.

Con mayor precisión que permite destacar la variedad de malware desarrollados recientemente, el Reporte de Seguridad Cibernética e Infraestructura Crítica de las Américas identifica los principales malware detectados en 2014, tal como se indica a continuación en la tabla N°3, pudiendo constatarse una proliferación de este tipo de software[29].

[26] UIT. Op cit. p. 9.

[27] GERCKE, Op cit. p.2.

[28] Ciberseguridad ¿Estamos preparados en América Latina y el Caribe?. EE.UU, OEA / BID, 2016.

[29] Seguridad Cibernética e Infraestructura Crítica en las Américas. EE.UU, OEA / Trend Micro, 2015.

**Tabla N°3: "Las principales familias de malware 2014".**

| FAMILIA DE MALWARE | DESCRIPCIÓN |
|---|---|
| **KEYGEN** | Genera números de serie para entrar a los programas que requieren números de serie válidos para que los programas funcionen completamente. |
| **DUNIHI** | Esta familia de malware normamente es malware VBS ofuscado que es capaz de propagarse infectando unidades. |
| **ACTIVATOR** | Quiebra la aplicación y el usuario puede instalarla manualmente. Sus rutinas le permiten a los usuarios evadir las técnicas de registro y protección de las aplicaciones. Esto permite utilizar la versión registrada de las aplicaciones. |
| **DOWNAD/Conficker** | Esta explota una vulnerabilidad del servicio que, cuando es explotada, permite que un usuario remoto ejecute el código arbitrario en el sistema infectado para propagarse en las redes. |
| **CONDUIT** | Se incluye en los paquetes de malware como un componente de malware, como un archivo entregado por otro malware, o como un archivo que los usuarios descargan sin darse cuenta cuando visitan sitios maliciosos. |
| **PRODUKEY** | Una aplicación que muestra la identificación del producto y la clave del CD de ciertos software si se instala en el sistema afectado. |
| **SAFNUT** | Se incluye en los paquetes de malware como un componente de malware. Llega al sistema un archivo entregado por otro malware o como un archivo que los usuarios descargan sin darse cuenta cuando visitan sitios maliciosos. |
| **AGENT** | Normalmente trae consigo cargas o realiza otras acciones maliciosas, que van desde moderadamente molestas hasta las irreparablemente destructivas. También pueden modificar las configuraciones del sistema para que se inicie automaticamente. Para restaurar los sistemas aferctados. |
| **CROSSRDR** | Se incluye en los paquetes de malware como un componente de malware. Llega al sistema como un archivo entregado por otro malware o como un archivo que los usuarios descargan sin darse cuenta cuando visitan sitios maliciosos. |
| **FAKEAV** | Crea carpetas en los sistemas afectados y entrega varios archivos, incluyendo una copia de sí mismos y un archivo malicioso. Realiza varios cambios al registro, uno de los cuales permite que se ejecute cada vez que el sistema arranca. |

Fuente: OEA y Trend Micro 2015

En el caso chileno, se observa que no hay una situación diferente, en términos de estar expuestos a ataque maliciosos. La Tabla N° 4 presenta las actividades maliciosas detectadas en la red de conectividad del Estado, según la PNCS.

**Tabla N°4: "Actividades maliciosas detectadas en al red de conectividad del Estado en Chile".**

| Cantidad de registros | Descripción |
|---|---|
| 58.375.435 | Intentos de acceder a información de diapositivosde red mediante protocolo de administración SNMP. |
| 45.903.511 | Escaneo de puertos de administración de diapositicos de la plataforma switch, router o seguridad. |
| 19.745.086 | Flujo web con traspaso de contraseña en texto claro (sin cifrar) |
| 7.805.544 | Detección de actualización dinámicas de DNS. |
| 5.570.661 | Detección de flijo TFTP (transferencia de archivos) usando protocolos tftp. |
| 4.463.394 | Detección de flujos portmap. |
| 3.359.194 | Detección de tráfico anómalo por el puerto DNS. |
| 2.479.277 | Detección de flujo de escritorio remoto. |
| 2.077.435 | Detección de consultas de DNS por dominios reconocidos como de uso de malware. |
| 2.023.403 | Detección de reconocimiento por PING. |
| 1.451.708 | Escaneo de puertos de administración de diapositicos de la plataforma switch, router o seguridad. |
| 1.428.461 | Detección de acceso a wordpress (componentes claves) |
| 1.400.697 | Detección de malware MORTO. |
| 1.120.311 | Detección de tráfico NO cifrado a tráves de puerto tradicionalmente utilizado para transmitir cifradamente (443) |
| 1.106.303 | Detección de accesos a zonas prohibidas de sitios web. |
| 1.025.252 | Flujo de credenciales en texto claro de login wordpress (utilizando sitios web de gobierno) |

Fuente: PNCS, 2017.

En síntesis, la seguridad como condición para alcanzar un objetivo, se relaciona con la existencia de riesgos proveniente de amenazas o vulnerabilidades que pueden colocar en peligro bienes considerados importantes como: la vida de personas y/o su patrimonio, la estabilidad institucional, la soberanía nacional y/o los objetivos e intereses nacionales. En una perspectiva del ciberespacio se reconoce la existencia de peligros que pueden afectarlos, cuyas manifestaciones causan importantes daños a personas, organizaciones y países. El caso chileno no es excepción en este tema.

## 2.Ciberinteligencia: Aproximación conceptual y características.

La existencia de peligros en el ciberespacio que pueden afectar la seguridad, estabilidad e inclusive el desarrollo de los países y sus habitantes, requiere de una capacidad que permita anticipar

> "las amenazas, las vulnerabilidades (incluida la evaluación del impacto), las medidas para contrarrestarlas y los mecanismos de seguridad", con el fin de:
>
> a)Identificar las vulnerabilidades del sistema;
>
> b)Analizar la probabilidad de amenazas cuyo objetivo sea explotar estas vulnerabilidades;
>
> c)evaluar las consecuencias de cada amenaza, en caso de que se llevase a cabo con éxito;
>
> d)Estimar el coste de cada ataque;
>
> e)Determinar el coste de las posibles medidas de respuesta; y
>
> f)Seleccionar los mecanismos de seguridad que se justifican (posiblemente recurriendo al análisis de rentabilidad)"[30].

En este contexto, la inteligencia en el ciberespacio tiene un rol irremplazable toda vez que puede aportar información clave en la identificación de actores, intencionalidades y objetivos e inclusive, en algunas ocasiones, anticipar la ocurrencia de ataques o problemas de funcionamiento que afecten los intereses nacionales del país o pongan en riesgo la vida de sus habitantes, por ejemplo, en el caso de un ataque a la infraestructura crítica de la nación.

Además, en caso de ocurrir un incidente de seguridad en el ciberespacio, puede apoyar en la identificación de su origen –o lo más cercano a ello-, interpretar las implicancias de la acción y proponer diversos escenarios de respuesta como de contingencia frente a una crisis en este ambiente. De esta manera, puede reconocerse una nueva dimensión de la seguridad que requiere ser protegida siendo la función inteligencia, aplicada al ciberespacio, una herramienta clave para el cumplimiento de esta tarea.

**"... la inteligencia en el ciberespacio tiene un rol irremplazable toda vez que puede aportar información clave en la identificación de actores, intencionalidades y objetivos e inclusive, en algunas ocasiones, anticipar la ocurrencia de ataques o problemas de funcionamiento que afecten los intereses nacionales del país o pongan en riesgo la vida de sus habitantes,..."**

En este sentido, emerge la noción de ciberinteligencia, la cual "surge dentro del ciberespacio"[31], pudiendo ser entendida en sentido amplio o restringido. El primero se refiere a la noción como origen de amenazas y vulnerabilidades a la seguridad de datos e información virtual que frecuentemente está contenida en el ciberespacio. La segunda como fuente específica de información que puede alertar sobre peligros a la seguridad en cualquier dominio o ambiente en el cual se producen relaciones e interacciones sociales que, tal como se indicó anteriormente, pueden corresponder a: tierra, mar, aire, espacio y ciberespacio.

En una perspectiva amplia del concepto, según Gruszczak se trata de "un conjunto de actividades que apuntan a obtener conocimiento previo de amenazas y vulnerabilidades a los sistemas de comunicación de información a través de una variedad de medios técnicos"[32], debido a que "al igual que cualquier dominio público, el ciberespacio es vulnerable a amenazas, ataques y acciones maliciosas de diferentes actores que tienen varias motivaciones, intenciones, objetivos y herramientas"[33].

[30] UIT. Op cit. p. 10.

[31] GRUSZCZAK, Artur. New Security Challenges. Polonia, Palgrave Macmillian, 2016. p. 75

[32] BRANTLY, A. Defining the role of intelligence in cyber. A hybrid push and pull. In M. Phythian (Ed.), Understanding the intleligence cycle. London/NewYork: Routledge, 2013, citado en Gruszczak, Artur. Loc cit.

[33] GRUSZCZAK, Artur. Op cit. p. 81.

En efecto, tal como el mismo autor explica

> "la interconectividad de los usuarios, o la arquitectura de los "sistemas de sistemas", crea problemas de seguridad que deben ser abordados por instituciones y servicios profesionales con conocimiento para prevenir daños, proteger fuentes de información y bases de datos, y salvaguardar elementos críticos de la infraestructura pública. El espionaje cibernético, las intrusiones y los ataques a los bancos de datos se han convertido en características cotidianas de las redes de comunicación globales"[34].

En sentido amplio, la noción de ciberinteligencia describe los elementos que contempla este concepto, como también, la finalidad de sus actividades, el contexto bajo el cual opera y el reconocimiento de la existencia de diversas acciones a efectuar en el ciberespacio para lograr sus objetivos.

En sentido estricto, correspondería un medio específico de obtención de información al que se puede acceder para obtener datos e información necesaria para los fines de la inteligencia, siendo su sigla en inglés CYBERINT[35], correspondiendo en español a CIBERINT. En efecto, bajo la premisa que el ciberespacio es una fuente que contiene diversos tipos de datos e información, se puede acceder a la información abierta, mixta o cerrada[36] que éste contiene en gran cantidad. Tal como indica un informe de la Agencia Nacional de Inteligencia Geoespacial (NGA, por su sigla en inglés), se trata de lo que puede denominarse un "tsunami de datos" y los explica de la siguiente manera

> "a fines de esta década habrá entre 50 mil y 200 mil millones de dispositivos ligados a la red sobre un planeta de 8 mil millones de personas. "Para la comunidad de inteligencia, esto equivale a 40 zettabytes de información, o 1 millón de quintillones de bytes", declara NGA. "Con una descripción en términos más familiares, equivales a que cada persona del planeta se le entreguen 174 periódicos cada día. Visto de otro modo, es más información que la que podrían almacenar 7 mil millones de bibliotecas del Congreso"[37],

esta situación ha planteado inclusive la existencia de un exceso de información que puede causar "infoxicación" si ésta no es seleccionada adecuadamente y procesada en forma oportuna.

Otra aproximación al término es planteada por Enrique Cubeiro[38] quien, al hacer referencia al ciberespacio, contempla la ciberinteligencia particularmente en sentido restringido, cuando entiende el ciberespacio como "la mayor fuente de obtención [de datos] entre las denominadas abiertas"[39], ofreciendo posibilidades de explotación útiles para las necesidades de inteligencia a bajo costo en comparación con otros medios y fuentes, cuando es posible elegir entre alternativas disponibles. En efecto, como expresa el autor

> "las redes sociales representan una fuente fundamental de obtención, tanto por la relativa facilidad con la que es posible explotar sus vulnerabilidades, como por la información que es publicada en ellas por sus usuarios (datos personales, filiaciones, posturas políticas e, incluso información sensible)"[40].

Sin embargo, sería en el ámbito defensivo donde

> "la ciberinteligencia contribuye de forma determinante a la alerta temprana y al conocimiento de la situación, mientras que en el ofensivo constituye una pieza clave para conocer la arquitectura de

[34] Ibíd.

[35] GRUSZCZAK, Artur. Ibíd. p. 82

[36] ESTEBAN Navarro, Miguel. Necesidad, funcionamiento y misión de un servicio de inteligencia para la seguridad y defensa. Cuadernos de Estrategia (127). España, 2004.

[37] BAMFORD, James. Every move you make. En Foreign Policiy edición argentina, Archivos del Presente. Nº 65, año 2017. Argentina. p. 100.

[38] CUBEIRO, Enrique. "Ciberinteligencia". En: Díaz, Antonio (ed). Conceptos Fundamentales de Inteligencia. España, Tirant lo Blanch, 2016. p. 50.

[39] Ibíd.

[40] Ibíd.

> redes y sistemas del enemigo, así como para la obtención de información sensible que puede ser explotada en beneficio propio. Esto se sustenta en que, por lo general, aunque las redes y sistemas militares tienen elevado grado de aislamiento, éste rara vez es absoluto; y, por otra, en que la "ciber-dependencia" está incrementando de forma exponencial las superficies y vectores de ataque"[41].

Desde la perspectiva de Cubeiro, el ciclo de inteligencia

> "en el ámbito cibernético se apoya en herramientas que posibilitan la obtención de datos conforme a complejos parámetros de búsqueda en ámbitos que abarcan no sólo fuentes abiertas o redes sociales, sino incluso la denominada "web profunda" y que cuenta con funcionalidades para apoyar a los analistas en las siguientes fases del ciclo, especialmente en el procesamiento y el análisis. Entre las funcionalidades típicas se incluyen la traducción, la geolocalización o la representación gráfica de las relaciones entre identidades digitales"[42].

El modo en que el autor explica la ciberinteligencia, se complementa con Gruszczak, reforzando su conceptualización en sentido restringido, toda vez que adiciona a la descripción de los elementos claves de la función y la naturaleza de la actividad, la idea de ciberinteligencia asociada a búsqueda de información en el ciberespacio tanto en fuentes abiertas como cerradas y cómo ello puede visualizarse en el ciclo de inteligencia. Asimismo, ambas definiciones comparten el contexto en el cual se desarrolla el término y coinciden en el sentido profundo de la noción.

Una integración de ambas aproximaciones –en sentido amplio y restringido- permitiría entender la ciberinteligencia como el resultado de un ambiente en el cual se producen interacciones sociales -el ciberespacio-, el cual es usado por las personas, organizaciones e instituciones para la generación, almacenamiento y transmisión de información, donde ante la necesidad de ofrecer ciberseguridad y anticipar los peligros que pueden afectarla es necesario contar con una capacidad capacidad de ciberinteligencia.

**"En una perspectiva de inteligencia estratégica, la ciberinteligencia requiere identificar actores, medios y objetivos que pueden afectar la seguridad o bienestar del país y/o sus habitantes. "**

En sentido amplio, la ciberinteligencia se trata del desarrollo de cada una de sus actividades propias de la función inteligencia[43] (búsqueda de datos, análisis de información, contrainteligencia y operaciones especiales) son efectuadas en el ciberespacio como dominio específico, con la finalidad de anticipar peligros que pueden afectar su funcionamiento o desde este ambiente poner riesgo la vida de personas, su patrimonio, la estabilidad institucional, integridad territorial y/o la soberanía nacional. En sentido estricto, puede entenderse como una fuente específica para acceder a información necesaria a los objetivos de un servicio de inteligencia, pudiendo tratarse de datos o información que se encuentra en formato abierto, cerrado o mixto, se reconoce por su sigla CIBERINT en español.

La ciberinteligencia, como dimensión específica desde donde se puede extraer información (sentido restringido) o como ambiente desde el cual pueden originarse peligros que afecten no solo la ciberseguridad sino también la vida o patrimonio de personas, la seguridad pública e inclusive del país (sentido amplio), puede desarrollarse en los diferentes niveles de la conducción (táctico, operacional y estratégico) y corresponde a una dimensión más que se adiciona a otras en la apreciación global del conductor o agente direccional.

[41] Ibíd.

[42] Ibíd

[43] FLACSO. Reporte del sector seguridad en América Latina y el Caribe. Chile, FLACSO, 2007.

En una perspectiva de inteligencia estratégica, la ciberinteligencia requiere identificar actores, medios y objetivos que pueden afectar la seguridad o bienestar del país y/o sus habitantes. Ello se complementa con información proveniente de otros dominios del conocimiento para una apreciación completa del escenario a enfrentar. La tabla N° 5 ilustra los diversos tipos

**Tabla N°5: "Resumen de Estado de riesgo del Ciberespacio"**

| AUTORÍA | OBJETIVOS | | |
|---|---|---|---|
| | Gobierno | Sector Privado | Ciudadanos |
| Ataques patrocinados por otros Estados | Espionaje, ataques contra infraestructura crítica, APT. | Espionaje, ataques contra infraestructuras crítivas, APT | |
| Ataques patrocinados por privados | Espionaje | Espionaje | |
| Terroristas, extremismo político e ideologico | Ataques contra redes y sistemas; contra servicios de internet; infección con *malware;* contra redes, sistemas o servicios de terceros | Ataques contra redes y sistemas; contra servicios de internet; infección con *malware;* contra redes, sistemas o servicios de terceros | |
| Hacktivistas | Robo y publicación de información clasificada o sensible, ataque contra las redes y sistemas, ataques contra servicios de Internet, infección con malware, ataques contra redes, sistemas o servicios de terceros | Robo y publicación de información clasificada o sensible, ataque contra las redes y sistemas, ataques contra servicios de Internet, infección con malware, ataques contra redes, sistemas o servicios de terceros | Robo y publicación de datos personales |
| Crimen Organizado | Espionaje | Robo de indentidad digital y fraude | Robo de identidad digital y fraude. |
| Ataques de bajo perfil | Ataques contra las redes y sistemas, ataques contra servicios de internet, infección con malware, ataques contra redes, sistemas o servicios de terceros | Ataques contra las redes y sistemas, ataques contra servicios de internet, infección con malware, ataques contra redes, sistemas o servicios de terceros | |
| Ataques de personal con accesos privelegiados (*insiders*) | Espionaje, ataques contra infraestructuras críticas, ataques contra las redes y sistemas, ataques contra servicios de terceros, robo y publicación de información clasificada o sensible, APT. | Espionaje, ataques contra infraestructuras críticas, ataques contra las redes y sistemas, ataques contra servicios de terceros, robo y publicación de información clasificada o sensible, APT. | |
| | Impacto | **Alto** | |
| | | **Medio** | |
| | | **Bajo** | |

Fuente: Instituto de Ciberseguridad de España, 2012.

de riesgos a la seguridad en el ciberespacio que la ciberinteligencia requiere monitorear y anticipar.

El desarrollo de ciberinteligencia implica el reconocimiento de la naturaleza y características del ciberespacio. En este sentido, en el caso de la inteligencia como proceso, el ciclo de inteligencia[44] considera las particularidades que presenta el ciberespacio, por ejemplo, en materia de acceso a la información. En efecto, la anticipación a los peligros identificados requiere en la etapa de la búsqueda de información, el desarrollo de un ciclo de inteligencia que contemple tanto la explotación de la información existente en el ciberespacio en fuentes abiertas (por ejemplo, redes sociales), mixtas (por ejemplo, bases de datos a la que es posible acceder con clave) y cerradas (por ejemplo, la "*Deep web*"[45] o "web profunda", también conocido como "dark web" o "el lado oscuro de internet").

Asimismo, en la etapa del procesamiento de la información, es necesario contar con bases de datos que sean interoperables y capaces de almacenar y sistematizar gran cantidad de información. En este sentido, una de las importantes tendencias en este ambiente es el "*big data*" entendido como

> "conjuntos de datos cuyo volumen, variedad y velocidad superan los correspondientes a los conjuntos de datos habituales. Su aparición denota adelantos tecnológicos que permiten captar, almacenar y procesar cantidades de datos cada vez mayores de diferentes fuentes de datos. De hecho, una de las tendencias primordiales que fomenta el surgimiento de "*big data*" es la "conversión en datos" y la digitalización masivas, también de actividad humana, en "árboles" o "huellas" digitales. En un mundo cada vez más digitalizado, los "*big data*" se generan de forma digital a partir de diversas fuentes, entre ellas registros administrativos (por ejemplo antecedentes bancarios o historiales clínicos electrónicos), transacciones comerciales entre dos entidades (como, por ejemplo, compras en línea o transacciones con tarjeta de crédito), sensores y dispositivos de localización (por ejemplo teléfonos móviles o dispositivos GPS) y actividades de los usuarios en Internet (entre ellas búsquedas y contenidos de los medios sociales)"[46].

Sus principales características son[47]: velocidad, debido a la rapidez con la que se generan y analizan los datos; variedad, contienen diferentes tipos y formas de datos, incluidos grandes volúmenes de datos no estructurados; valor, debido al desarrollo socioeconómico potencial de los "*big data*"; veracidad, dada por el nivel de calidad, exactitud e incertidumbre de los datos y las fuentes de datos y; volumen, pues son cantidades ingentes de datos generados a través de la "conversión en datos". De esta manera, las cualidades de los "*big data*" encierran posibilidades de mejorar la precisión e integridad de las estadísticas oficiales, constituyendo un aporte útil para el analista de inteligencia y la producción de ésta facilitando, de este modo, una serie de acciones que antiguamente requerían más tiempo y dinero.

En la etapa de análisis para la producción de inteligencia se requiere no solo que el analista sea experto en los temas bajo su responsabilidad, también es necesario que conozca las TIC a su disposición en el ciberespacio, para que realice búsquedas específicas en línea e identifique fuentes confiables de información, como también, sea versátil para usar diversas plataformas de información donde puede estar contenida lo que requiere.

La tabla N° 6 ilustra un modo de clasificar tanto la fuente desde donde se obtuvo la información como la calidad de ella, lo cual requiere especial importancia y dedicación, toda vez que se detecta

[44] Etapas del ciclo según Lowenthal, Mark. Intelligence. 3º ed. Estados Unidos, CQ Press, 2006.

[45] Al respecto ver CIANCAGLINI, V. , BALDUZZI, M. , MCARDLE, R. and RÖSLER M. Below the Surface: Exploring the Deep Web. TrendLabs Research Paper. S/L, Trend Micro, 2015.

[46] UIT. "Medición de la Sociedad de la Información 2014". Resumen Ejecutivo. Suiza, UIT, 2014. p. 39.

[47] Ibíd.

cómo en el ciberespacio proliferan las "*fake news*" o noticias falsas que buscan confundir a personas, analistas en temas estratégicos y/o con influencia en la opinión pública, e inclusive promover la desestabilización de instituciones o gobiernos con información que no tiene fundamentos en los hechos sino en deseos basados en intereses foráneos. En este sentido, adquiere relevancia la capacidad para detectar información que no tiene sustento empírico y,

**Tabla N°6: "Modelo de evaluación de fuente de información en inteligencia"**

| **Valoración de la fuente** | |
|---|---|
| **A** | Fuente bien conocida y que lleva tiempo porporcinando información valida |
| **B** | Fuente bien conocida y con larga trayectoria pero que a veces ha proporcionado información que con el tiempo ha demostrado ser erroenea. |
| **C** | La fuente parece fiable pero lelva poco tiempo informando. |
| **D** | Fuente dudosa que lleva tiempo proporcionando informaciones de escasa fiabilidad y a la que pueden afectar intereses o sesgos ideológicos que - consciente o inconscientemente. le llevan a alterar la percecpción de la realidad. |
| **E** | Fuente desconocida, sobre la que no existe experiencia previa. |

| **Valoración de la información** | |
|---|---|
| **1** | Información creible, que coincide tendencias o hechos previos bien constatados |
| **2** | Información que se corresponde de manera general con tendencias constatadas o con hechos previos. Sin embargo, existen ciertas discordancias que conviene investigar. |
| **3** | La información que contradice tendencias y hechos previos bien conocidos sin una explicación clara. La información puede ser incorrecta o puede ser necesario investigar para descubrir la causa de la discordancia. |
| **4** | Información inconsistente que choca con tendencias y hechos conocidos. Es altamente dudosa o simplemente incorrecta |
| **5** | Información que puede ser creible, pero no hay modo de compararla con informaciones previas. |

Fuente: Jordán, 2016 basado en Quiggin, 2007.

de este modo, alertar cuando se están tomando decisiones públicas o privadas que afecten a la ciudadanía con base a estas noticias falsas.

Los servicios de inteligencia tienen capacidad para confirmar información disponible en medios, particularmente en Internet en tiempos de "postverdad"[48], donde es detectada una tendencia a que medios de comunicación, especialmente digitales, sean inundados con información que tratan de dar soporte a deseos basados en sentimientos afectivos de personas más que basarse en hechos objetivos, con la finalidad de influir erróneamente en el proceso decisional de una persona en su rol de ciudadano, consumidor o elector. Esta práctica podría ser

[48] Al respecto ver: «The post-truth world: Yes, I'd lie to you». En: The Economist, 10 de septiembre de 2016. U.K. y ROBERTS, David. «Post-Truth Politics». Grist. 1 de abril de 2010. [Fecha de consulta: 10 de Octubre 2017]. Disponible en http://grist.org/article/2010-03-30-post-truth-politics/

[49] Por ejemplo, al respecto ver "Noticias falsas acerca de Chile fueron vistas o compartidas 3,5 millones de veces en redes sociales en 2017". En: El Mostrador, publicado el 26 de noviembre de 2017. [Fecha de consulta: 26 de noviembre de 2017]. Disponible en http://www.elmostrador.cl/noticias/pais/2017/11/26/noticias-falsas-acerca-de-chile-fueron-vistas-o-compartidas-35-millones-de-veces-en-redes-sociales-en-2017/

usada por individuos u organizaciones con fines personales o políticos y algunos países lo han considerado como un peligro ante el cual es necesario estar alerta[49]. En el primer caso se encuentra lo denominado "incendios digitales"[50], donde información falsa ha causado un serio trastorno en el normal desarrollo de las actividades de las personas, afectando la confianza de los ciudadanos en los medios de comunicación. Ejemplo de ello pudo observarse cuando las autoridades de EE.UU., los medios de comunicación, el mercado bursátil y la opinión pública mundial durante algunos minutos fueron sorprendidos con la noticia publicada en el twitter de la agencia Associated Press (AP) que indicaba: "Dos explosiones en la Casa Blanca y el Presidente Obama herido" (Figura N° 3), la cual correspondió a difusión de información falsa resultado de un hackeo a la cuenta de twitter de la agencia Associated Press (AP). No obstante,

**Figura N°3: "Cuenta AP intervenida"**


**Figura N°4: "Impacto en DOW Jones"**


Fuente: Linera, 2013.

hubo consecuencias inmediatas, como por ejemplo la baja en las acciones, según lo reflejó ese día el índice del DOW Jones (Figura N° 4).

El segundo caso puede presentarse ante procesos electorales, condicionando el resultado electoral a la cantidad de información falsa que tuvieron acceso los votantes. Ello plantea un desafío importante a servicios de inteligencia que posiblemente deban contar con una capacidad de monitoreo de información falsa que busca confundir a las personas en materias de interés público. Aunque este asunto no esté asociado a sus objetivos principales, esta medida se entendería pues son las organizaciones con mayor capacidad para rastrear información proveniente desde variadas fuentes y diversos medios, con la finalidad de confirmar o descartar noticias que pueden ser falsas y buscan confundir en procesos decisionales de interés público. Por ejemplo, ante este problema la Unión Europea (UE), para enfrentar ciberataques y propaganda en la Red ha creado un "Centro de Excelencia Europeo para la lucha contra las amenazas híbridas (Hybrid CoE, por sus siglas en inglés)"[51].

En efecto, los servicios de inteligencia han destacado como organización especializada para obtener información y valorarla según su calidad y a partir de ello hacer apreciaciones

[50] Al respecto ver World Economic Forum (2013). Global Risks, 2013. Ginebra. Disponible en http://www3.weforum.org/docs/WEF_GlobalRisks_Report_2013.pdf

[51] SOTO, Adrián. "La OTAN y la UE abren un centro contra las amenazas híbridas". En: El País de España, publicado el 2 de octubre de 2017. [Fecha de consulta: 10 de octubre de 2017]. Disponible en https://elpais.com/internacional/2017/10/02/actualidad/1506969497_610407.html

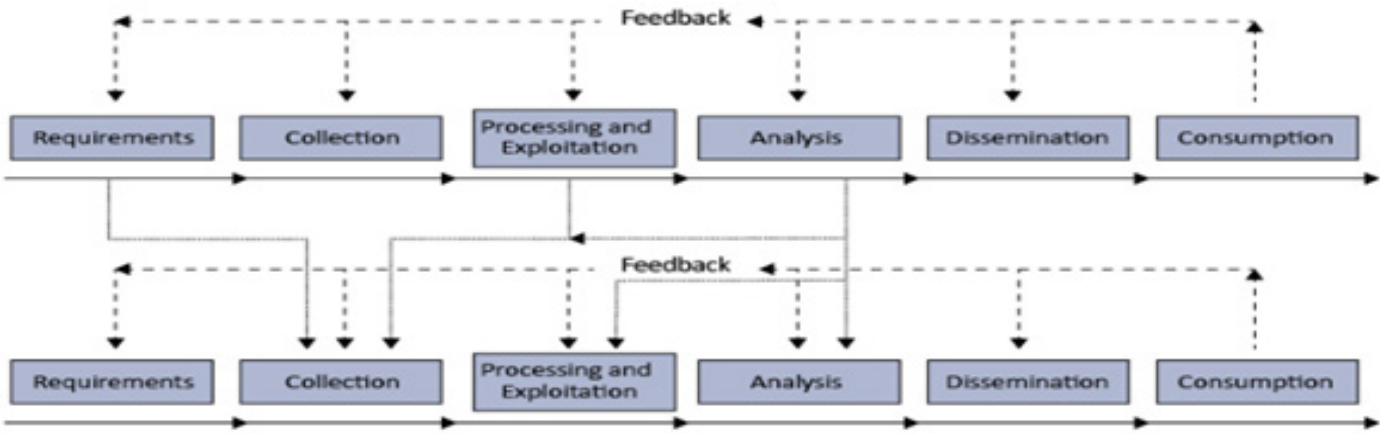
de inteligencia para asesorar a los más altos niveles decisionales de una organización o institución, siendo ello especialmente valioso en tiempos de una globalización de la información donde internet es el instrumento con el cual la mayor parte de la población se informa y que ha demostrado su capacidad para confundir con información no confiable en materia de interés nacional. Por este motivo, su experticia en valoración de información especialmente en el ciberespacio es útil.

En la etapa de difusión del ciclo es necesario que los diversos productos de inteligencia sean entregados en tiempo real a los decisores con la finalidad de anticiparles situaciones que requieren prevención, debido a que en caso de desarrollarse en el ciberespacio pueden en breve tiempo y a bajo costo generar daños de alto impacto. En efecto, con "la ayuda de programas instalados previamente, un mismo pirata puede atacar miles de computadoras en un sólo día utilizando sólo un computador. Si además el pirata tiene acceso a más computadores por ejemplo, una red zombi, puede atacar a mayor escala"[52] , tal como ocurrió recientemente con "*wannacry*"[53].

Finalmente, con relación a la etapa de la retroalimentación, es necesario que ésta se realice por parte del consumidor de inteligencia y que llegue instantáneamente al productor de inteligencia, con la finalidad de reorientar, profundizar, precisar o ampliar lo entregado. En este sentido, un ciclo de inteligencia que contemple esta fase resulta clave. Un modelo que ilustra la idea se indica en la figura N° 5, desarrollada por Lowenthal[54] y tal como la explica Jordán

> "Lowenthal (2012) propone un modelo algo más complejo pero también ajustado a la realidad, pues como han advertido por ejemplo Michael McConnell (antiguo Director Nacional de Inteligencia en Estados Unidos) y el académico Michael Herman, el ciclo está compuesto por una suma de feedbacks. A lo largo del ciclo surgen incidencias (nuevas necesidades de obtención,

**Figura N°5: "Proceso multi-estratos de Mark Lowenthal"**




Fuente: Jordán, 2016 basado en Lowenthal 2012.

[52] GERKE. Op cit. p.18.

[53] Al respecto ver "El virus WannaCry no se detiene: cientos de miles de nuevos infectados en Asia al comenzar la semana laboral". En: Infobae, publicado el 15 de mayo de 2017. [Fecha de consulta: 10 de octubre de 2017]. Disponible en https://www.infobae.com/america/mundo/2017/05/15/el-virus-wannacry-no-se-detiene-cientos-de-miles-de-nuevos-infectados-por-en-asia-al-comenzar-la-semana-laboral/ y Ciberataque global: últimas noticias del 'ransomware WannaCry' ". En: El País de España, publicado el 17 de mayo de 2017. [Fecha de consulta: 10 de octubre de 2017]. Disponible en https://elpais.com/tecnologia/2017/05/16/actualidad/1494927608_413489.html

[54] LOWENTHAL, Mark. Intelligence. 3º ed. Estados Unidos, CQ Press, 2006.

[55] JORDÁN, Javier. Una revisión del ciclo de inteligencia. Análisis GESI, 2/2016. España, Universidad de Granada, 2016. [Fecha de consulta: 10 de Octubre de 2017]. Disponible en http://www.seguridadinternacional.es/?q=es/content/una-revisi%C3%B3n-del-ciclo-de-inteligencia

> ambigüedades en el procesamiento, resultados de análisis, cambios en los requerimientos) que ponen en marcha un nuevo proceso, e incluso un tercero, cuarto… De modo que los estratos que aparecen en la figura inferior podrían multiplicarse por varios"[55].

La clave en cada una de las etapas del ciclo aplicado al ciberespacio en tema de ciberseguridad es la brevedad de tiempo en el cual una amenaza o vulnerabilidad de seguridad puede convertirse en realidad causando importantes daños. Ejemplo de esta situación fue en el ataque sufrido por Estonia en el año 2007, considerado por algunos como la primera "ciberguerra"[56]. Se habría producido entre Estonia y Rusia (aunque diversas fuentes le atribuyen el ataque, no han reconocido oficialmente su autoría) con motivo de la decisión de las autoridades de Estonia de retirar de una plaza una estatua que representa al soldado soviético y enviarla a un cementerio.

Esta medida produjo ataques simultáneos a páginas Web del Parlamento estonio, bancos, ministerios, periódicos y agencias de comunicación, entre otras. En efecto,

> "Estonia había sido víctima de un ataque distribuido de denegación de servicio o DDoS, por sus siglas en inglés. Por lo general, un DDoS es una molestia menor, no una de las principales armas del arsenal ciberespacial. Básicamente se trata de una avalancha programadas con antelación y diseñada para sobrecargar o bloquear la red con un gran flujo de información. El ataque es "distribuido" en el sentido de que en él participan miles de ordenadores, e incluso cientos de miles, que envían solicitudes de conexión electrónica a un puñado de blancos en Internet. Los ordenadores atacantes forman lo que se conoce como botnet, una red de ordenadores robots o "zombis" controlada en forma remota. Los zombis que participan en el ataque siguen instrucciones que se han cargado sin que sus propietarios se enteren. De hecho, usualmente los propietarios de estos ordenadores no pueden siquiera saber cuándo sus máquinas se convierten en zombis o están participando en un DDoS. Un usuario puede advertir que su portátil está funcionando un poco más lento de lo normal o que tarda más en acceder a la Web, pero ese será el único indicador de lo que realmente ocurre. Toda la actividad mal intencionada tiene lugar en segundo plano y no es visible en la pantalla del usuario. En este mismo momento, su propio ordenador podría formar parte de una botnet"[57].

Considerando las particularidades de un ciclo de inteligencia efectuado en el ciberespacio, a partir de eventos que es necesario monitorear o anticipar en este dominio, donde es imprescindible el trabajo en red, adquiere utilidad el modelo de ciclo planteado por Clark[58], el cual es explicado por Jordán[60] al señalar

> "Robert M. Clark (2013), ofrece una visión alternativa con su modelo de Target-Centric Intelligence (proceso de inteligencia centrado en el objetivo). Según él, la finalidad del proceso consiste en construir una imagen compartida del objetivo –del asunto de interés de la inteligencia. Una imagen de la que todos los participantes en el proceso puedan extraer elementos necesarios para su trabajo y a la que todos puedan contribuir con sus recursos y conocimientos con el fin de obtener un cuadro más ajustado de la realidad. No se trata de un proceso lineal ni cíclico, aunque contenga procesos de retroalimentación. Es más bien un trabajo en red, un proceso social, donde todos los participantes centran su atención en el objetivo"[60].

[56] CLARKE, Richard y KNAKE, Robert. Guerra en la red. España, Ariel, 2011.

[57] Ibíd. p 33.

[58] CLARK, Robert. Intelligence Analysis: A target – Centric Approach. EE.UU, CQ: Press, 2012.

[59] JORDÁN, Javier. Loc cit.

[60] Ibíd.

**Figura N°6: ”Proceso multi-estratos de Mark Lowenthal”**


Fuente: Jordán, 2017 basado en Clark, 2013..

Esta idea se ilustra en la figura N° 6.

En una perspectiva organizacional, el desarrollo de ciberinteligencia, no necesariamente implica la creación de una organización nueva y específica que desarrolle estas actividades. Aun cuando la ciberseguridad requiere de organizaciones e instituciones especializadas que pueden colaborar en materia de su ámbito de atribuciones y competencias formando o no parte de un sistema o comunidad de inteligencia. Siendo frecuente constatar que tradicionales agencias o servicios de inteligencia han incorporado en su trabajo cotidiano esta nueva dimensión de la función, agregando las nuevas amenazas y vulnerabilidades que aparecen a partir de los objetivos a monitorear para alertar con respecto a su prevención, defensa, recuperación y resiliencia.

No obstante, nuevas exigencias con relación a la coordinación interagencial y cooperación internacional resultan clave para un oportuno intercambio de información que permita identificar alertas de seguridad, como también, detectar peligros a la seguridad que es necesario evitar e inclusive enfrentar.

La ciberinteligencia desde la perspectiva del producto sobre el cual versa su trabajo, contempla en forma fundamental la seguridad de la información digital y los sistemas informáticos en el ciberespacio, particularmente los que se vinculan a la infraestructura crítica. Se busca proteger las propiedades de la información: disponibilidad, integridad y confidencialidad, para que no sean alteradas sin autorización de sus responsables o dueños. La disponibilidad de la información se refiere a los datos e informaciones obtenidas y almacenadas deben ser accesibles cuando sea necesario por parte de los usuarios autorizados. Un ejemplo típico de problema de disponibilidad de la información es cuando se produce un ataque de denegación de servicio distribuido o (DDoS). Ejemplo de esta situación se ejemplificó

anteriormente en el caso de incendios digitales.

La integridad de la información se refiere a que ésta no puede ser modificada por personas sin la autorización requerida. Toda modificación debe ser realizada por quienes están acreditados expresamente para ello. Además un cambio en la información debe basarse en datos verídicos. Por este motivo se asocia esta cualidad a la idea de autentificación, es decir, que toda modificación a los registros de información debe estar sustentado por antecedentes que avalan la veracidad de lo cambiado.

Ejemplo de casos donde esta cualidad de la información ha sido alterada ha ocurrido en el ámbito financiero cuando personas no autorizadas cambian estados de cuentas de clientes bancarios adicionando o sustrayendo dinero. También se ha detectado en el ámbito académico cuando estudiantes han ingresado al sistema informático de la universidad y cambiado sus notas, estado de pago de aranceles o puntaje de ingreso para postular a las universidades. Chile no ha estado ajeno a estos hechos y, por medio de la Ley 19.233 del año 1993 que tipifica figuras penales relativas a la informática, han sido perseguidos estos delitos.

La confidencialidad de la información está referida a que solo las personas autorizadas a conocerla pueden acceder a ella. Se relaciona con la privacidad de la información consagrada en las cartas fundamentales de los países democráticos. En el caso de la información disponible en el ciberespacio ha sido necesario la generación de leyes especializadas que regulen la privacidad de los datos personales de los ciudadanos entregados a diferentes organizaciones públicas y privadas con la finalidad de asegurar estándares internacionales en su gestión; es decir, la obtención, almacenamiento, difusión e inclusive eliminación y la rendición de cuenta al ciudadano sobre ello. En el caso chileno, la ley 19.628 del año 1999 denominada "Sobre Protección de la Vida Privada" regula esta actividad, sin embargo, son numerosas las críticas que ha recibido en cuanto a su debilidad para efectivamente cumplir su cometido, como también respecto a que no cuenta con estándares internacionales que inclusive dificultarían el intercambio de información, por ejemplo, en el marco de la Convención de Ciberdelito o de Budaspest. Por este motivo, hay planteamientos en términos de modificar esta normativa para actualizarla[61].

**"La ciberinteligencia desde la perspectiva del producto sobre el cual versa su trabajo, contempla en forma fundamental la seguridad de la información digital y los sistemas informáticos en el ciberespacio, particularmente los que se vinculan a la infraestructura crítica"**

Además de la seguridad de la información digital, en una perspectiva de ciberseguridad, es necesario proteger la Infraestructura Crítica (IC), entendida como "las instalaciones, redes, servicios y equipos físicos y de tecnología de la información cuya afectación, degradación, denegación, interrupción o destrucción pueden tener una repercusión importante en la salud, la seguridad o el bienestar económico de los ciudadanos o en el eficaz funcionamiento de los gobiernos de los Estados"[62], puede verse afectada por los denominados "Malware", es decir, software maliciosos. Ellos han causado daño en sistemas de información e inclusive IC en algunos países alertando del peligro

[61] VIOLLIER, Pablo. El Estado de la Protección de Datos Personales en Chile. S/L, Derechos Digitales América Latina, 2017. S/L. Derechos Digitales América Latina, 2017. [Fecha de consulta: 10 de octubre de 2017]. Disponible en https://www.derechosdigitales.org/wp-content/uploads/PVB-datos-int.pdf

[62] CHILE. Bases para una Política Nacional de Ciberseguridad. Op cit. p.14

existente. De acuerdo a un reporte de la empresa de seguridad informática Kaspersky, los malware pueden agruparse "en amenazas conocidas (70%), amenazas desconocidas (29%) y amenazas sofisticadas (1%)"[63], siendo estas últimas denominadas también como "*Advanced Persistent Threats"* (APT) o "Amenazas Avanzadas Permamentes" y son particularmente peligrosas porque se trata de "ataques polivalentes, continuados y dirigidos. Diseñados para introducirse en una red, merodear de forma invisible y recopilar datos confidenciales, una vez introducidos pueden pasar desapercibidos durante años"[64].

Para ilustrar su modo de funcionamiento y posibles daños que pueden generar se hará referencia a tres de ellos: Darkhotel, Flame y Stuxnet. El primero es descrito en un reporte de Kaspersky

> "Una APT conocida como "Darkhotel" utilizó el Wi-Fi en hoteles de lujo para robar los datos de los huéspedes durante siete años antes de que se descubriera. Esta fue especialmente interesante, ya que tenía un objetivo muy específico (los altos ejecutivos y directores ejecutivos) e ilustraba de forma muy clara el reto que se presenta a la seguridad de IT cuando los endpoints [terminales] (portátiles y tablets empresariales) operan fuera del perímetro de seguridad de la red de la empresa"[65].

En el caso de *Flame*, este fue detectado en 2010, aun cuando se sospecha que ya en 2006 estaba operando en los sistemas informáticos. Tiene la capacidad de que al infectar el sistema comienza a realizar una compleja serie de operaciones, incluyendo espiar en el tráfico de Internet, tomar imágenes de pantallas de computador, grabar conversaciones, interceptar teclados y demás[66], explicó Vitaly Kamluk, experto en malware de la empresa Kaspersky. Entre los países afectados se encuentran Irán, Israel, Sudán, Siria, Líbano, Arabia Saudita y Egipto.

Por su parte, el gusano informático Stuxnet presenta un mayor riesgo por cuanto espía y reprograma sistemas industriales, particularmente los SCADA (Supervisión, Control y Adquisición de Datos)[67], además cuenta con capacidad para afectar instalaciones industriales. En Irán, fue usado para afectar incluso infraestructura nuclear entre 2009 y 2010, donde atacó en forma reiterada cinco plantas a lo largo de 10 meses, según un análisis realizado por Symantec. Actualmente es considerado el primer virus para afectar sistemas industriales.

En el ciberespacio es posible identificar dos modos de acceder a la información en forma clandestina violando su confidencialidad. Mediante el acceso "a sistemas informáticos o a un dispositivo de almacenamiento y extraer la información; o tratar de manipular a los usuarios para que revelen la información o los códigos de acceso que les permitan acceder a la información ("peska")"[68]. El acceso clandestino a la información puede estar asociado al ciberdelito o por motivos de seguridad nacional, en ambos casos el objetivo es el mismo, conseguir bases de datos con información privada de las personas o sensible del Estado respectivamente, lo cual puede ser comprado en el mercado que se ha desarrollado exponencialmente en este tema. En efecto, "un estudio publicado en 2014 se indica que los datos disponibles en el cibermercado negro, obtenidos

[63] Los riesgos futuros: Protéjase. Karpesky. 2015. p. 3. [Fecha de consulta: 10 de octubre] Disponible en http://go.kaspersky.com/rs/802-IJN-240/images/APT_Report_ONLINE_AW_ES.pdf

[64] Ibíd.

[65] Ibíd.

[66] "Karpesky habla sobre el virus flame". Coordinación en Seguridad. México. 2012. [Fecha de consulta: 10 de octubre] Disponible en http://www.seguridad.unam.mx/noticia/?noti=377

[67] ANABALÓN, Juan y DONDERS, Eric. Una revisión de ciberdefensa de infraestructura crítica. En: revista ESD, Estudios de Seguridad y Defensa Nº 3. Chile, ANEPE, 2014. [Fecha de consulta: 10 de octubre] Disponible en http://esd.anepe.cl/wp-content/uploads/2014/11/art5.pdf

[68] GERCKE, Marco. Op cit. p. 20.

[69] Ibíd.

por medio del robo de datos, contemplan credenciales de hasta 360 millones de cuentas"[69].

Junto a lo indicado, se encuentran las vulnerabilidades del propio sistema, en términos de no poder resguardar la confidencialidad de la información que obtiene y genera, produciéndose fugas no deseadas de información siendo más fácil y en mayor cantidad cuando se trata de información electrónica. La filtración de información, particularmente desde los Servicios de Inteligencia –lo que constituye un problema de contrainteligencia- puede afectar la seguridad de los países. Situaciones recientes, asociadas al clásico problema de la protección de la información sensible para evitar fugas y difusión no deseada de ella, han alcanzado alta visibilidad y recuerdan que el problema está vigente.

**"Junto a lo indicado, se encuentran las vulnerabilidades del propio sistema, en términos de no poder resguardar la confidencialidad de la información que obtiene y genera, produciéndose fugas no deseadas de información siendo más fácil y en mayor cantidad cuando se trata de información electrónica"**

Por ejemplo, algunas situaciones en los EE.UU. han generado repercusiones más allá de sus fronteras en diferentes continentes. Se trata de los casos protagonizados por el soldado Manning y el ex-funcionario de la Agencia Nacional de Seguridad (NSA) Edward Snowden. Ambos accedieron a información secreta del Departamento de Defensa de EE.UU. y la difundieron a la opinión pública por medio de Wikileaks, produciendo problemas diplomáticos y de seguridad al gobierno norteamericano. En opinión del general Michael Hayden, Director de la Agencia Central de Inteligencia (CIA) y de la NSA durante el período de dos presidentes de Estados Unidos (Bill Clinton y George W. Bush), los documentos filtrados por Snowden han sido "la destrucción de secretos legítimos de Estados Unidos más grande de la historia de mi país (…) casi mil objetivos de inteligencia extranjeros han cambiado su comportamiento basándose en las revelaciones de Snowden"[70].

En síntesis, la ciberinteligencia puede ser entendida en sentido amplio y estricto. En el primero, corresponde a la realización de las diferentes actividades propias de la función inteligencia en el ciberespacio, lo cual implica que cada una de sus dimensiones (organización, proceso, producto) adapta su misión y funcionamiento a la naturaleza del ciberespacio. En el segundo, se trata de una fuente específica de acceso a información disponible en forma abierta, cerrada o mixta.

## 3.Desafíos en Ciberinteligencia

La función inteligencia para el cumplimiento de su misión requiere actualmente desarrollarse en las más nueva de las dimensiones donde se producen la interacciones de las personas: el ciberespacio. En efecto, en este ambiente son detectadas peligrosas amenazas y vulnerabilidades que en caso de concretarse pueden poner en riesgo la seguridad de las personas organizaciones e instituciones de los países que pueden inclusive poner en riesgo su estabilidad y soberanía. Siendo necesario contar con una capacidad a nivel estatal que pueda monitorear y generar alertas tempranas para evitar situaciones críticas que afecten seguridad pública e inclusive la nacional. Ello refuerza su vigencia de conocer pronósticos de especialistas sobre el tema cuando señalan para el 2018

[70] XIMENEZ, Pablo. Michael Hayden: "Me preocupa que Trump pueda ser presidente". En: El País de España, publicado el 5 de marzo de 2016. España. [Fecha de consulta: 15 de octubre de 2017] Disponible en http://internacional.elpais.com/internacional/2016/03/04/actualidad/1457076618_844331.html

> "ver actores de amenazas avanzadas que desplieguen sus nuevas capacidades, que perfeccionen sus nuevas y aterrorizantes herramientas. Los temas y tendencias de cada año no deben observarse de manera aislada; se construyen unos sobre otros para crear un panorama de la amenaza e inseguridad creciente que todos enfrentan, desde individuos hasta negocios y el gobierno. Dónde terminará, no lo sabemos; pero el conocimiento y la comprensión serán recursos poderosos"[71].

Un exitoso desarrollo de la ciberinteligencia como parte de la función inteligencia en organizaciones e instituciones presenta al menos cuatro requisitos, como condición necesaria más no suficiente:

a) Voluntad política: La convicción de las más altas autoridades organizacionales de contemplar el ciberespacio como fuente desde donde pueden provenir riesgos importantes a la seguridad, como asimismo, considerarlo como una fuente de información útil en la búsqueda de información, resulta clave en el desarrollo de la ciberinteligencia, pues la generación de este espacio en una primera instancia estará condicionada por el liderazgo que realicen en este tema, al posicionar este dominio en el trabajo de la inteligencia.

b) Capacidad: Contar con una infraestructura mínima para aprovechar el ciberespacio de acuerdo a las necesidades de información en inteligencia requiere de recursos económicos nuevos para acceder a tecnología especializada y equipos con una capacidad superior para procesar gran cantidad de datos e información, acceso a bases de datos electrónicas y software especializados, como también, personal especializado o que es necesario capacitar para: hacer búsquedas en redes sociales o la web profunda, entre otros; análisis en software nuevos; monitorear los sistemas informáticos para detectar una amenaza o vulnerabilidad; y leer un reporte de ciberseguridad.

c) Coordinación interagencial: Son diferentes las instituciones que monitoreando el ciberespacio o haciendo uso de éste para sus propios objetivos tendrán información clave para prever, anticipar o enfrentar una amenaza o vulnerabilidad a la seguridad en el ciberespacio. Estas instituciones pueden o no ser parte del sistema de inteligencia del Estado o de una comunidad de inteligencia. No obstante, es necesario que existan flujos de información entre las entidades que pueden aportar para emitir una alerta de seguridad o entender un incidente que se está produciendo en el ciberespacio.

d) Cooperación internacional: Debido a que ningún Estado por si solo puede obtener toda la información que requiere en materia de inteligencia, se ha justificado tradicionalmente la cooperación entre diferentes países. En el caso de situaciones relacionadas con el ciberespacio, se refuerza esta necesidad toda vez que ante un potencial o efectivo ciberincidente, los ilícitos manifiestos o latentes en este dominio obligan a contar con información en tiempo real, que muchas veces está en servidores cuya jurisdicción pertenece a diferentes países y los responsables tras lo investigado pueden tener una identidad anónima para los afectados, pues podrían estar actuando encubiertamente desde lugares diferentes a donde se ha planeado y/o ejecutado el evento potencial, en desarrollo o efectuado que es investigado.

Junto a lo indicado, debido a que la cooperación entre diferentes organizaciones requiere dos requisitos previos: conocimiento y confianza; además de una capacidad de interlocución válida entre los funcionarios involucrados, adquiere relevancia la generación de instancias internacionales compartidas de formación, capacitación y actualización para funcionarios de inteligencia y vinculados a ella, relacionados

[71] BAUMAGTNER K., GUERRERO-SAADE, J. COSTIN RAIU, C . Boletín de seguridad Kaspersky: Predicciones sobre amenazas para el 2018. Publicado en Secure list, el 15 de noviembre de 2017. Búsqueda efectuada el 20 de noviembre de 2017[Fecha de consulta: 20 de Noviembre de 2017]. Disponible en https://securelist.lat/boletin-de-seguridad-kaspersky-predicciones-sobre-amenazas-para-el-2018/85748/

con eventos o incidentes en el ciberespacio que afecte la seguridad de personas, organizaciones, instituciones y/o países. Asimismo, en un nivel avanzado de cooperación orientado a la generación de entidades especializadas multilaterales es posible considerar la creación de un centro de fusión de información e inteligencia relacionados con incidentes en el ciberespacio a partir de lo proporcionado por los países y eventualmente preparado por analistas de esta entidad, quienes trabajarían en base a estándares compartidos de trabajo. Experiencias en el tema pueden encontrarse en el caso de la Unión Europea (UE), con tres organizaciones: ENISA, El Centro Europeo para el Ciberdelito y el mencionado Centro de Excelencia Europeo para la lucha contra las amenazas híbridas[72].

La Agencia de la UE para la Seguridad de las Redes y la Información (ENISA), fue creada en 2004, para

> "resistir, con un determinado nivel de confianza, eventos accidentales o acciones ilícitas o maliciosas que comprometen la disponibilidad, autenticidad, integridad y confidencialidad de los datos almacenados o transmitidos y los servicios relacionados ofrecidos o accesibles a través de redes y sistemas [de información]. Se decidió que la agencia debería ayudar a la Unión y a los Estados Miembros a mejorar y fortalecer su capacidad y preparación para prevenir, detectar y responder a problemas e incidentes de seguridad de la red y de la información. Las tareas de ENISA incluyen la recopilación, procesamiento y análisis de datos y la diseminación de información e informes sobre incidentes de seguridad de TI en la UE, así como también sobre riesgos emergentes y amenazas a la seguridad. ENISA ha desarrollado un marco conceptual para el análisis y la presentación de informes de riesgos emergentes y futuros en el área de seguridad de la información de red"[73].

Para el ciberdelito en el año 2013 con el apoyo de INTERPOL fue establecido el

> "Centro Europeo de Ciberdelincuencia (EC3). El centro se centra en la fusión de datos: recopilación de información sobre ciberdelito entregada por los Estados miembros y recopilada a partir de fuentes abiertas. También procesa y analiza información e inteligencia preproducida con el fin de entregar evaluaciones de amenazas. De acuerdo con la información en el sitio web de EC3, el Centro "actúa como un centro analítico, procesando y analizando información crítica de diversas fuentes de forma continua. El objetivo es ampliar la imagen de la información sobre el delito cibernético en Europa a lo largo del tiempo a fin de identificar rápidamente las amenazas emergentes"[74].

Para el problema de ciberataques y muy especialmente la propaganda en la Red sin sustento empírico y manifestada fundamentalmente por medio de "noticias falsas" fue creado en 2017 el Centro de Excelencia Europeo para la lucha contra las amenazas híbridas (Hybrid CoE)"[75].

En síntesis, el desarrollo exitoso de la ciberinteligencia requiere de liderazgo en organizaciones que contemple diversos factores relacionados con la convicción de la gestión en aprovechar el máximo el ciberespacio, contar con los recursos mínimos necesarios y promover la coordinación y cooperación entre organizaciones e instituciones vinculadas al tema.

[72] En el caso del Continente Americano, la Organización de Estados Americanos (OEA) efectúa importantes esfuerzos en el tema, generando documentos que orientan el trabajo de los países en la materia. Por ejemplo, al respecto ver AG / Res 2004 Estrategia de Seguridad Cibernética. CICTE. OEA. EE.UU.

[73] GRUSZCZAK, Artur. Op. cit. pp. 81-82

[74] Ibíd

[75] SOTO, Adrián. Loc. cit.

## Consideraciones finales

El ciberespacio constituye parte de la vida cotidiana de las personas, organizaciones, instituciones y países, cambiando el modo en que se desarrollan las principales activdades cotidianas, planteandose un nuevo paradigma denominado “cuarta revolución industrial”. No obstante, el ciberespacio no está exento de riesgos a la seguridad. En efecto, la mayor parte de las amenazas en el ciberespacio son transnacionales y se caracterizan por ser: flexibles (presentan una estructura horizontal), ambiguas (su arquitectura es difusa), globales (su ámbito de acción es transnacional) y versátiles (son capaces readaptarse al entorno).

El ciberespacio puede ser tanto un medio como un objetivo e inclusive ambas al mismo tiempo para la realización de ilícitos que pueden afectar la seguridad del país, la estabilidad de sus instituciones, la soberanía nacional y/o la vida de sus habitantes. En el primer caso se trata especialmente de prácticas delictuales con un daño limitado a personas, organizaciones o instituciones. En el segundo, la probabilidad de generar importantes daños a la infraestructura crítica del país (energía, comunicaciones, transporte, sistema financiero, sanitario, de alimentación, entre otros) puede convertirse en un problema de seguridad nacional.

En este contexto, la ciberseguridad adquiere importancia y es una condición necesaria más no suficiente para el uso confiable del ciberespacio. Siendo necesario no solo abordar en términos prácticos sino también por medio de un marco teórico que explicite y precise la naturaleza, características y desafíos que presentan estos términos. Ello para facilitar la compresión del fenómeno y el trabajo interagencial que implica.

De esta manera, conceptos como ciberespacio, ciberseguridad e infraestructura crítica han ido aparejados de un marco teórico conceptual a nivel internacional y nacional que es coincidente, estando el desafío pendiente en el caso de la ciberinteligencia. En efecto, la inteligencia es un concepto asociado a la seguridad en el marco de un espacio definido y es frecuente encontrarla en organizaciones complejas. No es la excepción en el dominio cibernético, encontrándose el término ciberinteligencia que da cuenta de ello. Sin embargo, presenta un menor nivel de desarrollo a nivel internacional y faltan documentos públicos nacionales que expliciten el modo en que es entendida esta parte de la función inteligencia, aun cuando es efectuada en los servicios de inteligencia.

**“... la ciberseguridad adquiere importancia y es una condición necesaria más no suficiente para el uso confiable del ciberespacio. Siendo necesario no solo abordar en términos prácticos sino también por medio de un marco teórico que explicite y precise la naturaleza, características y desafíos que presentan estos términos. ”**

A partir de las aproximaciones conceptuales revisadas, en una perspectiva teórica ciberinteligencia puede entenderse en sentido amplio y estricto. En efecto, siguiendo la literatura internacional, es posible entenderla como la aplicación de la función inteligencia al ciberespacio, como también, como una fuente de información específica, desde donde se puede responder a la necesidad del saber.

Abordar los desafíos identificados que presenta su implementación haría posible un exitoso desarrollo de la ciberinteligencia. Estos se relacionan con la convicción de las máximas autoridades responsables en aprovechar el máximo el ciberespacio, contar con los recursos mínimos necesarios y promover la coordinación y cooperación entre organizaciones e instituciones vinculadas al tema.

## Bibliografía

"Ciberataque global: últimas noticias del 'ransomware WannaCry' ". En: El País de España, publicado el 17 de mayo de 2017. [Fecha de consulta: 10 de octubre de 2017]. Disponible en https://elpais.com/tecnologia/2017/05/16/actualidad/1494927608_413489.html

"El virus WannaCry no se detiene: cientos de miles de nuevos infectados en Asia al comenzar la semana laboral". En: Infobae, publicado el 15 de mayo de 2017. [Fecha de consulta: 10 de octubre de 2017]. Disponible en https://www.infobae.com/america/mundo/2017/05/15/el-virus-wannacry-no-se-detiene-cientos-de-miles-de-nuevos-infectados-por-en-asia-al-comenzar-la-semana-laboral/

"Karpesky habla sobre el virus flame", Coordinación en Seguridad. México. 2012. [Fecha de consulta: 10 de octubre]. Disponible en http://www.seguridad.unam.mx/noticia/?noti=377

"La UIT publica las cifras de 2016 de las TIC". Suiza, UIT, 2017. [Fecha de consulta: 10 de julio de 2017].Disponible en http://www.itu.int/es/mediacentre/Pages/2016-PR30.aspx

"Noticias falsas acerca de Chile fueron vistas o compartidas 3,5 millones de veces en redes sociales en 2017". En: El Mostrador, publicado el 26 de noviembre de 2017. [Fecha de consulta: 26 de noviembre de 2017]. Disponible en: http://www.elmostrador.cl/noticias/pais/2017/11/26/noticias-falsas-acerca-de-chile-fueron-vistas-o-compartidas-35-millones-de-veces-en-redes-sociales-en-2017/

"The post-truth world: Yes, I'd lie to you". En: The Economist, 10 de septiembre de 2016. U.K

AG / Res 2004 Estrategia de Seguridad Cibernética. CICTE. OEA. EE.UU.

ANABALÓN, Juan y DONDERS, Eric. Una revisión de ciberdefensa de infraestructura crítica. En: revistaESD, Estudios de Seguridad y Defensa Nº 3. Chile, ANEPE, 2014. [Fecha de consulta: 10 de octubre] Disponible en http://esd.anepe.cl/wp-content/uploads/2014/11/art5.pdf

BACHELET, Michelle. "Una política de Ciberseguridad para Chile". En Política Nacional de Ciberseguridad. Chile, Gobierno de Chile, 2017. p. 5. [Fecha de consulta: 15 de julio de 2017].Disponible en http://www.ciberseguridad.gob.cl/media/2017/05/PNCS-ES-FEA.pdf

Banco Mundial. Informe sobre el desarrollo Mundial 2016: "Dividendos Digitales", panorama general. EE.UU. Banco Mundial, 2016. [Fecha de consulta: 20 de noviembre de 2017]. Disponible en: http://documents.worldbank.org/curated/en/658821468186546535/pdf/102724-WDR-WDR2016Overview-SPANISH-WebResBox-394840B-OUO-9.pdf

BAUMGARTNER, K. , GUERRERO-SAADE, J. y COSTIN RAIU, C . Boletín de seguridad Kaspersky: Predicciones sobre amenazas para el 2018. Publicado en Secure list, el 15 de noviembre de 2017. Búsqueda efectuada el 20 de noviembre de 2017. [Fecha de consulta: 20 de noviembre de 2017]. Disponible en https://securelist.lat/boletin-de-seguridad-kaspersky-predicciones-sobre-amenazas-para-el-2018/85748/

BORG, Scott. No es una guerra fría. En: Vanguardia Dossier Nº 54. España, 2015.

BAMFORD, James. Every move you make. En: Foreign Policiy edición argentina, Archivos del Presente. Nº 65, año 2017. Argentina.

BRANTLY, A. Defining the role of intelligence in cyber. A hybrid push and pull. In M. Phythian (Ed.), Understanding the intleligence cycle. London/NewYork: Routledge, 2013.

CIANCAGLINI, V. , BALDUZZI, M. , MCARDLE, R. and RÖSLER M. Below the Surface: Exploring the Deep Web. TrendLabs Research Paper. S/L, Trend Micro, 2015.

Ciberseguridad ¿Estamos preparados en América Latina y el Caribe? Informe Ciberseguridad 2016. BID / OEA. Disponible en https://publications.iadb.org/handle/11319/7449?locale-attribute=es&

CLARK, Robert. Intelligence Analysis: A target – Centric Approach. EE.UU, CQ: Press, 2012.

CLARKE, Richard y KNAKE, Robert. Guerra en la red. España, Ariel, 2011.

CUBEIRO, Enrique. "Ciberinteligencia". En: Díaz, Antonio (editor) Conceptos Fundamentales de Inteligencia. España, Tirant lo Blanch, 2016.

CHILE. Bases para una Política Nacional de Ciberseguridad. Chile, Ministerio del Interior y Seguridad Pública y Ministerio de Defensa Nacional, 2015. [Fecha de consulta: 10 de julio de 2017]. Disponible en http://ciberseguridad.interior.gob.cl/media/2015/12/Documento-Bases-Pol%C3%ADtica-Nacional-sobre-Ciberseguridad.pdf

CHILE. Política Nacional de Ciberseguridad. Chile, Gobierno de Chile, 2017. [Fecha de consulta: 15 de julio de 2017]. Disponible en http://www.ciberseguridad.gob.cl/media/2017/05/PNCS-ES-FEA.pdf

Decreto 533/2015, Ministerio del Interior y Seguridad Pública. CREA COMITÉ INTERMINISTERIAL SOBRE CIBERSEGURIDAD. Chile.

Ley 19.223/1993 del Ministerio de Justicia. TIPIFICA FIGURAS PENALES RELATIVAS A LA INFORMATICA. Chile.

Ley 19.628/1999 del Ministerio Secretaría General de la Presidencia. SOBRE PROTECCIÓN DE LA VIDA PRIVADA. Chile.

ESTEBAN Navarro, Miguel. Necesidad, funcionamiento y misión de un servicio de inteligencia para la seguridad y defensa. Cuadernos de Estrategia (127). España, 2004.

FLACSO. Reporte del sector seguridad en América Latina y el Caribe. Chile, FLACSO, 2007.

GERCKE, Marco. Informe "Comprensión del Ciberdelito: Fenómeno, Dificultades y Respuesta Jurídica. Suiza, UIT, 2014. [Fecha de consulta: 10 de julio de 2017]. Disponible en www.itu.int/ITU-D/cyb/cybersecurity/legislation.html

Global Risks, 2013. Ginebra, World Economic Forum, 2013. Disponible en http://www3.weforum.org/docs/WEF_GlobalRisks_Report_2013.pdf

GOODMAN, Marc. Los delitos del futuro. España, Ariel, 2015.

GRUSZCZAK, Artur. New Security Challenges. Polonia, Palgrave Macmillian, 2016.

JORDÁN, Javier. Una revisión del ciclo de inteligencia. Análisis GESI, 2/2016. España, Universidad de Granada, 2016. [Fecha de consulta: 10 de octubre de 2017]. Disponible en http://www.seguridadinternacional.es/?q=es/content/una-revisi%C3%B3n-del-ciclo-de-inteligencia

La Ciberseguridad Nacional, un compromiso de todos. Instituto de Ciberseguridad de España. España, INSTITUTO DE CIBERSEGURIDAD DE ESPAÑA, 2012.

LINERA, Reyes. “Un pirata publica un falso atentado contra Obama en el Twitter de AP”. En: El País de España, publicado el 23 de abril de 2013. [Fecha de consulta: 15 de julio de 2017] Disponible en https://elpais.com/internacional/2013/04/23/actualidad/1366738727_668448.html

Los riesgos futuros: Protéjase. Karpesky. 2015. [Fecha de consulta: 10 de octubre] Disponible en http://go.kaspersky.com/rs/802-IJN-240/images/APT_Report_ONLINE_AW_ES.pdf

LOWENTHAL, Mark. Intelligence. 3º ed. Estados Unidos, CQ Press, 2006.

NAÍM, Moisés. El fin del poder. España, Debate, 2013.

NYE, Joseph. “¿Se puede ejercer la disuasión en la guerra cibernética?”. EE.UU., Project Sindicate, 2015. [Fecha de consulta: 10 de octubre de 2017] Disponible en https://www.project-syndicate.org/print/cyber-warfare-deterrence-by-joseph-s--nye-2015-12/spanish

OBERMAIER, Frederick y OBERMAYER, Bastián. Panamá Papers. Colombia, Planeta, 2016.

ROBERTS, David. “Post-Truth Politics”. Grist. 1 de abril de 2010. [Fecha de consulta: 10 de octubre 2017]. Disponible en http://grist.org/article/2010-03-30-post-truth-politics/

ROBLEDO, Marcos. “Una política de Ciberseguridad para Chile”. En: Política Nacional de Ciberseguridad. Chile, Gobierno de Chile, 2017. p. 9. [Fecha de consulta: 15 de julio de 2017].Disponible en http://www.ciberseguridad.gob.cl/media/2017/05/PNCS-ES-FEA.pdf

SANCHO, Carolina. “El ciberespacio como bien público y la ciberseguridad como problema: algunos dilemas y desafíos en tiempos de globalización”. En: VV.AA. Desafíos de la Seguridad y Defensa en el mundo contemporáneo”. Chile, ANEPE, 2016.

SANCHO, Carolina. “Ciberespacio bien público mundial en tiempos de globalización: Política pública de ciberseguridad una necesidad imperiosa y la ciberdefensa como desafíos en el siglo XXI”, en Ciberdefesa e ciberseguranca: Novas ameaças a segurança nacional. Brasil, XVII Conferencia de Directores de Colegios de Defesa Ibero-americanos, 2016.

SCHWAB Klaus. La cuarta revolución industrial. Argentina, Debate, 2017.

Seguridad Cibernética e Infraestructura Crítica en las Américas. EE.UU, OEA / Trend Micro, 2015.

SOTO, Adrián. “La OTAN y la UE abren un centro contra las amenazas híbridas”. En: El País de España, publicado el 2 de octubre de 2017. [Fecha de consulta: 10 de octubre de 2017]. Disponible en https://elpais.com/internacional/2017/10/02/actualidad/1506969497_610407.html

UIT. Medición de la Sociedad de la Información 2014. Resumen Ejecutivo. Suiza, UIT, 2014. [Fecha de consulta: 20 de octubre de 2017]. Disponible en https://www.itu.int/dms_pub/itu-d/opb/ind/D-IND-ICTOI-2014-SUM-PDF-S.pdf

UIT. Medición de la Sociedad de la Información 2015. Resumen Ejecutivo. Suiza, UIT, 2015. [Fecha de consulta: 20 de Octubre de 2017]. Disponible en https://www.itu.int/en/ITU-D/Statistics/Documents/publications/misr2015/MISR2015-ES-S.pdf

UIT. Recomendación UIT-T X.1205 (04/2008).

UIT. Measuring the Information Society Report. Ejecutive summary. Suiza, UIT, 2017. [Fecha de consulta: 20 de noviembre de 2017]. Disponible en https://www.itu.int/en/ITU-D/Statistics/Documents/publications/misr2017/MISR2017_ExecutiveSummary.pdf

VILLAMEDIANA, Miriam. "Los datos son el nuevo petróleo del siglo XXI". En: Euroexpress, publicado el 1 de julio de 2015. Disponible en http://www.euroxpress.es/noticias/los-datos-son-el-nuevo-petroleo-del-siglo-xxi

VIOLLIER, Pablo. El Estado de la Protección de Datos Personales en Chile. S/L, Derechos Digitales América Latina, 2017. S/L. Derechos Digitales América Latina, 2017. [Fecha de consulta: 10 de octubre de 2017]. Disponible en https://www.derechosdigitales.org/wp-content/uploads/PVB-datos-int.pdf

XIMENEZ, Pablo. Michael Hayden: "Me preocupa que Trump pueda ser presidente". En: El País de España, publicado el 5 de marzo de 2016. España. [Fecha de consulta: 15 de octubre de 2017] Disponible en: http://internacional.elpais.com/internacional/2016/03/04/actualidad/1457076618_844331 .html

## DIRECCIÓN DE LA REVISTA

### DIRECTOR



### CONSEJO EDITORIAL


CENTRO DE INVESTIGACIONES Y ESTUDIOS ESTRATÉGICOS
ANEPE.CL