Aportes para la discusión sobre hallazgos de investigación en ciberdefensa y ciberseguridad

Autores: Guillermo Rutz, Luis Enrique Arellano González, Miguel Blanco, Rodrigo Cárdenas Holik, María Elena Darahuge, Karina Martínez, Nidia Osimani, Agostina Taverna, Juan Carlos Velásquez Quiroz [1]

Resumen: Este artículo pretende incentivar la discusión académica sobre ciberdefensa y ciberseguridad como un camino para poner en agenda tales temas. En tal sentido propone aportes de investigación referidos a los siguientes temas: ciberdefensa como nuevo campo, Software libre y educación, certificaciones en ciberseguridad, capacitación y gestión de infraestructuras críticas, sistemas de gestión de aprendizaje, algoritmos y ciberespacio, dominios de la ciberdefensa, prevención y resilencia, ciberinteligencia e interoperabilidad.

Palabras Claves: ciberdefensa – ciberseguridad – investigación.

[1] Mails de contacto: Rutz, Guillermo: rutzguillermo@gmail.com; Arellano González, Luis Enrique: larellano@fra.utn.edu.ar; Blanco, Miguel: tcnl.blanco@gmail.com; Cárdenas Holik, Rodrigo: lic.cardenas.holik@gmail.com; Darahuge, María Elena: mdarahuge@fra.utn.edu.ar; Martínez, Karina: ingkarinamartinez@gmail.com; Osimani, Nidia: nidia.osimani@posgrado.económicas.uba.ar; Taverna, Agostina: agostaverna@gmail.com; Velásquez Quiroz, Juan Carlos: velasquezjuance@gmail.com

Introducción

La formación en ciberdefensa y ciberseguridad constituye un nuevo campo del saber con interés estratégico para el sector público y privado. Al mismo tiempo, presentan múltiples dimensiones aún no desarrolladas: lo económico, tecnológico, educativo, político, normativo y militar. Esto aparece como un interrogante de interés para la Defensa Nacional, donde su abordaje lleva a preguntarnos sobre las necesidades y estrategias de formación que tanto el sector estatal como estratégico productivo requieren.

Diversos países han incluido la problemática del ciberespacio en sus agendas de estrategia nacional de seguridad (Trama y de Vergara, 2017). En el caso argentino las investigaciones consideran "necesario la conceptualización de categorías como ciberespacio, ciberpoder, cibercrimen, ciberguerra, ciberseguridad y ciberdefensa (Gastaldi y Justribró, 2014b:16), donde además "el marco normativo nacional establece una separación jurídica, orgánica y funcional entre Defensa Nacional y Seguridad Interior" (Gastaldi y Justribró, 2014a:10).

En cuanto al marco teórico, "en la actualidad no existen definiciones comunes para expresiones relacionadas con la cibernética, ni siquiera en el contexto regional, lo cual dificulta la cooperación entre los Estados" (Trama y de Vergara, 2017: 21). Esta dificultad es expuesta también por Singer y Fridman (2014). Si bien como lo plantean Eissa, Gastaldi, Poczynok y Di Tullio (2012) siguiendo la legislación nacional, es necesario separar la seguridad cibernética nacional de la defensa cibernética nacional; Ballesteros (2016: 60) considera que "como construcción intelectual esta postura es útil, aunque dificulta su implementación dadas las características del espacio cibernético".

Al igual que la categoría anterior, el concepto de *guerra cibernética* es abordado por Feliú (2013) para quien cada vez que aparece una nueva dimensión real o virtual que el hombre quiere utilizar, 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 (2009:17), 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, siendo necesario tal como lo plantean Christopher, Porche y Axelband, comprensión de matices culturales, humanos y

todos aquellos que permitan comprender 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.

Aportes para la discusión

El siglo XX en principio y el siglo XXI, en particular, se han caracterizado por el surgimiento y declive de diversos vocablos y, con frecuencia intentos de sustituir viejos conceptos, procedimientos o actitudes por medio de un lenguaje innovador. En tal sentido, palabras como ciberespacio, cibercultura, buteo y muchas otras, se han incorporado en las producciones académicas de muchas disciplinas profesionales. ¿Ocurre lo mismo con la ciberdefensa?

Los conceptos involucrados en ciberdefensa y ciberseguridad son los mismos que caracterizan a la inteligencia y contrainteligencia clásicas. Los métodos característicos de ataque y defensa son idénticos a los tradicionales quid pro quo. El factor más importante y vulnerable, dentro de una organización de ciberdefensa, sigue siendo el recurso humano. La capacitación de los cuadros de toda la sociedad se constituye en la solución más importante para la implementación de una estrategia de ciberdefensa, efectiva, eficiente y eficaz. Dicha capacitación debe incluir la formación actitudinal de la persona, para que responda en forma preventiva y proactiva ante las amenazas y sus indicios. La ciberdefensa, afecta a todos los integrantes de la sociedad, de manera indistinta y de diferentes formas, por lo que una estrategia en tal sentido requiere del compromiso de toda la ciudadanía y sus cuadros jerárquicos.

A partir de esto cabe reflexionar si es la ciber defensa un nuevo campo científico, tecnológico o técnico, o si se está sólo en presencia de un cambio en el teatro de operaciones clásico, que los conflictos humanos, bélicos o no, han desarrollado a lo largo del recorrido evolutivo de la humanidad. Respondiendo este interrogante, podemos afirmar que la ciberdefensa escapa al marco nacional y sólo puede ser entendida en un entorno globalizado e integrado en redes. Por otra parte, la ciberdefensa en Argentina ha logrado sentar las bases y progresar en forma sostenida hacia la creación y consolidación de un nuevo campo intelectual y profesional que se evidencia en las ofertas de posgrados existentes al igual que en la producción académica.

Entre las discusiones que se dan en este nuevo campo intelectual en construcción, se halla la necesidad de reflexionar sobre el impacto que produce el Software Libre en la ciberdefensa. En el año 2000 Phillip Glen Armour, (autor de The Five Orders of Ignorance) sostenía que el software no es un producto, sino un medio para el almacenamiento de conocimiento, ubicado en el quinto puesto, los otros medios donde se guarda el conocimiento son: ADN, cerebros, hardware y libros. Esto lo fundamenta en que el software se ha convertido en un medio de almacenamiento superador. Se trata de conocimiento activo y evolutivo que ha sorteado el confinamiento y la volatilidad del conocimiento en los cerebros; supera el estado pasivo del conocimiento impreso en los libros; tiene la flexibilidad y la velocidad de cambio que carecen el conocimiento del ADN o a la evolución del hardware. Sin dudas el producto del esfuerzo en la producción de software es el conocimiento contenido en dicho software, por lo tanto, el desarrollo de software no es una actividad de generación de productos, es una actividad de adquisición de conocimientos.

En el ámbito de la defensa estaban bien definidas las dimensiones de tierra, mar, aire, e incluso el espacio. Ahora contamos con una dimensión nueva denominada "quinto dominio", de inusual intangibilidad comparada con las anteriores (Bejarano, s. f., p. 51). El software ejerce una influencia preponderante en todos los procesos beligerantes del quinto dominio, no sólo constituye la materia prima de las armas cibernéticas sino que puede afectar entre otras actividades los procesos electorales o la seguridad de cualquier Infraestructura Crítica. Richard Stallman, fundador de este movimiento, planteó la disyuntiva entre el uso de software libre, que respeta la libertad del usuario (GNU/Linux), o el software privativo, que impide la transparencia y la modificación del código fuente, y no respeta las libertades del usuario.

En nuestro país fue lanzado en 2004 como FLOSS la distribución Linuxmil primera en su tipo orientada al empleo militar, cuyo desarrollo tuvo el aporte de la comunidad del Software Libre representada por la asociación civil SOLAR (Software Libre de la Argentina) y el apoyo internacional de la Free Software Foundation. "Las capacidades cibernéticas tienen la posibilidad de ser una capacidad asimétrica y un multiplicador de fuerzas que podría ser una consecuencia importante para la ciberdefensa en nuestro país y la región" (Lobato, 2017). Las tecnologías FLOSS en Ciberdefensa se justifican porque otorgan soberanía e independencia tecnológica. "¿Cómo hubieran reaccionado los troyanos si el caballo de los griegos hubiera sido de vidrio? Habrían impedido su acceso", dijo Bob Gourley, ex director de tecnología de la Agencia de Inteligencia de Defensa. "Eso es clave sobre el SL, todos pueden examinar el código, buscar y eliminar las vulnerabilidades antes de que se introduzcan."

En el marco de la irrupción del quinto dominio, se suma el actual contexto de pandemia mundial por el covid-19. Uno de sectores impactado es el de la educación, particularmente el universitario,[2] que en 2016 se hallaba integrado por 131 instituciones educativas, contando con 1.975.190 estudiantes y 183.908 cargos docente. Tal situación presenta la necesidad de desarrollar un marco de referencia para la evaluación de sistemas de gestión de aprendizaje en el contexto universitario. Para ello es necesario abordarlo desde enfoques institucional-académico y técnico-pedagógico donde se analice la situación actual de las investigaciones en el tema, comparando los paradigmas anteriores y actuales. Además, se hace necesario identificar características, elementos claves y actores interesados; al igual que las características de los modelos de calidad y normativas sobre la temática, teniendo en cuenta: la evaluación de producto software tipo: web, implementado como plataforma de aprendizaje sistemas de gestión abiertos, gratuitos y libres. Así, estos estudios podrían aportar propuestas para evaluar el atributo de calidad de seguridad: en el que se evalúa la seguridad informática de los LMS implementados en contextos universitarios ejecutados por usuarios con diferentes roles.

El campo de la ciencia de datos aplicada, orientado a la detección de perfiles y patrones que permitan inferir prácticas compatibles con ilícitos en el ciberespacio, se presenta como tema de interés del quinto dominio mediante la necesidad de propuestas de investigación aplicada. En este sentido, demostrar el aporte de los algoritmos mediante estudios descriptivos y correlacionales basados en estadística inferencial aporta valor y un desafío adicional a este campo en construcción, especialmente al ámbito del blanqueo en el ciberespacio.

La relevancia del tema se fundamenta en la complejidad que plantea el delito mencionado y su crecimiento exponencial en un escenario tan complejo como es el ciberespacio, dado que el mismo involucra a la macroeconomía y los desequilibrios que genera. El desarrollo vertiginoso de la tecnología en las últimas décadas, en particular de la inteligencia artificial, constituye una herramienta tanto para los Estados y fuerzas de seguridad como para el crimen organizado. Por esto, resulta imperioso contar con instrumentos que logren la capacidad de prevención de este delito mediante la detección de perfiles y patrones de comportamiento para anticiparse a su comisión.

El creciente desarrollo tecnológico -donde tecnologías como la cadena de bloques e inteligencia artificial han favorecido la transferencia de importantes volúmenes de dinero en escasos minutos- ha favorecido el incremento exponencial y el perfeccionamiento del

[2] http://estadisticasuniversitarias.me.gov.ar/#/home/1

blanqueo de activos hasta alcanzar niveles difíciles de determinar con precisión. En consecuencia, el efecto de distorsiones económicas y financieras a escala global resulta complejo de cuantificar. Si bien existen diferentes modelos predictivos de inferencia de patrones y perfiles sobre delitos económicos y financieros basados en algoritmos neuronales de aprendizaje automático, no se aplican técnicas de muestreo no probabilísticas. La ampliación de este tipo de investigación dependerá del conocimiento en ciencia de datos con la que cuenten quienes decidan abordarla además de una sólida formación económica y financiera.

Tanto la ciberseguridad como la ciberdefensa, plantean el desafío de la interoperabilidad, dado que la resolución de sus escenarios demanda el abordaje interdisciplinario y multiagencial. La interoperabilidad es importante para lograr una correcta provisión de servicios, datos y para una toma de decisiones de calidad en el Estado Nacional. Además, permite evitar la duplicación de datos, reducir los costos de implementación y mantenimiento de sistemas, motivar la creación de servicios agregados, incrementar la confiabilidad entre los sistemas y principalmente es la base que permite a los gobiernos beneficiarse del uso intensivo de las TIC. En este sentido, un aporte al campo surge de la investigación sobre la implementación de la plataforma de interoperabilidad para el intercambio de datos, X-Road.

Para la integración de aplicaciones la normativa argentina permite utilizar un módulo del "Sistema de Gestión Documental Electrónica (GDE)" o realizarla punto a punto teniendo en cuenta recomendaciones. Esta opcionalidad y la falta de promoción de la interoperabilidad hacen que la misma no forme parte de las estrategias de los organismos. Analizar el tema permitiría disponer de las bases para incrementar los niveles de seguridad, eficiencia, economía, eficacia y calidad de los servicios que se prestan y el cumplimiento efectivo de las normas nacionales de manera generalizada y gestionable. El control y administración de la interoperabilidad a escala nacional no solo impacta en términos económicos y de eficiencia para el Estado, sino que lateralmente impacta en aspectos de prevención, detección y corrección de mecanismos que permiten el fraude o corrupción, debido a la alineación tecnológica, semántica, procedimental y legal.

Diferentes países, en los cuales la interoperabilidad fue considerada un tema estratégico, se han visto afectados por distintos aspectos. La "opcionalidad" normativa es la principal barrera que retrasa la implementación de la interoperabilidad. No existe una gestión integral de la interoperabilidad, con fuerte presencia de islas de información y procesos disjuntos. La "obligatoriedad" e "institucionalización" de la interoperabilidad como medida doblega las barreras iniciales. La implementación de políticas de interoperabilidad e

información relacionada establece la nivelación tecnológica a gran escala, reimplementando procesos transversales así como el monitoreo de la evolución de las diferentes implementaciones a nivel nacional. De igual manera, la falencia técnica que aún resta por actualizar es la infraestructura de firma digital argentina, relacionada con el componente de sello de tiempo, un aspecto a considerar. Con respecto a X-Road, se evidencia la posibilidad de uso en el Estado nacional desde una perspectiva técnico-legal.

"En la actualidad es posible afirmar que cada vez es mayor la dependencia de las sociedades al complejo sistema de infraestructuras que soportan servicios esenciales de información. Si a eso se le suma el incremento en los riesgos y amenazas no tradicionales contra la seguridad nacional, se torna imprescindible que el Estado realice mayores esfuerzos a favor de prevenir y proteger, en un corto plazo, las infraestructuras críticas de la información"

La complejidad del tema delata la necesidad de una capacitación profesional, donde entra la institucionalización y necesidad de una carrera profesional tecnológica por fuera de la administrativa nacional. El inconveniente de la baja competitividad económica estatal, en conjunto con una baja capacitación tecnológica de los niveles de mandos medios, con el tiempo va generando una migración de los profesionales TIC al sector privado. Un análisis profundo de la "jerarquización" profesional debido al dinamismo propio de la evolución tecnológica permitiría planear una disminución de los tiempos de formación y especialización disminuyendo la brecha entre el formalismo de grado y las necesidades laborales reales.

El mercado de las certificaciones internacionales en el campo de la ciberseguridad es amplio y puede estar vinculado o no a un producto o marca. Puede ser táctico, como configurar un dispositivo de red, operativo, como analizar el riesgo de TI de una migración a la nube, o estratégico, como planificar la seguridad de la información de una organización. Saber cuántas certificaciones existen en la actualidad no solamente muestra que la oferta es importante, sino que además hay una demanda de la especialidad.

Las personas dedicadas a la ciberseguridad obtienen un cierto nivel de especialización en este campo de la computación, lo que conlleva un alto grado de experiencia. Esta experiencia, acompañada con el desarrollo profesional y la carrera administrativa en cualquier organización, requiere de algún tipo de legitimación. Algunos tornan a la titulación de grado en paralelo a su trabajo. Otros, en cambio, acuden a certificaciones internacionales en

ciberseguridad, ya que cubren diferentes dominios o temas. Estos diplomas se traducen en credenciales de presentación y muestras de idoneidad para el cumplimiento de los objetivos propios de cada profesional. Conocer la variedad, criterios de elegibilidad, costos, formas de estudio y acceso a material, entre otras características, son percibidas como el puntapié de la carrera, para avanzar o incluso para mantenerla.

El estado del arte da cuenta de una gran cantidad de organizaciones que proveen certificaciones (43), ascendiendo a un total de 442 opciones. Dichas certificaciones se clasifican en diferentes criterios como las vinculadas a un proveedor y las que son ajenas o independientes; las referentes a la implementación de seguridad, a la arquitectura de seguridad, a la gestión de seguridad, al análisis de seguridad; aquellas certificaciones sobre operaciones defensivas (forense y manejo de incidentes) y operaciones ofensivas (pruebas de penetración y explotación); y si corresponde a un nivel principiante o novato, intermedio, avanzado o experto.

Al respecto, se hallan en curso de investigación tres temas: las certificaciones internacionales en ciberseguridad y una posible clasificación, la relación entre los sistemas institucionales nacionales y la necesidad de crear un sistema nacional que articule íntegramente aquellos sistemas existentes con enfoque en las infraestructuras críticas de la información argentinas y la capacitación mediante ciberejercicios para la defensa de las infraestructuras críticas. Desde la perspectiva de política educativa se podría investigar el costo de cada certificación, la cantidad de créditos (CPE) necesarios para mantener los criterios de capacitación continua, los dominios de cada certificación, cuáles son comunes entre las distintas opciones y qué porcentaje se debe obtener de cada dominio o en general para aprobar el examen. De igual modo, interesa comparar las principales certificaciones desde los temas que cubren con la oferta académica de posgrado a nivel nacional, determinando si es valor agregado o una meta estipulada que personal dedicado a la ciberdefensa obtenga dichas certificaciones, o relevar, donde sea posible, el nivel de inserción de dicho mercado de certificaciones en nuestro país.

El concepto de infraestructuras críticas de la información y sus riesgos han ido evolucionando, junto con el crecimiento acelerado de la tecnología, hasta convertirse en un activo esencial para cualquier sociedad. En la actualidad, las infraestructuras críticas de un país se encuentran en el plano terrestre, marítimo, aéreo, espacial y/o ciberespacial y requieren un plan de prevención y protección a favor de conservar los servicios esenciales de la comunidad.

En la actualidad es posible afirmar que cada vez es mayor la dependencia de las sociedades al complejo sistema de infraestructuras que soportan servicios esenciales de

información. Si a eso se le suma el incremento en los riesgos y amenazas no tradicionales contra la seguridad nacional, se torna imprescindible que el Estado realice mayores esfuerzos a favor de prevenir y proteger, en un corto plazo, las infraestructuras críticas de la información.

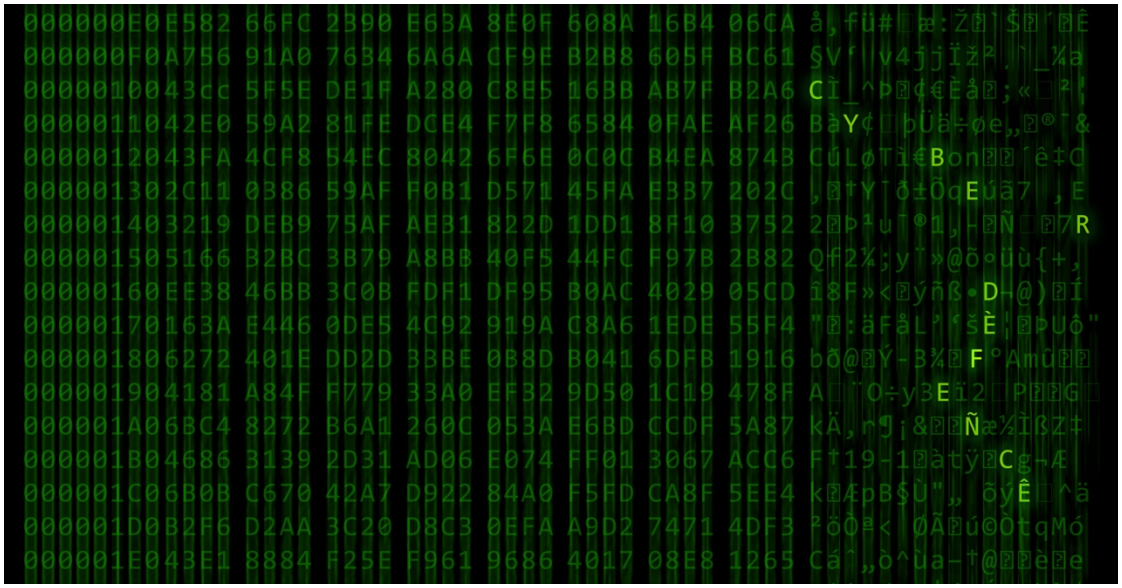
Considerando que las infraestructuras críticas han incorporado una gran cantidad de componentes informáticos, los ciberatacantes aprovechan para afectarlas generando un impacto en el funcionamiento efectivo de un Estado, la salud, la seguridad, la defensa, el bienestar social y la economía de un país. La ciberguerra, el ciberterrorismo, el ciberespionaje y el ciberdelito, lejos de reemplazar las formas tradicionales de ataque, en general conviven con estas. Frente a ello, los gobiernos han comenzado a trabajar en la ciberseguridad y ciberdefensa de sus países.

El análisis y revisión del plexo normativo relacionado con las funciones del Ministerio de Seguridad, Ministerio de Defensa, Secretaría de Modernización y Agencia Federal de Inteligencia en lo que respecta a infraestructuras críticas de la información nacionales es un tema de interés para la investigación. Para ello se hace necesaria la identificación, relevamiento, determinación y catálogo de infraestructuras críticas de la información; la capacitación de los operadores considerados como críticos; la investigación, desarrollo e innovación de tecnología de ciberseguridad y la cooperación entre los sectores públicos y privados.

Si bien en la actualidad el desarrollo investigativo, práctico y estratégico de las infraestructuras críticas como activo esencial de cualquier sociedad ha sido amplio, la Argentina se encuentra normativa y funcionalmente demorada. En efecto, la multiplicidad de dimensiones, complejidades y evolución constante del ciberespacio, requiere de un enfoque que posea el mismo dinamismo, pero con la estructura organizativa adecuada que permita un trabajo mancomunado de todos los actores vinculados con las infraestructuras críticas de la Argentina.

Frente a ello, es imprescindible que nuestro país desarrolle un Plan Estratégico Nacional en lo que hace a las infraestructuras críticas de la información con el fin último de prevenir una afectación parcial o total, defender los activos esenciales de nuestra nación para proteger a la sociedad y los principales intereses de la República contemplando la capacidad de resiliencia de los sistemas y redes informáticas del Instrumento Militar, los organismos de gobernanza y todo aquel actor externo al Sistema de Defensa Nacional que, en la esfera de sus funciones, impacte en la zona de influencia que abarca la Defensa Nacional, en particular, los objetivos estratégicos que determinen como parte de su alcance funcional y operacional.

Las investigaciones futuras deberán centrarse en el estudio de las distintas tecnologías existentes y a desarrollar, para una protección, prevención y resiliencia efectiva de las infraestructuras críticas argentinas. Por otra parte, se debería efectuar un análisis exhaustivo sobre las distintas metodologías a emplear para la identificación de las infraestructuras críticas, en base a los criterios y sectores detallados en la normativa nacional, para realizar un relevamiento intersectorial contemplando la dependencia e interdependencia de las distintas infraestructuras. Finalmente, las investigaciones deben dar cuenta de la capacitación y concientización del recurso humano que opera y se relaciona con los sistemas y redes que se emplean en las infraestructuras críticas y la interrelación, cooperación y coordinación de los actores del sector público y privado que se relacionan estratégicamente con dichas infraestructuras.



La importancia de la investigación, desarrollo e innovación en ciberseguridad de las infraestructuras críticas de la información, requiere de un abordaje multifacético; como también un instituto nacional que articule al Sistema Nacional de Ciencia y Tecnología e Innovación existente y aquellos institutos que puedan investigar en materia de ciberseguridad. Es preciso entender a la ciberseguridad como un ámbito donde interactúan múltiples actores, objetivos y procesos tanto sociales, como técnicos, económicos y legales. Frente a ello, se torna imprescindible la mejora en la tecnología y las prácticas existentes con el fin de fomentar el empleo de sistemas seguros a nivel nacional y considerando la normativa, es posible afirmar que la Estrategia Nacional de Ciberseguridad trae luz a la necesidad de desarrollar la industria nacional y potenciar las capacidades tecnológicas, aunque no satisface los medios mediante los cuales articular y cumplir con dicho objetivo.

Resulta de interés investigar no solo el diseño del organismo articulador de la investigación, desarrollo e innovación en ciberseguridad, sino también la definición sobre el rol que debe tomar la innovación en los recursos humanos en materia de capacitación y concientización -principalmente de los operadores de las infraestructuras críticas de la Argentina- dado que independientemente del avance en I+D+i, es claro que un buen manejo de la tecnología y las herramientas que pudieran diseñarse, es imprescindible para la evolución y posicionamiento de la Argentina a nivel mundial con capacidades propias.

La ciberdefensa es un nuevo campo intelectual con implicancias en diferentes agencias estatales y el sector productivo. Esto significa que, en cada una de las Fuerzas Armadas, en el Ministerio de Defensa, en las universidades, en los ámbitos de investigación y desarrollo, en empresas del sector productivo, en las diferentes posiciones de toma de decisiones políticas, se necesitan puestos laborales con características particulares que atiendan a las cuestiones e intereses de la ciberdefensa y la ciberseguridad. Estos puestos de nivel tácticos, operativos o estratégicos demandan un determinado perfil y ese perfil se consigue, en parte, mediante la educación, formación y entrenamiento. Saber qué puestos laborales, al igual que dónde y para qué tareas se los necesita, permite definir los perfiles profesionales. Conocer los perfiles profesionales permitirá pensar en trayectos formativos y curriculares. De este modo podrán pensarse políticas públicas basadas en datos empíricos, fortaleciendo las formaciones y orientándolas a cubrir necesidades existentes, evitando por otro lado duplicar esfuerzos o baches sin cubrir.

Desde la perspectiva de la teoría de campos, se comienza a perfilar la ciberdefensa como un nuevo campo. Esto significa que hay actores en juego, reglas del juego propias, capital (cultural y simbólico) en disputa, producción académica, ámbitos institucionales diferenciados, intereses y retribuciones que motivan el ingresar y pertenecer. Sin embargo, el estado actual de investigación y del propio campo muestran que el abordaje educativo sobre un aspecto del tema como podrían ser los dominios de la ciberdefensa, presenta diferentes propuestas curriculares que evidencian dificultades para comprenderse y consensuar interacciones. Se observan tres perspectivas que demandan mayor interacción y comunicación entre sí: la técnica, la política y la de gestión. Se observa la necesidad de intercambio académico de: experiencias, enfoques, investigaciones, profesionales; se hace necesario poder identificar y visibilizar la existencia de equipos de investigación, sus propuestas y perspectivas. No hay evidencias claras de vínculos entre el sector académico y el sector productivo. Los estudios actualmente publicados, presentan debilidad en sus estados del arte. Por otra parte, parecieran hallarse dispersos, sin un plan estratégico sobre necesidades o prioridades de investigación, perspectivas y enfoques de abordajes. Se hace visible la necesidad de incorporar

mayor trabajo de campo (entrevistas, testimonios, análisis etnográficos, mayor densidad de fuentes primarias y documentales).

Desde una perspectiva sociológica aportarían a este campo estudios que ayuden a comprender posturas y visiones estratégicas; circuitos de información, vínculos y aportes entre sector académico, productivo y estatal; grupos de poder e interés vinculados a diferentes temas del campo; debilidades y necesidades de instituciones y actores. Desde el punto de vista de la educación en ciberdefensa, hay necesidad de abordar estudios que indaguen, reflexionen y propongan sobre: puestos laborales en diferentes ámbitos, instituciones y niveles; perfiles profesionales para dichos puestos y desarrollos curriculares para la formación de estos perfiles, tanto para tareas tácticas, operativas o estratégicas, de investigación y desarrollo. Es necesario identificar las urgencias, las necesidades y las posibilidades actuales, para decidir cuál es el camino más corto y eficaz para obtener el recurso humano que se necesita. Las investigaciones que analicen y reflexionen sobre cuestiones técnicas, tecnológicas, políticas, legales; como también sobre metodologías, enfoques y tipos de análisis, doctrinas, teorías y, desde allí infieran nuevas necesidades u orientaciones de investigación que nutran a cátedras, analistas, grupos de investigación, empresas, agencias estatales, asesores y decisores políticos, entre otros, se hallan pendientes en la producción académica.

Conclusión

Argentina reconoce la importancia que posee la ciberdefensa para la estrategia de defensa y el diseño de su instrumento militar. Esta situación se ve reflejada a nivel local mediante una creciente actividad académica donde surgieron diferentes ofertas de formación. Dentro de este marco, la formación en ciberdefensa y ciberseguridad cobra interés y su abordaje lleva a preguntarnos por necesidades y estrategias de formación que tanto el sector estatal como productivo requieren, como un camino necesario para el planeamiento de la política de ciberdefensa y ciberseguridad, entendidas como una herramienta pública para la gestión en el ciberespacio.

En este sentido, el presente artículo brinda elementos orientadores para estudiantes, profesores, investigadores, planificadores de políticas públicas, decisores políticos del sector militar, civil y empresarial de modo de contribuir a la discusión teórica y metodológica que permitan delinear futuras investigaciones.

En el aspecto académico, la investigación en ciberdefensa y ciberseguridad en Argentina se encuentra en desarrollo, contando con una diversidad de temas y enfoques que aún esperan ser abordados y comunicados. No alcanza con el conocimiento circunscripto a lo personal o institucional. Hace falta socializarlo, debatirlo, consensuarlo, integrarlo al circuito

de producción académica, y esto es una tarea aún por desarrollar que demanda el compromiso y esfuerzo de los estudiantes, profesores, investigadores, pero también de las autoridades académicas y políticas.

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

Bejarano, M. J. C. (s. f.). Alcance y ámbito de la Seguridad Nacional en el ciberespacio. 35.

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

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.

Eissa, S.G; Gastaldi, S.; Poczynok, I. y Di Tullio, M. E. (2012). El 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

Elustondo, M. M. (2011, febrero 24). El proyecto GNU LINUXMIL Socio de Honor de la Asociación gvSIG. Recuperado 1 de noviembre de 2019, de Comunidad GvSIG Argentina website: http://gvsig-argentina.blogspot.com/2011/02/el-proyecto-gnu-linuxmil-socio-de-honor.html

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, L. (2013). 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. (2014a). Informes de actualidad y temáticas de defensa. EDENA: Secretaría de Investigación, 11-08-2014, p. 9.

Gastaldi, S. y Justribró, C. (2014b). Informes de actualidad y temáticas de defensa. EDENA: Secretaría de Investigación, 25-08-2014, p. 16.

Lobato, L. C. (2017). La política brasileña de ciberseguridad como estrategia de liderazgo regional/The brazilian cybersecurity policy as a strategy of regional leadership. URVIO. Revista Latinoamericana de Estudios de Seguridad, (20), 16-30. https://doi.org/10.17141/urvio.20.2017.2576

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

SOLAR. (s. f.). Entrevista al Proyecto LINUXMIL | Software Libre Argentina. Recuperado 1 de noviembre de 2019, de http://solarargentina.org/entrevista-al-proyecto-linuxmil-0

Soler Muñoz, R. (2013). Economía, bienes públicos puros e Internet: Revelando el caso del FLOSS ("Free/Libre Open Source Software" o "Software Libre y Software de Código Abierto"). Recuperado de http://roderic.uv.es/handle/10550/27074

Stallman, R. M. (, & Lessig, L. (. (2007). Software libre para una sociedad libre. Madrid: Traficantes de Sueños.

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.