Ciberdefensa y formación de posgrados en Argentina: reflexiones a partir de perspectivas políticas y sociales para el interés de la Soberanía Nacional

Cyber defense and postgraduate education in Argentina: reflections from political and social perspectives for the interest of national sovereignty

GUILLERMO RUTZ
Facultad de la Defensa Nacional,
Universidad de la Defensa Nacional, Argentina
rutzguillermo@gmail.com

En este artículo, se reflexiona desde un abordaje social, educativo, de políticas públicas y cuestiones curriculares sobre los hallazgos respecto a la formación de posgrado en Ciberdefensa para Argentina en 2019. En dichas aproximaciones, se presentan miradas que buscan interpelar respecto a la realidad local a partir de recorridos comparativos de las agendas latinoamericanas y española sobre las siguientes cuestiones: criterios curriculares, estructura y marco curricular, orientación de la formación, Inclusión de Políticas, Doctrinas y Directivas, vínculos o cooperación con universidades, empresas y Estado, ejercicios de simulación, reconocimiento de otros actores, planteos que los posgrados se hacen frente a los desafíos, forma de abordar la cuestión curricular, dependencia curricular y tecnológica, desafíos y dilemas que se reconocen, orientaciones y demandas sobre perfiles a formar, perfiles profesionales a los que se orientan los posgrados.

1. Introducción

La ciberdefensa es un área de reciente incursión en el ámbito de la Defensa Nacional, donde las noticias dan cuenta de su aparición en la agenda pública recién en 2014. Las primeras normativas que plasman la estrategia nacional sobre el tema surgen en 2019. El presente siglo, atravesado y caracterizado por la irrupción e impacto de las tecnologías de la información y de las comunicaciones, donde cada momento, hecho y acción humana, organizacional y estatal están vinculadas a internet y las tecnologías digitales, impuso nuevos desafíos, retos y vulnerabilidades a la actividad del Estado de preservar su Soberanía Nacional. Esto ha llevado a pensar y proponer nuevas políticas, estructuras agenciales e instancias académicas de formación vinculadas a la temática.

La "convergencia digital"[1] del ciberespacio que hace posible la conexión en tiempo real del conocimiento, actividades e información local con lo global en ámbitos como el comercio, las relaciones entre individuos, Estados y organizaciones, genera vínculos entre sociedades con características de mayor vulnerabilidad en cuanto a seguridad y defensa. En este contexto, la información se ha convertido en un activo estratégico cuyo uso se convierte en un factor de poder que afecta las relaciones e intereses nacionales tanto de forma positiva como negativa.

La agenda universitaria ha respondido con celeridad ante este nuevo camp. En tal sentido, en Argentina se crearon ofertas de posgrados tanto en cursos de especialización como maestrías que se orientan a la ciberdefensa y ciberseguridad. Esta nueva realidad en el ámbito académico, y con implicancias para la Defensa Nacional, dio lugar a la investigación sobre la cual reflexionamos en este artículo. Dicha investigación fue llevada a cabo en el contexto de Universidad de la Defensa

1 Dalbello, M. (2015). Digital Convergence: The past in the present. En Spence Richards, P. et al. (eds.) A Histoy of Modern Librarianship: Constructing the Heritage of Western Cultures. California: Libraries Unlimited Ed.

Nacional, en la Facultad de la Defensa Nacional, en el marco del Equipo de investigación UNDEFI: "Soberanía nacional y ciberdefensa. Elementos teóricos y político-estratégicos del desafío ciberespacial para la Defensa Nacional" cuya línea de investigación corresponde a la "Formación de posgrado en Ciberdefensa y Ciberseguridad".

De este modo, en el presente artículo se reflexiona desde un abordaje social, educativo, de políticas públicas y cuestiones curriculares sobre los hallazgos respecto a la formación de posgrado en Ciberdefensa para Argentina en 2019. En dichas aproximaciones, se presentan miradas que buscan interpelar respecto a la realidad local a partir de recorridos comparativos de las agendas latinoamericanas y española sobre las siguientes cuestiones: criterios curriculares, estructura y marco curricular, orientación de la formación, Inclusión de Políticas, Doctrinas y Directivas, vínculos o cooperación con universidades, empresas y Estado, ejercicios de simulación, reconocimiento de otros actores, planteos que los posgrados se hacen frente a los desafíos, forma de abordar la cuestión curricular, dependencia curricular y tecnológica, desafíos y dilemas que se reconocen, orientaciones y demandas sobre perfiles a formar, perfiles profesionales a los que se orientan los posgrados.

2. Categorías investigadas

Aspectos curriculares

Respecto a los *criterios curriculares*[2], podemos decir que la mayoría de los casos analizados surgen de experiencias profesionales previas o de carreras en seguridad informática. De igual manera, aparecen como relevantes las experiencias de empresas que sufrieron ataques informáticos. Asimismo, se identificó que todos los criterios curriculares se guían por

2 Ver referencias consultadas en bibliografía.

enfoques pragmáticos del ejercicio profesional, los cuales son orientados por los activos a proteger y el modo de hacerlo. Sólo 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 los hallazgos sobre criterios curriculares, en el marco de esta investigación, considero que el estado actual de la formación sobre ciberdefensa/seguridad en Argentina debe evolucionar, en primer lugar, hacia criterios y concepciones curriculares basadas en diagnósticos y prognosis vinculadas a las necesidades locales y regionales. Los avances tecnológicos en el ámbito ciber han aumentado los ciberataques en todos los frentes. Esto demanda un esfuerzo en todas las ramas de las Fuerzas Armadas para pensar, adecuar e incrementar la capacidad de formación de los recursos humanos con ciertas particularidades, como por ejemplo la dificultad para la disuasión en un quinto dominio donde es muy difícil probar la autoría, lo cual conlleva a la dificultad para responder. Por ello, la ciberdefensa y la ciberseguridad deben ser abordadas tanto en su formación como en sus políticas (ya sean del ámbito público, académico o del sector productivo) desde lo multidisciplinar, en donde estén presentes: el diseño de sistemas, la creación de arquitecturas seguras, la concientización, los diferentes perfiles profesionales que se requieren, entre otros aspectos. Para este cometido, es indispensable una financiación adecuada, la presencia y colaboración entre diferentes organismos del Estado, la investigación permanente y la cooperación a nivel nacional e internacional.

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 tanto de la estructura como del marco curricular, es válido destacar el lugar otorgado a los cursos cortos de formación. Al respecto, si bien todos los entrevistados con-

sideran que no alcanzan 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 lo que se habla.

Hay quienes creen que lo curricular es fácil de resolver, tanto en tiempo como en pensamiento. Hay quienes creen que lo curricular es de una importancia menor, no estratégica o no apropiada para detener en ella la mirada de los analistas políticos o de la Defensa. También hay quienes creen que lo curricular es un paquete cerrado de fácil adquisición, que basta sacar del estante el diseño curricular. Ante estos puntos de vista, es necesario decir que las cuestiones curriculares ocupan un lugar central en la investigación educativa desde siempre. Para saber qué enseñar, para poder enseñar y de un modo determinado, para conseguir éste o aquél resultado como producto del proceso formativo, para pensar una política educativa, es necesario antes detenerse, diagnosticar, evaluar y decidir qué se quiere hacer, con qué herramientas, en qué dirección, con qué recursos, en cuánto tiempo, entre otras consideraciones e indicadores a tener en cuenta. Esta investigación, sin embargo, no da cuenta que todas estas cuestiones estén contempladas por políticas públicas, por equipos de asesores de decisores políticos o por las instancias académicas.

Pasar por alto, o no detenerse apropiadamente en las cuestiones curriculares de lo que demanda para Argentina y para las particularidades estratégicas que la política le quiera dar a la formación de recursos humanos en temas de ciberdefensa, es comenzar a transitar este nuevo campo con una gran debilidad. En el área de Ciberdefensa, la formación de los recursos humanos debería implicar una cuestión estratégica respecto de las cuestiones técnicas, tecnológicas, conceptuales, doctrinales, de infraestructura, de vínculos y relaciones locales, regionales e internacionales, entre otros aspectos a considerar y que no aparecen tenidos en cuenta,

en lo que esta investigación devela con sus limitaciones.

Pensar las cuestiones curriculares también implica pensar cuánto de la formación será teórica y cuánto de práctica. ¿Qué aspectos, alcances y orientaciones tendrá cada una de ellas? ¿Se brindará una formación en base mayoritariamente a bibliografía en español para que todos los alumnos tengan facilidad de comprensión? O, en caso de considerarse más pertinente una bibliografía en otro idioma, ¿se dispondrá de traducción de obras? ¿Qué impacto tendrá una u otra decisión en los potenciales alumnos? Por ejemplo, un soldado, o un civil con cualidades y potenciales para el área, si no domina otro idioma, ¿debería verse restringido en formarse? ¿Cuántos de estos casos tendría el modelo formativo implementado y qué impactos representaría para la formación de recursos del área? Estas y otras cuestiones fundamentales, que hacen a una política educativa en la materia, no se ven contempladas actualmente en las consideraciones curriculares y el marco normativo existentes.

Si miramos la *orientación de la formación*[3], un primer aspecto develado es que estas se encuentran orientadas a la gestión o management sin focalizar 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

3 Ver referencias consultadas en bibliografía.

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.

El *machine learning* es una herramienta que permite automatizar el diagnóstico temprano de incidentes y agilizar procesos, liberando el trabajo de los analistas. Las grandes firmas dedicadas a la ciberseguridad consideran que el aprendizaje automático, junto con la inmersión en la nube, serán los pilares del desarrollo futuro en este tema. Para Roman Yampolskiy, vamos camino a "una especie de carrera armamentística en el ciberespacio" donde la inteligencia artificial permite, cada vez más, ataques informáticos de ingeniería artificial más automatizados y elaborados.

En el año 2018, se llevó a cabo una de las mayores conferencias de ciberseguridad organizada por la OTAN, el *Information Assurance Symposium* (NIAS18), en donde se destacó la importancia y necesidad en el entrenamiento tecnológico de ciberdefensa, donde el papel de las personas y su formación deben ser tenidos en cuenta, no sólo las tecnologías.

Podemos entonces pensar qué áreas comprende o lleva implícita la formación en ciberdefensa. En primer lugar, hay que considerar la formación en tres niveles: estratégico, que comprende lo político y lo gerencial, táctico y operativo. Dentro de estos niveles, se deben pensar los aspectos legales, tecnológicos, intra e inter agenciales, aspectos de cooperación nacional e internacional, inteligencia y contrainteligencia, además de marcos referenciales y doctrinarios, entre otros aspectos de la formación.

Algunos especialistas en el tema consideran que es necesario contar con personal calificado, con aptitudes suficientes orientadas a todos los niveles institucionales mediante programas generales y especializados de formación, capacitación y sensibilización. Al respecto, creo que es necesario pensar y definir qué tipo y nivel de

certificaciones deben proponerse como objetivos para la formación del personal, en qué sentido y alcance son necesarias según el nivel institucional de desempeño. Luego, en función de estas definiciones conceptuales, curriculares y metodológicas, se deberán definir los programas, los cuales requerirán particularidades distintivas, ya sean generales o especializadas, de formación o capacitación. De acuerdo a esta investigación, todo esto aún no está plasmado en políticas, programas, proyectos o documentos, como tampoco es un tema que esté visible en las agendas institucionales o políticas.

Es necesario, más aún dado que no fue posible hacer visible mediante este trabajo, acciones al respecto, que el Ministerio de Defensa, sus instituciones dependientes, relacionadas y vinculadas o posibles de vincular, identifiquen y definan los diferentes roles que deberán o necesitarán asumir los recursos humanos en los diferentes niveles y espacios institucionales de la Defensa Nacional, ya sean civiles o militares. Al mismo tiempo, deberán aportar a la definición y orientación de los modelos formativos que consideren necesarios para dichos roles. De estas definiciones y orientaciones surgirán en el ámbito educativo las especialidades, subespecialidades, especialidades secundarias o vinculadas en el área de la ciberdefensa, las cuales se deberán vincularse conceptual y curricularmente con los requerimientos conceptuales, técnicos y profesionales de los puestos a ocupar efectivamente.

En la orientación de la formación, es necesario trabajar sobre un plan de acción o propuesta para presentar a la CONEAU, de modo que, como política universitaria, las universidades promuevan sumar esta disciplina en sus carreras de posgrado. Esta política universitaria debería también contemplar mecanismos para que las universidades detecten la importancia y necesidad nacional de formar profesionales en esta disciplina. Asimismo, sería recomendable fomentar en las universidades que dictan la carrera de Ingeniería en Computación para que sean las *idea-*

factories de proyectos de soluciones para la Ciberseguridad y la Ciberdefensa en Argentina. Por otra parte, dado que en el sector privado, el área de informática y ciberseguridad tiene un alto porcentaje de idóneos que adquirieron experiencia y herramientas para su desempeño por fuera de acreditaciones universitarias, es necesario pensar la manera de sumarlos a la formación y acreditación académica para poder integrarlos al sistema. De lo contrario, quedarían excluidos de la posibilidad de completar formaciones académicas acordes.

Finalmente, sobre aspectos curriculares se tuvo en cuenta la *inclusión de políticas, doctrinas y directivas*[4], tanto para la estructuración de la formación como para la discusión en los abordajes pedagógicos de estas. 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 manifiestan tenerlo presente mediante el análisis normativo.

La formación, conocimiento y discusión del marco normativo y doctrinario en torno a la ciberdefensa es fundamental para comprender el contexto y las políticas públicas en el cual se van gestando y desarrollando tanto el tema como el área en sus diferentes dimensiones. Esto debería darse en los ámbitos institucionales de organismos del Estado, en las universidades, en el sector privado, en los aspectos profesionales de las diferentes Fuerzas Armadas, en los espacios de investigación o en las formaciones que se desarrollen o puedan pensar. Conocer las cuestiones normativas es también conocer los alcances, los vacíos y las debilidades del tema, donde se requiere poner mayor esfuerzo.

La inclusión de políticas, normativas y doctrinas en la formación permite pensar y revisar los marcos institucionales

4 Ver referencias consultadas en bibliografía.

y legales, las estrategias de desarrollo de sistemas informáticos, los planes y programas de concientización orientados a la población, las agencias e instituciones del Estado, como también el sector privado. Esto permite conocer y pensar marcos de cooperación local e internacional para la capacitación y formación de profesores, científicos, funcionarios, expertos y personal operativo. Se ve como una debilidad de la formación el abordaje curricular reflexivo y crítico del marco normativo actual y sus proyecciones futuras.

Cooperación entre actores y estructuras

Al considerar *vínculos o cooperación con universidades, empresas y Estado*[5], 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, que participó de ejercicios con la Escuela Superior de Guerra Aérea y el Comando Conjunto de Ciberdefensa.

En países como España se pueden observar ejemplos de cooperación entre Estado y sector productivo a través de casos como los proyectos Cyber Situational Awareness (Cysa) y Airbone Electronic Attack (Aea). En el caso de Cysa, se enfoca al desarrollo de una plataforma para mejora de la conciencia situacional en ciberdefensa, mientras que Aea se basa en el desarrollo de capacidades aéreas de ataque electrónico. A su vez, desde el proyecto Cysa España, Alemania e Italia acordaron, en el marco de la Agencia Europea de Defensa, la creación de un grupo investigación sobre los desafíos que tienen los responsables militares en la toma de decisiones en el ciberespacio. Por su parte, Aea busca aprovechar la experiencia del sector productivo en el desarrollo de pods de

5 Ver referencias consultadas en bibliografía.

guerra electrónica para aeronaves.

Estos ejemplos de cooperación son frecuentes a lo largo de toda Europa y están visibles en las agendas, tanto sociales como de los tres componentes del triángulo sabatino (Estado, Universidades y Sector Productivo). Ello se debe a que consideran que los retos del sector ciber representan desafíos tecnológicos muy complejos y que es un sector en rápido crecimiento que demanda soluciones efectivas, donde la solución es la cooperación no sólo dentro de un mismo país, sino también entre países miembros de coaliciones.

En una entrevista, el jefe del Mando Conjunto de Ciberdefensa de España comenta que este Mando trabaja estrechamente con la industria para desarrollar productos y capacidades. De igual modo, lleva adelante proyectos con las universidades en áreas de enseñanza y formación. En este sentido, han desarrollado un campo de maniobras virtual que permite generar escenarios para ejercicios. En cuanto a retos, considera que la inversión y la formación son los dos ejes fundamentales, donde la formación no puede detenerse y es clave para contar con el personal calificado que se requiere, lo que se transforma en una necesidad y un desafío.

Un punto interesante es considerar las expresiones del entonces Ministro de Defensa de España, Pedro Morenés, quien afirmó en 2014 que "la clave en torno al ciberespacio es la integración de los saberes y la acción común de todos los actores de la sociedad" y que en materia de ciberdefensa "es una responsabilidad compartida entre Estado, sociedad civil y empresas", afirmaciones en concordancia con lo postulado por Sábato en su teoría del triángulo de relaciones científico–tecnológicas. Para Morenés, el personal abocado a la ciberdefensa "debe contar con las mejores herramientas, necesitando además innovación tecnológica e investigación continua".

En materia de vínculos y cooperación es importante que profesionales, profesores e investigadores cuenten con

canales y contextos institucionalizados de cooperación con el Estado y el sector productivo vinculados a los aspectos ciber, dado que esto permitirá generar líneas de desarrollo y mejora en la formación de futuros especialistas, al mismo tiempo que permitirá desarrollar un saber plural con una visión global. El conocimiento, la anticipación y la capacitación de recursos humanos son aspectos esenciales para enfrentar los nuevos retos vinculados a la ciberdefensa.

Por otra parte, cuando se indagó sobre *ejercicios de simulación*[6] o entrenamiento real en cuestiones de ciberdefensa o ciberseguridad y las características de su contexto, de la investigación surge que sólo el personal militar que integra el Comando Conjunto de Ciberdefensa participa de este tipo de ejercicios con otras fuerzas regionales o españolas.

Para muchos expertos y concepciones políticas, los incidentes cibernéticos constituyen o podrían constituir amenazas profundamente globales, dado que una persona, un grupo de ellas o un Estado en cualquier lugar, dentro o fuera del país y sin importar la distancia, podrían afectar las infraestructuras críticas, los sistemas de tecnología de la información y comunicación tanto del sector estatal como privado. El crecimiento vertiginoso que las tecnologías posibilitan en este sentido demanda de profesionales altamente entrenados para hacer frente a dichas cuestiones. En tal sentido, en los países con mayor madurez en la temática ciber, el desarrollo y disponibilidad de simuladores para el entrenamiento de personal del ámbito estatal, privado, civil y militar es una prioridad.

Contar con simuladores y realizar ejercicios de simulación permite a quienes se forman poner en práctica y en tiempo real técnicas, acciones y comportamientos para aprender a contrarrestar o mitigar ataques, así como utilizar la tecnología disponible de manera de estar altamente preparados para

6 Ver referencias consultadas en bibliografía.

sobreponerse a un ataque lo mejor y más rápidamente posible (lo cual se conoce como resiliencia), como también comprender y tener internalizada la gestión continua del riesgo mediante medidas permanentes y continuas de prevención, detección y reacción.

Concebir un sistema de simulación implica también vincularse y posicionarse desde lo curricular, porque antes se debe pensar en el modelado y formalización del conocimiento necesario para plantear los escenarios de simulación que se vinculen efectivamente con la realidad de la ciberdefensa. Para ello, se deben identificar, definir y elaborar previamente catálogos de vulnerabilidades, ataques y contramedidas, lo cual también demanda tener en cuenta cuestiones curriculares de conceptos, contenidos, desarrollos, estrategias metodológicas, definiciones, opciones doctrinarias y políticas.

Disponer de un sistema de simulación demanda previamente la creación de un laboratorio donde sea posible el diseño y reingeniería de *malware* y producción de contramedidas, en concordancia con los diferentes ejercicios de simulación que se elaboren. También implica haber pensado, diseñado e implementado una arquitectura tecnológica estable para virtualizar sistemas de información y redes de comunicación complejos. Estas etapas llevan a pensar la necesidad de contar con otras posteriores, como el desarrollo de herramientas de análisis forenses de uso posterior al ejercicio, de manera tal que permita adquirir conocimientos sobre el comportamiento de los ataques y mejorar las capacidades y técnicas utilizadas. Todo lo mencionado está estrechamente vinculado con lo tecnológico, las definiciones políticas y doctrinarias, la investigación permanente y los diferentes aspectos curriculares implícitos, lo cual hace evidente la presencia y necesidad del vínculo sabatino dado por Estado, sector productivo (público y privado) y universidades.

En este eje, la investigación se propuso mapear el

reconocimiento a otros actores, de modo de poder dar cuenta respecto a vínculos entre pares e identificación de especialistas en el área. En general, nadie ha podido o 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

Respecto de *planteos que los posgrados se hacen frente a los desafíos* actuales de la ciberdefensa o ciberseguridad en Argentina, el primero que surgió es que en el país estamos a años luz de tomar conciencia sobre riesgos e implicancias de la ciberdefensa y ciberseguridad[7]. Otro aspecto relevante surgido de la investigación tiene que ver con la masa crítica de especialistas[8] altamente formados con que cuentan India, Pakistán, Rusia, China, EE. UU., Corea del Norte o 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, 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[9] 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,

7 Ver referencias consultadas en bibliografía.

8 Ver referencias consultadas en bibliografía.

9 Ver referencias consultadas en bibliografía.

vinculado a cuestiones curriculares, la necesidad de que quienes se formen en el área tienen que aprender estrategia, inteligencia y contrainteligencia, alertas tempranas y determinación efectiva de si algo está debidamente protegido o no[10].

Cuando se menciona "tomar conciencia sobre riesgos e implicancias del entorno ciber" cabe preguntarse sobre qué aspectos de la realidad podemos reflexionar. Al respecto, las experiencias de incidentes cibernéticos demuestran que los componentes de las infraestructuras críticas pueden ser objetos de ciberagresiones que impliquen consecuencias devastadoras para un país. Entre estos blancos, se pueden citar las centrales hidroeléctricas, las plantas nucleares, las destilerías de petróleo, los sistemas de aerotransporte, el sistema de telecomunicaciones, el sistema bancario, el sistema de seguridad social o el de salud. Al respecto, desde la producción científica académica faltan estudios y publicaciones que den cuenta de políticas, proyectos, planes, investigaciones y estado de situación de los entornos de cada uno de estos y otros componentes de infraestructuras críticas y su relación con acciones concretas para su protección. No se conocen estudios sobre estado del arte, de reflexiones críticas o análisis –tanto civiles como militares– de la cuestión o prospectivas respecto al nivel de vulnerabilidad, acciones, como tampoco surgen investigaciones tendientes a evitar que minerías de datos puedan ser incorrectamente derivadas a destinatarios nacionales o internacionales que no correspondan.

Sobre los riesgos e implicancias, es necesario, sin entrar en estados paranoicos, entender y tomar conciencia que en lo relacionado al espacio cibernético existe una industria ilegal que para muchos expertos está en primer lugar y altamente profesionalizada. En esa industria, los cibercriminales usan inteligencia artificial para complejizar y efectivizar sus

10 Ver referencias consultadas en bibliografía.

ataques. En este mismo sentido, para Yampolskiy hay una tendencia clara y cierta donde el ciberespacio se encamina hacia una especie de carrera armamentística que unos usarán para proteger y otros para delinquir, robar o atacar.

Un riesgo concreto con implicancias reales –muchas veces desconocidas– es la forma en que se utilizan en distintos entornos, las computadoras de redes corporativas, ya sean públicas o privadas. Con mayor frecuencia de la que se conoce, se cargan y descargan software no verificado, conectando multiplicidad de dispositivos propios y ajenos, sin que sean chequeados previamente y, por esto mismo, poniendo las redes a altos riesgos de todo tipo. Son los propios usuarios y empleados de dichas organizaciones, con acceso autorizado en la mayoría de los casos, quienes comprometen la seguridad de las redes corporativas, trabajando sin saberlo para aquellos que quieren intervenirlas externamente para beneficio propio.

De acuerdo a la información disponible a fines de 2018, en promedio se han requerido más de dos meses para descubrir las infiltraciones, tres días para contenerlas y un mes más para realizar análisis forenses. Es decir que cada incidente cibernético demanda 105 días o 5 meses (suponiendo que se trabaja en días hábiles laborales: 20 por mes, continuos). En estos 5 meses, hay otros 105 días de posibilidades de sufrir otros incidentes cibernéticos.

Para muchos especialistas y referentes de la temática, el robo de información es un tema preocupante y creciente a nivel global, donde además consideran que el mayor valor no está en los sistemas en sí mismos, sino en los datos almacenados y procesados en ellos. Es un concepto generalizado que, actualmente, es mucho más fácil atacar una red que defenderla.

En cuanto al desafío de la formación en recursos humanos, por un lado está la necesidad en cuanto a seguridad informática. Al respecto, podemos tomar como referencia los

estudios de Accenture que detectan a nivel bancos: si bien éstos quieren invertir en temas de seguridad, no siempre lo hacen en lo que podrían prepararlos para los problemas que deberán afrontar. Parecería que siempre están resolviendo problemas de ayer que ya deberían estar resueltos. Aquí entra en juego la figura del CISO (*chief information security officer*) que para el caso argentino siguen atados al pasado, reportan al área de sistemas y con un impacto organizacional de su accionar muy limitado. Con el crecimiento de la banca electrónica, lo cual atraviesa a individuos, grupos, empresas, sector privado y estatal, los incidentes cibernéticos y la cibercriminalidad aumentan exponencialmente. En tal sentido, expertos del área opinan que lo fundamental es obtener una rápida detección del incidente, capacidad de respuesta, poder para minimizar el impacto y restablecer el normal funcionamiento. Todo esto se vincula ciertamente con los aspectos curriculares y con mayor entrenamiento en la formación mediante ejercicios de simulación.

En relación más estrecha con la Defensa Nacional, el ex Ministro de Defensa Aguad mencionó la "formación de reservistas mediante la convocatoria de profesionales y técnicos especialmente de la ingeniería para atender el desafío del mapa de amenazas". En tal sentido, se puede decir que es necesario pensar, expresar e incluir en políticas, planes y programas la formación de niveles técnicos operativos dentro de la Defensa, ya que como expresa un experto (fuente reservada) "del Ministro baja al General, de este al Coronel y sigue…, siendo recién el Teniente o Soldado quien se arremanga operativamente y son los que no están formados". Chile habla de escasez de ciberanalistas diestros para sus soluciones de ciberdefensa con estándar militar. La OTAN, la agencia para el entrenamiento de fuerzas de seguridad de la Unión Europea (CEPOL) y el Instituto de Ciberseguridad Español (INCIBE) entre otros, prevén para 2022, en Europa, un déficit de más de 350.000 especialistas en ciberdefensa, que ascenderían a 1,5 millones a nivel global. En Argentina, no se

han hecho visibles estrategias, políticas, planes o programas de formación de recursos humanos para la ciberdefensa. No aparecen en medios periodísticos, no dan cuenta de ello las universidades, no hay acceso a documentos públicos ni son temas desarrollados en investigaciones académicas o que se manejen en los ámbitos políticos. Los jefes de operaciones y especialistas en el tema reconocen que la gestión de la crisis en situaciones de ciberdefensa es compleja y fácilmente el más débil en apariencia puede vencer a grandes Estados o Ejércitos convencionales. Para afrontar esto, coinciden en la necesidad de pensar la formación mediante especializaciones más intensas y específicas que las actuales, además de la necesidad de pasar de las palabras a los hechos.

En cuanto al planteo de la necesidad de que haya formación en temas de ciberestrategia e inteligencia, en general podemos decir que en Argentina, fuera de ámbitos muy técnicos, por desconocimiento, prejuicios o posturas ideológicas, las cuestiones de estrategia e inteligencia no son fácilmente abordadas, divulgadas o aceptadas. Sin embargo, tanto para la seguridad como para la Defensa, tanto las instancias políticas como académicas y los futuros profesionales que quieran vincularse con el área deben conocer y comprender que las amenazas cibernéticas sofisticadas provienen de organizaciones militares y agencias de inteligencias de otros Estados. Éstas cuentan con profesionales altamente capacitados y donde la estrategia e inteligencia son ejes centrales de sus formaciones y acciones, la ingenuidad o la ceguera ideológica no nos permitirán resguardar la seguridad cibernética. El cibercrimen, como ya fue mencionado, es para muchos analistas la primera industria ilegal a nivel global. Este es un sector altamente profesionalizado, donde algunas de estas organizaciones recurren incluso al reclutamiento de los mejores profesionales del área, lo cual se ve demostrado por el crecimiento de los incidentes informáticos de inteligencia artificial, cada vez más automatizada y sofisticada.

Tener en cuenta, en la formación tanto de ciberdefensa

como de ciberseguridad, aspectos de estrategia e inteligencia, es tomar conciencia de la realidad actual donde la Internet de las cosas ha generado un crecimiento exponencial en el perímetro de exposición. Esto implica mínimamente ciertos riesgos, como la desprotección de la cadena logística y el uso de software obsoleto y con agujeros de seguridad en los dispositivos de bajo costo. Por otra parte, es salir de la zona de confort brindada por la ingenuidad y aceptar el desafío de comprender al delito como lucrativo y, en tal sentido, la posibilidad de ser utilizado en conflictos económicos, políticos, geopolíticos con el riesgo de una generalización hacia el ciberespacio.

En la realidad actual de este mundo globalizado e interconectado, toda organización que posea algo de valor es susceptible de un ciberataque. De acuerdo a diferentes voces de expertos, la capacidad y posibilidades de atacar superan holgadamente a las capacidades para idear sistemas de defensa. En este sentido, pensar y diseñar estructuras de toma de decisiones para la protección frente a estos casos, también demanda saber estrategia e inteligencia.

Por otra parte, frente al interrogante sobre *cómo abordan la actualización curricular*[11], 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 a la *dependencia tecnológica y curricular*[12], la cuestión no es un tema abordado en los posgrados.

11 Ver referencias consultadas en bibliografía.

12 Ver referencias consultadas en bibliografía.

Respecto a la actualización curricular, es muy importante que haya un entendimiento común sobre el ciberespacio y los conceptos que sobre el mismo se abordan, discuten y enseñan. Si entendemos al ciberespacio en los términos que lo define Turner (2018) como "un dominio donde interactúan redes, información, máquinas y dispositivos que intersectan en las vidas de las personas en cuestiones personales y laborales", y teniendo en cuenta que los conocimientos relativos al ciberespacio cambian de forma vertiginosa, esto demanda una atención especial sobre la actualización curricular en cada centro educativo donde se aborde el tema ciber.

Por otra parte, como quinto dominio, en el ámbito de la Defensa y particularmente en el campo militar, esto tiene que ver con áreas que también son propias de los otros cuatro espacios. De este modo, la ciberdefensa incluye logística, inteligencia, comando, control, táctica, operaciones, estrategia, política, todo esto conforman un ecosistema de conocimientos específicos donde cada uno de ellos a su vez constituyen un sistema propio de conocimientos, prácticas, costumbres, doctrinas, teorías, que deben estar plasmadas curricularmente para poder ser transmitidas, analizadas, comparadas, evaluadas, modificadas, perfeccionadas. En tal sentido, sobre estos aspectos en particular no se han encontrado evidencias de orientaciones políticas o doctrinarias, como tampoco desarrollos curriculares en lo que a esta investigación le compete como objeto de estudio. Sin embargo, antes de poder pensar la actualización curricular hay que contar con estructuras curriculares a las cuales poder analizar. Si bien estas existen en las carreras, cursos y posgrados existentes, no es un tema que ocupe la centralidad en las agendas académicas. Es decir, no es fácilmente identificable, en las instituciones, en las carreras, cursos y posgrados, como tampoco en las cátedras, investigaciones, reflexiones o equipos de trabajos que lleven adelante la tarea de pensar, mirar, comparar, comprobar, criticar, reflexionar, proponer sobre las cuestiones curriculares de la ciberdefensa.

En muchos casos, se da por sentado que se copia y pega fácilmente, que está todo disponible y sólo hay que tomarlo de alguna nube o estantería de biblioteca, o que se lo saca de la galera de la experiencia y está todo solucionado, que es un tema menor y cuasi desprestigiado.

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[13]. 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[14]. 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 identifica 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.

En cuanto al desafío de determinar necesidades y tipos de abordajes conceptuales, doctrinarios y legales, en Argentina existen diferencias en las posturas tanto de académicos como de la dirigencia política respecto a estos tres aspectos. Por un lado, están quienes siguen o toman en consideración las posturas de Estados Unidos, países de la Unión Europea y de la OTAN; sin embargo, hay quienes son críticos a las propuestas

13 Ver referencias consultadas en bibliografía.

14 Ver referencias consultadas en bibliografía.

de esa línea conceptual, doctrinaria y legal. En tal sentido, existe la posibilidad de que cada postura desarrolle una corriente o línea de pensamiento propio de un lado u otro, y que estas se vayan alternando según quienes tengan las oportunidades de ocupar puestos de decisión política. La otra posibilidad es que con un gran esfuerzo se logren consensuar posturas en pos de una política de Estado en la materia. No obstante, según los alcances de esta investigación, aún falta madurar en la comprensión y desarrollo de los abordajes conceptuales, doctrinarios y legales referidos a la ciberdefensa, al menos desde el punto de vista curricular para implementarlos en instancias de investigación académica o desarrollo de clases.

A su vez, cuando prestamos atención al hecho de que las instancias académicas de formación en el tema plantean como desafío o dilema conocer y/o determinar en cada una de las Fuerzas Armadas y las diferentes agencias del Estado la existencia o no de un plan de formación, sus criterios y características, encontramos un evidente punto ciego sobre el cual no tienen todo el conocimiento o la información básica al respecto. Desde los puntos de vista estratégico, de políticas educativas o de políticas públicas, esto representa una debilidad estructural, porque indica que las instituciones académicas que llevan a cabo actualmente la formación han elaborado programas y ofrecen recorridos curriculares que no han partido de un diagnóstico y una demanda concreta de aquellos actores que serán usuarios de los recursos que ésta forme. Con suerte, podrán estar correctamente orientados a las necesidades que luego tendrán que resolver estos espacios institucionales, pero podría suceder que haya una dispersión de tiempo, esfuerzo y conocimiento no necesario y esto estaría jugando en contra al costo-beneficio que, por otra parte, también se plantea en cuanto a la escasez de recursos económicos, de conocimiento, de personas formadas y de tiempo para enfrentar esta nueva área de conocimiento, tanto a nivel táctico, operativo y estratégico, como también en cuanto a profesionales dedicados a la formación.

Por último, cuando desde las instancias académicas de formación (distinción importante, ya que el planteo no proviene de un espacio de investigación, de conducción institucional o de decisores de políticas públicas) plantean como un desafío encontrar la forma de traducir los objetivos del área en conocimientos o recorridos curriculares, lo que surge es la necesidad de investigar aspectos curriculares que acerquen propuestas de formación y adecuación curricular para cumplir con las políticas públicas que estructuran y guían el área. Esto también nos evidencia que la formación actual ha surgido antes que las políticas públicas expresadas en las recientes normativas que la conforman y, por ello, demanda una profunda investigación para la redefinición y adecuación de sus criterios, contenidos, alcances, metodologías, teorías y doctrinas a implementar, dejando las que son pertinentes, adecuando las que requieren ajustes e incorporando las que aún no están. Para todo esto, se necesita también investigación de lo educativo, al igual que desde lo político, lo estratégico o lo tecnológico. Sin embargo, no se han observado abordajes o planteos de agenda orientados a la investigación curricular o educativa.

Posgrados y perfiles profesionales

En cuanto a *orientaciones o demandas sobre perfiles*[15], este trabajo da cuenta de que nadie tiene conocimiento sobre demandas u orientaciones de perfiles a formar tanto del sector privado como del estatal. Al respecto, consideran que se podría 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 2018, Chile –por tomar un ejemplo cercano y regional–, publicó la aprobación de la nueva Política de Ciberdefensa. Esta expresa que, además de recursos y herramientas técnicas,

15 Ver referencias consultadas en bibliografía.

requiere contar con personal calificado en número y aptitudes en todos los niveles institucionales. A su vez, contar con dicho personal requiere programas generales y especializados de formación, capacitación y sensibilización.

En este sentido, el Ministerio de Defensa de Chile reconoce la necesidad de que éste organismo y sus instituciones dependientes identifiquen y definan el rol del recurso humano en ciberdefensa, implementen los modelos formativos adecuados para concretar este logro, a la vez que deben definir y crear las especialidades y subespecialidades en el área de ciberdefensa. Frente a esta situación, podemos decir que en 2018 Chile no tenía definidas (al menos todas) las orientaciones y demandas de perfiles y modelos formativos para reproducirlos (en términos de Bourdieu) pero sí tenía presente su importancia y necesidad. Esta investigación devela en los términos de sus alcances que, en el caso argentino, si existen definiciones de roles y modelos formativos para perfiles de recursos humanos en el área de ciberdefensa, no llegaron al conocimiento de las universidades o instancias académicas para su implementación. Esta situación local determina el estado de madurez política, académica e institucional de la cuestión, lo cual justifica la necesidad de abordajes académicos, políticos y prácticos-profesionales en función de pensar y definir necesidades, roles y modelos formativos.

La formación en ciberdefensa y ciberseguridad es una demanda y una necesidad estratégica que los Estados no discuten a nivel global. En el caso de España, el director del Centro Nacional de Excelencia en Ciberseguridad (CNEC) y jefe del Área de Seguridad de la Guardia Civil consideraba, en 2017, que en este campo se necesitan (referidos a la formación) todos los recursos que se encuentren disponibles. Para Ávila es necesario pensar estrategias de detección, formación y reclutamiento temprano del talento en edades cada vez más bajas. Hay una necesidad imperiosa de replantearse todos los modelos hoy conocidos, y es en este sentido donde la investigación en cuestiones educativas (ya sea políticas,

curriculares, tecnológica u otras) cobra sentido e importancia. En Argentina, este nivel de definición política y conceptual sobre la formación de los recursos humanos no se evidencia en la agenda periodística ni en las instancias académicas.

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, 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.

Si hacemos el ejercicio de imaginar perfiles profesionales orientados a la ciberdefensa y luego pensamos qué recorridos curriculares podrían o deberían adecuarse para satisfacer académicamente los requerimientos operativos de esos puestos de trabajo, podemos comenzar por preguntarnos qué áreas o funciones tiene implícita la ciberdefensa en su transcurrir diario. Ante esto, y en función de la bibliografía periodística y académica, podemos inferir que en la gestión y ejecución de tareas de ciberdefensa hay insertas cuestiones logísticas, legales, tecnológicas, de cooperación nacional e internacional, de inteligencia, de conducción, de formación, entre otras. También es posible inferir que existen tres grandes niveles de actuación: táctico, operativo y estratégico.

Ahora bien, teniendo en claro áreas, funciones y tareas con las que se vinculan y desarrollan los profesionales al ocuparse de la ciberdefensa, es necesario dilucidar qué conocimientos, habilidades y aptitudes deben tener éstos para ocupar óptimamente esos puestos. Cabe entonces preguntarse si la logística, la inteligencia, la conducción de operaciones, las operaciones en sí mismas, etc., son idénticas a las que se

desarrollan en los otros cuatro dominios o si existen diferencias específicas y cuáles son. Quien conduce una operación militar o estratégica de defensa, en el ámbito del Ejército, la Marina, la Fuerza Aérea o una oficina civil del Ministerio de Defensa, ¿es linealmente intercambiable a un área similar (supongamos logística, legal o inteligencia) dentro de la ciberdefensa? O por el contrario, ¿podrá haber similitudes de cuestiones conceptuales, operacionales o tecnológicas, etc., pero con ciertas particularidades específicas de la ciberdefensa? Y, en caso de existir estas particularidades específicas, ¿ameritan ser enseñadas, entrenadas, concebidas curricularmente para una mayor eficiencia, eficacia y profesionalismo del personal que allí se desempeña? Todas estas cuestiones no están hoy planteadas en las agendas institucionales de las instancias de formación académicas.

Es válido preguntarse qué puestos y tareas relativas a la ciberdefensa pueden y deben ocupar por ejemplo un soldado en la Quiaca, en la Triple Frontera o Tierra del Fuego, en una oficina del Ministerio de Defensa o el Comando Conjunto de Ciberdefensa; o un guardiamarina en la Fragata Libertad. Del mismo modo, es necesario hacer estas reflexiones para el caso de un Teniente, un Coronel, un General o un egresado civil de cualquier carrera que luego se desempeñe en dependencias de la Defensa, en el país o en el exterior. Cuando tengamos estas respuestas, podremos pensar en líneas de investigación curricular para fortalecer la formación del personal civil y militar que ocupe con idoneidad puestos operativos o de conducción. Luego se deberá indagar si se cuenta con profesionales civiles y militares con el conocimiento y la experiencia necesaria para formar en aquellos aspectos antes develados y, en caso negativo, qué acciones son necesarias para cubrir estas necesidades. La academia tiene la obligación de preguntarse estas cuestiones, más allá de las aplicaciones e instrumentaciones prácticas que, la política en su ejercicio, pueda hacer de dichos puestos y personal disponible.

Conclusiones

Aspectos curriculares

Esta investigación concluye que tanto la ciberdefensa como la ciberseguridad deben ser abordadas en su formación y en sus políticas (ya sean del ámbito público, académico o del sector productivo) desde lo multidisciplinar. Para esto, es indispensable una financiación adecuada, la presencia y colaboración entre diferentes organismos del Estado, la investigación permanente y la cooperación a nivel nacional e internacional. Además, se hace visible la necesidad de detenerse, diagnosticar, evaluar y decidir qué se quiere hacer, con qué herramientas, en qué dirección, con qué recursos, en cuánto tiempo, entre otras consideraciones e indicadores a tener en cuenta. Según los alcances de la presente investigación, no se pudo comprobar que todas estas cuestiones estén contempladas por políticas públicas, por equipos de asesores políticos o por las instancias académicas. La formación de los recursos humanos debería implicar una mirada estratégica respecto de las cuestiones técnicas, tecnológicas, conceptuales, doctrinales, de infraestructura, de vínculos y relaciones locales, regionales e internacionales, inteligencia y contrainteligencia, además de marcos referenciales, entre otros aspectos. En tal sentido, es necesario pensar curricularmente que áreas comprende o lleva implícita la formación en ciberdefensa. Para ello, se deben pensar y definir qué tipo y nivel de certificaciones deben proponerse como objetivos para la formación del personal. En tal sentido, aparece como necesidad que el Ministerio de Defensa, sus instituciones dependientes, relacionadas y vinculadas o posibles de vincular, identifiquen y definan los diferentes roles que deberán o necesitarán asumir los recursos humanos en los diferentes niveles y espacios institucionales de la Defensa Nacional. De estas definiciones y orientaciones surgirán en el ámbito educativo las especialidades, subespecialidades, especialidades secundarias o vinculadas. Por otra parte, dado

que en el sector privado el área de informática y ciberseguridad tiene un alto porcentaje de idóneos que adquirieron experiencia y herramientas para su desempeño por fuera de acreditaciones universitarias, es necesario pensar la manera de sumarlos a la formación y acreditación académica para poder integrarlos al sistema.

Cooperación entre actores y estructuras

En materia de vínculos y cooperación, es importante que profesionales, profesores e investigadores cuenten con canales y contextos institucionalizados de cooperación con el Estado y el sector productivo, vinculados a los aspectos ciber, dado que esto permitirá generar líneas de desarrollo y mejora en la formación de futuros especialistas, al mismo tiempo que desarrollar un saber plural con visión global. El crecimiento vertiginoso de las tecnologías y lo que estas posibilitan demanda de profesionales altamente entrenados para hacer frente a la multiplicidad de cuestiones ciber. En tal sentido, en los países con mayor madurez en la temática, el desarrollo y disponibilidad de simuladores para el entrenamiento de personal del ámbito estatal, privado, civil y militar es una prioridad. Esto, en el caso argentino, presenta una debilidad a tener en cuenta. Concebir un sistema de simulación implica también vincularse y posicionarse desde lo educativo o formativo porque antes se debe pensar en el modelado y formalización del conocimiento necesario para plantear los escenarios de simulación que se vinculen efectivamente con la realidad de la ciberdefensa; para ello, se debe previamente identificar, definir y elaborar catálogos de vulnerabilidades, ataques y contramedidas, lo cual también demanda tener en cuenta cuestiones curriculares de conceptos, contenidos, desarrollos, estrategias metodológicas, definiciones, opciones doctrinarias y políticas. Todo lo mencionado está estrechamente vinculado con lo tecnológico, las definiciones políticas y doctrinarias, la investigación permanente y los

diferentes aspectos curriculares implícitos, lo cual hace evidente la presencia y necesidad del vínculo sabatino dado por Estado, sector productivo (público y privado) y universidades, conocer en detalle estas cuestiones y promover su desarrollo y fortalecimiento, demanda de investigaciones que se ocupen de mirar tales cuestiones.

Desafíos y dilemas

Desde la producción científica académica faltan estudios y publicaciones que den cuenta de políticas, proyectos, planes, investigaciones y estado de situación de los entornos de cada una de los diferentes componentes de infraestructuras críticas y su relación con acciones concretas para su protección. No se conocen estudios sobre estado del arte, de reflexiones críticas o análisis tanto civil como militar de la cuestión como tampoco prospectivas respecto al nivel de vulnerabilidad de cada uno de ellos. Respecto de la formación de recursos humanos, está el desafío de resolver que certificaciones les permitirá afrontar con menor desfasaje de tiempo y experiencia, los problemas de seguridad informática para no quedar rezagados en el tiempo. Para esto, se necesita un diagnóstico certero de la realidad y una prognosis futura, acompañado de un mayor entrenamiento mediante simulación. En cuanto al área de defensa, se puede decir que es necesario pensar, expresar e incluir en políticas, planes y programas la formación de niveles técnicos operativos vinculados a la ciberdefensa, ya que son éstos quienes tienen la responsabilidad operativa en el tema. Por otra parte, se evidencia como necesidad tener en cuenta en la formación tanto de ciberdefensa como ciberseguridad aspectos de estrategia e inteligencia, dado que la Internet de las cosas ha generado un crecimiento exponencial en el perímetro de exposición. En Argentina, no se han hecho visibles estrategias, políticas, planes o programas de formación de recursos humanos para la ciberdefensa (en los términos de esta investigación y a excepción de los posgrados

mencionados). No aparecen en medios periodísticos, no dan cuenta de ellas las universidades, no hay acceso a documentos públicos ni son temas desarrollados en investigaciones académicas o que se manejen en los ámbitos políticos, lo que quiere decir que es un área de vacancia para la investigación académica.

Respecto de la actualización curricular, es muy importante que haya un entendimiento común sobre el ciberespacio y los conceptos que sobre el mismo se abordan, discuten y enseñan. En el ámbito de la Defensa, y particularmente en el campo militar, tiene que ver con áreas que también son propias de los otros cuatro espacios. De este modo, la ciberdefensa incluye logística, inteligencia, comando, control, táctica, operaciones, estrategia, política. Todo esto conforma un ecosistema de conocimientos específicos donde cada uno de ellos, a su vez, constituyen un sistema propio de conocimientos, prácticas, costumbres, doctrinas, teorías, que deben estar plasmadas curricularmente para poder ser transmitidas, analizadas, comparadas, evaluadas, modificadas, perfeccionadas. En tal sentido, sobre estos aspectos en particular no se han encontrado evidencias de orientaciones políticas o doctrinarias como tampoco desarrollos curriculares, especialmente en el ámbito civil. En cuanto al desafío de determinar necesidades y tipos de abordajes conceptuales, doctrinarios y legales, en Argentina existen diferencias en las posturas tanto de académicos como de la dirigencia política. En ese sentido, existe la posibilidad de que cada postura desarrolle una corriente o línea de pensamiento propio de un lado u otro y que estas se vayan alternando según quiénes tengan las oportunidades de ocupar puestos de decisión política. O bien, la otra posibilidad es que con un gran esfuerzo se logren consensuar posturas en pos de una política de estado en la materia. A su vez, podemos decir que las instancias académicas de formación en el tema (y según los alcances de esta investigación) no conocen las necesidades y demandas de formación del personal de las Fuerzas Armadas y agencias

del Estado. Esto, desde el punto de vista estratégico, de las políticas educativas o de políticas públicas, representa una debilidad estructural: las instituciones académicas que llevan a cabo actualmente la formación han elaborado programas y ofrecen recorridos curriculares que no han partido de un diagnóstico y una demanda concreta de aquellos actores que serán usuarios de los recursos que ésta forme. Por otra parte, los actores académicos plantean la necesidad de investigar aspectos curriculares que acerquen propuestas de formación y adecuación curricular para cumplir con las políticas públicas que estructuran y guían el área. Esto también evidencia que la formación actual ha surgido antes que las políticas públicas expresadas en las recientes normativas (2019) que la conforman y, por ello, demanda una profunda investigación para la redefinición y adecuación de sus criterios, contenidos, alcances, metodologías, teorías y doctrinas a implementar.

Posgrados y perfiles profesionales

Esta investigación devela en los términos de su alcance que, en el caso argentino, si existen definiciones de roles y modelos formativos para perfiles de recursos humanos en el área de ciberdefensa, no llegaron al conocimiento de las universidades o instancias académicas para su implementación. Tal situación determina el estado de madurez política, académica e institucional de la cuestión, lo cual justifica la necesidad de abordajes académicos, políticos y prácticos-profesionales en función de pensar y definir necesidades, roles y modelos formativos.

La academia tiene la obligación de preguntarse estas cuestiones, más allá de las aplicaciones e instrumentaciones prácticas que la política, en su ejercicio, pueda hacer de dichos puestos y personal disponible.

Referencias bibliográficas

1. Referencias consultadas acerca de criterios curriculares.

Cubeiro (26-9-2018). Un ciberataque es una amenaza tan seria como un torpedo. Infodefensa. Recuperado de https://www.infodefensa.com/es/2018/09/26/noticia-cubeiro-ciberataque-amenaza-seria-torpedo.html

Watson, P. (11-9-2018). Cap. Turner (EEUU): "Todo lo que se hace en el mar está respaldado en el ciberespacio". Infodefensa. Recuperado de https://www.infodefensa.com/latam/2018/09/11/noticia-turner-respaldo-ciberespacio.html

2. Referencias consultadas con respecto a orientación de la formación.

Aránguiz, O. E. (20-4-2018). Espina dará prioridad a la ciberdefensa en su proyecto político. Infodefensa. Recuperado de https://www.infodefensa.com/latam/2018/04/20/noticia-espina-prioridad-ciberdefensa-proyecto-politico.html

Aránguiz, O. E. (21-3-2018). Chile creará un Comando Conjunto de Ciberdefensa. Infodefensa. Recuperado de https://www.infodefensa.com/latam/2018/03/21/noticia-chile-creara-comando-conjunto-ciberdefensa.html

Donoso, R. (29-11-2017). Ciberseguridad en el contexto militar (y2). Infodefensa. Recuperado de https://www.infodefensa.com/latam/2017/11/29/opinion-ciberseguridad-contexto-militar.php

González Pascual, M. (26-11-2018). ¿Dejarías la seguridad de tu empresa en manos de un robot? La Nación. Recuperado de https://www.lanacion.com.ar/opinion/de-los-lectores-cartas-mails-nid2156758

Uzal, R. ( ). Ciberdefensa. La Nación. Recuperado de https://www.lanacion.com.ar/opinion/de-los-lectores-cartas-mails-nid2151449

Redacción de Infodefensa. (24-10-2018). Indra, primera empresa española en la coalición de ciberdefensa de la OTAN. Infodefensa. Recuperado de https://www.infodefensa.com/es/2018/10/24/noticia-indra-ciberdefensa.html

3. Referencias consultadas respecto al abordaje de Políticas, Doctrinas y Directivas.

Aránguiz, O. E. (05-10-2018). Chile y la OEA firman un acuerdo de cooperación en Ciberseguridad. Infodefensa. Recuperado de https://www.infodefensa.com/latam/2018/10/05/noticia-chile-firman-acuerdo-cooperacion-ciberseguridad.html

Watson, P. (11-9-2018). Todo lo que se hace en el mar está respaldado en el ciberespacio. Infodefensa. Recuperado de https://www.infodefensa.com/latam/2018/09/11/noticia-turner-respaldo-ciberespacio.html

4. Referencias consultadas acerca de vínculos y cooperación con universidades, empresas y Estado.

Carrasco, B. (25-03-2019). Indra presenta ante la UE sus proyectos de ciberdefensa y guerra electrónica. Infodefensa. Recuperado de https://www.infodefensa.com/es/2019/03/25/noticia-indra-presenta-bruselas-proyectos-ciberdefensa-guerra-electronica.html

Carrasco, B. (27-07-2017). Gral. Medina (Ciberdefensa): “Las empresas, sobre todo las pequeñas, tienen que invertir más en ciberseguridad”. Infodefensa. Recuperado de https://www.infodefensa.com.es/2017/07/27/noticia-entrevista-mando-ciberdefensa.html

Redacción de Infodefensa. (04-03-2019). España y Marruecos acuerdan cooperar en ciberdefensa y emergencias. Infodefensa. Recuperado de https://www.infodefensa.com/es/2019/03/04/noticia-espana-marruecos-acuerdan-cooperar-ciberdefensa-emergencias.html

Redacción de Infodefensa. (17-04-2018). Rosemont (ADS):

"Las áreas ciber y protección inteligente están creciendo rápido". Infodefensa. Recuperado de https://www.infodefensa.com/es/2018/04/17/noticia-rosemont-areas-ciber-proteccion-inteligente-esta-creciendo-rapido.html

Redacción de Infodefensa. (26-06-2014). Morenés dará prioridad a la ciberdefensa en el presupuesto de su cartera para 2015. Infodefensa. Recuperado de https://www.infodefensa.com/es/2014/06/26/noticia-morenes-prioridad-ciberdefensa-presupuesto-cartera.html

5. Referencias consultadas sobre ejercicios de simulación.

Redacción de Infodefensa. (25-07-2017). Indra diseña el escenario del ejercicio internacional CyberEx de Incibe. Infodefensa. Recuperado de https://www.infodefensa.com/es/2017/07/25/noticia-indra-diseña-escenario-ejercicio-internacional-cyberex-incibe.html

Redacción de Infodefensa. (17-02-2014). Indra ultima un simulador avanzado para el entrenamiento en ciberdeffensa. Infodefensa. Recuperado de https://www.infodefensa.com/es/2014/02/17/noticia-indra-desarrolla-simulador-avanzado-entrenamiento-ciberdefensa.html

6. Referencias consultadas respecto de riesgos e implicancias de la ciberdefensa / ciberseguridad.

Dinatale, M. (11-02-2018). Los hackeos aumentaron un 700% en Argentina y el gobierno aceleró el comando de ciberseguridad. Infobae. Recuperado de https://www.infoabe.com/politica/2018/02/11/los-hackeos-aumentaron-un-700-en-argentina-y-el-gobierno-acelero-el-comando-de-ciberseguridad/

Montoto, M. (08-02-2018). El desafío de la ciberdefensa. Infobae. Recuperado de https://www.infobae.com/opinion/2018/02/08/el-desafio-de-la-ciberdefensa/

Watson, P. (11-09-2018). Cap. Turner (EEUU): "Todo lo que

se hace en el mar está respaldado en el ciberespacio". Infodefensa. Recuperado de https://www.infodefensa.com/latam/2018/09/11/noticia-turner-respaldo-ciberespacio.html

Uzal, R. (23-08-2018). Ciberresguardo y sistema de salud. Infobae. Recuperado de https://www.infobae.com/opinion/2018/08/23/ciberresguardo-y-sistema-de-salud/

González Pascual, M. (26-11-2018). ¿Dejarías la seguridad de tu empresa en manos de un robot? La Nación. Recuperado de https://www.lanacion.com.ar/opinion/de-los-lectores-cartas-mails-nid2156758

Redacción de Infodefensa. Carlos Suárez, director general de Indra: "Nuestras soluciones de inteligencia para Ciberdefensa se anticipan al ataque". Infodefensa. Recuperado de https://www.infodefensa.com/es/2012/01/30/noticia-carlos-suarez-director-general-de-indra-nuestras-soluciones-de-ciberdefensa-incluyen-soluciones.html

Watson, P. (08-09-2018). Schilling (USAF) critica la ligereza con que se valoran los riesgos ciber. Infodefensa. Recuperado de https://www.infodefensa.com/latam/2018/09/08/noticia-schilling-denuncia-ligereza-valoran-riesgos-ciber.html

7. Referencias consultadas sobre la formación de recursos humanos.

Aránguiz, O. E. (20-04-2018). Espina dará prioridad a la ciberdefensa en su proyecto político. Infodefensa. Recuperado de https://www.infodefensa.com/latam/2018/04/20/noticia-espina-prioridad-ciberdefensa-proyecto-político.html

Aránguiz, O. E. (21-03-2018). Chile creará un Comando Conjunto de Ciberdefensa. Infodefensa. Recuperado de https://www.infodefensa.com/latam/2018/03/21/noti-

cia-chile-creara-comando-conjunto-ciberdefensa.html

Carrasco, B. (03-06-2017). El Mando de Ciberdefensa reclama más recursos económicos y personal cualificado. Infodefensa. Recuperado de https://www.infodefensa.com/es/2017/06/03/noticia-mando-ciberdefensa-reclama-recursos-economicos-personal-cualificado.html

García, N. (24-12-2018). Pegasus ofrece el TPS de Verint para proteger a Chile de las ciberamenazas. Infodefensa. Recuperado de https://www.infodefensa.com/latam/2018/12/24/noticia-pegasus-ofrece-verint-proteger-chile-ciberamenazas.html

Manzoni, C. (10-03-2019). Bancos. ¿Es seguro operar por Internet? La Nación. Recuperado de https://www.lanacion.com.ar/economia/ciberataquesa-la-banca-afinarla-punteriael-desafio-local-nid2226809

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

Redacción de Infodefensa. (21-12-2018). Indra forma a los militares del Mando Conjunto de Ciberdefensa. Infodefensa. Recuperado de https://www.infodefensa.com/es/2018/12/21/noticia-indra-forma-militares-mando-conjunto-ciberdefensa.html

Redacción de Infodefensa. (03-04-2017). Indra, la universidad y los centros oficiales forman a los futuros profesionales de la ciberseguridad. Infodefensa. Recuperado de https://www.infodefensa.com/es/2017/04/03/noticia-indra-mando-ciberdefensa-inciben-forman-futuros-profesionales-ciberseguridad.html

Redacción de Infodefensa. (03-02-2017). El Mando de Ciberdefensa propone incorporar la ciberseguridad a la Educación. Infodefensa. Recuperado de https://www.infodefensa.com/

es/2017/02/03/noticia-mando-ciberdefensa-apuesta-incorporar-ciberseguridad-educacion.html

Carrasco, B. (02-02-2017). Enrique Ávila (CNEC): "Es necesario destinar más recursos a la formación en Ciberseguridad". Infodefensa. Recuperado de https://www.infodefensa.com/es/2017/02/02/noticia-entrevista-enrique.html

8. Referencias consultadas respecto a la separación entre ciberdefensa y ciberseguridad.

Rodríguez Niell, P. (19-06-2018). Aguad: "La obsolescencia del material de las FF. AA. tiene que ver con la decadencia integral del país". La Nación. Recuperado de https://www.lanacion.com.ar/politica/aguad-la-obsolescencia-del-material-de-las-ffaa-tiene-que-ver-con-la-decadencia-integral-del-pais-nid2145220

9. Referencias consultadas sobre aspectos de formación.

Carrasco, B. (02-02-2017). Enrique Ávila (CNEC): "Es necesario destinar más recursos a la formación en Ciberseguridad". Infodefensa. Recuperado de https://www.infodefensa.com/es/2017/02/02/noticia-entrevista-enrique.html

Dinatale, M. (27-02-2019). A partir de los últimos cambios, el Gobierno busca unificar las tareas de Defensa con la Cancillería. Infobae. Recuperado de https://www.infobae.com/politica/2019/02/27/a-partir-de-los-ultimos-cambios-el-gobierno-busca-unificar-las-tareas-de-defensa-con-la-cancilleria/

Redacción de Infodefensa. (16-09-2014). El Mando de Adiestramiento del Ejército y la EDA lideran el experimento multinacional de Ciberdefensa. Infodefensa. Recuperado de https://www.infodefensa.com/es/2014/09/16/noticia-mando-adiestramiento-ejercito-lideran-experimento-multinacional-ciberdefensa.html

Uzal, R. ( ). Ciberdefensa. La Nación. Recuperado de https://www.lanacion.com.ar/opinion/de-los-lectores-cartas-mails-nid2156758

10. Referencias consultadas respecto de actualización curricular.

Redacción de Infodefensa. (30-01-2012). Carlos Suárez, director general de Indra: "Nuestras soluciones de inteligencia para Ciberdefensa se anticipan al ataque". Infodefensa. Recuperado de https://www.infodefensa.com/es/2012/01/30/noticia-carlos-suarez-director-general-de-indra-nuestras-soluciones-de-ciberdefensa-incluyen-soluciones.html

Watson, P. (11-09-2018). Cap. Turner (EEUU): "Todo lo que se hace en el mar está respaldado en el ciberespacio". Infodefensa. Recuperado de https://www.infodefensa.com/latam/2018/09/11/noticia-turner-respaldo-ciberespacio.html

11. Referencias consultadas acerca de dependencia curricular y tecnológica.

Iglesias, L. (15-08-2018). Sistemas interoperables, la clave para hacer frente a los ciberataques. Infodefensa. Recuperado de https://www.infodefensa.com/es/2018/08/15/noticia-ejercito-confia-interoperabilidad-ciberdefensa.html

Mercado, S. (24-12-2018). Cómo funciona la empresa israelí de seguridad que inventó la cúpula de hierro y ya opera en la Argentina. Infobae. Recuperado de https://www.infobae.com/politica/2018/12/24/la-empresa-israeli-de-seguridad-que-invento-la-cupula-de-hierro-ya-esta-en-la-argentina/

Scolnik, H. D. (30-08-2018). La clave es crear tecnología propia. La Nación. Recuperado de https://www.lanacion.com.ar/

opinion/la-clave-es-crear-tecnologia-propia-nid2166904

12. Referencias consultadas sobre abordajes conceptuales, doctrinarios y legales.

Aránguiz, O. E. (05-10-2018). Chile y la OEA firman un acuerdo de cooperación en Ciberseguridad. Infodefensa. Recuperado de https://www.infodefensa.com/latam/2018/10/05/noticia-chile-firman-acuerdo-cooperacion-ciberseguridad.html

Redacción de Infodefensa. Carlos Suárez: "No existe un marco legal internacional que gobierne el Ciberespacio". Infodefensa. Recuperado de https://www.infodefensa.com/es/2012/01/30/noticia-carlos-suarez-no-existe-un-marco-legal-internacional-que-gobierne-el-ciberespacio.html

13. Referencias consultadas acerca de planes y criterios para la formación en esta disciplina.

Redacción de Infodefensa. (26-05-2018). Cospedal: "La Ciberdefensa ha de estar en el proceso de planeamiento militar". Infodefensa. Recuperado de https://www.infodefensa.com/es/2018/05/26/noticia-cospedal-ciberdefensa-proceso-planeamiento-militar.html

14. Referencias consultadas respecto de perfiles profesionales.

Aránguiz, O. E. (21-03-2018). Chile creará un Comando Conjunto de Ciberdefensa. Infodefensa. Recuperado de https://www.infodefensa.com/latam/2018/03/21/noticia-chile-creara-comando-conjunto-ciberdefensa.html

Carrasco, B. (02-02-2017). Enrique Ávila (CNEC): "Es necesario destinar más recursos a la formación en Ciberseguridad". Infodefensa. Recuperado de https://www.infodefensa.com/

es/2017/02/02/noticia-entrevista-enrique.html

Redacción de Infodefensa. (24-10-2018). Indra, primera empresa española en la coalición de ciberdefensa de la OTAN. Infodefensa. Recuperado de https://www.infodefensa.com/es/2018/10/24/noticia-indra-ciberdefensa.html

Redacción de Infodefensa. (03-04-2017). Indra, la universidad y los centros oficiales forman a los futuros profesionales de la ciberseguridad. Infodefensa. Recuperado de https://www.infodefensa.com/es/2017/04/03/noticia-indra-mando-ciberdefensa-incibe-forman-futuros-profesionales-ciberseguridad.html

Redacción de Infodefensa. (03-02-2017). El Mando de Ciberdefensa propone incorporar la ciberseguridad a la Educación. Infodefensa. Recuperado de https://www.infodefensa.com/es/2017/02/03/noticia-mando-ciberdefensa-aprueba-incorporar-ciberseguridad-educacion.html

Palabras clave: *Defensa nacional — educación — ciberdefensa — políticas públicas — currículum*

Keywords: *National defense — education — cyber defense— public policies —curriculum*

Abstract

In this article, we reflect from a social, educational, public policy and curricular issues approach to the findings regarding postgraduate degrees in cyber defense for Argentina in 2019. Those approaches present looks that seek to challenge the local reality from of comparative tours of the Latin American and Spanish agendas on the following issues: curricular criteria, structure and curriculum framework, education orientation, Inclusion of Policies, Doctrines and Directives, relations or cooperation with universities, companies and the State, simulation exercises, recognition of other actors, postgraduate degrees proposals when facing the challenges, how to address the curricular issue, curricular and technological dependence, challenges and dilemmas that are recognized, orientations and demands on profiles to be educated, professional profiles towards which the postgraduates degrees are oriented.