Recepción del original: 07/05/2021 . Aceptación: 20/10/2021

Aportes a la ciberdefensa y ciberseguridad para la gestión de las infraestructuras críticas de la información en Argentina

Contributions to cyber defense and cybersecurity for the management of critical information infrastructures in Argentina

AGOSTINA TAVERNA Y GUILLERMO RUTZ
Facultad de Ingeniería del Ejército, Universidad de la Defensa Nacional, Argentina
agostaverna@gmail.com
*Proyecto UNDEFI 2020 "Ciberdefensa y Educación".

En el contexto mundial de ciberataques, en donde el ciberespacio es un nuevo campo de batalla, la ciberseguridad es un tema de preocupación internacional por parte de los Estados. Si bien nuestro país adhiere a dicha preocupación, el desarrollo de infraestructura y tecnologías se encuentra aún rezagado. El presente trabajo indaga en la necesidad de formación de una sólida infraestructura de la información como medida de prevención y protección. Focaliza, además, en la investigación, desarrollo e innovación en la ciberdefensa de los activos esenciales para la sociedad argentina, así como en la capacitación de los operadores relacionados con las infraestructuras críticas.

Introducción

En los años recientes, la Defensa Nacional argentina ha subrayado la importancia de la ciberdefensa aplicada a la estrategia de defensa y al diseño de instrumento militar. Esta preocupación, que se hace extensiva a todo el terreno de la defensa a nivel internacional, viene de la mano de los denominados "ciberataques", que ya han empezado a afectar las relaciones interestatales y a generar conflictos estratégicos para los Estados. La ciberdefensa, por lo tanto, implica la puesta en marcha de un sistema totalmente diseñado para tal ocasión, desde la formación de profesionales hasta la aplicación efectiva de estrategias y tecnologías. En ese contexto, será de crítica relevancia la creación de instituciones afines a este campo, capaces de afrontar la problemática que suponen los conflictos en el ciberespacio. A continuación, se abordará el tema de la gestión de las infraestructuras críticas de la información en la Argentina.

El presente trabajo fue desarrollado en el marco del Proyecto UNDEFI "Ciberdefensa y Educación. Aspectos curriculares, políticos-estratégicos y estratégicos-productivos vinculados a la Formación Ciber para los intereses de la Defensa y de la Soberanía Nacional", y se ubica en el terreno de las actividades de ciencia y tecnologías interdisciplinarias. Codirigida por la Doctora María Elena Darahuge y el Doctor Guillermo Rutz, esta investigación se circunscribe a la línea de investigación en ciberdefensa y posgrados en la Argentina.

La infraestructura de la información para diseñar y mejorar tanto la ciberdefensa como la ciberseguridad constituye un nuevo campo del saber, que crece a paso vigoroso y que implica un sector de interés para el dominio público y privado. Al mismo tiempo, presenta múltiples dimensiones a desarrollar: lo económico, tecnológico, educativo, político, normativo, militar. Para cada una de estas áreas implicadas en los procesos de sistematización y puesta en marcha de una infraestructura de la información existen y existirán necesidades específicas, comunes y diferenciadas en torno a lo ciber. En ese aspecto,

uno de los intereses primordiales estará relacionado con los recursos humanos, con el patrimonio material y con las características organizativas. Para esto, será una necesidad –no solo del ámbito académico sino también de los sectores políticos– pensar en la información y en la ciberdefensa a partir de bases comunes, pero con perfiles diferenciales.

El actual proyecto de investigación se propuso como objetivo analizar los aspectos que contribuyen a la formación en ciberdefensa en el marco de los intereses de la Defensa y Soberanía Nacional, optando por un abordaje cualitativo. Del mismo modo, la investigación también buscó contribuir de manera positiva al desarrollo de planeamiento y catalogación de las distintas etapas de la información en el proceso de promover la ciberdefensa y la capacitación de profesionales en ciberseguridad.

Estado actual del conocimiento en el marco del proyecto

El ciberespacio, al igual que los espacios terrestres, marítimos, aéreo y espacial, es objeto de análisis por parte de numerosas instituciones públicas y privadas, tanto nacionales como internacionales. En los últimos años, y especialmente luego del ataque cibernético a Estonia en 2007, este interés se ve reflejado en instituciones globales y regionales, como la Organización de las Naciones Unidas, la Organización de Estados Americanos, la Organización del Tratado del Atlántico Norte o la organización para la Seguridad y Cooperación en Europa, tanto en la producción escrita como en la incorporación a sus estructuras institucionales de organismos especializados en el tema. Del mismo modo diversos países han incluido la problemática en sus agendas de estrategia nacional de seguridad (Trama y de Vergara, 2017).

En el caso argentino, Gastaldi y Justribró delimitan 5 dimensiones referidas a la ciberdefensa: Ciberseguridad o Seguridad Informática, Ciberinteligencia, Ciberdefensa, Geopo-

lítica del Ciberespacio y Derechos Humanos, dando comienzo a una investigación sobre el tema en el contexto de la ex Escuela de Defensa Nacional –actualmente Facultad de la Defensa Nacional, dependiente de la Universidad de la Defensa Nacional–. Así, develan la existencia de "gran cantidad de conceptos y categorías para identificar los mismos fenómenos", destacando además que "el marco normativo nacional establece una separación jurídica, orgánica y funcional entre Defensa Nacional y Seguridad Interior" (Gastaldi y Justribró, 2014a: 10). Las autoras consideran necesario estudiar el tema desde la visión de la doctrina argentina, que difiere de otras, como el caso de los miembros de la Organización del Tratado del Atlántico Norte. Para ello es necesario la conceptualización de categorías como ciberespacio, ciberpoder, cibercrimen, ciberguerra, ciberseguridad y ciberdefensa (Gastaldi y Justribró, 2014b: 16).

En cuanto a la formación de posgrado en la especialidad, en 2018 la Universidad de Buenos Aires, en convenio con la Escuela de Inteligencia Nacional, ofreció la maestría en ciberdefensa y ciberseguridad, que pone el foco en la gestión y no en la formación de tecnólogos de la especialidad. Por otro lado, en julio de 2019 la Facultad de Ingeniería del Ejército, dependiente de la Universidad de la Defensa Nacional, implementó un segundo año en su carrera de Especialización en Criptografía y Seguridad Teleinformática, mediante el cual se accederá a la maestría en ciberdefensa con una orientación netamente tecnológica del área de ingeniería. Además de estas únicas maestrías en la especialidad, existen dos diplomaturas en universidades privadas: "Diplomatura Gestión y Estrategia en Ciberseguridad", ofrecida por la Universidad del CEMA, y "Diplomatura en Ciberseguridad", dictada por la Universidad CAECE, ambas especialmente dirigidas, aunque no restrictivamente, a profesionales que se desempeñan en actividades de seguridad informática, generalmente vinculados al ámbito bancario y al sector legal.

Respecto a políticas públicas, en 2011 se creó el Programa Nacional de Infraestructuras Críticas de Información y Ciber-

seguridad (RES N°580/2011) para dar un marco regulatorio para identificar y proteger las infraestructuras críticas y estratégicas del sector público y privado. Tres años más tarde se conformó la Unidad de Coordinación Cibernética en la Jefatura de Gabinetes de Asesores del Ministerio de Defensa (RES 385/13) y, al año siguiente, se creó el Comando Conjunto de Ciberdefensa, dependiente del Estado Mayor Conjunto de las Fuerzas Armadas, por Resolución N° 343/14. Por su parte, el Ministerio de Defensa, en el año 2015, puso en funcionamiento la Dirección General de Ciberdefensa, que tenía entre sus competencias asistir en cuestiones de política de ciberdefensa, entre otras. La misma fue elevada a Subsecretaría en enero de 2016 por Decreto N° 226/2016, contando con dos direcciones: la Dirección Nacional para el Desarrollo Científico de la Ciberdefensa y la Dirección Nacional de Diseño de Políticas de Ciberdefensa. Al mismo tiempo, el entonces Ministerio de Modernización –hoy Secretaría– creó dentro de su órbita la Subsecretaría de Tecnología y Ciberseguridad, mediante Decreto N° 13/2016, con el propósito de entender en políticas de infraestructuras tecnológicas, protección de infraestructuras de información y capacitación en seguridad informática al sector público nacional, privado y ONG que así lo requiriera. Al año siguiente surgió el Comité de Ciberseguridad (Decreto N° 577/2017) integrado por representantes de Modernización, Defensa y Seguridad, con el objeto de impulsar un marco normativo de Ciberseguridad y participar en acciones de Ciberseguridad a nivel nacional. Finalmente, el 24 de mayo de 2019 la Secretaría de Gobierno de Modernización dictó la Estrategia Nacional de Ciberseguridad (RES N° 829/2019).

En cuanto al marco teórico, "en la actualidad no existen definiciones comunes para expresiones relacionadas con la cibernética, ni siquiera en el contexto regional, lo cual dificulta la cooperación entre los Estados" (Trama y de Vergara, 2017: 21). Esta dificultad es expuesta también por Singer y Fridman (2014) para quienes las nuevas discusiones entre Estados requieren un encuadramiento de vocabulario especialmente en los temas ciber, donde los tópicos se mezclan con asuntos

técnicos y conceptos demasiados amplios. Tal como lo plantean Eissa, Gastaldi, Poczynok y Di Tullio (2012), siguiendo la legislación nacional, es necesario separar la seguridad cibernética nacional de la defensa cibernética nacional. Ballesteros (2016: 60) considera que "como construcción intelectual esta postura es útil, aunque dificulta su implementación dadas las características del espacio cibernético".

La cibernética –término acuñado por Nobert Wiener en 1948 cuando publicó *Cybernetics, or Control and Communication in the Animal and the Machine*, libro escrito desde una perspectiva matemática en el que propuso su teoría del control y la comunicación en máquinas y animales–, surge de la combinación de matemáticas y neurofisiología, proponiéndose como ciencia que permitirá el control de factores inherentes a la naturaleza y al funcionamiento de la sociedad (Wiener, 1998). En ese contexto, el espacio cibernético es una categoría central de la especialidad que presenta multiplicidad de abordajes conceptuales. Para Bloch (2008) es una disciplina que busca lograr un dispositivo capaz de realizar complejas funciones similares al pensamiento, con lo cual en ella coexisten dos teorías principales: la Teoría de la Información y la Teoría de la Robótica. En el mismo orden, Orciuoli (2005: 14) la entiende como "una ciencia interdisciplinaria que al ponerse en movimiento transforma la información en un resultado deseado". Eissa et al. (2012) consideran que "no constituye un espacio en sí mismo, sino más bien una dimensión superpuesta, que atraviesa a los espacios físicos tradicionales", coincidiendo de este modo con Sheldon (2011) sobre que el ciberpoder genera efectos en todos los espacios de forma absoluta y simultánea. De este modo es que resulta de interés para los Estados, dada su capacidad de producir modificaciones en el mundo físico.

Por su parte, Sierra (2015: 16) lo define como "el conjunto de medios y procedimientos basados en las TIC –Tecnologías de la Información y Comunicaciones– configurados para la prestación de servicios", de lo cual surge que internet forma parte del espacio cibernético, porque internet es comunicaciones y comunicaciones es solamente el escenario. En la mis-

ma línea que Sierra, Feliú Ortega (2012: 42-43) considera que "el espacio cibernético es más que Internet, más que los mismos sistemas y equipos e incluso que los propios usuarios, es un nuevo espacio con sus propias leyes físicas que, a diferencia de los demás espacios, ha sido creado por el hombre para su servicio". Ottis y Lorents (2012), por su parte, sostienen que "es un conjunto de sistemas de información interconectados dependientes del tiempo y los usuarios humanos que interactúan con estos sistemas", compartiendo la línea de razonamiento con Uzal (2013), quien lo define como "la dimensión generada durante el tiempo de interconexión e interoperabilidad de redes, sistemas, equipo y personal".

A su vez, Desforges (2014: 67) sostiene que "el término ciberespacio no es neutral, sino que conlleva varias representaciones, algunas contrapuestas, y que dan origen a las concepciones de ciberespacio que luego se transcriben en las estrategias de los Estados, que luego son instrumentos o herramientas de geopolítica". Finalmente, es de interés destacar la noción de ciberespacio como espacio cognitivo abordada tanto por Ocón (2019) como por Libicki (2009), Strate (2018) o Grant (2014). Al igual que la categoría anterior, la de "guerra cibernética" es abordada por Feliú (2013), para quien cada vez que aparece una nueva dimensión real o virtual que el hombre quiere utilizar, este tratará de dominarla y obtener la superioridad con el objeto de actuar desde ella en su beneficio e impedir su uso al adversario. Blasco (2015) considera que esta complementa la tradicional y al mismo tiempo refleja sus usos y costumbres. Al mismo tiempo, para Conti y Surdu (2009: 17) este aspecto de la ciberdefensa "requiere no solo habilidades técnicas, sino también aquellas para solucionar problemas de creatividad y actuar bajo pensamiento crítico". En esta concepción de Conti y Surdu, seguida por otros pensadores actuales, radica la importancia del estudio sobre la formación de posgrado en el tema, dado que esta requiere la adquisición de complejas habilidades informáticas, siendo necesaria, tal como lo plantean Christopher, Porche y Axelband, la comprensión de matices culturales, humanos y todos aquellos que ayuden a entender

e implementar diseños que permitan tener un impacto en el dominio cognitivo del adversario.

La gestión de las infraestructuras críticas de la información en Argentina

El concepto de infraestructura crítica de la información ha ido evolucionando junto con el crecimiento de la tecnología hasta convertirse en un activo esencial para cualquier sociedad. En la actualidad, dichas infraestructuras de un país se encuentran en el plano terrestre, marítimo, aéreo, espacial o ciberespacial, y requieren de un plan de prevención y protección para conservar los servicios esenciales de la comunidad ya que, de lo contrario, la interrupción de los mismos ocasionaría consecuencias perjudiciales para la sociedad.

Considerando que las infraestructuras críticas han incorporado una gran cantidad de componentes informáticos, los ciber atacantes aprovechan sus puntos débiles para generar impacto en el funcionamiento de un Estado (salud, seguridad, defensa, bienestar social y economía), empleando técnicas que se renuevan constantemente, indicando que la prevención ya no es la única acción efectiva a realizar. Lejos de reemplazar las formas tradicionales de ataque –la ciberguerra, el ciberterrorismo, el ciberespionaje y el ciberdelito–, los gobiernos han comenzado a trabajar en la ciberseguridad y ciberdefensa de sus países. Efectivamente, la estabilidad del país y la confianza del ciudadano en el Estado se verían comprometidas si ocurriera un ataque masivo y coordinado a alguno o varios de los sectores definidos como infraestructura crítica, y es por ello que el Estado debe centrarse en medidas de prevención, protección y resiliencia de las mismas.

Ciertamente, "la amplitud del concepto de infraestructura crítica y la multiplicidad de sectores afectados requiere afrontar la protección de dicha infraestructura de forma integral y multidisciplinaria" (Sánchez, 2012). Inclusive, desde el año

2004 la Organización de los Estados Americanos (OEA) enfatiza la importancia de desarrollar una estrategia comprensiva para proteger las infraestructuras críticas que adopte un enfoque integral, multidisciplinario e internacional (Organization of American States, Microsoft, 2018).

Ante el análisis y la revisión del plexo normativo relacionado a las infraestructuras críticas de la información y a los organismos del Poder Ejecutivo Nacional relacionados con las mismas, se concluye como resultado preliminar que, a pesar del extenso marco normativo imperante en Argentina, este no es suficiente. En principio, se omite –especialmente en la Estrategia de Ciberseguridad (resolución n° 829/2019)– la necesidad e importancia de efectuar una lista exhaustiva de los componentes entendidos como infraestructuras críticas de la información. Por otra parte, no se define al organismo que debiera identificar dichas infraestructuras y declararlas como tales. Finalmente, y dada la importancia en la prevención de la afectación de dichas infraestructuras, se torna necesario hacer hincapié en la investigación, desarrollo e innovación en ciberseguridad, en la ciberdefensa de los activos esenciales para la sociedad argentina y en la capacitación de aquellos operadores relacionados con las infraestructuras críticas.

En el marco del presente proyecto, la investigación abordó tres temas: la investigación, desarrollo e innovación en ciberseguridad para la protección de las infraestructuras críticas; la relación entre los sistemas institucionales nacionales y la necesidad de crear un sistema nacional que articule los existentes con enfoque en las infraestructuras críticas de la información argentinas; y la capacitación para la ciberdefensa de las infraestructuras críticas.

En relación al primer tema, basado en la importancia de una inversión continua y en el diseño de un plan a mediano y largo plazo para la Investigación, Desarrollo e Innovación (en adelante "I+D+i") en ciberseguridad, se evidenció la necesidad de estudios sobre las infraestructuras críticas de la información en Argentina con el fin de generar mecanismos, métodos y procedimientos eficaces y eficientes para su pro-

tección. Asimismo, se analizó la importancia de la I+D+i en ciberseguridad haciendo énfasis en la situación de las infraestructuras críticas de la información en Argentina. El estudio también propone un análisis y enfoque integral y sucinto de la normativa, donde busca enumerar los aportes necesarios para avanzar en la protección de las infraestructuras críticas en cumplimiento con la Estrategia Nacional de Ciberseguridad. A respecto se puede decir que la temática requiere un abordaje multifacético y un instituto nacional que articule al Sistema Nacional de Ciencia y Tecnología e Innovación existente con aquellos institutos que puedan investigar en materia de ciberseguridad.

El abordaje de los Sistemas de Protección de Infraestructuras Críticas de la República Argentina desarrolla la idea respecto a que el auge de las ciberamenazas y los ciberataques ocurridos contra infraestructuras críticas (en adelante "IICC") en el mundo obliga a la Argentina a estar preparada para anticipar, prevenir, proteger y defender aquellas infraestructuras que brindan servicios esenciales. Considera que el Estado debe garantizar el normal y continuo funcionamiento de dichos servicios, y para ello es indispensable trabajar y desarrollar conceptos como inteligencia, ciberinteligencia, ciberamenazas, ciberataques, ciberseguridad y ciberdefensa en torno a la protección de las infraestructuras críticas, con el fin de decidir qué camino deberá tomar la Argentina con relación a la ciberseguridad. La investigación permite afirmar que crear el Sistema de Protección de Infraestructuras Críticas de la República Argentina (SIPICRA) permitirá coordinar todos los sistemas institucionales ya existentes en pos de la protección de la sociedad y los servicios que son esenciales mediante el empleo de un esquema innovador y multisectorial. El SIPICRA –junto al Sistema de Inteligencia Nacional– no solo significaría más capacidades para la identificación, detección y mitigación de ciberamenazas y ciberataques, sino también la obtención de un lenguaje común para entender el fenómeno y aplicar las técnicas necesarias con el fin de gestionar las contramedidas que garanticen la resiliencia de las infraestructu-

ras críticas de la Nación y sus valores democráticos.

El tercer tema hace referencia a la importancia en el uso y práctica consistente de simuladores de ciberseguridad como medio de ejercitación de los operadores críticos de las infraestructuras críticas. El aumento del uso de las tecnologías de la información y las comunicaciones provocado por la crisis pandémica de 2020 ha provocado un aumento de la compleja interrelación entre sistemas en infraestructuras críticas. Esto, a su vez, provoca nuevas vulnerabilidades de seguridad y ciberamenazas que podrían afectar a la sociedad. Además, las simulaciones en forma de ciberejercicios se consideran herramientas para proporcionar una comprensión de cómo se realizan los ciberataques y cómo pueden afectar las infraestructuras críticas nacionales. Estos métodos sobre cómo protegerlos a escala mundial desde un único punto de vista remoto pueden convertirse en una ventaja estratégica.

A medida que los soldados realizan simulacros para adquirir experiencia de primera mano antes de enfrentarse a la realidad, los ciberejercicios buscan imitarlos para responder de forma eficaz contra determinadas cibercrisis y, por tanto, defender la infraestructura crítica. En consecuencia, este estudio explora si las simulaciones son aceptadas en la comunidad educativa como un método para desarrollar habilidades en los estudiantes antes de que se enfrenten a cualquier desafío en la vida real. De tal manera se puede establecer la relevancia de facilitar los ciberejercicios a través de simuladores que fueron desarrollados e implementados para satisfacer la necesidad de nutrir esas habilidades específicas para el personal del Security Operation Center que, actualmente, trabaja de forma remota.

Conclusiones

Si bien en la actualidad el desarrollo investigativo, práctico y estratégico de las infraestructuras críticas ha sido amplio, la

Argentina se encuentra normativa y funcionalmente demorada. En efecto, la multiplicidad de dimensiones, complejidades y evolución constante del ciberespacio requiere de un enfoque dinámico, con una estructura organizativa adecuada.

Frente a ello, es imprescindible que nuestro país desarrolle un Plan Estratégico Nacional en lo que hace a las infraestructuras críticas de la información, con el fin de prevenir una afectación parcial o total, defender los activos esenciales de nuestra nación y los principales intereses de la República. Para ello, es vital poder desarrollar sistemas y redes informáticas dentro del Instrumento Militar que operen eficazmente dentro de la zona de influencia que abarca la Defensa Nacional.

Las investigaciones futuras deberán centrarse en el estudio de las distintas tecnologías existentes y a desarrollar para una protección, prevención y resiliencia efectiva de las infraestructuras críticas argentinas. Por otra parte, se debería efectuar un análisis exhaustivo sobre las distintas metodologías a emplear para la identificación de las infraestructuras críticas en base a los criterios y sectores detallados en la normativa nacional para, de ese modo, realizar un relevamiento intrasectorial que contemple la dependencia e interdependencia de las distintas infraestructuras.

Finalmente, las investigaciones deben dar cuenta de la capacitación y concientización al recurso humano que opera y se relaciona con los sistemas y redes que se emplean en las infraestructuras críticas y la interrelación, cooperación y coordinación de los actores del sector público y privado que se relacionan estratégicamente con dichas infraestructuras.

BALLESTEROS, M. A. (2016). "Hacia una Estrategia de Seguridad Nacional". Instituto de Estudios Estratégicos de España, Madrid. Recuperado de: http://www.ieee.es/Galerias/fichero/OtrasPublicaciones/Nacional/2016/MABM_ESN.pdf

BLASCO, J. (2015). "El más fuerte es el más vulnerable". *El País*. Recuperado de: http://internacional.elpais.com/internacional/2015/02/07/actualidad/1423330690_981628.html

BLOCH, R. (2008). "Cibernética". Recuperado de: http://uprociber.blogspot.com.ar/2008/04/ cibernetica.html

CONTI, G. y SURDU, J. (2009). "Army, Navy, Air Force, and Cyber – Is It Time for a Cyberwarfare Branch of Military?". *Anewsletter*, *12*(1): pág.17.

DESFORGES, A. (2014). "Les représentations du cyberespace: un outil geopolítique". Recuperado de https://www.cairn.info/revue-herodote-2014-1-page-67.htm

EISSA, S.G; GASTALDI, S.; POCZYNOK, I. y DI TULLIO, M. E. (2012). "El ciberespacio y sus implicancias en la defensa nacional.Aproximacionesalcasoargentino".Recuperadode: http://sedici.unlp.edu.ar/bitstream/handle/10915/40210/Documento_completo.pdf?sequence=1

FEILÚ, L. (2013). "Seguridad Nacional y Ciberdefensa, una aproximación conceptual". Conferencia en la UPM, Madrid. Recuperado de: http://catedraisdefe.etsit.upm.es/wp-content/uploads/2013/01/Ponencia-Luis-Feliu.pdf.

FEILÚ ORTEGA, L. (2012). "El espacio cibernético nuevo escenario de confrontación". Cuadernos del CESEDEN, págs. 42-43. Recuperado de: http://www.defensa.gob.es/ceseden/Galerias/destacados/publicaciones/monografías/ficheros/126_EL_ESPACIOCIBERNETICO_NUEVO_ESCENARIO_DE_CONFRONTACION.pdf

GASTALDI, S. y JUSTRIBRÓ, C. (2014a). "Informes de actualidad y temáticas de defensa". EDENA: Secretaría de Investigación, pág. 9.

GRANT, T. J. (2014). "On the Military Geography of Cyberspace". En LILES, S. (eds.), *Proceedings, 9th International Conference on Cyber Warfare & Security (ICCWS 2014)*. West Lafayette, Estados Unidos: Purdue University.

LIBICKI, M. C. (2009). *Cyberdeterrence and Cyberwar*. RAND Corporation.

OCÓN, A. L. (2019). "Educación, conocimiento y poder: debates lógicos-epistémicos y enfoques alternativos respecto de la naturaleza humana". *Anacronismo e Irrupción, 9*(16): págs. 113-147.

ORCIUOLI, A. (2005). Citado por STEL, E. en "Guerra Cibernética". Círculo Militar, 1ra Edición. Buenos Aires, 2005.

ORGANIZATON OF AMERICAN STATES, MICROSOFT (2018). "Critical Infrastructure Protection in Latin America and the Caribbean 2018". Recuperado de: https://www.oas.org/es/sms/cicte/cipreport.pdf

OTTIS, R. y LORENTS, P. (2012). "Cyberespace: Definition and Implications". *Coperative Cyber Defence Centre of Excelence*.

SÁNCHEZ, M. (2012). Protección de Infraestructuras Críticas. Un nuevo reto para la convergencia de las seguridades.

Recuperado de: https://manuelsanchez.com/2012/05/28/proteccion-de-infraestructuras-criticas-un-nuevo-reto-para-la-convergencia-de-las-seguridades/

SHELDON, J. B. (2011). "Deciphering Cyberpower. Strategic Purpose in Peace and War". Recuperado de: https://www.airuniversity.af.edu/Portals/10/SSQ/documents/Volume-05_Issue-2/Sheldon.pdf

SIERRA, D. (2015). "Las dos caras de la tecnología" *Opinión Ciberelcano*. Informe mensual de ciberseguridad.

SINGER, P. y FRIDMAN, A. (2014). "Cybersecurity and Cyberwar" *Oxford University Press, Library of the Congress*. Recuperado de https://news.asis.io/sites/default /files/Cybersecurity_and_Cyberwar.pdf

STRATE, L. (2018). "Eight Bits About Digital Communication". *Razón y Palabra*, *22*(1_100): págs. 589-618.

TRAMA, G. A. y DE VERGARA, E. A. (2017). *Operaciones militares cibernéticas: planeamiento y ejecución en el nivel operacional*. Buenos Aires, Argentina: Escuela Superior de Guerra Conjunta de las Fuerzas Armadas.

UZAL, R. (2013). "Ciberdefensa-Ciberseguridad: Riesgos y Amenazas". Conferencia pronunciada en el Consejo Argentino para las Relaciones Internacionales, CARI, noviembre 2013.

WIENER, N. (1998). *Cibernética o el control y comunicación en animales y máquinas*. Barcelona: Tusquets.

Palabras clave: ciberdefensa - ciberseguridad - Argentina - infraestructuras críticas

Keywords: cyberdefense - cybersecurity - Argentina - critical infrastructures

Abstract

In a world context of cyberattacks, where cyberspace is the new battlefield, cybersecurity is a matter of international concern for states. Although our country adheres to this concern, the development of infrastructure and technologies is still lagging behind. This paper investigates the need for the formation of a solid information infrastructure as a prevention and protection measure and also focuses on research, development and innovation in the cyber defense of essential assets for Argentine society, as well as on the training of operators related to critical infrastructures.