CIBERDEFENSA Y FORMACIÓN DE POSGRADO EN ARGENTINA. INDAGACIONES PRELIMINARES PARA UN APORTE AL DESAFÍO CIBER DE LA DEFENSA NACIONAL.

GUILLERMO RUTZ

Doctor en Ciencias Sociales (FLACSO). Magíster en Estrategia y Geopolítica (ESG). Magíster en Defensa Nacional (FADENA). Magíster en Educación y Ciencias Sociales (FLACSO). Especialista en Políticas Educativas (FLACSO). Licenciado en Bibliotecología y Documentación (UNMDP). Investigador UNDEF sobre Educación, Defensa Nacional y Ciberdefensa.

Resumen

Este artículo busca dar a conocer avances de la investigación sobre formación de posgrado y ciberdefensa. El propósito de tal estudio es conocer el aporte de la formación de posgrado en ciberdefensa y ciberseguridad a los elementos teóricos y político-estratégicos, en un contexto de desafío ciberespacial para la Defensa Nacional. Para ello, se analizaron siete ejes: aspectos curriculares, vínculos entre currículum y contexto normativo, cooperación entre actores y estructuras, desafíos y dilemas actuales, posgrados y perfiles profesionales, políticas públicas referidas a la formación y, por último, incentivos a la formación, investigación e innovación.

El enfoque metodológico es cualitativo, basado en tres aspectos: la indagación en la agenda periodística local de publicaciones en línea de mayor publicación en idioma español; realización de entrevistas semiestructuradas

a directores de carrera de formación de posgrado en ciberdefensa y ciberseguridad, como también a decisores de políticas públicas expresamente vinculadas a la temática; análisis de la normativa vigente y marcos teóricos relativo al aspecto social y de políticas públicas.

El estado actual de la investigación permitió identificar, en los cinco primeros ejes, doce categorías de análisis con cuarenta y dos hallazgos, que se mencionan en esta publicación. Tales categorías y hallazgos permiten estructurar una nueva línea de investigación dentro del área ciber: formación en ciberdefensa y ciberseguridad. Ambas constituyen un nuevo campo del saber, con interés estratégico para el sector público y privado, el cual presenta múltiples dimensiones a ser estudiadas y desarrolladas por ejemplo desde lo económico, tecnológico, educativo, político, normativo, militar, entre otros aspectos o enfoques.

Palabras clave:

Ciberdefensa – Ciberseguridad – Formación –Posgrados –Argentina – Defensa Nacional

Abstract

This article seeks to publicize advances in research on postgraduate and cyber defense training. The purpose of this study is to know the contribution of postgraduate training in cyber defense and cyber security to the theoretical and political-strategic elements, in a context of cyberspace challenge for National Defense. For this, seven axes were analyzed: curricular aspects, links between curriculum and regulatory context, cooperation between actors and structures, current challenges and dilemmas, professional profiles and profiles, public policies related to training, and finally incentives to training, research and innovation.

The methodological approach is qualitative, based on three aspects: the investigation in the local journalistic agenda of online publications of greater publication in Spanish language; conducting semi-structured interviews with directors of postgraduate training in cyber defense and cyber security, as well as public policy makers expressly linked to the subject; analysis of current regulations and theoretical frameworks related to the social aspect and public policies.

The current state of the research allowed identifying, in the first five axes, twelve categories of analysis with forty-two findings, which are mentioned in this publication. Such categories and findings allow structuring a new line of research within the cyber area: cyber defense and cyber security training. Both constitute a new field of knowledge, with strategic interest for the public and private sector, which has multiple dimensions to be studied and developed for example from the economic, technological, educational, political, regulatory, military, among other aspects or approaches.

Keywords:

Cyber Defense - Cyber Security - Postgraduate-Argentina - National Defense

Introducción

Luego del ataque cibernético a Estonia en 2007, el ciberespacio despertó un interés que se vio reflejado en instituciones globales y regionales. 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 delimitaron cinco dimensiones referidas a la ciberdefensa, y dieron comienzo a una investigación sobre el tema en el contexto de la ex Escuela de Defensa Nacional, develando la existencia de "gran cantidad de conceptos y categorías para identificar los mismos fenómenos". Además, destacaron que "el marco normativo nacional establece una separación jurídica, orgánica y funcional entre Defensa Nacional y Seguridad Interior" (Gastaldi y Justribró, 2014, p.10).

En cuanto al marco teórico, "en la actualidad no existen definiciones comunes para expresiones relacionadas con la cibernética" (Trama y de Vergara, 2017, p.21). Esta dificultad es expuesta también por Singer y Fridman (2014) para quienes las nuevas discusiones entre Estados requieren un encuadramiento de vocabulario. Si bien, como 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, p.60) considera que "como construcción intelectual esta postura es útil, aunque dificulta su implementación dadas las características del espacio cibernético".

La cibernética surge proponiéndose como ciencia que permitirá el control de factores inherentes a la naturaleza y al funcionamiento de la sociedad (Wiener, 1998) donde *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. En el mismo orden, Orciuoli (citado en Stell, 2005, p.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". Así, coinciden con Sheldon (2011), en el sentido de que el ciberpoder genera efectos en todos los espacios de forma absoluta y simultánea. Feliú Ortega (2012, p.42-3) considera que "el espacio cibernético es más que internet, los sistemas, equipos y usuarios, es un nuevo espacio con sus propias leyes físicas, creado por el hombre para su servicio". A su vez, Desforges (2014, p.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 por Ocón (2019) como también Libicki (2009), Strate (2018) o Grant (2014).

Al tratar sobre la guerra cibernética, Feliú (2013) considera que cada vez que aparece una nueva dimensión real o virtual que el hombre quiere utilizar, éste 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 ésta complementa la tradicional y, al mismo tiempo, refleja sus usos y costumbres. Al mismo tiempo, para Conti y Surdu (2009, p.17) este aspecto de la ciberdefensa "requiere no sólo 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 ésta requiere y va más allá de adquirir habilidades informáticas. Por ello, es necesario, tal como lo plantean Christopher, Porche y Axelband, comprender matices culturales, humanos y todos aquellos que permitan entender e implementar diseños para tener un impacto en el dominio cognitivo del adversario. Por otra parte, Theohary y

Harrington (2015) abordan la dificultad para trazar líneas claras entre guerra cibernética, ciberdelito, ciberterrorismo y ciberespionaje, dado que todo el tiempo actores estatales y no estatales llevan a cabo estas acciones, generalmente desde el anonimato, por lo cual no siempre es posible identificar si el agresor es un Estado o no.

El proyecto contempló un abordaje cualitativo para lo cual, en primera instancia, se procedió a la indagación en medios periodísticos argentinos y de habla hispana especializados en el tema, con el objeto de identificar la visibilidad del tema en la agenda nacional y sus aspectos de interés. Luego, se pasó a la etapa de recolección de información mediante entrevistas a los responsables de las ofertas de posgrados vigentes sobre la temática en el ámbito de universitario de la Ciudad Autónoma de Buenos Aires.

De esta manera, el enfoque metodológico presenta tres componentes. En primer lugar, la visibilidad del tema en el ámbito social, a partir de la indagación en la agenda periodística en general y especializada disponible en formato online, en particular las publicaciones de mayor circulación y consulta como Perfil[1], La Nación[2], Infobae[3] e Infodefensa[4]. En el caso de Infodefensa, cabe señalar que este medio recopila noticias e informes periodísticos de España y Latinoamérica.

El segundo componente es el análisis y reflexión en la perspectiva de construcción del conocimiento con actores relevantes para el objeto de la investigación. Esto significó el desarrollo de un modelo de entrevistas y su análisis desde enfoques habituales de las Ciencias Sociales que incorpora el diálogo con representantes del proceso de gestión de estructuras curriculares orientadas a la formación de posgrado en Ciberdefensa. Los entrevistados fueron los directores de carreras o formación de posgrado en Ciberdefensa/

1 *Perfil.* Recuperado de https://www.perfil.com/buscador?q=ciberdefensa

2 *La Nación.* Recuperado de https://buscar.lanacion.com.ar/ciberdefensa/

3 *Infobae.* Recuperado de https://www.infobae.com/search/ciberdefensa/?q=ciberdefensa

4 Infodefensa. Recuperado de https://www.infodefensa.com/directorio/buscador.php?busqueda=ciberdefensa&x=0&y=0

seguridad de las siguientes universidades: CEMA[5], CAECE[6], UNDEF-FADENA[7], UNDEF-Facultad de Ingeniería del Ejército[8], UBA-ENI[9]. De igual modo, incluye entrevistas con decisores de alta política pública en el tema correspondiente a las siguientes áreas: Comando Conjunto de Ciberdefensa – Estado Mayor Conjunto de las Fuerzas Armadas, Subsecretaría de Ciberdefensa (Mindef - Ministerio de Defensa), Dirección de Diseño de Políticas para la Ciberdefensa (Mindef), Secretaría de Estrategia y Asuntos Militares (Mindef), Dirección Nacional de Formación (Mindef).

En tercer lugar, el proyecto incorporó componentes normativos y teóricos. El primero permitió dar cuenta, por un lado, de la estructura organizacional en el contexto de la Defensa Nacional para entender posibles vínculos e inserciones de actores e instituciones. Por otra parte, mediante el mismo se pudo analizar diferentes aspectos de la política de ciberdefensa y sus relaciones con los componentes antes mencionados, como también los objetivos que las diferentes estructuras orgánicas-burocráticas-políticas de la Defensa se propusieron para la temática y sus implicancias en el contexto de esta investigación. A su vez, el componente teórico facilitó la incorporación de consideraciones para el abordaje del tema desde la perspectiva de políti cas públicas; lo cual permite una mirada que implica indagar la intervención de una actividad pública (en este caso, del Ministerio de Defensa) sobre una realidad social (la formación de posgrados en Ciberdefensa) con el objeto de generar conocimiento que facilite una posterior mejora de intervención (Nirenberg, Brawerman y Ruiz, 2000).

5 Diplomatura Gestión y Estrategia en Ciberseguridad, Universidad del CEMA. Buenos Aires, Argentina: CEMA. Recuperado de https://ucema.edu.ar/educacion-ejecutiva/ciberseguridad

6 Diplomatura en Ciberseguridad, Universidad CAECE. Buenos Aires, Argentina: CAECE. Recuperado de http://www.ucaece.edu.ar/agenda/diplomatura-en-ciberseguridad/

7 Maestría y Curso Superior en Defensa Nacional, Universidad de la Defensa Nacional. Buenos Aires, Argentina: UNDEF. Recuperado de http://www.undef.edu.ar/fadena/

8 Maestría en Ciberdefensa, Facultad de Ingeniería del Ejército, Universidad de la Defensa. Buenos Aires, Argentina: UNDEF. Recuperado de https://www.undef.edu.ar/nueva-oferta-de-posgrado-ciberdefensa/, http://www.fie.undef.edu.ar/?p=7226

9 Maestría en Ciberdefensa y Ciberseguridad, Universidad de Buenos Aires. Buenos Aires, Argentina: UBA. Recuperado de http://www.economicas.uba.ar/posgrado/posgrados/ciberdefensa-y-ciberseguridad/

En función del análisis de los componentes metodológicos mencionados, esta investigación busca dar cuenta de reflexiones en torno a los siguientes interrogantes: aspectos curriculares; vínculo entre lo curricular y el contexto normativo e institucional; vínculos de cooperación entre diferentes actores y estructuras, nacionales e internacionales; desafíos y dilemas del ámbito ciberespacial para la Defensa Nacional; posgrado y perfiles profesionales requeridos por la especialidad; incentivos para la innovación, investigación y formación en Ciberdefensa; políticas públicas respecto a la formación en Ciberdefensa.

Contextos

Contexto periodístico

Como primera acción en el contexto de la investigación, se buscó develar cuál era la visibilidad del tema en la agenda periodística local e internacional; qué actores surgían como voceros y qué aspectos de la temática se abordaba. Para ello, se llevó a cabo un relevamiento de todos los artículos periodísticos online, en español, en los que aparecieran los siguientes términos: "ciberdefensa", "ciberespacio", "ciberseguridad". En particular, se consideraron las publicaciones de mayor circulación y relevancia en el medio social como Perfil[10], La Nación[11], Infobae[12] e Infodefensa[13]. Cabe señalar que Infodefensa recopila noticias e informes periodísticos sobre diferentes temas de la defensa, de países latinoamericanos y de España.

En una primera aproximación respecto a la indagación periodística, se puede distinguir que en las noticias argentinas se encontraron, en los tres portales de noticias mencionados previamente, 77 artículos: La Nación 45, Perfil 22 e Infobae 10 –en el período 2013 hasta 27 de marzo de 2019– referidos de manera general y sin profundización a la ciberdefensa. Además,

10 Perfil. Recuperado de https://www.perfil.com/buscador?q=ciberdefensa

11 *La Nación*. Recuperado de https://buscar.lanacion.com.ar/ciberdefensa/

12 Infobae. Recuperado de https://www.infobae.com/search/ciberdefensa/?q=ciberdefensa

13 Infodefensa. Recuperado de https://www.infodefensa.com/directorio/buscador.php?busqueda=ciberdefensa&x=0&y=0

es válido aclarar que los artículos no varían en sustancia o contenido político-conceptual entre un portal y otro, solo se distinguen cuestiones de estilo de redacción. Por su lado, Infodefensa trató específicamente el tema a través de 326 notas periodísticas con diferentes niveles de especificidad técnica o política. Otra observación posible que surge del relevamiento es que en Argentina el tema aparece de manera sistemática a partir del año 2014, mientras que Infodefensa y, en particular, España lo aborda desde 2009. De tal modo, las noticias con mayor relevancia por el contenido –político o técnico– que desde 2009 aparecen en Infodefensa pueden clasificarse del siguiente modo: España (2009)-54-, Chile (2016)-14-, Colombia (2009)-9-, Perú (2013)-4-, México (2013)-4-, Brasil (2013)-3-, Ecuador (2015)-1- donde el dato entre paréntesis corresponde al año de la primera publicación sobre el tema y el número entre guiones indica la cantidad de publicaciones entre el primer año de publicación y el 27 de marzo de 2019 –fecha de cierre del relevamiento de la presente investigación–.

De acuerdo al portal informativo Infodefensa y lo antes mencionado, en materia de ciberdefensa a nivel regional, incluido España y exceptuando Argentina –que se analiza posteriormente–, se puede decir que la agenda periodística latinoamericana y española aborda los siguientes temas: marcos doctrinales, Directivas políticas para la ciberdefensa, planes de obtención de capacidades; ejercicios para la comprobación de desarrollos y procedimientos teóricos de integración y planeamientos ciber; desafíos ciber en los aspectos humano, legislativo, tecnológico y educativo; planes formativos para posgrados, objetivos y proyectos de los altos mandos militares y civiles de la defensa respecto a la ciberdefensa; detalles de objetivos estratégicos en la materia; definiciones de política sobre desarrollo de capacidades para la ciberdefensa; aspectos técnicos y políticos sobre el cibersoldado; la ciberdefensa en el proceso de planeamiento militar; aspectos políticos de acuerdos de cooperación bilateral en la materia; sector privado, sus ofertas, vínculos y soluciones ciber para la defensa; riesgos internos y amenazas externas en el entorno ciber; capacidades ciber ofensivas y defensivas de un Estado y sus Fuerzas Armadas; aspectos de interoperabilidad entre Fuerzas Armadas respecto a la ciberdefensa; cursos de formación y necesidades futuras de analistas, colaboración industrial y tecnológica entre sector privado, público en la materia, necesidades para la estabilidad regional en materia de ciberdefensa, gestión de emergencias, creación de grupos de investigación sobre desafíos en la toma de decisiones ciberespaciales para la defensa.

La agenda periodística en Argentina sobre ciberdefensa hace referencias no específicas a cuestiones como necesidades de grandes lineamientos políticos, comentarios sin especificaciones técnicas o políticas sobre intercambio de información en la temática, porcentajes de *hackeos* sufridos por el Estado y el sector privado sin dar detalles, ciberseguridad vinculada con el sector privado y bancario en particular, la seguridad en la cumbre del G20 realizada en el país, referencias a incidentes cibernéticos en Rusia o países miembros de la OTAN, aspectos no específicos sobre necesidades tecnológicas y de profesionales para el área, nuevo rol de las Fuerzas Armadas vinculado a las ciberdefensa, capacitación de jueces en ciberterrorismo, Estonia como referencia central del tema, referencia a modo de titular de noticia sobre acuerdo entre los Ministros de Defensa de Brasil y Argentina para encargarse del tema, ciberdefensa vinculada a actividades de inteligencia y espionaje interno mencionando cuestiones judiciales de exfuncionarios de perfil técnico y político en la temática, formación de militares en el Reino Unido en ciberdefensa. En general se puede decir que la agenda periodística nacional, entre finales de 2013 y marzo de 2019, hace referencia a algunos aspectos de la ciberdefensa de manera no específica; no aparecen citas concretas sobre las voces de funcionarios (a excepción de algunas notas que mencionan al Ministro Aguad de manera referencial), sus puntos de vista, como tampoco perspectivas o lineamientos políticos, sociales, académicos o militares sobre el tema.

La primera noticia[14] encontrada en medios periodísticos nacionales hace referencia al acuerdo entre Brasil y Argentina para combatir el ciberespionaje, y aparece publicada el 13 de septiembre de 2013. El tema comienza a instalarse el mismo año en la agenda política con el pedido[15] de Argentina por una estrategia regional de ciberdefensa. El segundo artículo[16] sobre el

14 Redacción de Perfil (14-9-2013). Argentina y Brasil acuerdan combatir el ciberespionaje. *Perfil*. Recuperado de https://www.perfil.com/…/argentina-y-brasil-acuerdan-combatir-el- ciberespionaje-20130914-0036.phtml

15 Perfil (19-10-2013). Rossi reclamó una estrategia regional de ciberdefensa. *Perfil*. Recuperado de https://www.perfil.com/…/rossi-reclamo-una-estrategia-regional-de-ciberdefensa-20131018-0075.phtml

16 Aurelio, T. (01-01-2015). Milani ya tiene un centro de ciberdefensa para sus espías. Perfil. Recuperado de https://www.perfil.com/…/milani-ya-tiene-un-centro-de-ciberdefensa-para-sus -espias-20150201-0030.phtml

tema aparece el 31 de enero de 2015 dando cuenta de la creación, un mes antes, del Centro de ciberdefensa del Ejército. En mayo de 2017, se dio cuenta por primera vez en los medios periodísticos nacionales sobre acuerdos[17] en materia de ciberdefensa con Estados Unidos. En noviembre de 2018 la agenda de ciberdefensa se centró en la cumbre del G20 a realizarse en Buenos Aires, mediante lo cual se fortalecieron aspectos tecnológicos y operativos referidos a ella.[18] En enero de 2019, se hizoe visible la idea de crear un plantel de reservistas en el ámbito de las Fuerzas Armadas para que se ocupen de la ciberdefensa.[19]

Contexto normativo

Dados los antecedentes históricos de Argentina en la década de 1970, a partir de la recuperación democrática en 1983 se produjo una separación conceptual, intelectual, normativa y operativa entre Defensa y Seguridad, dualidad que se completó con la Ley de Inteligencia Nacional. Así, en Argen tina la Seguridad Interior cuenta con una estructura política administrativa y operacional regida por un ministerio y ley propia. Lo mismo sucede con la Defensa Nacional y la Inteligencia Nacional.

Esta distinción está contemplada en sus respectivas leyes: por un lado, la Ley de Defensa Nacional N° 23.554[20] y, por otro, la Ley de Seguridad Interior

17 Aurelio, T. (26-5-2017). Luego del ingreso de los limones a EEUU avanzan acuerdos por visas y ciberdefensa. Perfil. Recuperado de https://www.perfil.com/noticias/politica/luego-del-ingreso-de-los-limones-a-eeuu-avanzan-acuerdos-por-visas-y-ciberdefensa.phtml

18 Perfil (01-11-2018). Buenos Aires aumenta ciberseguridad por cumbre G20. Perfil. Recuperado de https://www.perfil.com/noticias/politica/buenos-aires-aumenta-ciberseguridad-por-cumbre-g20.phtml

19 Redacción de La Nación (03-01-2019). Impulsan la creación de un plantel de reservistas en las FFAA. La Nación. Recuperado de https://www.lanacion.com.ar/politica/impulsan-la-creacion-de-un-plantel-de-reservistas-en-las-ffaa-nid2207493

20 Ley de Defensa Nacional. Recuperado de http://servicios.infoleg.gob.ar/infolegInternet/anexos/20000-24999/20988/texact.htm

24.059[21]. A su vez, la Ley de Inteligencia Nacional N° 25.520[22], en su artículo 4, prohíbe a todos los organismos que integran el Sistema Nacional de Inteligencia realizar tareas de inteligencia sin orden judicial. Reserva para las Fuerzas de Seguridad la producción de Inteligencia Criminal y para las Fuerzas Armadas la Inteligencia Estratégica Militar, cada una en sus respectivos ámbitos de actuación.

En el campo de la Ciberdefensa / Ciberseguridad, los incidentes de Estonia en 2007 motivaron a los gobiernos del mundo a desarrollar políticas y estrategias en cuanto a seguridad de la información, así como competencias en operaciones cibernéticas de seguridad y defensa. En este contexto internacional, comenzaron a surgir normativas que van organizando la temática, de acuerdo al siguiente proceso.

En el año 2011, se creó en Argentina el Programa Nacional de Infraestructuras Críticas de Información y Ciberseguridad[23] mediante la Resolución de la Jefatura de Gabinete de Ministros N° 580/2011. Posteriormente, por Resolución 385/13 se conformó la Unidad de Coordinación Cibernética en el ámbito de la Jefatura de Gabinete de Asesores del Ministerio de Defensa, integrada por diferentes organismos del Ministerio de Defensa y la Fuerzas Armadas.

En 2014, se dictó la Directiva de Política de Defensa Nacional (DPDN), que determinó que el Ministerio de Defensa adhiera al Programa Nacional de Infraestructuras Críticas de la Información y Ciberseguridad perteneciente a la Oficina Nacional de Tecnologías de la Información bajo la órbita de la Jefatura de Gabinete de Ministros. En el mismo año, mediante la Resolución 343/14, se creó el Comando Conjunto de Ciberdefensa, dependiente del Estado Mayor Conjunto de las Fuerzas Armadas.

En el año 2015, en el ámbito de Ministerio de Defensa, se creó la Dirección General de Ciberdefensa mediante la Decisión Administrativa N°15[24] de la Jefatura de Gabinete de Ministros. El 21 de enero de 2016, por Decreto

21 Ley de Seguridad Interior. Recuperado de http://servicios.infoleg.gob.ar/infolegInternet/anexos/0-4999/458/norma.htm

22 Ley de Inteligencia Nacional. Recuperar de http://servicios.infoleg.gob.ar/infolegInternet/anexos/70000-74999/70496/norma.htm

23 Programa Nacional de Infraestructuras Críticas de Información y Ciberseguridad. Recuperado de http://www.icic.gob.ar/

24 Decisión Administrativa N° 15/2015 JGM. Recuperado de http://servicios.infoleg.gob.ar/infolegInternet/anexos/240000-244999/244566/norma.htm

226/2016[25] se la elevó al rango de Subsecretaría de Ciberdefensa, y depende de la Secretaría de Ciencia, Tecnología y Producción para la Defensa en el ámbito del citado Ministerio. La nueva Subsecretaría cuenta con la Dirección Nacional para el Desarrollo Científico de la Ciberdefensa y la Dirección Nacional de Diseño de Políticas de Ciberdefensa.

Al año siguiente, en la órbita del entonces Ministerio de Modernización, se creó la Subsecretaría de Tecnología y Ciberseguridad mediante el Decreto 13/2016[26]. De igual modo, por Decreto 577/2017[27] del Poder Ejecutivo Nacional, se creó el Comité de Ciberseguridad en la órbita del Ministerio de Modernización. Posteriormente, el 2 de marzo de 2018, mediante el Decreto 174/2018[28], se aprobó el Organigrama de Aplicación de la Administración Nacional hasta el nivel de Subsecretaría. En tal sentido, mediante esta normativa, quedaron establecidos los objetivos de la Subsecretaría de Ciberdefensa, también en marzo de 2018, se dictó la Decisión Administrativa N° 310/2018 de la Jefatura de Gabinete de Ministros, por medio de la cual se aprobaron las estructuras organizativas de primer y segundo nivel operativo y determinaron sus responsabilidades primarias y acciones pertinentes. Durante el desarrollo de esta investigación, la Secretaría de Gobierno de Modernización, dependiente de Jefatura de Gabinete de Ministros, dictó la Estrategia Nacional de Ciberseguridad, mediante la Resolución 829/2019[29], aprobada el 24 de mayo de 2019. En los considerandos surge como paradigma que las Tecnologías de la Información y las Comunicaciones se constituyen en algunos de los principales motores del progreso y bienestar humano. Por ello, el ciberespacio pasó a ser un elemento esencial en la vida de las personas y el Estado Nacional

25 República Argentina. Decreto N° 226/2016. Buenos Aires, 21/01/2016. Disponible en: https://www.argentina.gob.ar/normativa/nacional/decreto-226-2016-258020/texto

26 República Argentina. Decreto N° 13/2016 Decreto N° 357/2002. Modificación, Buenos Aires, 05/01/2016. Recuperado de http://servicios.infoleg.gob.ar/infolegInternet/anexos/255000-259999/257556/norma.htm

27 República Argentina. Decreto N° 577/2017. Buenos Aires, 31/07/2017. Recuperado de https://www.argentina.gob.ar/normativa/nacional/decreto-577-2017-277518/texto

28 República Argentina. Decreto N° 174/2018. Buenos Aires, 02/03/2018. Recuperado de http://servicios.infoleg.gob.ar/infolegInternet/anexos/305000-309999/307419/norma.htm

29 Estrategia Nacional de Ciberseguridad. Recuperado de http://servicios.infoleg.gob.ar/infolegInternet/anexos/320000-324999/323594/norma.htm

fijó en sus planes de largo plazo dotar al país de capacidades de prevención, detección y neutralización de actividades ciberespaciales maliciosas. Entre los objetivos centrales de esta Estrategia Nacional de Ciberseguridad se encuentran la generación de un marco normativo, la capacidad de respuesta a incidentes de seguridad a gran escala, la protección de infraestructuras críticas, integración con otros países y la creación de una cultura de ciberseguridad.

Contexto académico institucional. Posgrados existentes

- Diplomatura Gestión y Estrategia en Ciberseguridad, Universidad del CEMA[30]: el programa está dirigido a todas aquellas personas del ámbito público y privado que quieran formarse como profesionales y líderes en la gestión de la ciberseguridad. El perfil general de los participantes es de profesionales y/o expertos en seguridad, tecnología, gestión de riesgos, derecho en nuevas tecnologías u otras materias relacionadas, con expectativas de desarrollo y potencial de crecimiento que se encuentren interesados en fortalecer las herramientas de gestión, liderazgo y visión estratégica de la Ciberseguridad desde la visión de CISOs y líderes de opinión del mercado. El plan curricular consta de 8 módulos, en los cuales se abordan las siguien tes temáticas: la ciberseguridad y sus tendencias; gobierno y liderazgo de la seguridad de la información; operaciones y gestión de riesgos de cibersegu ridad; protección de activos de información; aspectos jurídicos de la ciber seguridad; informática forense; inteligencia, espionaje e ingeniería social; el paradigma de la seguridad ofensiva. Además, cuenta con conferencias magistrales que se refieren a temáticas de actualidad, tales como Seguridad en la Nube, *blockchain*, Seguridad en infraestructuras críticas, Seguridad en la transformación digital, entre otras.

- Diplomatura en Ciberseguridad, Universidad CAECE[31]: el objetivo de la

30 Diplomatura Gestión y Estrategia en Ciberseguridad, Universidad del CEMA. Buenos Aires, Argentina: CEMA. Recuperado de https://ucema.edu.ar/educacion-ejecutiva/ciberseguridad

31 Diplomatura en Ciberseguridad, Universidad CAECE. Buenos Aires, Argentina: CAECE.

diplomatura es proveer conocimientos básicos de seguridad informática y física, a fin de que los profesionales tomen conocimiento de esta disciplina, se familiaricen con la terminología, normas, productos, servicios y riesgos existentes. Además, que puedan asesorar a su empresa y/o a sus clientes, y despertar en la audiencia la prevención correspondiente. Se encuentra dirigida a alumnos de carreras informáticas con nociones básicas de redes de telecomunicaciones; profesionales informáticos y de seguridad; personal de operaciones de IT y redes de empresas privadas y organismos públicos; profesionales informáticos miembros de las FFAA y FFSS; profesionales cuya misión los vincule con el manejo de información privada y confidencial (abogados, escribanos, secretarios de juzgados, personal de estudios jurídicos y contables).

- Maestría en Ciberdefensa, Facultad de Ingeniería del Ejército, Universidad de la Defensa[32]. La Carrera de grado en criptología implementó un segundo año de especialización en la temática ciber, mediante la cual se accedería a la maestría en Ciberseguridad. Fue aprobada por el Ministerio de Educación el 4 de septiembre de 2019 mediante Resolución Ministerial N° 2660/19.

- Maestría en Ciberdefensa y Ciberseguridad, Universidad de Buenos Aires.[33] La maestría busca complementar la formación de agentes gubernamentales y de ejecutivos empresariales mediante una la formación conceptual e instrumental en Ciberdefensa y Ciberseguridad, de manera de posibilitar su actuación en los casos de cibercrimen organizado transnacional, ciberespionaje, activismo *hacker,* ciberterrorismo y también en los casos de ciberagresiones entre Estados naciones. Entre los objetivos que se plantea figuran: capacitar y formar en el diseño e implementación de sistemas de detección de ciberintrusiones y en arquitecturas de hardware/software robustas; en el desarrollo de software seguro; en la detección de la circulación de *malware*

Recuperado de http://www.ucaece.edu.ar/agenda/diplomatura-en-ciberseguridad/

32 Maestría en Ciberdefensa, Facultad de Ingeniería del Ejército, Universidad de la Defensa. Buenos Aires, Argentina: UNDEF. Recuperado de https://www.undef.edu.ar/nueva-oferta-de-posgrado-ciberdefensa/, http://www.fie.undef.edu.ar/?p=7226

33 Maestría en Ciberdefensa y Ciberseguridad, Universidad de Buenos Aires. Buenos Aires, Argentina: UBA. Recuperado de http://www.economicas.uba.ar/posgrado/posgrados/ciberdefensa-y-ciberseguridad/

en las redes teleinformática; en la preservación de la infraestructura crítica de diversos tipos de ciberagresiones; en *backtracing* y en resolver el "problema de la atribución"; en generar elementos probatorios acerca del ciberataque y del ciberatacante; para formar parte de CERT (*Computer Emergency Response Team*) y para liderar dichos equipos; para desempeñarse en posiciones de liderazgo en diversos tipos de emprendimientos en el contexto de la Ciberdefensa y de la Ciberseguridad.

El plan de estudios consta de veinte materias, separadas en una etapa de formación general con trescientas veinte horas y otra etapa que incluye asignaturas específicas referidas a aspectos operativos de Ciberdefensa y Ciberseguridad, que suman doscientas veinticuatro horas. Además, cuenta con talleres de investigación supervisada. Los temas abordados curricularmente en la formación general son: tecnología de la Información, ética y normativa jurídica, introducción al gerenciamiento innovador, introducción a los paradigmas de programación, tecnología de la información, introducción a la Criptología, evolución de la tecnología militar hasta el enfoque *network-centric warfare,* tecnología de tedes, *malware,* fundamentos y gerenciameinto de la Ciberdefensa y de la Ciberseguridad, ciberataques masivos a sistemas de información. Mientras que en los aspectos operativos de la especialidad el currículum considera: principios y enfoques de diseño de software seguro, proyecto sobre principios y enfoques de diseño de software seguro, teoría organizacional y psicología organizacional, diseño y desarrollo de la *data exchange layer* en ambientes de gobierno, data *mining – data warehousing – big data*, seguridad en redes de computadoras.

En función de lo expuesto y del trabajo desarrollado, se presentan a continuación los primeros resultados de la investigación.

Ejes de investigación

Aspectos curriculares

El primer eje indagado sobre la formación de posgrado en Ciberdefensa y Ciberseguridad abordó algunas cuestiones que tienen que ver con los aspectos curriculares. Al respecto, nos propusimos conocer las formas en que se estructuran dichas formaciones, los criterios que siguieron y de dónde surgieron los mismos. De igual manera nos interesó conocer cómo se esta-

blecieron los contenidos a enseñar y qué corrientes o doctrinas siguen. En el mismo sentido indagamos sobre qué aspectos y especialidad del área se orienta cada uno, y qué rol tienen en esta formación los cursos cortos. Además, nos interesó conocer si las currículas incluyen las políticas, marcos doctrinarios o directivas para la formación de capacidades humanas y tecnológicas en la especialidad. Finalmente buscamos develar si los abordajes curriculares tratan sobre planeamiento estratégico, táctico u operacional, ciberinteligencia, entre otros y qué características presentan estos abordajes.

Respecto a los criterios curriculares, podemos decir que la mayoría de los casos analizados surge de experiencias profesionales previas o de carreras en seguridad informática. De igual manera, aparecen como relevantes las experiencias de empresas que sufrieron ataques informáticos. De igual modo, se identificó que todos los criterios curriculares se guían por enfoques pragmáticos del ejercicio profesional, que son orientados por los activos a proteger y el modo de hacerlo. Solo un caso de los analizados –el de la maestría ofrecida por la UBA-ENI– sigue el modelo de la universidad de Talin en la misma especialidad.

En cuanto a estructura y marco curricular, en general no pudieron dar cuenta sobre esto, salvo la maestría UBA-ENI, que manifestó seguir un modelo adaptado de una carrera similar ofrecida por la universidad de Talin y con los criterios de la OTAN. En relación a la estructura y al marco curricular, es válido destacar el lugar otorgado a los cursos cortos de formación. Al respecto, si bien todos los entrevistados consideran que no son suficientes como única formación en el tema, los conciben como la mejor propuesta práctica para aprender o socializar el tema y evitar, en muchas instancias y ámbitos, un diálogo de sordos donde no se entienden o no comprenden de qué se habla.

Si miramos la orientación de las formaciones, un primer aspecto develado es que estas se encuentran orientadas a la gestión o *management,* sin focalizar en lo técnico, excepto la maestría de ingeniería del Ejército, con base en criptología y casi exclusivamente dirigida a ingenieros y técnicos de la especialidad. Algunas currículas incluyen en su orientación técnica aspectos sobre desinfección de equipos, detección de fallos de seguridad y aspectos normativos para montar un sistema de gestión de seguridad informática. La investigación también permitió observar que en las orientaciones de estas formaciones de posgrados se incluyen cuestiones jurídicas de delitos informáticos, protección de datos, cuantificación y valuación de activos, aspectos

de gestión tanto en la ciberseguridad como, aunque menos, de la ciberdefensa. Finalmente, podemos decir que los actuales posgrados tienen una orientación operativa gerencial. En el estado actual de los planes curriculares y las pretensiones políticas-académicas, éstos no se plantean la formación de tecnólogos en ciberdefensa o seguridad.

Finalmente, respecto de los aspectos curriculares, se tuvo en cuenta la inclusión de políticas, doctrinas y directivas tanto para la estructuración de las formaciones como para la discusión en sus abordajes pedagógicos. Al respecto, las especializaciones mencionaron no incluir estos contenidos, dado que no tienen vínculos con el Estado y porque su enfoque es meramente pragmático. En contraposición a esta postura, tanto la maestría UBA-ENI como el abordaje del tema en el Curso Superior en Defensa Nacional manifestaron tenerlo presente mediante el análisis normativo.

Vínculo entre currículum y contexto normativo

El vínculo entre lo curricular y el contexto normativo e institucional de la Ciberdefensa y Ciberseguridad constituyó el segundo eje de la investigación. Para ello, buscamos develar de qué manera y en qué medida la estructura normativa que constituyen las políticas públicas en la materia son incluidas y abordadas en las formaciones existentes y cómo lo aborda cada posgrado.

En un sentido amplio, se puede afirmar que algunos posgrados incluyen en su formación, de manera indirecta o a título informativo las siguientes normativas: ley de delitos informáticos, Ley de firma digital, Ley de protección de datos personales y ley de propiedad intelectual. En tanto que el Curso Superior de Defensa Nacional en FADENA aborda la Ley de seguridad interior, Ley de Defensa Nacional, Ley de inteligencia, la Política modelo seguridad de la información, Ley de firma digital, la Ley de protección de datos personales, la normativa A del BCRA e incluso la Ley de delitos informáticos.

Cooperación entre actores y estructuras

En el tercer eje de investigación se puso la mirada en los vínculos de cooperación entre actores, instituciones e instrumentos o dispositivos pedagógicos que fortalezcan y consoliden tanto la formación como la construcción

colectiva del conocimiento en este incipiente, pero vertiginoso campo intelectual y profesional.

Al considerar vínculos o cooperación con universidades, empresas y Estado sobre aspectos técnicos, políticos, presupuestarios o curriculares vinculados a la ciberdefensa o ciberseguridad, únicamente aparecieron mencionados vínculos a título personal (tanto académicos como profesionales). Sin embargo, no se evidenciaron vínculos institucionales, a excepción de la maestría UBA/ENI quien participó de ejercicios con la Escuela Superior de Guerra Aérea y el Comando Conjunto de Ciberdefensa.

Por otra parte, cuando se indagó sobre ejercicios de simulación o entrenamiento real en cuestiones de ciberdefensa o ciberseguridad y las características de su contexto, de la investigación surge que solo el personal militar que integra el Comando Conjunto de Ciberdefensa participa de este tipo de ejercicios con otras Fuerzas regionales o de España.

En este eje, la investigación se propuso mapear el reconocimiento a otros actores, de modo de poder dar cuenta de los vínculos entre pares e identificar especialistas en el área. En general, nadie ha podido o ha querido dar cuenta sobre este aspecto, tanto en lo general como en lo particular. De igual manera, no surgieron disputas intelectuales, doctrinarias o curriculares que se pudieran identificar entre las ofertas de formación en el tema.

Desafíos y dilemas

En cuarto lugar, se trabajó sobre desafíos y dilemas del ámbito ciberspacial, percibidos y abordados por los diferentes posgrados. Al respecto, la investigación buscó conocer qué tipo de planteos hacen los posgrados sobre los desafíos y dilemas de este ámbito tanto para la Defensa Nacional como para la Seguridad Ciberespacial, y la manera en que los abordan. También se indagó en torno al cambio vertiginoso que representa el ciberespacio y su implicancia en la formación, pretendiendo develar la forma de pensar y responder frente a ella que tienen los posgrados en la especialidad. De igual manera, buscamos conocer la percepción de estas formaciones respecto a la dependencia tecnológica y curricular.

Respecto a los planteos de los posgrados que hacen frente a los desafíos actuales que representa la ciberdefensa o ciberseguridad en Argentina, el primero que surgió es que en el país estamos a años luz de tomar conciencia

sobre los riesgos e implicancias de la ciberdefensa y seguridad. Otro aspecto relevante surgido de la investigación tiene que ver con la masa crítica de especialistas altamente formados con que cuentan India, Pakistán, Rusia, China, EE. UU. , Corea del Norte y del Sur, entre otros, quienes disponen de alrededor de 12 mil especialistas en temas ciber, según los entrevistados. En lo particular, plantean que en Argentina estamos muy lejos en todos los sentidos y no se observan políticas claras y concretas para achicar la brecha. También surge como un planteo recurrente la cuestión sobre cómo hacer entender a quienes toman decisiones en los niveles más altos de las necesidades, prioridades y conveniencia de los aspectos ciber, para evitar que piensen que la postergación es una opción. De igual modo, surge el planteo sobre la separación entre ciberdefensa- ciberseguridad dada por las leyes actuales y los inconvenientes en la aplicación práctica. Consideran que esto demanda estrategias para ensamblar los diferentes componentes. Finalmente, en cuanto a planteos aparece, vinculada a cuestiones curriculares, la necesidad de que quienes se formen en el área tengan que aprender estrategia, inteligencia y contrainteligencia, alertas tempranas y determinación efectiva si algo está debidamente protegido o no.

Por otra parte, frente al interrogante sobre cómo abordan la actualización curricular, no se dan precisiones. Todos comentan que la propia realidad y práctica va actualizando la currícula. También expresan que es un tema no tenido en cuenta por varias razones: estado de madurez o desarrollo curricular de la temática, orientaciones más técnicas profesionales y no tanto académica de algunos posgrados, apuro en armar la oferta dada la demanda del mercado en la temática. En el mismo sentido, podemos decir que cuando se indagó respecto de la dependencia tecnológica y curricular, se pudo constatar que la cuestión no es un tema abordado en los posgrados.

Por último, en el cuarto eje de investigación se buscó develar los desafíos-dilemas que reconocen los posgrados en ciberdefensa o Ciberseguridad. En primer lugar, se visibiliza el desafío-dilema de determinar necesidades y tipos de abordajes para diferentes términos, conceptos y marcos doctrinarios y legales. En el mismo sentido, podemos determinar a nivel interno de cada Fuerza Armada y agencias del Estado si hay un plan y/o criterios para la formación en esta disciplina. Por otra parte, todos coinciden en que “estamos en pañales” en cuanto al desarrollo, comprensión y formación en Ciberdefensa/ciberseguridad: el tema ya surgió, está instalado, pero hay mucho por recorrer. La investigación también develó la necesidad de

definir, consensuar, adoptar un cuerpo doctrinario rector que guíe y estructure la formación en la disciplina, dado que la formación actual, altamente dispersa en enfoques, contenidos y capacidad técnica, presenta baches de conocimiento que luego demandan más formaciones en muchos aspectos. Finalmente, se identificó que actualmente existe el desafío (actual problema teórico-metodológico-normativo) de encontrar cómo bajar los objetivos del área (que son claros) a nivel de conocimiento.

Posgrados y perfiles profesionales

Como quinto eje, la investigación indagó sobre los perfiles profesionales requeridos por la especialidad y la relación que presentan con este aspecto los posgrados en su situación actual. Tanto en el sector público como en el privado, en materia de ciberdefensa o ciberseguridad, existen distintos tipos y niveles de requerimientos de formación orientados al personal. En tal sentido, se buscó identificar en las diferentes orientaciones curriculares de los posgrados, los aspectos tenidos en cuenta para tal fin.

En cuanto a orientaciones o demandas sobre perfiles, este trabajo da cuenta que nadie tiene conocimiento sobre demandas u orientaciones de perfiles a formar tanto del sector privado como del estatal. Al respecto, consideran que se podrían inferir dichos perfiles a partir de las políticas y objetivos de la normativa sobre ciberdefensa o ciberseguridad, como también de lo que muestra el Comando Conjunto de Ciberdefensa.

En función a los perfiles a los que se orientan los posgrados, podemos decir que en general no están dirigidos a la formación de un perfil específico, y que muestran ampliamente –y de modo general– aspectos de ciberseguridad. De acuerdo a la investigación, las especializaciones están dirigidas a profesionales de niveles medios y altos vinculados a temas de seguridad informática, con la mirada puesta en futuros CISOS. Por otra parte, la maestría UBA/ENI se orienta al gerenciamiento y, si bien no forma tecnólogos en la especialidad, busca que puedan interactuar y comprender a aquellos cuando dirijan y tomen decisiones ciber.

Quedan por comunicar otros aspectos de la investigación que se hallan en desarrollo: incentivos para la formación, investigación e innovación en ciberdefensa, políticas públicas respecto a la formación en ciberdefensa y las conclusiones de cada eje.

Conclusiones parciales

El estado actual de la investigación permitió identificar, en los cinco primeros ejes, doce categorías de análisis con cuarenta y dos hallazgos. Tales categorías y hallazgos permiten estructurar una nueva línea de investigación con identidad propia dentro del área ciber: formación en Ciberdefensa y Ciberseguridad. Ambas constituyen un nuevo campo del saber (si bien son incipientes, presentan un crecimiento vertiginoso), con interés estratégico para el sector público y privado. Al mismo tiempo, presentan múltiples dimensiones desde las cuales pueden ser estudiadas y desarrolladas. Por ejemplo, desde lo económico, tecnológico, educativo, político, normativo, militar, entre otros.

Tanto para empresas del sector público y privado, como para los diferentes organismos del Estado y las áreas de defensa y seguridad, existen y existirán necesidades específicas, comunes y diferenciadas en torno a lo ciber. En función de ello, uno de sus intereses estará puesto en los recursos humanos que necesitan según sus características organizativas y objetivos o necesidades. Para ello, pensar la formación de dichos recursos a partir de bases comunes, pero con orientaciones o perfiles diferenciales, será una necesidad no solo de los ámbitos académicos sino también de aquellos que toman decisiones políticas (públicas y privadas). En este sentido, la investigación académica en torno a la formación sobre ciberdefensa y ciberseguridad adquiere relevancia y un interés estratégico.

Bibliografía

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. (7-02-2015). *El más fuerte es el más vulnerable.* Diario El País, España. 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, Vol. 12 (1), pp.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). E*l ciberespacio y sus implicancias en la defensa nacional. Aproximaciones al caso argentino.* Recuperado de http://sedici.unlp.edu.ar/bitstream/handle/10915/40210/Documento_completo.pdf?sequence=1

Feliú, L. (2013). *Seguridad Nacional y Ciberdefensa, una aproximación conceptual*. Conferencia en la UPM, Madrid, 21 de enero 2013. Recuperado de http://catedraisdefe.etsit.upm.es/wp-content/uploads/2013/01/Ponencia-Luis-Feliu.pdf.

Feliú Ortega, L. (2012). *El espacio cibernético nuevo escenario de confrontación*. Cuadernos del CESEDEN, febrero de 2012, pp. 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. (2014). *Informes de actualidad y temáticas de defensa*. EDENA: Secretaría de Investigación, 11-08-2014, p. 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) (pp. 66-67). West Lafayette, EE. UU.: Purdue University, 24-25 marzo de 2014.

Libicki, M. C. (2009). C*yberdeterrence and Cyberwar.* RAND Corporation.

Ocón, A. L. (2019). *Educación, conocimiento y poder: debates lógicos-epistémicos y enfoques alternativos respecto de la naturaleza humana.* Anacronis-

mo e Irrupción, Vol. 9 (16), pp. 113-147.

Stel, E. (2005). *Guerra Cibernética*. Buenos Aires, Argentina: Círculo Militar, 1ra Edición.

Sheldon, J. (2011). *Deciphering Cyberpower. Strategic Purpose in Peace and Ward*. Strategic Studies Quarterly. Summer Edition. Recuperado de http://www.airuniversity.af.mil/SSQ/

Singer, P. and 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), pp. 589-618.

Theohary, C. y Harrington, A. I. (2015). *Cyber Operations.* DDD Policy and Plans: Issues for Congress, January 5. Recuperado de https://www.hsdl.org/?view&did=761572

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.

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