COLABORACIÓN EXTERNA N°4

Seguridad y ciberseguridad: precisiones sobre una tarea compartida

Marcelo Masalleras

ATHENALAB
International relations · Security · Defense
CHILE

**Los comentarios y opiniones vertidas en este documento representan el pensamiento de sus autores, no necesariamente de la institución.*

Seguridad y ciberseguridad: precisiones sobre una tarea compartida

Marcelo Masalleras
Investigador Asociado AthenaLab

INTRODUCCIÓN

En 2012, el secretario de Defensa de los Estados Unidos, León E. Panetta, planteó la posibilidad de que su país enfrentara un "Ciber Pearl Harbor", en referencia al sorpresivo ataque que recibió la base estadounidense en Hawái el 7 de diciembre de 1941, por parte de fuerzas japonesas, y que marcó el inicio de su activa participación en la Segunda Guerra Mundial. Lo significativo de la metáfora es el uso de suceso histórico, por el profundo impacto sicológico que tuvo y sigue teniendo este hecho en la cultura norteamericana, lo que permite destacar la condición de creciente vulnerabilidad que ese gobierno percibía, frente a amenazas principalmente de tipo interestatal[1].

El prefijo "ciber" llegó para quedarse. Así como la penetración de la tecnología ha crecido enormemente en la vida cotidiana de las personas, también lo han hecho las amenazas relacionadas con el uso de distintos dispositivos y plataformas informáticas. El prestigioso Centro de Estudios Internacionales y Estratégicos (CSIS, por sus siglas en inglés) desarrolla, dentro de múltiples informes, un conjunto de programas asociados a la detección y seguimiento de eventos y desafíos sociales, económicos y de seguridad generados por tecnologías disruptivas[2]. También este *think tank* elabora y actualiza desde 2006, una lista con los mayores incidentes informáticos que van ocurriendo a nivel mundial y que abarcan principalmente ciberataques a agencias gubernamentales y de defensa relevantes, compañías de tecnología y crímenes de carácter económico que hayan reportado más de un millón de dólares en pérdidas[3]. Los incidentes reportados en 2020 ascienden a 135, mientras que los acumulados en 2021 hasta el 27 de septiembre, alcanzan ya los 95[4]. Los objetivos de los ataques son variados, al igual que su origen, atribuyéndose a gobiernos extranjeros, crimen organizado transnacional, ciberdelincuentes aislados o

[1] Leon E. Panetta, citado en artículo publicado el 11 de octubre de 2012 por The New York Times. Ver: https://www.nytimes.com/2012/10/12/world/panetta-warns-of-dire-threat-of-cyberattack.html

[2] Para más información sobre el Center for Strategic & International Studies, visitar: https://www.csis.org/programs/strategic-technologies-program

[3] Center for Strategic & International Studies, Strategic Technologies Program. Ver: https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents.

[4] Strategic Technologies Program, "Significant Cyber Incidents", Center for Strategic & International Studies, https://csis-website-prod.s3.amazonaws.com/s3fs-public/210901_Significant_Cyber_Incidents.pdf?iZAairy6vNXrSEp9cFC_TCaB0IxnkE3D

incluso una mezcla entre esas causas y errores de los usuarios.

Por ejemplo, pudimos observar el aumento de los químicos en una planta de tratamiento de agua del estado de Florida, Estados Unidos, a niveles potencialmente peligrosos para el ser humano, producto de un ataque informático a los sistemas de control industrial, debido al débil control de acceso que poseían los sistemas, lo que permitió que la contraseña fuera fácilmente vulnerada[5]. Otro ataque provocó que la empresa operadora de uno de los más grandes oleoductos de Estados Unidos, el "Colonial Pipeline", tuviera que pagar cerca de US$ 4,4 millones de dólares para recuperar los datos que fueron encriptados producto de un ataque *ransomware*[6] y que la tuvo varios días sin poder operar, lo que además generó grandes pérdidas al tener que detener sus operaciones.

Si tomamos en cuenta la cobertura global del ciberespacio, las acciones realizadas por agentes negativos —amparados en condiciones de anonimato—, una jurisdicción difusa y un acceso abierto[7], se genera un escenario especial para actores tanto estatales como no estatales. De esta manera, nuestro país no se encuentra ajeno a los efectos de estos ataques. Así, un reporte de la empresa Fortinet[8] indica que, en el segundo trimestre del año 2021, Chile fue víctima de múltiples ataques en el ciberespacio, de distinta magnitud, a saber: más de 12 millones de detecciones de virus; 40 millones de redes "bot", y cerca de 1.600 millones de detecciones de explotaciones de vulnerabilidades. A estas cifras se pueden sumar la pérdida de 10 millones de dólares del Banco de Chile el año 2018[9] y la sustracción masiva de claves únicas e identificación biométrica en el Servicio de Registro Civil e Identificación el año 2020[10].

Para enfrentar este escenario, gobierno, instituciones públicas y privadas, universidades y centros de estudios han desarrollado distintas iniciativas las que, a pesar de los esfuerzos, siguen siendo insuficientes. Aunque pareciera que el campo de la ciberseguridad estaría reservado solo para los especialistas, dada su complejidad técnica, esta visión no es acertada, debido a que las ciberamenazas son preocupación en toda la cadena y amplitud de los ecosistemas digitales. En consecuencia, la robustez de los sistemas será tan fuerte como su eslabón más débil, y este es, en mayor medida, "el usuario".

Consecuente con lo anterior, resulta

[5] Cybersecurity & Infrastructure Security Agency, "Alert (AA21-042A) Compromise of U.S. Water Treatment Facility", US Department of Homeland Security, https://us-cert.cisa.gov/ncas/alerts/aa21-042a

[6] El *ransomware* es un tipo de ciberataque que busca encriptar los datos de la víctima y cobrar una recompensa por su recuperación. Para esta y otras definiciones de uso común, revisar glosario de algunos términos adjunto a este artículo.

[7] Wilner, Alex S, "US Cyber deterrence: Practice Guiding Theory", en *Journal of Strategic Studies*, no. 43 (2020), https://www.tandfonline.com/doi/abs/10.1080/01402390.2018.1563779?journalCode=fjss20 (Consultado el 28 de septiembre de 2021)

[8] Fortinet, Threat Intelligence Insider, Regional Executive Summary, Q2-2021, https://www.fortiguardthreatinsider.com/es/bulletin/Q2-2021.

[9] Artículo publicado en el diario El Mercurio, Santiago, el 9 de junio de 2018.
Ver
https://www.emol.com/noticias/Economia/2018/06/09/909234/Banco-de-Chile-confirma-que-ataque-informatico-de-mayo-robo-US-10-millones.html.

[10] Artículo publicado en el diario La Tercera, Santiago, el 15 de octubre de 2020.
Ver:
https://www.latercera.com/nacional/noticia/hackeo-a-gobierno-digital-obliga-a-iniciar-proceso-de-actualizacion-de-la-clave-unica/M4PXICHSKFFV3NFTDOBOFYWDBI/

conveniente que desde los escalones más básicos se comprenda la importancia de estas materias y se dominen algunos conocimientos que permitirían prevenir acciones externas; muchas veces facilitadas por ignorancia, errores, pasividad o incluso indolencia de usuarios de distintas redes y plataformas.

El presente texto abordará inicialmente algunas ideas y conceptos que, se estima, facilitarán la comprensión del fenómeno, comenzando con identificar la relación entre seguridad y ciberseguridad. Del mismo modo, se indagará sobre cómo afectan las acciones en el ciberespacio y de qué manera podríamos enfrentarlas para evitar o disminuir sus efectos. Finalmente, se plantearán algunas ideas sobre los desafíos que como país debemos hacer frente en el futuro inmediato, y así mejorar las condiciones de seguridad, en general, y de ciberseguridad, en particular. Debe entenderse que este trabajo no tiene un carácter técnico ni persigue un fin doctrinario, sino más bien, solo pretende entregar antecedentes básicos para comprender el fenómeno y contar con un conocimiento general.

SOBRE LA CIBERSEGURIDAD

La situación de seguridad internacional evoluciona con la humanidad. Lo expresado en esta afirmación se ha acelerado después de la Segunda Guerra Mundial y, particularmente, después del término de la Guerra Fría. A las amenazas tradicionales representadas por otros estados y su poder militar, se han agregado la proliferación de otros agentes no estatales, lo que ha modificado el abanico de amenazas a la seguridad. De la misma manera, el enfoque de la seguridad ha cambiado. En 1994, la publicación del "Human Development Report" por parte del Programa para el Desarrollo de las Naciones Unidas (PNUD), incluyó el concepto de "seguridad humana". Si bien no fueron necesariamente los creadores de la categoría, dicho reporte significó un factor relevante para visibilizar otras amenazas. Por un lado, el informe criticaba lo que denominaba una visión acotada de la seguridad, que se circunscribía a aspectos territoriales ante amenazas externas o a asuntos referidos a intereses nacionales por parte de los Estados. Por otro, se amplió la visión para atender otros problemas de seguridad que afectan a las personas, especialmente en países con bajos niveles de desarrollo, donde se reconoce la necesidad de "protección contra enfermedades, hambruna, desempleo, crimen, conflictos sociales, represión política y riesgos medioambientales"[11].

Desde el término de la Segunda Guerra Mundial en 1945, tres cuartas partes de los conflictos armados no han sido de carácter interestatal, vale decir, se trata de violencia política al interior de los Estados, y las muertes totalizadas en el mismo período por guerras entre países equivalen a las producidas por conflictos internos solo desde 1980[12]. Dan Caldwell y Robert E. Williams en 2006 ejemplificaban el cambio en la agenda de seguridad planteando que la mayor parte de los más de seis billones y medio de seres humanos, de aquel entonces, estaban inseguros por razones distintas a las armas de

[11] Programa para el Desarrollo de las Naciones Unidas (UNDP), "Human Development Report", (Nueva York: Naciones Unidas, 1994) 22. Ver en http://hdr.undp.org/sites/default/files/reports/255/hdr_1994_en_complete_nostats.pdf

[12] Colin H. Kahl, *States, Scarcity and Civil Strife in the Developing World* (Princeton, NJ: Princeton University Press, 2006), 1-2.

destrucción masiva; 42 millones de personas estaban infectadas con VIH y, ante la ausencia de tratamiento médico, la mayoría seguramente moriría; cada año se estimaba que más de 11 millones de niños menores de 5 años fallecería, la mitad a causa de la desnutrición y hambruna; entre 600.000 y 4.000.000 personas era traficadas cada año, la mayoría mujeres y niños. Todo esto sin considerar conflictos civiles y étnicos, pues en Sudán, alrededor de 2.000.000 de personas han sido asesinadas desde 1993; en Ruanda, hubo del orden de 750.000 muertos en alrededor de 100 días de genocidio; mientras que en la República Democrática del Congo, alrededor de 3,8 millones de seres humanos han muerto a causa de la guerra civil desde 1998[13]. Con todo, lo que se pretende mostrar es que los problemas de seguridad actuales más recurrentes y persistentes no se relacionan con el fenómeno de la guerra en su concepción tradicional, sino que con otras amenazas.

Si bien el escenario ha cambiado, resulta más preciso indicar que se ha ampliado y han variado algunas prioridades, pues las grandes potencias siguen con un enfoque más bien realista de la seguridad, privilegiando sus propios intereses. No obstante, esta nueva agenda ha evidenciado dos elementos. Por un lado, que la seguridad tiene características multidimensionales y el reporte del PNUD lo dejó de manifiesto, y por otro lado, que el foco de la seguridad dejó de ser exclusivo de los Estados y abordó una gama muy amplia de amenazas para las personas.

Paralelamente, la evolución de la tecnología en los últimos 40 años ha sido vertiginosa. La aparición y explosión de internet, así como de dispositivos de comunicaciones y computadores, cambiaron el panorama y la vida de las personas, instituciones y gobiernos, facilitando el quehacer de los individuos y, al mismo tiempo, haciéndolos cada vez más dependientes de la tecnología. Esta dependencia se ha multiplicado significativamente durante el último año, derivado de las necesidades y demandas producto de la pandemia del coronavirus, lo que ha obligado a desarrollar trabajo remoto, conferencias y reuniones a distancia, sin mencionar el explosivo incremento del comercio *online*. Las características distintivas de internet, tales como su universalidad (está abierta a todos), globalidad (se puede acceder desde cualquier punto del planeta), permanencia (funciona 24/7) e inmediatez, la convierten en una herramienta tremendamente útil y poderosa, pero al mismo tiempo genera problemas, pues estas mismas características dificultan su regulación, el control, la persecución de responsabilidades en la red y facilitan el actuar anónimo.

En consecuencia, al identificarse riesgos y amenazas provenientes del ciberespacio, tanto para gobiernos, instituciones y las personas, es que se considera que el ciberespacio, o quinto dominio[14], constituye una fuente de amenazas para la seguridad. De esta manera, el concepto de ciberseguridad es una condición que se posee para disminuir riesgos y responder a las amenazas contra el ecosistema digital nacional. Al respecto, no hay una sola definición de ciberseguridad

[13] Dan Caldwell and Robert E. Williams, Jr., *Seeking Security in an Insecure World,* (Lanham, MD: Rowman & Littlefield Publishers, 2006) p. 2.

[14] Se identifica a los dominios donde se desarrollan las operaciones militares tradicionales, tales como: tierra, mar, aire y espacio. En este sentido, se reconoce al ciberespacio como un quinto dominio.

acordada académicamente, sino que existen distintas acepciones que se encuentran disponibles en leyes, estándares, marcos de trabajo y artículos. Entre los aspectos más o menos comunes, se le reconoce como la condición, estado, prevención, proceso o habilidad, tener la finalidad de asegurar los sistemas de información y protegerlos de los riesgos y amenazas en el ciberespacio.

Así como en el ámbito de las relaciones internacionales existen los conceptos de seguridad y de guerra, en el plano del ciberespacio están sus análogos ciberseguridad y ciberguerra. Si bien estos conceptos están acuñados y claramente definidos para el ámbito de la seguridad estatal, también es cierto que su uso no se limita a las relaciones internacionales. En efecto, se suele utilizar estos términos para demostrar situaciones de conflicto entre distintos entes, por lo que seguridad/ciberseguridad y guerra/ciberguerra, así como están asociados a los Estados, aunque también se emplean en el uso general para abordar otros niveles en que se experimentan conflictos, como son el de organizaciones y corporaciones públicas y privadas, e incluso a nivel de los individuos.

Como se evidencia, existen múltiples términos y definiciones en relación a la ciberseguridad, por lo que para efectos de este trabajo, se incluirán aquellos que se estiman son más comunes y recurrentes, los que podrían ayudar a entender de mejor manera esta temática. A continuación, se presenta un glosario con estos términos:

GLOSARIO DE TÉRMINOS DE USO FRECUENTE	
Antivirus (**)	Se trata de un *software* diseñado para prevenir, detectar y eliminar virus u otros tipos de *malware* de un computador.
Ataque con fuerza bruta (*)	Método de acceso a un dispositivo bloqueado por medio del intento de múltiples combinaciones de contraseñas alfanuméricas.
Backdoor (*)	Forma indocumentada de acceder al sistema informático. Una puerta trasera es un riesgo potencial para la seguridad.
Bad toolbars/ Barras maliciosas (**)	Herramientas de *malware* que se instalan sin conocimiento del usuario y que se transmiten ocultas en programas no deseados.
Bombas (lógicas y de tiempo) (**)	Virus cuya finalidad es destruir los datos de un ordenador o causar otros daños. Entre otros efectos, pueden inundar la dirección del correo electrónico de la víctima con una enorme cantidad de *spam,* u otros mensajes no deseados, u ocultar la fuente de los mensajes recibidos.
Botnet (*)	La palabra "botnet" se forma a partir de las palabras "robot" y "red". Los ciberdelincuentes utilizan virus troyanos especiales para violar la seguridad de las computadoras de varios usuarios, tomar el control de cada computadora y organizar todas las máquinas infectadas en una red de "bots" que el delincuente puede administrar de forma remota.
Carding (**)	Programas creados específicamente para realizar fraudes con tarjetas de crédito. Puede monitorear las actividades comerciales en internet y rastrear la información de la tarjeta.
Ciberataque (^)	Una operación o actividad en el ciberespacio, ya sea ofensiva o defensiva, que se espera que cause heridas o muerte a personas, o daño o destrucción de objetos.
Ciberdefensa (^)	Conjunto de principios, políticas e instrumentos destinados a proteger el ciberespacio desde un punto de vista de la defensa nacional y estratégico-militar.
Ciberespacio (^)	Conjunto de infraestructuras físicas, lógicas e interacciones que ahí se producen.
Ciberguerra (**)	Dimensión cibernética de un conflicto armado interestatal o intraestatal. Sus protagonistas pueden ser estatales y no estatales.
Ciberseguridad (^)	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.
Cookie (**)	Pequeño archivo de texto en el que un sitio web recoge información, como por ejemplo, el nombre y la contraseña del usuario. Agiliza la navegación en el sitio, pero su uso es controvertido, ya que pone en riesgo la privacidad del usuario.
DDoS (Distributed	Técnica de denegación de servicio que utiliza numerosos *hosts* para

Denial of Service) (*)	realizar el ataque.
Gusano/*Worn* (Write-Once Read-Many) (**)	Programa que se replica a sí mismo hasta ocupar toda la memoria. Es un virus que suele llegar a través del correo electrónico o del chat en forma de archivo adjunto. Aunque no infecta otros archivos, consigue ocupar el espacio disponible de la memoria o el disco duro y puede acabar colapsando el acceso a los archivos o crear nuevos. Es difícil de detectar.
Hacker (**)	Pirata informático. Programador con experiencia que accede a otras computadoras en forma subrepticia.
Infraestructura de la información (^)	Aquella infraestructura conformada por las personas, procesos, procedimientos, herramientas, instalaciones y tecnologías que soportan la creación, uso, transporte, almacenamiento y destrucción de la información.
Infraestructuras críticas de la información (^)	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 seguridad, la salud, el bienestar de los ciudadanos y el efectivo funcionamiento del Estado y del sector privado.
Malware (*)	Un programa que se inserta en un sistema, generalmente de manera encubierta, con la intención de comprometer la confidencialidad, la integridad o la disponibilidad de los datos, las aplicaciones o el sistema operativo de la víctima, o de molestar o interrumpir de alguna otra manera a la víctima. Se trata de códigos maliciosos, como virus, gusano, caballo de troya, etc.
Operaciones en el ciberespacio (*)	*The employment of cyberspace capabilities where the primary purpose is to achieve objectives in or through cyberspace.*
Pharming (**)	Otra forma con que los *hackers* redirigen a los usuarios a sitios web falsos a través de un virus inoculado por medio de un correo electrónico que contamina el Sistema de Nombres de Dominio, SND local del usuario.
Phishing (**)	Suplantador de identidad. El "*phifer*" envía *e-mails* falsificados que simulan provenir de sitios legítimos de bancos o de sistemas como eBay o PayPal. Si la víctima "muerde el anzuelo" introduciendo sus datos personales u otros como tarjeta de crédito, el pirata puede acceder a ellos.
Proxy (**)	Cortafuegos capaz de bloquear un ataque y recuperar una conexión entre dos terminales. Tiene la capacidad de ocultar a un atacante de un usuario, o viceversa.
PUP (Potencially Unwanted Program) (**)	Es un programa que rechaza mensajes, aunque no sean abiertamente maliciosos o lesivos para el computador.
Ransomware (*)	El *ransomware* es un tipo de *malware* que cifra los datos de una organización y exige un pago como condición para restaurar el acceso a esos datos. En algunos casos, el *ransomware* también puede robar la información de una organización y exigir un pago adicional a cambio de

	no revelar la información a las autoridades, la competencia o el público. Los ataques de *ransomware* se dirigen a los datos o la infraestructura crítica de las organizaciones, interrumpiendo o deteniendo las operaciones.
Spam (**)	Correo electrónico no deseado. Las herramientas para propagar este tipo de mensajes pueden recopilar direcciones de *e-mail* desde varios sitios web y difundir programas maliciosos.
Spyware (*)	*Software* que se instala secreta o subrepticiamente en un sistema de información para recopilar información sobre personas u organizaciones sin su conocimiento; un tipo de código malicioso.
Trackware (**)	Aplicación de *software* capaz de capturar datos o información personal a través del navegador.
Troyano o caballo de troya (*)	Programa informático que parece tener una función útil, pero también tiene una función oculta y potencialmente maliciosa que evade los mecanismos de seguridad, a veces mediante la explotación de autorizaciones legítimas de una entidad del sistema que invoca el programa.
Virus (**)	Programas que pueden crear, destruir o infectar archivos (o parte de ellos), modificar direcciones, consumir memoria y provocar disfunciones en el computador.
(*) Para la definición de estos términos, se utilizó el glosario disponible en el Centro de Recursos de Seguridad Computacional del "National Institute of Standards and Technology", perteneciente al gobierno de Estados Unidos. Para acceder, ir a https://csrc.nist.gov/glossary.	
(**) La definición de estos términos se obtuvo de la revista Vanguardia, Nº 54, La Vanguardia Ediciones, Barcelona, ENE/MAR 2015.	
(^) Definiciones obtenidos del Glosario de términos incluidos en la "Política de Ciberdefensa" del Estado de Chile, disponible en https://www.diariooficial.interior.gob.cl/publicaciones/2018/03/09/42003/01/1363153.pdf	

CÓMO NOS AFECTA LA CIBERSEGURIDAD

A diferencia de otras amenazas en que el Estado es quien realiza el esfuerzo principal para neutralizarlas, u otras donde el riesgo es geográficamente localizado, dado el alcance y nivel de penetración del ciberespacio, la participación del Estado y de las entidades públicas y privadas, así como de todas las personas, resulta trascendental, pues incluso el menos "conectado" de los individuos está sujeto a riesgos a la seguridad de su identidad y datos personales. De esta manera, es posible identificar que la ciberseguridad se expresa en tres niveles: Estado-gobierno, instituciones u organizaciones públicas y privadas, y las personas.

Si bien las condiciones, énfasis y otros aspectos pueden variar entre un nivel y otro, lo cierto es que, por las características del ciberespacio, las distintas amenazas pueden afectar a los tres niveles. A nivel del Estado, se acepta que las amenazas están representadas principalmente por otros Estados, así como organizaciones criminales locales y transnacionales, pero no están ajenos a la acción de *hackers* aislados. Resulta fundamental considerar que la ejecución de operaciones en el ciberespacio presenta muy bajas barreras de entrada, pues no es difícil conseguir el conocimiento y equipamiento para ejecutarlas. Un problema que enfrentan particularmente los Estados es que, por las características del ciberespacio, se plantea una gran dificultad para identificar el origen de las acciones cometidas en su contra, es decir, lograr individualizar al autor y luego atribuir la responsabilidad correspondiente y la ubicación geográfica específica. Además, las características de las capacidades de ciberdefensa son mayormente de carácter ofensivo, lo que las hacen aún más desestabilizadoras.

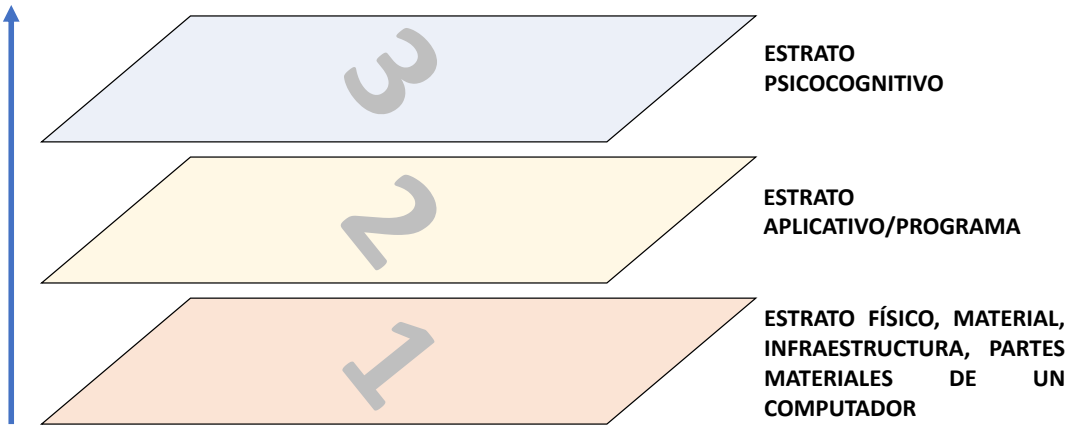
Con lo anterior, no es extraño enfrentarnos a un escenario de "dilema de seguridad", o de ciberseguridad, con las consecuentes "carreras ciberarmamentistas". Esta combinación de dificultad de atribuir un ataque también dificulta justificar una represalia. Ahora, si se lograra identificar al atacante y este resulta ser otro Estado, el Estado víctima podría invocar la legítima defensa y actuar en consecuencia; sin embargo, siguiendo en el plano de la seguridad internacional, surge la necesidad de solucionar la condicionante de proporcionalidad, lo que complejiza aún más la situación.

Para hacer frente a este tipo de amenazas, Estados Unidos creó lo que denominó "Cyber Command" o Cibercomando. Esta unidad, que inicialmente desde su formación en 2010 dependía del Comando Estratégico, pasó a constituirse como un comando independiente en 2018, al igual que los que se conocen como "Unified Combatant Command". Del mismo modo, después de sufrir el ataque del virus "Stuxnet" contra las plantas de enriquecimiento de uranio, Irán inició su propio programa de ciberseguridad. Dos años después habría ejecutado ataques a la compañía de petróleos Saudi Aramco y, más tarde, a bancos estadounidenses. Además, se presume que Irán fue responsable de múltiples ciberataques a instalaciones de tratamiento de aguas en Israel, entre abril y julio de 2020. Estos ejemplos demuestran la relevancia que las principales potencias asignan a la ciberseguridad y los medios que destinan para estos fines, creando organizaciones especiales para su desarrollo,

generando lo que se podría identificar como arsenales con capacidades de ataque en el ciberespacio[1].

Se reconoce que el uso del ciberespacio con fines ofensivos (ataques) puede darse en tres estratos o ámbitos: el estrato cognitivo, el estrato aplicativo y el estrato físico[2]. Los ejemplos de ataques con medios que emplean el ciberespacio son numerosos. Dentro de los más relevantes, además de los expuestos, se puede mencionar también los ciberataques masivos de que fueron objeto Estonia en 2007 y Georgia en 2008[3]. Pero precisando mejor el caso de "Stuxnet", sabemos que se trató de un "gusano" que afectó gravemente instalaciones del programa nuclear iraní de Natanz. Conforme a lo que se conoce, este programa malicioso se creó para infectar y dañar el funcionamiento de equipamiento industrial. La evidencia disponible sugiere que "Stuxnet" fue diseñado para perjudicar, particularmente, a las centrífugas empleadas en la obtención de uranio enriquecido, insumo fundamental para el desarrollo de armas nucleares. Del mismo modo, se presume que esta ciberarma fue efectiva en su propósito, pues se estima que logró infectar los sistemas objetivos, mantenerse oculto y afectar los componentes de la forma prevista[4].

REPRESENTACIÓN DE LOS TRES ESTRATOS DEL ESPACIO CIBERNÉTICO



FUENTE: Cuadro extraído de la Revista "Vanguardia", Nº54, La Vanguardia Ediciones, Barcelona, ENE/MAR 2015.

[1] Para una mejor idea de las capacidades que se pueden lograr, se sugiere revisar el informe de Oficina del Director Nacional de Inteligencia, "Annual Threat Assessment of the Intelligence Community" (Estados Unidos,) de abril de 2021, disponible en: https://www.dni.gov/files/ODNI/documents/assessments/ATA-2021-Unclassified-Report.pdf; así como el artículo de Jeffrey Carr "La capacidad de ciberguerra de un país", publicado en el volumen Nº 54 de la revista Vanguardia, de enero/marzo de 2015.

[2] Ventre, D. "Evolución de la guerra desde hace un siglo: aparición de la ciberguerra", en *Vanguardia*, Nº 54 (2015): 24.

[3] Rid, T. "Cyber War Will Not Take Place," en *Journal of Strategic Studies* N° 35 (London: Routledge, 2012): 5-32.

[4] Shakarian, P. "Stuxnet: Cyberwar Revolution in Military Affairs.", en *Small Wars Journal*, (2011), https://smallwarsjournal.com/jrnl/art/stuxnet-cyberwar-revolution-in-military-affairs.

ASOCIACIÓN DE CADA ESTRATO A SUS PROTAGONISTAS Y ACCIONES

		CARACTERÍSTICAS	FORMA DE ATAQUES POSIBLES CONTRA EL ESTRATO
ESTRATO 3	**ESTRATO ALTO**	**Estrato cognitivo**.	Modificar la visualización de los ordenadores, desfigurar los sitios, introducir mensajes modificadores de las percepciones, realizar operaciones de propaganda, piratería informática cognitiva.
ESTRATO 2	**ESTRATO MEDIANO**	**Estrato aplicativo**: programas, aplicaciones, estrato de los bits, del código, de los protocolos, de los datos.	Ataques por código: piratería informática, propagación de virus…
ESTRATO 1	**ESTRATO BAJO**	**Estrato físico**: partes materiales del computador, cables, redes, satélites infraestructura conectada.	Cortar cables submarinos, destruir o desviar satélites de tu trayectoria, bombardear edificios de servidores e infraestructura de comunicación, uso de bombas de pulso electromagnético.

FUENTE: Cuadro extraído de la Revista "Vanguardia", Nº54, La Vanguardia Ediciones, Barcelona, ENE/MAR 2015.

Como ha quedado en evidencia, las amenazas en el ciberespacio son de diversa índole y pueden provenir de distintos orígenes, desde actores estatales y no estatales hasta grupos individuales o incluso ser causadas por desastres naturales. Con la intención de revisar cómo estas amenazas pueden actuar sobre aquellos atributos que la ciberseguridad busca proteger, es que en los siguientes párrafos estas se analizarán desde la perspectiva de los principios de la tríada "CIA", es decir, confidencialidad, integridad y disponibilidad (por sus siglas en inglés *confidentiality, integrity y availability*). Esta clasificación permite comprender tanto los propósitos de los actores que amenazan el ciberespacio, como generar ideas de medidas de mitigación.

OBJETIVOS	FUENTES DE RIESGO Y TIPOS DE AMENAZA		
	ESTADOS	ACTORES NO ESTATALES	OTRAS FUENTES
- ESTADOS - ORGANIZACIONES PÚBLICAS - CORPORACIONES PRIVADAS - INDIVIDUOS	• Ciberguerra • Cibersubversión • Cibersabotaje • Ciberespionaje	• Cibersabotaje • Cibercrimen • Ciberespionaje • Cibersubversión • Ciberterrorismo	• Accidentes por fallas o mala operación. • Desastres naturales.

Amenazas a la confidencialidad

La confidencialidad en ciberseguridad se puede definir como las medidas ejecutadas para asegurar que el acceso a la información secreta de datos, objetos o recursos se realice de manera controlada y solamente por quienes tengan la autorización para ello. De manera general, para mantener la confidencialidad en una red, los datos deben ser protegidos del acceso no autorizado, uso o su publicación, y en este contexto, su protección se realiza durante su almacenamiento, tránsito y procesamiento[5].

Los ataques más comunes que buscan vulnerar la confidencialidad están dados por una diversidad de acciones; sin embargo, se pueden mencionar como las más importantes y comunes: ingeniería social, *phishing*, *shoulder surfing*, escalamiento de privilegios, y ataques de fuerza bruta a las contraseñas. Estas acciones que se realizan por quienes quieren obtener acceso a información restringida, tienen un componente en común importante y es que en su gran mayoría son facilitados por malas prácticas de los usuarios de los sistemas, lo que finalmente radica en una grave vulnerabilidad a toda la organización.

La implementación de un control de acceso robusto es la práctica más recomendada para aumentar los niveles de seguridad a la confidencialidad, dentro de los cuales se recomienda normalmente emplear autenticación multifactor, es decir, de más de un factor de autenticación[6]. Sin embargo, estas prácticas se ven debilitadas por conductas de los usuarios; por ejemplo, no emplear contraseñas robustas, como ocurrió en el caso mencionado de la planta de tratamiento de aguas en el estado de Florida, EE.UU.

También existen herramientas que emplean los especialistas en ciberseguridad para aumentar el grado de confidencialidad de la información almacenada. Algunos ejemplos de acciones recomendadas son: el empleo de criptografía para el manejo de los datos almacenados y en tránsito; crear una estructura de acceso a la información segura y robusta, y desarrollar aplicaciones y programas computacionales que empleen las buenas prácticas recomendadas y que son actualizadas en diversos sitios de manera permanente, entre otros. Estas herramientas deberían ser adoptadas por toda aquella institución u organización estatal y no estatal que requiera proteger su información. En algunas oportunidades, esto no es una opción, sino más bien una obligación; está determinado por la legislación del país donde se esté trabajando, como en el caso de la protección de los datos personales y de salud de las personas.

Amenazas a la integridad

Para asegurar la integridad de los sistemas de información se debe entender que este elemento tiene un importante grado de dependencia de la confidencialidad y requiere

[5] Chapple, M.; Stewart, J. M. and Gibson, D. *Certified Information Systems Security Professional.* (Indianapolis, Indiana: Sybex), 4.

[6] Un factor de autenticación puede ser algo que se sabe (una contraseña, por ejemplo), algo que se tiene (una tarjeta de coordenadas) y/o algo que se es (identificación biométrica, como la huella digital).

de medidas integrales para que esta sea asegurada. En consecuencia, la integridad dice relación con la capacidad de "proteger la información de su modificación o destrucción no apropiada e incluye asegurar el no-repudio[7] y la autenticidad"[8].

En este contexto, la pérdida de integridad no se limitaría solo a los ataques intencionales hacia esta, sino que además puede producirse producto de errores cometidos por cualquier usuario. Algunos de los ataques a la integridad que pueden ser realizados son: virus, bombas lógicas, acceso no autorizado a los datos, errores en la programación de códigos y aplicaciones, modificaciones maliciosas de datos, entre otros[9]. Los ataques de estas características, con la intención de violar la integridad, normalmente pueden ser enfrentados con herramientas tan sencillas como emplear contraseñas robustas, no abrir correos desconocidos, solo emplear dispositivos de almacenamiento que provengan de fuentes confiables y, de ser necesario, asegurar los lugares físicos donde se administra la información, por nombrar algunas.

Amenazas a la disponibilidad

La disponibilidad dice relación con asegurar un acceso oportuno y confiable a los recursos y datos por parte del personal que se encuentre autorizado, vale decir, tener los recursos en condiciones de ser empleados cuando el usuario lo requiera. Lo anterior involucra la necesidad de tener los medios disponibles y que, a su vez, sean capaces de recuperarse de una manera rápida y segura de las interrupciones que puedan haberse generado. El gran problema en este caso es la gran cantidad de servicios que actualmente deben mantenerse operando para que una red de computadores funcione, tales como: servidores, *routers*, *switch*, *firewalls*, diversos terminales, etc.

En consecuencia, las distintas amenazas que afectan la disponibilidad son: fallas de equipos, errores en los programas y problemas ambientales que pueden afectar los sistemas computacionales. Asimismo, también existen ataques por parte de agentes externos que se enfocan en limitar o negar la accesibilidad a los sistemas, como son: los ataques de denegación de servicio (DoS); destrucción física de equipos, y la interrupción de las comunicaciones, ya sea por medio de cortes físicos o lógicos de las redes, entre otros[10].

Finalmente, son las amenazas a la disponibilidad de los servicios las que principalmente exigen tener planes de contingencia para poder asegurar la continuidad de las operaciones y la supervivencia de los servicios, ante la ocurrencia de un incidente. Este es un trabajo integral donde deben asumir responsabilidades todos los integrantes de la organización y no solo debe constituir una preocupación de los especialistas en ciberseguridad.

---

[7] El "no-repudio" dice relación con que un sujeto o actividad, o quien haya causado un evento específico, no sea capaz de negar su autoría (Chapple, Stewart y Gibson 2018).

[8] Centro de Recursos de Seguridad Computacional, "Glossary", NIST/National Institute of Standars and Technology, https://csrc.nist.gov/glossary/term/integrity

[9] Chapple *et al.*, "*Certified Information Systems Security Professional*". 5.

[10] Chapple *et al.*, "*Certified Information Systems Security Professional*". 6

QUÉ PODEMOS HACER

Tal como se ha presentado, los problemas de ciberseguridad exigen una aproximación global e integrada de todos los actores, cada cual a su nivel y conforme a sus capacidades. En términos generales, se estima que cualquier aproximación debería abordar tres áreas: arquitectura / organización, tecnología / equipamiento y educación.

Respecto del Estado, este es el principal responsable de diseñar una arquitectura de ciberseguridad que entregue la organización, políticas, regulación, doctrina y definición de roles y responsabilidades a todo el espectro de entidades involucradas, particularmente bajo una mirada que comprenda a todo el Estado. Dicha arquitectura debe proveer, al menos, las políticas sectoriales, una estructura y organización acorde al desafío, tareas y responsabilidades de los entes comprometidos, además de doctrina común para enfrentar estas amenazas.

En este caso, el Estado de Chile ha realizado algunos avances orientados a generar y robustecer su marco regulatorio para permitir enfrentar el problema de la ciberseguridad desde una visión integral y con una dirección centralizada. A modo de ejemplo, recientemente el presidente de la República, Sebastián Piñera, anunció el trámite de un proyecto de ley para la creación de una agencia nacional de ciberseguridad[11]. Por otra parte, el trabajo estatal ha permitido elaborar documentos relevantes, como son la Política Nacional de Ciberseguridad[12], la Política de Ciberdefensa[13] y la Política de Defensa, todas difundidas y vigentes.

[11] Noticia publicada en el sitio del Equipo de Respuesta ante Incidentes de Seguridad Informática del Ministerio del Interior y Seguridad Pública de Chile. Ver: https://www.csirt.gob.cl/noticias/presidente-pinera-anuncia-proyecto-de-ley-que-crea-la-agencia-nacional-de-ciberseguridad/

[12] Gobierno de Chile, "Política de Ciberseguridad", Santiago, 2017. Ver: https://biblioteca.digital.gob.cl/bitstream/handle/123456789/1158/Pol%C3%ADtica%20de%20ciberseguridad.pdf?sequence=1&isAllowed=y

[13] Gobierno de Chile, "Política de Ciberdefensa", Santiago, 2017. Ver: https://www.diariooficial.interior.gob.cl/publicaciones/2018/03/09/42003/01/1363153.pdf

POLÍTICA NACIONAL DE CIBERSEGURIDAD

Se elaboró para tener efecto entre los años 2017 y 2022. Su propósito es "alcanzar el objetivo de contar con un ciberespacio libre, abierto, seguro y resiliente" y se fundamenta en la necesidad de "resguardar la seguridad de las personas en el ciberespacio", "proteger la seguridad del país", "promover la colaboración y coordinación entre instituciones" y "gestionar los riesgos del ciberespacio".

Esta política propuso una hoja de ruta con dos ejes centrales que buscaban disminuir los riesgos en el ciberespacio y pavimentar el camino para robustecer la estructura de ciberseguridad en Chile: tener una política de Estado con la visión al 2022, y una agenda de medidas específicas para ser implementadas entre los años 2017 y 2018.

Dentro de las medidas que se adoptan con esta política se encuentra: 1) La creación de una Agenda Digital 2020, la cual fue levantada y en este momento se encuentra en actualización por la actual administración del Estado; 2) Se dispone la preparación y publicación de una Política Nacional de Ciberdefensa, la cual fue publicada y será explicada a continuación, y 3) Se dispone la creación de una Política Internacional para el Ciberespacio, lo cual debe ser llevada a cabo por la Unidad de Ciberseguridad del Ministerio de Relaciones Exteriores.

Los objetivos planteados por esta política permiten identificar las líneas de acción y desafíos buscados:

- El país contará con una infraestructura de información robusta y resiliente, preparada para resistir y recuperarse de incidentes de ciberseguridad, bajo una óptica de gestión de riesgos.
- El Estado velará por los derechos de las personas en el ciberespacio.
- Chile desarrollará una cultura de la ciberseguridad en torno a la educación, buenas prácticas y responsabilidad en el manejo de tecnologías digitales.
- El país establecerá relaciones de cooperación en ciberseguridad con otros actores y participará activamente en foros y discusiones internacionales.
- El país promoverá el desarrollo de una industria de la ciberseguridad que sirva a sus objetivos estratégicos.

No es objeto de este artículo evaluar el grado de cumplimiento y los efectos logrados por esta política. Sin embargo, pareciera que a cuatro años de su implementación y a la falta de solo un año para la concreción del plazo autoimpuesto, aún hay áreas por desarrollar y trabajar en beneficio del cumplimiento de los objetivos.

POLÍTICA DE CIBERDEFENSA

Esta política fue publicada en el Diario Oficial de Chile el 9 de noviembre de 2017, como parte de las medidas impuestas por la Política Nacional de Ciberseguridad.

Así, esta política "constituye una respuesta a los nuevos riesgos y amenazas que el ciberespacio genera para las capacidades de la Defensa Nacional, las cuales incluyen, entre otros elementos, la información, la infraestructura y las operaciones de defensa" (Ministerio de Defensa Nacional 2018), donde además busca fijar los objetivos que deberán ser cumplidos hasta el año 2022.

La Política de Ciberdefensa forma parte de la Política de Defensa Nacional, siendo parte integral de los objetivos y principios de esta. Además, se relaciona con la Agenda Digital 2020, con la Política Nacional de Ciberseguridad y con la Política Internacional para el Ciberespacio.

Esta política identifica cinco principios:

- La Política de Ciberdefensa forma parte del esfuerzo del Estado por ofrecer seguridad a todos los habitantes, generando las condiciones para que puedan hacer un uso pacífico, equitativo y seguro del ciberespacio, y estableciendo tanto las regulaciones para el ejercicio de sus derechos como el marco de conducta para que se lleven a cabo dichas actividades.
- La Política de Ciberdefensa es parte de la Política de Defensa Nacional y forma parte integral de los objetivos y principios de estas.
- La Política de Ciberdefensa requiere de una estrecha colaboración con otros actores de la institucionalidad del Estado.
- La Política de Ciberdefensa requiere para su eficacia de una intensa cooperación con otros actores equivalentes en el plano internacional, preservándose en lo que corresponda a la seguridad operacional de las capacidades del país.
- La Política de Ciberdefensa reconoce que el desarrollo tecnológico en materia de tecnologías de la información es decisivo y crítico para el desarrollo y empleo de las capacidades, tanto en la dimensión digital como cinética.

Este documento establece políticas sobre el empleo de los medios de ciberdefensa; para la cooperación internacional y promoción de la transparencia y la confianza entre los Estados, y para el desarrollo de capacidades.

Dentro de los medios que identifica la Política de Ciberdefensa, se destacan las subsecretarías de Defensa y para las Fuerzas Armadas, el Estado Mayor Conjunto y las Fuerzas Armadas (Ejército, Armada y Fuerza Aérea).

Se establece que esta política debe ser revisada cada cuatro años o cuando las circunstancias lo exijan.

Existen dos aspectos importantes a destacar que están incluidos en este documento. El primero dice relación con que al considerar un ataque en el ciberespacio tan dañino como un ataque armado, se puede hacer uso de los medios que se estimen apropiados para responder a esta en concordancia con el artículo 51 de la Carta de Naciones Unidas, en ejercicio de la legítima defensa. El otro se refiere a que el Estado de Chile protegerá su infraestructura crítica de la información, ejerciendo soberanía sobre aquellas redes y recursos digitales, lo que tiene relación con las amenazas mencionadas anteriormente.

En cuanto a instituciones públicas y privadas, junto con participar en el esfuerzo nacional de ciberseguridad, deben establecer sus propias políticas y planes para enfrentar ciberamenazas. Junto con ello, la incorporación de tecnología resulta fundamental, tanto en equipamiento material (*hardware*) como en relación con programas especializados en ciberseguridad (*software*). Esto se debe complementar con instancias de capacitación y entrenamiento a sus colaboradores e incluso a clientes, todo con la intención de minimizar al máximo los riesgos que se derivan de los usuarios. Amenazas como el espionaje industrial y la acción de crimen organizado son un gran riesgo a estas organizaciones. En este ámbito, aún queda mucho por hacer. Según el último "Security Report – Latinoamérica 2021" de ESET[14], elaborado sobre encuestas realizadas a cerca de 1.000 ejecutivos y representantes de empresas en 17 países de Latinoamérica para conocer el panorama de la seguridad corporativa en la región, se identificó que "para el 76% de los ejecutivos y responsables en la toma de decisiones, el presupuesto para el área de seguridad se mantuvo o se redujo con respecto a años anteriores, y el 81% aseguró que los recursos con los que cuentan para seguridad resultan insuficientes."

En el mismo orden de ideas, instituciones de educación y otros centros de pensamiento, tales como universidades y centros de estudios, deben continuar la investigación y el análisis de este ámbito y ofrecer instancias de perfeccionamiento. En el último tiempo se ha multiplicado la oferta de diplomados y posgrados especializados en temas relacionados con ciberseguridad, tecnologías de la información, *big data* y otros, lo que es un elemento positivo que va en la dirección correcta. La finalidad es entregar alternativas actualizadas, tanto a especialistas como al público en general.

Por parte de los individuos, el principal desafío es mantenerse actualizados y seguir las orientaciones que entregan autoridades y organizaciones. Informarse por canales confiables, no relajar medidas básicas de ciberseguridad y actuar responsablemente, ya sea en el ámbito particular o en su rol como integrante de un equipo de trabajo dentro de una organización.

Antes de finalizar esta sección, se estima necesario contextualizar algunos factores para no dejar una sensación exagerada de pesimismo sobre esta materia:

- Primero, se reconoce la creciente dependencia de Estados, organizaciones y personas en la tecnología y, por ende, un mayor riesgo a ser afectados; sin embargo, las personas tienden a sobrerreaccionar ante las amenazas, especialmente en escenarios de alta incertidumbre, por lo que la sensación de vulnerabilidad percibida es mayor que el riesgo que realmente representa una amenaza, y lo relacionado con ciberseguridad no es ajeno a este comportamiento[15].

- Segundo, si bien las operaciones en el ciberespacio y las ciberarmas pueden

[14] Welivesecurity - ESET, "Security Report, Latinoamérica 2021", ESET, https://www.welivesecurity.com/wp-content/uploads/2021/06/ESET-security-report-LATAM2021.pdf

[15] Esta situación acarrea la "securitización" del fenómeno, vale decir, se termina levantando una mayor demanda por seguridad que la que es realmente necesaria.

estar disponibles o ser desarrolladas por una amplia gama de actores en el ciberespacio (gobiernos, crimen organizado, corporaciones privadas, grupos anarquistas e incluso ciberdelincuentes individuales), las principales amenazas directas para las personas no son letales (o tienen muy bajas posibilidades de serlo) y pueden ser neutralizadas con hábitos simples aplicados de manera responsable.

- Tercero, a pesar de que los Estados cuentan con importantes capacidades ofensivas y defensivas en el ámbito de la ciberseguridad, las mayores capacidades están radicadas en el sector privado, particularmente en países desarrollados.

- Cuarto, al menos por ahora, la amenaza de una ciberguerra no resulta tan real y apocalíptica como pareciera. Es cierto que las capacidades para realizar acciones en el ciberespacio han aumentado en cantidad y sofisticación, pudiendo llegar a causar graves daños; sin embargo, desde el punto de vista de la seguridad internacional y la ciberseguridad, dichas capacidades no son capaces de ocasionar los daños suficientes como para alcanzar la derrota de un Estado adversario, por lo que el uso coercitivo del ciberespacio todavía continúa siendo limitado para los fines bélicos y actúa, más bien, como complemento al empleo militar[16].

CONCLUSIONES Y DESAFÍOS

- La agenda de seguridad internacional ha transitado desde un enfoque único en los Estados y amenazas de carácter militar hacia un enfoque multidimensional, donde el Estado dejó de ser el único sujeto, adquiriendo importancia la seguridad humana. Este concepto de seguridad ampliada considera amenazas de distinta naturaleza, dentro de las cuales se encuentran las derivadas del uso del ciberespacio.

- La invención de internet, así como de dispositivos de comunicaciones y computadores, han facilitado las interacciones entre Estados, organizaciones y personas, pero, al mismo tiempo, la mayor dependencia en la tecnología incrementa el riesgo ante ciberamenazas. En este contexto, la ciberseguridad se relaciona con aquellas condiciones que se caracterizan por presentar menores riesgos y que permitan evitar o aminorar los efectos de las amenazas contra el ecosistema digital nacional.

- Dadas las características de las ciberamenazas, la ciberseguridad se presenta transversalmente en tres niveles: el Estado, organizaciones públicas y privadas, e individuos. Las implicancias de las acciones en el ciberespacio afectan a servicios públicos, manifestándose también en áreas como la defensa, industria, salud, sector financiero, *retail* y *e-commerce*, por lo que se debe trabajar

[16] Para abordar con mayor profundidad esta idea, se sugiere revisar los artículos publicados en la revista Vanguardia, edición Nº 54 de marzo de 2015.

en el establecimiento de un "ecosistema digital" robusto para la integración de soluciones y capacidades que vayan en concordancia con las necesidades de todo el país.

- Por las características del ciberespacio, las acciones que en él se realizan son muy difíciles de detectar en cuanto a su autoría y localización, dificultando acciones de respuesta y la persecución de los autores, ya sea dentro del territorio o en cualquier parte del mundo, lo que representa grandes desafíos para los Estados a la hora de resolver represalias.

- El desarrollo de capacidades para ejecutar acciones ofensivas en el ciberespacio conlleva el riesgo evidente de la escalada de una carrera "ciberarmamentística", pudiendo provocar un dilema de seguridad y la consecuente afectación a la seguridad. Esta situación demandará la colaboración de los Estados y la participación de organismos supranacionales, con la finalidad de establecer una eficiente arquitectura y más y mejores métodos de control.

- Para hacer frente a las amenazas a la ciberseguridad (las que se manifiestan afectando los atributos de confidencialidad, integridad y disponibilidad), se requiere de la participación de todos los niveles involucrados en la explotación del ciberespacio, conforme a las capacidades y niveles de control. Del mismo modo, toda respuesta exige contar con una arquitectura/organización adecuada, la tecnología/equipamiento (*hardware-software*) indicado y la educación, tanto para especialistas como usuarios. En este sentido, instituciones de educación superior deben continuar proporcionando instancias de capacitación, así como participar, junto a centros de estudio, en la difusión y análisis de estas materias.

- Considerando que se está a pocos meses del año 2022, debe realizarse la actualización de la Política de Ciberseguridad y sus correspondientes políticas subsidiarias. Estos renovados documentos deben plantear nuevos desafíos, conforme a la evaluación y experiencias obtenidas de la implementación desde el año 2017, incluida la pretendida Agencia Nacional de Ciberseguridad.

- Finalmente, se estima necesario reiterar sobre el real desafío que representa para todos los actores la generación de programas amplios y sólidos de formación en el área de ciberseguridad. Y esto, no solo en el gobierno, corporaciones y universidades, sino que en todo el espectro de actores, partiendo desde los niveles escolares primarios. Esto permitiría enfrentar las amenazas desde distintos ángulos y perspectivas y así, poder disminuir una de las principales vulnerabilidades en el ciberespacio, que son las malas prácticas de los usuarios.

MARCELO MASALLERAS
OCTUBRE 2021

| SOBRE EL AUTOR

Marcelo Masalleras es exoficial del Ejército de Chile. Licenciado en Ciencias Militares. Graduado como Oficial de Estado Mayor en las academias de guerra del Ejército, Fuerza Aérea de Chile y del US Army Command and General Staff College, Fort Leavenworth, Texas, USA. Magíster en Ciencias Militares de la ACAGUE. M.A. en Seguridad Internacional de la Universidad de Georgetown. Ha desempeñado actividades docentes en la Academia de Guerra del Ejército y en la Fuerza Aérea de Chile, así como en la Academia Militar de West Point de los Estados Unidos, impartiendo clases en los departamentos de Instrucción Militar y Estudios de Defensa y Estratégicos.

WWW.ATHENALAB.ORG