DOI 10.21057/10.21057/repamv15n2.2021.36509 dossiê

Ciberdefensa como campo intelectual: Aportes y propuestas de investigación en Ciberdefensa y Ciberseguridad para la realidad argentina.

Guillermo Rutz[1]

Introducción

En los últimos años, la Defensa Nacional argentina viene reconociendo la importancia que posee la ciberdefensa para la estrategia de defensa y el diseño de su instrumento militar. No se trata de una preocupación aislada, sino que se encuentra a la vez inserta en un escenario internacional en el que los denominados "ciberataques" han empezado a afectar las relaciones interestatales y a generar dilemas estratégicos para la acción estatal. Paralelamente, desde el año 1993 desde uno de los centros estadounidenses más influyentes para la academia y el planeamiento estratégico de la defensa como es la RAND CORPORATION se acuñó el concepto de "ciberguerra" como una nueva modalidad de conflicto (Arquilla; Ronfelt, 1993). Los casos de las operaciones cibernéticas contra Estonia en 2007 e Irán en 2010 fueron tomados como el preludio de esta nueva guerra cibernética. Esta situación se ve reflejada a nivel local mediante una creciente actividad académica donde entre otros aspectos surgieron diferentes ofertas de formación.

Este complejo escenario emergente marcado por la vulnerabilidad estratégica que puede provocar a los Estados mediante el impacto de las nuevas tecnologías de la información y las comunicaciones (TIC) y las distintas respuestas académicas locales orientadas a la formación de recursos humanos, requieren ser objeto de análisis científico. Dentro de este marco, la formación en ciberdefensa en los niveles operativos, tácticos y estratégicos aparece como un interrogante de interés para la Defensa Nacional. Su abordaje lleva a preguntarnos sobre las necesidades y estrategias de formación que, tanto el sector estatal como estratégico productivo, requieren como un camino necesario para el planeamiento de la política de ciberdefensa, entendida como una herramienta pública para la gestión de la Defensa Nacional en el ciberespacio.

La formación en ciberdefensa y ciberseguridad constituye un nuevo campo del saber e incipiente, pero con un crecimiento vertiginoso, 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. Tanto para empresas del sector público y privado, como también para los diferentes organismos del Estado y las áreas de defensa y seguridad, existen y existirán necesidades específicas, comunes y diferenciadas en torno a lo ciber. En función de ello, uno de sus intereses estará puesto en los recursos humanos acorde a sus características organizativas y objetivos o necesidades. Para esto, pensar su formación a partir de bases comunes, pero con orientaciones o perfiles diferenciales, será una necesidad no sólo de los ámbitos académicos sino también de aquellos que toman decisiones políticas.

En función de lo expuesto, el artículo presenta futuras líneas de investigación en relación a ciberdefensa y ciberseguridad a partir de miradas y abordajes heterogéneos vinculados a problemáticas de interés para el área. El mismo, tiene por objeto dar continuidad a la línea de investigación "Ciberdefensa y posgrados en Argentina. Aproximaciones desde una perspectiva social y de políticas públicas", desarrollada en 2019 dentro del Proyecto UNDEFI-FADENA "Soberanía nacional y ciberdefensa. Elementos teóricos y político-estratégicos del desafío ciberespacial para la Defensa Nacional".

1 **Guillermo Rutz** es Doctor en Ciencias Sociales (FLACSO), Magíster en Estrategia y Geopolítica (ESG), Magíster en Defensa Nacional (FADENA), Magíster en Educación y Ciencias Sociales (FLACSO), Especialista en Políticas Educativas (FLACSO), Especialista en Desarrollo Local (ONU-OIT), Diplomado en Gestión de la Ciberdefensa (ESGCFFAA), Licenciado en Bibliotecología y Documentación (UNMDP). Cuenta con numerosas capacitaciones en Administración Pública Nacional (INAP). Dirigió e investiga temas de Defensa Nacional y Ciberdefensa vinculados a la educación, recursos humanos, políticas públicas. Contacto: e-mail: rutzguillermo@gmail.com; https://padlet.com/rutzguillermopublicaciones/Bookmarks; https://independent.academia.edu/GuillermoRutz

Lo Ciber en el contexto argentino

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

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

En cuanto a la formación de posgrado en la especialidad, en el año 2018 la Universidad de Buenos Aires – en convenio con la Escuela de Inteligencia Nacional – ofreció la maestría en ciberdefensa y ciberseguridad que pone el foco en la gestión, no así en formar tecnólogos de la especialidad. Por otro lado, en julio del año 2019 la Facultad de Ingeniería del Ejército – dependiente de la Universidad de la Defensa – implementó un segundo año en su carrera de criptología, mediante el cual se accederá a la maestría en ciberdefensa con una orientación netamente tecnológica del área de ingeniería. Además de estas maestrías, existen dos diplomaturas en universidades privadas especialmente dirigidas, aunque no restrictivamente, a profesionales que se desempeñan en actividades de seguridad informática generalmente vinculados al ámbito bancario y del sector legal: la "Diplomatura Gestión y Estrategia en Ciberseguridad", ofrecida por la Universidad del CEMA, y la "Diplomatura en Ciberseguridad" dictada por la Universidad CAECE. Por otra parte, hay varias maestrías y especializaciones que se enfocan en componentes técnicos y específicos debido a la complejidad técnica que se requiere en la temática como, por ejemplo redes de datos, redes y seguridad, entre otros.

Respecto a políticas públicas, en el año 2011 se crea el Programa Nacional de Infraestructuras Críticas de Información y Ciberseguridad (Resolución N° 580/2011) para dar un marco regulatorio para identificar y proteger las infraestructuras críticas y estratégicas del sector público y privado. Unos años más tarde se conforma la Unidad de Coordinación Cibernética en la Jefatura de Gabinetes de Asesores del Ministerio de Defensa (Resolución N° 385/13), y al año siguiente se crea el Comando Conjunto de Ciberdefensa, dependiente del Estado Mayor Conjunto de las Fuerzas Armadas por medio de la Resolución N° 343/14. Por su parte, el Ministerio de Defensa en el año 2015 puso en funcionamiento la Dirección General de Ciberdefensa, que debía asistir en cuestiones de política de ciberdefensa –entre otras–; y fue elevada a Subsecretaría en enero del año 2016 mediante el Decreto N° 226/2016 contando con dos direcciones: la Dirección Nacional para el Desarrollo Científico de la Ciberdefensa y la Dirección Nacional de Diseño de Políticas de Ciberdefensa.

Al mismo tiempo el entonces Ministerio de Modernización – hoy Secretaría– creó dentro de su órbita la Subsecretaría de Tecnología y Ciberseguridad mediante el Decreto N° 13/2016, con el propósito de entender en políticas de infraestructuras tecnológicas, protección de infraestructuras de información y capacitación en

seguridad informática al sector público nacional, privado y ONGs que lo requieran. Al año siguiente, surge el Comité de Ciberseguridad (Decreto N° 577/2017) integrado por representantes de Modernización, Defensa y Seguridad, con el objeto de impulsar un marco normativo de Ciberseguridad y participar en acciones de Ciberseguridad a nivel nacional. Finalmente, en mayo del año 2019, la Secretaría de Gobierno de Modernización dicta la Estrategia Nacional de Ciberseguridad (Resolución N° 829/2019) resultando pendiente la Estrategia Nacional de Ciberdefensa que, si bien fue publicada en el último mes de la administración del ex Presidente Mauricio Macri, se derogó en el año 2020.

El lenguaje en cuanto a la definición conceptual de lo Ciber

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

El término cibernética fue acuñado por Nobert Wiener en "Cybernetics, or Control and Communication in the Animal and the Machine" (1948) donde propone su teoría del control y la comunicación en máquinas y animales desde una perspectiva matemática. Allí surge, de la combinación de matemáticas y neurofisiología, que es una ciencia que permitirá el control de factores inherentes a la naturaleza y al funcionamiento de la sociedad (Wiener, 1998), siendo el espacio cibernético una categoría central que presenta una multiplicidad de abordajes conceptuales.

Para Bloch (2008), la cibenética es una disciplina que busca lograr un dispositivo capaz de realizar complejas funciones similares al pensamiento, donde coexisten dos teorías principales: la Teoría de la Información y la Teoría de la Robótica. En el mismo orden, Orciuoli (2005:14) la entiende como "una ciencia interdisciplinaria que al ponerse en movimiento transforma la información en un resultado deseado" mientras que Eissa et. al. (2012) considera que "no constituye un espacio en sí mismo, sino más bien una dimensión superpuesta, que atraviesa a los espacios físicos tradicionales" coincidiendo de este modo con Sheldon (2011) en el sentido que el ciberpoder genera efectos en todos los espacios de forma absoluta y simultánea. De este modo es que resulta de interés para los Estados dada su capacidad de producir modificaciones en el mundo físico. Por su parte, Sierra (2015:16) lo define como "el conjunto de medios y procedimientos basados en las TIC –Tecnologías de la Información y Comunicaciones– configurados para la prestación de servicios" de lo cual surge que internet forma parte del espacio cibernético porque internet es comunicaciones y comunicaciones es solamente el escenario.

En la misma línea que Sierra, Feliú Ortega (2012:42-3) considera que "el espacio cibernético es más que internet, más que los mismos sistemas y equipos e incluso que los propios usuarios, es un nuevo espacio con sus propias leyes físicas que, a diferencia de los demás espacios, ha sido creado por el hombre para su servicio". Ottis y Lorents (2012), por su parte, sostienen que "es un conjunto de sistemas de información interconectados dependientes del tiempo y los usuarios humanos que interactúan con estos sistemas", compartiendo la línea de razonamiento con Uzal (2013) quien lo define como "la dimensión generada durante el tiempo de interconexión e interoperabilidad de redes, sistemas, equipo y personal". A su vez, Desforges (2014:67) sostiene que "el término ciberespacio no es neutral, sino que conlleva varias representaciones, algunas contrapuestas, y que dan origen a las concepciones de ciberespacio que luego se transcriben en las estrategias de los Estados, que luego son instrumentos o herramientas de geopolítica". Finalmente es de interés destacar la noción de ciberespacio como espacio cognitivo abordada por Ocón (2019) como también Libicki (2009), Strate (2018) o Grant (2014).

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.

La Ciberdefensa y el Triángulo Sabatino

Sábato postula que para que exista una estructura científico-tecnológica productiva es necesaria la presencia del Estado como diseñador y ejecutor de políticas, la infraestructura científico-tecnológica dada por el sector académico y un sector productivo que demande esta estructura; donde su éxito requiere de una interrelación fuerte y permanente entre ellos (Sábato y Botana, 1968. Sábato, 1975). Si el Estado y/o el sector productivo prescinden del científico-académico, éstos carecerán del conocimiento y metodologías para sostener el modelo triangular sabatino. La interrelación de este triángulo requiere de la capacidad de entablar y fortalecer vínculos institucionales a menudo debilitados por falta de coordinación, carencias de canales de comunicación o problemas de asimetrías en la información donde "el peligro del encierro y diálogos sordos entre empresarios y científicos se presenta como un obstáculo muchas veces insuperable" (Sábato, 2011: 226). Para lograr lo planteado por Sábato, se requiere de un esquema de planificación a largo plazo que permita integrar visiones, objetivos y metas. En este sentido, la investigación académica aquí planteada podría ser considerada como un recurso y componente esencial, en lo que a ciberdefensa concierne, dado su incipiente pero acelerado desarrollo en el campo estratégico de la Defensa y la soberanía nacional.

Lo que frecuentemente desvela a quienes toman decisiones e implementan acciones públicas es saber si, lo que hacen a través de las políticas, tiene el efecto esperado sobre el problema que motivó su intervención. Esta inquietud lleva de manera directa a considerar la perfectibilidad de cualquier iniciativa (Bertranou, 2015). La evaluación implica un proceso que indaga sistemáticamente en la intervención que realiza una actividad pública sobre la realidad social, con el objeto de generar un conocimiento que facilite luego la mejora de esta actividad, en términos de eficacia, eficiencia y equidad (Nirenberg, Brawerman y Ruiz, 2000). Sin embargo, generar conocimiento sobre el desempeño de una política o de un programa no es una cuestión exenta de discrepancias y disputas, principalmente por el proceso a partir del cual se construye un juicio sobre la realidad empírica. Para el enfoque interpretativo, la realidad se nos presenta mucho más compleja e incierta, y las discrepancias sobre lo que observamos provienen de las diversas posiciones valorativas de los observadores, de los distintos criterios a partir de los cuales es posible realizar un juicio sobre un programa y de la imprecisión de los métodos de observación en relación con la complejidad de la realidad social. Este enfoque admite que existen distintas miradas y distintas evaluaciones posibles, y confía en métodos cualitativos para generar conocimientos, de esta manera, la experiencia es también una importante fuente de aprendizaje y de conocimiento (Feinstein, 2007). Para Carol Weiss, la relación entre la evaluación —y el conocimiento que eventualmente genera— y la práctica de las políticas públicas no es directa. Esto ilustra cierto escepticismo

acerca del uso de las evaluaciones por parte de hacedores y políticos en las políticas públicas. Para la experta, la evaluación, como investigación, puede estar destinada a proveer: evidencia empírica; nuevas aproximaciones posibles a un problema y Argumentos, es decir especificaciones de causa-efecto o de relaciones sociales alrededor de un problema y su resolución (Weiss, 1999).

En el marco de lo expuesto precedentemente, este artículo se propone analizar aspectos que aporten a la formación e investigación en ciberdefensa-ciberseguridad vinculada a los intereses de la Defensa y la Soberanía Nacional. En este sentido, se buscará identificar categorías y aportes relacionados a la formación en ciberdefensa-ciberseguridad; proponiéndose identificar orientaciones para la formación en ciberdefensa a nivel operativo, táctico y estratégico. La publicación pretende tomar como elementos de análisis las distintas líneas de investigación desarrolladas durante el 2020 en un Proyecto UNDEFI promovido por la Universidad de la Defensa (UNDEF), con ello se espera aportar a la discusión para fortalecer la formación de recursos humanos tanto para el sector público como para el estratégico productivo.

Ciberdefensa como Campo intelectual: aproximaciones a los desafíos de la acción pedagógica relativa a sus dominios.

Este tema reflexiona sobre la ciberdefensa a partir de los siguientes elementos de un campo intelectual, según la teoría de Bourdieu: estructura, interés, lucha por la distribución de capital, actores en juego, mercado específico, búsqueda de autonomía y arbitrio de la acción pedagógica. Busca con ello, distinguir indicios que la acerquen o no a las condiciones para constituirse en un campo intelectual dentro del cual surjan desarrollos teóricos y debates conceptuales. A partir de aquella reflexión, toma el sentido de la acción pedagógica para mirar los diferentes dominios de la defensa cibernética: Operaciones de seguridad, Desarrollo de carrera, Arquitectura de seguridad, Estándares de seguridad, Evaluación de riesgos, Gobernanza, Inteligencia de amenazas, Educación del usuario, Seguridad física, Políticas de ciberdefensa, Amenaza cibernética; y en torno a ellos pensar qué desafíos se le presentan a este campo en construcción, desde lo pedagógico y conceptual sobre sus dominios.

La ciberdefensa es un nuevo campo intelectual con implicancias en diferentes agencias estatales como también en 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 los puestos políticos (asesores, legisladores, decisores de políticas, entre otros), por nombrar algunos espacios sociales, se necesitan distintos y diferentes puestos laborales que atiendan a las cuestiones e intereses de la ciberdefensa. Estos puestos de nivel tácticos, operativos o estratégicos demandan un determinado perfil y ese perfil se consigue, en parte, mediante la educación y formación.

Saber qué puestos laborales, al igual que dónde y para qué tareas se los necesita, permite definir los perfiles profesionales que la ciberdefensa en Argentina, hoy y a futuro necesita. Contar (en producciones académicas) con los perfiles profesionales permitirá pensar en trayectos formativos y curriculares, de este modo podrán pensarse políticas públicas basadas en datos empíricos, fortaleciendo en este sentido las posibles formaciones orientándolas a cubrir necesidades existentes, evitando por otro lado duplicar esfuerzos o baches sin cubrir. Resolver esta necesidad de conocimiento (para el entorno académico, dado que para el ámbito institucional podría estar resuelto, pero no difundido) a partir de estudios empíricos y no solamente teóricos-especulativos, con el aporte institucionalizado de actores y agencias públicas-privadas involucradas, generará ventajas y fortalezas estratégicas para cada uno de los sectores mencionados y para el país en su conjunto.

La importancia de estudiar diferentes aspectos vinculados a la educación y formación en ciberdefensa se evidencia en estudios de organismos internacionales como la OEA cuyo reciente investigación regional "Educación en ciberseguridad: Planificación del futuro mediante el desarrollo de la fuerza laboral" deja fuera

de discusión las dudas al respecto. O a nivel local el Congreso IEEE ARGENCON 2020 que constituye el evento premium de la Sección Argentina del IEEE concentrando el interés de la comunidad científica y tecnológica vinculada a la ingeniería, con una frondosa sección dedicada a la educación. También así lo demuestran las trayectorias de investigación de aquellos países que lideran el desarrollo educativo, formativo y tecnológico en el tema. Comprender académica, política y socialmente la importancia, relevancia y necesidad de estos estudios permite brindar una visión estratégica al desarrollo del campo de la ciberdefensa que permita posicionarnos como actores proactivos en el tema.

La ciberdefensa desde la óptica sociológica de la Teoría de Campos, se comienza a perfilar como un nuevo campo intelectual. 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. En tal sentido van surgiendo cátedras, carreras, grupos de interés, producciones académicas, foros, agenda propia en lo político, social, militar y sector productivo. Por esto es un fenómeno social, con implicancia estratégica, que resulta de interés su estudio desde las ciencias sociales; esto implica conocer redes de poder, vínculos, procesos de producción de conocimientos, aportes a las diferentes áreas, necesidades propias, demandas desde el conocimiento, la política, lo militar, lo científico, lo técnico y tecnológico, entre otros aspectos a relevar, demostrar y explicar.

El estado actual de esta investigación y del propio desarrollo del campo, muestran que el abordaje educativo sobre un aspecto del tema como podrían ser los dominios de la ciberdefensa, presenta marcadas diferencias entre las propuestas curriculares vigentes; las cuales no siempre logran validar, aceptar y consensuar la necesidad de dichas diferencias como un aporte positivo y necesario para la comprensión y constitución global del campo. Se observa una pronunciada diferenciación curricular que se corresponde a tres perspectivas que demandan mayor interacción y comunicación entre sí: la técnica, la política y la de gestión. No todas las propuestas curriculares presentan intercambio académico de: experiencias, enfoques, investigaciones, profesionales; se hace necesario poder identificar y visibilizar la existencia o no de equipos de investigación, sus propuestas y perspectivas de sustentabilidad académica desde el punto de vista de la Investigación, Desarrollo e Innovación; no hay evidencias claras, plasmadas en producciones académicas fundamentadas empíricamente, de vínculos entre el sector académico, la investigación y el sector productivo. Los estudios que actualmente se publican sobre los distintos aspectos de este campo en fase de desarrollo, 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 observa que las actuales producciones académicas reflexionan sobre la base de otras producciones, no siempre ahondando en el análisis de las mismas; por lo cual se hace visible la necesidad de incorporar mayor trabajo de campo (entrevistas, testimonios, análisis etnográficos, mayor densidad de fuentes primarias y documentales).

En cuanto a la ciberdefensa como nuevo campo intelectual en construcción, no se observan estudios (es incluso un aspecto desestimado para algunos sectores), que ciertamente aportarían a comprender: las posturas y visiones estratégicas, políticas, sociales y culturales; los flujos de información y vínculos entre sector académico, productivo y estatal; el fortalecimiento y dificultades de los vínculos entre actores, agencias estatales, grupos de poder-interés e instituciones vinculadas al tema; las debilidades y necesidades de diferentes espacios, instituciones y actores. En tal sentido, desde las ciencias sociales faltan estudios con perspectivas desde la sociología, la historia, el derecho, la gestión y/o administración, entre otras que, si bien usen como soporte de análisis las teorías propias, se basen o demuestren empíricamente el tema o caso indagado.

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 laborales y desarrollos curriculares para la formación de estos perfiles generales o específicos, tanto para tareas tácticas, operativas o estratégicas, de investigación y desarrollo. Es

necesario identificar las urgencias, las necesidades y las posibilidades actuales, pudiendo contribuir a decidir cuál es el camino más corto y eficaz para obtener el recurso humano que se necesita, con la especificidad de cada caso. Es necesario dar cuenta en diferentes tipos de investigaciones sobre los equipos de investigación en el tema, sus composiciones, métodos de abordajes, trayectorias profesionales de sus integrantes, canales y espacios donde publican, dificultades e incentivos que tienen, impactos de sus resultados. Otros aspectos de importancia sobre los cuales existen vacancias de investigación son: conocer sobre relación, interacción y cooperación entre agencias del Estado, la Academia, el sector Productivo y de Investigación + Desarrollo + innovación, vinculándolos a los procesos educativos.

En igual medida, es necesario una metacognición sobre las investigaciones en curso. En tal sentido no se observan investigaciones que analicen y reflexionen a partir de artículos, tesis y eventos académicos sobre cuestiones técnicas, tecnológicas, políticas, legales, entre otras, desde la perspectiva educativa. Es necesario reflexionar sobre metodologías, enfoques, tipos de análisis, doctrinas, teorías utilizadas en dichas investigaciones; luego, desde allí se debe inferir y reflexionar, como también identificar nuevas necesidades u orientaciones de investigación que nutran a cátedras, analistas, grupos de investigación, empresas, agencias estatales, asesores y decisores políticos, entre otros posibles interesados.

En primer lugar, las investigaciones futuras deben fortalecerse mediante antecedentes más exhaustivos y en profundidad, citados en las mismas. Por otra parte, necesitan fundamentarse, en mayor proporción, mediante estudios empíricos y/o de campo y no sólo en reflexiones teóricas. Hay necesidad de generar y profundizar vínculos de confianza e intercambios entre investigadores, como también mayor acceso a las realidades específicas y requerimientos concretos del tema que cada sector propone para fortalecerse mediante la investigación. Las investigaciones sobre Ciberdefensa y educación deben también poder dar cuenta sobre vínculos de cooperación entre distintos países, instituciones, cátedras, equipos de investigación, profesionales y estudiantes de manera tal que sean posibles identificar redes y estructuras académicas; cómo se retroalimentan y fortalecen desde el intercambio de conocimiento, experiencias y prácticas documentadas.

Ciber defensa, mito y realidad

¿Es la ciber defensa un nuevo campo científico, tecnológico o técnico, o 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 humana sociedad? El siglo XX en principio y el siglo XXI, en particular, se han caracterizado por el surgimiento y declive cada vez más espectacular y estruendoso de diversos vocablos, pocas veces novedosos, algunas veces repetitivos y con frecuencia simples intentos de sustituir viejos conceptos, procedimientos o actitudes por medio de un lenguaje pseudo innovador, cuyo principal efecto recae en los medios de comunicación masiva y en la jerga cultural de moda. En tal sentido, palabras como ciberespacio, cibercultura, millenials, centenials, buteo, cliquear, wasapear, guglear y muchas otras, se han incorporado a la vida cotidiana y forman parte de las conversaciones diarias con familiares, amigos y conocidos, con la intención de mantenerse en todo momento "en onda", con el argot de moda en cada una de las disciplinas profesionales que se enfrentan a diario. ¿Ocurre lo mismo con la ciber defensa?.

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. La ciberdefensa escapa al marco nacional y sólo puede ser entendida en un entorno globalizado e integrado en redes. De acuerdo con los argumentos con perspectiva sociológica desarrollados en la investigación sobre Ciberdefensa como campo intelectual, se puede afirmar que 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.

El Software Libre: Alternativa para la educación en ciberdefensa sostenible

En esta línea de investigación se abordó el impacto que produce el Software Libre, en la formación específica en Ciberdefensa, a partir del análisis de las características singulares y herramientas que este tipo de software, pone en manos de las organizaciones de formación, educación y entrenamiento, que sorpresivamente pasan desapercibidas por gran parte de los decisores en su adopción y aplicación en operaciones de Ciberdefensa, como asimismo su poca inclusión en las currículas de las materias de formación en la temática.

Para entender la problemática comenzaremos por definir como software libre (SL) a los programas cuyas licencias públicas generales (GPL) dan a los usuarios las libertades de ejecutar el programa con cualquier propósito, (Aún con finalidad de Defensa Nacional) estudiar y modificar el programa y redistribuir copias del programa original o modificado, sin tener que por ello pagar regalías, licencias o patentes, por supuesto todo los antes dicho presupone la disponibilidad del código fuente o "la receta con la que fue confeccionado".

La sencillez con que se define, no hace honor a la problemática que desata y los complicados cuestionamientos a los que se somete el empleo del Software Libre, ¿Qué hay detrás? ¿De qué viven los del SL? ¿Es más inseguro? Sin embargo, estudios cuantitativos han demostrado que, en numerosos casos, el uso de SL es una alternativa no sólo razonable sino incluso superior en comparación con su competencia, el software privativo (Software por el cual hay que pagar licencias para usar en las condiciones que exige la Empresa desarrolladora), basta mencionar la supremacía del uso de SL a nivel servidores en todo el mundo.

Lo que simplemente esgrime el SL es la Libertad, si bien existe un ahorro significativo en licencias, no es lo más importante, la adopción del SL puede ser muy costosa, si no se hace inteligentemente, pero los resultados van más allá de lo económico, pese que este factor económico, es casi el único que los decisores visualizan en un primer momento, si lo miramos con una lupa y con mayor detalle, desde lo político permite desarrollar independencia y soberanía tecnológica, desde lo social favorece el trabajo colaborativo (que tanto se pregona en ciberdefensa pero que no se sabe cómo lograr) entre los países o agencias de Ciberdefensa, el SL para ello abre una puerta, a partir del concepto compartir el esfuerzo de mejorar software ya desarrollado y obtener beneficios para todos, con el condimento de hacerle sin violar aspectos legales. Pero lo que nos lleva hoy a centrar la atención en este trabajo, es el aporte invalorable en la formación, a partir de la transferencia del conocimiento que permite el SL con su sencilla definición.

El software como medio de almacenamiento del conocimiento. 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.

Si el software se comporta como una caja negra, entonces cuánto conocimiento nos puede proporcionar, si no podemos acceder a cómo está confeccionado, cómo podemos asegurar que hace lo que dicen

que hace efectivamente, 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.

El software Libre en la Ciberdefensa y en el Estado. En la actualidad y a través de la propia creación humana ha emergido una nueva dimensión donde pueden materializarse las amenazas: el ciberespacio. En el ámbito de la defensa estaban bien definidas las dimensiones de tierra, mar, aire, e incluso el espacio, ahora contamos con una quinta dimensión, de inusual intangibilidad comparada con las anteriores.(Bejarano, s. f., p. 51)

Algunos autores que analizan la evolución de la tecnología Militar definen como campo de batalla al espacio geográfico donde se desenlazan los enfrentamientos, en consecuencia su elección y dominio es una condición fundamental para salir triunfante, este enunciado, como los mismos principios de la conducción pese a su antigüedad mantiene plena vigencia, pero la innovación tecnológica ha introducido este quinto escenario virtualmente novedoso y en donde los milenarios principios de la guerra tienen un enfoque un tanto peculiar.

De acuerdo con el "Diccionario Enciclopédico de la Guerra" (1958) el campo de batalla se define como: "[…] el terreno en que combaten dos ejércitos, o tiene lugar una batalla"; sin entrar en detalles de lo que la doctrina militar en Argentina diferencia entre el combate y la batalla, relacionado con el nivel de la conducción y magnitud de quienes se enfrentan,(EJERCITO ARGENTINO, 1992, p. 5,8,9,11) podemos resumir que el combate tiene un carácter táctico y la batalla muestra un alcance estratégico, pero en sus definiciones no tienen en cuenta al dominio virtual, lugar donde hoy es posible que se desarrollen acciones o enfrentamientos más allá de la tierra, mar, aire y espacio según los propósito perseguidos. Se trata de un ambiente diferente de los anteriores, creado por el hombre, de inusual intangibilidad, que propone un cambio de paradigma radical en la definición de conceptos en materia de conducción militar. (Arreola García, 2017)

En consecuencia, para la conducción militar aparece el cibercampo de batalla que puede interpretarse como el espacio virtual en que se llevan a cabo uno o varios combates entre oponentes, pero ahí no termina la cuestión, es mucho más complejo y esto se refleja en lo que enuncia la Estrategia de Ciberseguridad de nuestro país "La realidad nos muestra que en el Ciberespacio existen, entre otras, dificultades originadas en aspectos relacionados con la atribución de responsabilidad, las vulnerabilidades de las infraestructuras críticas, las grandes asimetrías que se manifiestan entre los países a partir de la globalización y las cuestiones vinculadas con el ejercicio de la soberanía. Este último concepto en particular, entendido como el ejercicio supremo del poder del Estado, está necesariamente vinculado a lo territorial. Sin embargo, Internet representa un dominio global e intangible y un flujo infinito de datos sobre el cual no se ejerce dominio ni soberanía, poniendo a prueba el concepto antes mencionado e instaurando un nuevo paradigma que es necesario entender"

El software ejerce una influencia preponderante en todos estos procesos beligerantes del quinto dominio, no sólo constituye la materia prima de las armas cibernéticas sino que puede afectar entre otras actividades procesos electorales. Ha quedado demostrado en ejemplos recientes que la Ciberseguridad juega un papel clave en las elecciones, ya que afecta a muchos elementos de la cadena del sufragio: los votantes, los dispositivos electrónicos intervinientes, los registros en los padrones electorales, la seguridad y coordinación del acto electoral, los recuentos, las transmisiones de los datos a las juntas electorales, la publicación de los resultados y las diferentes amenazas desde el phishing, la denegación de servicios, en la publicación de resultados— o incluso las fake news para influir en el votante antes de las elecciones.(País, 2018)

En virtud de la importancia del Software en la Ciberdefensa y en la Ciberseguridad vamos a centrar la atención en el denominado FLOSS (Free Libre Open Sources Software), del cual podemos afirmar que es cada vez más habitual en casi cualquier entorno informático pero sin embargo, es también un gran desconocido, sobre todo a la hora de comprender las condiciones que ya enunciamos vinculadas a las libertades, que se trata de un modelo de negocio distinto y que tiene otros tipos de licencias que fundamentan su existencia.(González-Barahona, 2011, p. 2)

Una cuestión vital sobre la que se concentra el movimiento del Software Libre es su utilización en el Estado. “Las razones para defender el uso de tecnologías libres incluyen: la seguridad, la no dependencia respecto de proveedores de servicios, el respeto por el uso de estándares, el incentivo hacia los desarrollos locales, sus menores costos de implementación y su correspondencia con la transparencia en el acceso y la gestión de la información pública” (Zanotti, s. f.-b, p. 81)

Los orígenes del SL, se remonta a los años setenta y al manifiesto de la ética hacker, cuyo término tiene nacimiento hace más de medio siglo, en las bromas estudiantiles del MIT, a través de trozos de códigos de programación, que llamaban hacks, y dieron lugar al término hacker (Levy, 1984, 23). Con el paso del tiempo, los hackers (Levy, 2010, pp. 17-19-31) del MIT fundaron el Laboratorio de Inteligencia Artificial (Ai Lab), donde floreció la utopía del software libre y esta solidaria filosofía con la poderosa capacidad de transformar el mundo.

Richard Stallman, fundador de este movimiento, fue quien por primera vez 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 la libertad del usuario como por ejemplo Microsoft y Apple en otros. Esta perspectiva técnica, sociológica y política de un filósofo cuyo origen es el mundo de la informática, constituye la base del manifiesto Hackers y los ideales que enarbolan todas las demandas ciudadanas, de la prensa y las distintas organizaciones humanas que defienden la privacidad del usuario, la libertad, la democracia, el conocimiento compartido, el trabajo en equipo, la transparencia y la tecnología basada en un uso eficiente de los recursos.(Zanotti, s. f.-a)

Apreciamos entonces que es un tanto injusto y muy agresivo considerar a los Hackers piratas” del ciberespacio, situación aún más extrema cuando esa calificación proviene de organizaciones gubernamentales, universidades, o documentos oficiales, como es el caso del diccionario de la Real Academia Española (RAE), que en su vigesimotercera edición de 2014 identifica al hacker como “pirata informático”. Con el correr del tiempo esto parcialmente ha ido cambiando al extremo tal, que la misma España, hace una convocatoria a Hackers patriotas para que se sumen a proteger a su país. («Los “hackers” españoles que vencen a todos en Europa (sin dinero ni ordenadores)», 2017)

El desarrollo de software como lo plantea el FLOSS, se trata de colaboración e involucra para cada proyecto a una comunidad de desarrolladores de distintos países inclusive, este modelo en muchos casos descreído (Raymond, s. f., p. 2) en cuanto a su efectividad, ha logrado sobresalientes resultados. En contrapartida, otra forma del desarrollo es el del modelo privativo, cuyo modelo de negocio se sostiene en la venta de permisos de uso, llamados licencias de software.

En materia de ciberdefensa se enuncia en forma permanente, que para enfrentar las ciberamenazas es menester hacerlo en forma colaborativa, tanto en un Estado como en el concierto Regional (Instituto Español de Estudios Estratégicos, 2017, p. 101,197,213), y es el modelo del FLOSS, que muestra una posibilidad cierta de este tan mentado trabajo colaborativo. Según dichos de Antonio Missiroli, secretario general adjunto para los desafíos de seguridad emergentes de la OTAN y expresiones del Brent Scowcroft Center on International Security, afirman que la OTAN ha creado un pequeño equipo de respuesta cibernética para ayudar a las naciones que lo soliciten.(Group, 2019) El Programa Multinacional de Capacidad de Defensa Cibernética de la OTAN ha desarrollado paquetes de trabajo para las naciones patrocinadoras de Canadá, los Países Bajos y Rumania que permiten compartir información dentro de una comunidad confiable y está trabajando en otras capacidades. El Centro de Excelencia Cooperativo de Ciberdefensa de la OTAN (MICHAEL N. SCHMITT, s. f., p. 8), con sede en Estonia, tiene una “misión para mejorar la capacidad, cooperación e intercambio de información entre la OTAN, sus países miembros y socios en defensa cibernética en virtud de la educación, la investigación y el desarrollo, las lecciones aprendidas y la consulta”.

La incorporación y empleo de software de código abierto está creciendo a nivel mundial, también en ámbitos de la Defensa. En la industria y la comunidad tecnológica en general, muchos consideran el código abierto como un movimiento social centrado en el libre intercambio de ideas tecnológicas; Cuando de Defensa, se trata naturalmente debe primar el pragmatismo, no sólo en los aspectos económicos sino relacionado con la Tecnología de la Información, y en ese sentido el SL es a menudo la mejor solución para los desafíos tecnológicos militares que requieren no depender de un proveedor y menos cuando este puede responder a intereses de otros Estados.

Los proyectos de código abierto en el sector privado naturalmente atraen a los técnicos involucrados y la participación comunitaria organizada, era de esperar que lo mismo ocurriera en ámbitos de Defensa, en nuestro país fue lanzado en 2004 como FLOSS la distribución Linuxmil primera en su tipo orientada al empleo militar, cuyo desarrollo tuvo el invalorable aporte de la comunidad del Software Libre representada por la asociación civil SOLAR (Software Libre de la Argentina) y el apoyo internacional a través de la Free Software Foundation liderada en aquel entonces por Richard Stallman, por otra parte el Departamento de Defensa de EEUU impulsó en 2017 la iniciativa Code.mil, experimento de código abierto, con la finalidad de fomentar la colaboración con la comunidad de desarrolladores de todo el mundo en proyectos de Software abierto para la Defensa, por otro lado el Military Open Source (Mil-OSS), organiza una convención anual llamada Grupo de trabajo donde los miembros de las Fuerzas Armadas se reúnen para aprender, compartir y discutir proyectos, los próximos cambios en las políticas y cómo entender y apoyar a los militares en satisfacer las necesidades de adopción de este tipo de Software.

En relación a un Programa de formación que impulse la transformación, las organizaciones de ciberdefensa deberían crear programas de formación internos a su dotación, y qué mejor oportunidad que la que brinda el SL,que permite que el personal adquiera las competencias que necesita a través de la práctica y transferencia del conocimiento que se produce, cuando se es capaz de comprender cómo fueron creadas las herramientas de software que debe aplicar, esto facilita adaptarse a los cambios y desempeñar sus cibertareas eficientemente.

Esta propuesta innovadora de reentrenar al personal que ya forma parte de nuestras organizaciones (utilizando el SL como motor para lograrlo) podríamos asociarla a los conceptos de upskilling, reskilling y reverse mentoring que se encuentran de moda tras la "Transformación Digital" de las organizaciones.

- Reskilling: se trata de una reconversión laboral, es necesario e inevitable que un cibercombatiente adquiera competencias tecnológicas para desempeñarse en el área de forma exitosa.

- Upskilling: es una adquisición de una capacidad adicional, se trata de aportar otras aptitudes que le permitan su desempeño con más efectividad.

- Reverse mentoring: es una tendencia organizacional en expansión, en la que los subalternos o más jóvenes enseñan a sus superiores o más antiguos en temas relacionados con la ciberdefensa, tecnología y las redes.

Para lograr este propósito de impulsar la transformación, el SL también ofrece una gama importante de Sistemas de Gestión de Aprendizaje (Learning Management System en inglés) que permite a los integrantes de las organizaciones de ciberdefensa acceder, de manera virtual, a cualquier tipo de formación a distancia. Durante la pandemia este tipo de recursos se ha destacado, y el SL los deja accesible para cualquier organización que disponga de un servidor y conectividad, estos sistemas le permitirán intercambiar archivos, capacitar y evaluar los resultados pedagógicos.

Luego de este recorrido histórico y variado, sobre el advenimiento del quinto dominio, los esfuerzos que deben efectuar las Fuerzas Armadas para comprenderlo apropiarse y adaptarse a lo que propone el SL, podemos concluir que su dominio y adopción es una oportunidad para iniciar un camino de liderazgo en ciberdefensa, con la posibilidad de hacerlo como trabajo en equipo, compartiendo esfuerzos y datos.

Debemos evaluar al SL teniendo en cuenta que "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 si bien son empleadas en Ciberdefensa, su uso se justifica y se asocia casi exclusivamente a la relación de costos, sin embargo aspectos mucho más importantes como: la soberanía e independencia tecnológica, la transferencia del conocimiento, la velocidad de actualización ante contingencias y el control real y efectivo sobre los programas informáticos empleados en la Ciberdefensa, constituyen valores que sustentan y justifican la adopción del SL, para mantener en un ciberconflicto principios básicos de la guerra como la iniciativa, la sorpresa, la libertad de acción y la unidad de comando como asimismo iniciar un camino de liderazgo en esta especialización.

Certificaciones, el jutsu de la ciberseguridad

Con el fin de conocer las opciones de formación profesional en materia de ciberseguridad en el mercado internacional, se ha realizado un relevamiento de las organizaciones existentes y la cantidad de certificaciones específicas del campo del conocimiento, para luego efectuar su clasificación bajo los tipos de inteligencia, ya sea estratégica, operativa o táctica. En la presente investigación, se consideró como inteligencia estratégica al tipo de conocimiento que planifica los objetivos y tiene en cuenta factores globales y/o nacionales para llevar a cabo las acciones; la inteligencia operacional es sobre el conjunto que acciones que realizan individuos, es decir, el aspecto grupal de una campaña; y la inteligencia táctica es la que corresponde a la acción individual de un actor, es decir, donde este tiene un efecto próximo.

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 que al momento de tomar la decisión de obtener tal codiciada presea, un buen indicador es dimensionar el universo de oportunidades.

Las personas dedicadas a la ciberseguridad obtienen un cierto nivel de especialización en este campo de la computación, lo que conlleva a 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 como parte del material de estudios y el examen para acceder a tal presea. 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, metodología del examen, requisitos para obtener la certificación y mantener la membresía con la entidad organizadora, y si hay una demanda real de personal dedicado a la ciberseguridad, en especial si las certificaciones son percibidas como el puntapié de la carrera, para avanzar o incluso para mantenerla.

Se encontró una gran cantidad de organizaciones que proveen certificaciones (43), ascendiendo a un total de 442 opciones, con una de estas organizaciones acumulando 64 certificaciones. Dichas certificaciones se clasifican de distintas formas como ser 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. Se propuso una nueva forma de clasificar las certificaciones, por el tipo de inteligencia: estratégica, operativa y táctica.

La investigación se centró principalmente en el desarrollo de 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.

Queda por investigar el costo de cada certificación, la cantidad de créditos (CPE) necesarios para mantener los criterios de capacitación continua, los dominios de cada certificación y cuáles son comunes entre las distintas opciones y qué porcentaje se debe obtener de cada dominio o en general para aprobar el examen.

Posibles cursos para investigaciones futuras pueden ser comparar las principales certificaciones desde los temas que cubren, con la oferta académica de posgrado a nivel nacional, determinar si es valor agregado o una meta estipulada que personal dedicado a la ciberdefensa (sea del Comando Conjunto de Ciberdefensa o de la Subsecretaría de Ciberdefensa) obtenga dichas certificaciones, o relevar, donde sea posible, el nivel de inserción de dicho mercado de certificaciones en nuestro país.

Aporte de los algoritmos evolutivos a la predicción del blanqueo de activos en el ciberespacio: Desarrollo de un sencillo caso de aplicación

El tema remite a una investigación aplicada, metodológica, mixta y experimental. A tal fin se trabaja en el desarrollo de un modelo de aprendizaje automático sustentado en algoritmos estadísticos, predictivos y econométricos enmarcados en el campo de la ciencia de datos aplicada, a datos económicos, financieros, fiscales y/o transaccionales, sobre perfiles que permitan detectar patrones para la predicción del blanqueo de activos en el ciberespacio.

El objetivo general es demostrar el aporte de los algoritmos evolutivos a la predicción de este delito en el ciberespacio, y la funcionalidad que el modelo basado en los mismos puede ofrecer a la inteligencia proactiva. El estudio, descriptivo y correlacional basado en estadística inferencial, busca establecer la relación entre la variable dependiente (en este caso la probabilidad de blanqueo de activos en el ciberespacio), y las variables explicativas, que serán seleccionadas a partir de información obtenida explorando fuentes abiertas OSINT (Open Source Intelligence), para la detección de patrones, usando métodos de muestreo no probabilísticos, debido a la sensibilidad del tema y la dificultad de acceso a datos de la población bajo estudio. La relevancia del tema se fundamenta, no solo en la complejidad que plantea el delito de lavado de activos en sí, sino en el crecimiento exponencial de la misma en un escenario tan vasto y complejo como es el ciberespacio.

Es importante señalar que el blanqueo de activos involucra plenamente a la macroeconomía global en virtud de los desequilibrios que genera, derivados de las distorsiones en sus variables fundamentales o indicadores básicos. Lo dicho quedó plasmado en las conclusiones a las que se llegó en una de las sesiones especiales de Naciones Unidas celebrada a mediados de 1998 sobre el tratamiento del blanqueo de activos: “La infiltración, y a veces la saturación de dinero sucio en sectores financieros legítimos y cuentas nacionales, puede amenazar la estabilidad económica y política. El lavado de dinero afecta el comportamiento financiero y el desempeño macroeconómico de varias maneras, incluidos errores de política debido a errores de medición en las estadísticas de cuentas nacionales; volatilidad en los tipos de cambio y de interés, debido a transferencias transfronterizas de fondos no anticipadas; la amenaza de inestabilidad monetaria debido a estructuras de activos poco sólidas; efectos sobre la recaudación de impuestos y la asignación del gasto público debido a informes erróneos de ingresos; mala asignación de recursos debido a distorsiones en los precios de activos y productos básicos; y efectos de contaminación en transacciones legales debido a la posibilidad percibida de estar asociado con el crimen” . Son empresas subterráneas que trabajan con cantidades de dinero a veces inimaginable. “Sea cual fuere la agencia

internacional que se consulte, los delincuentes lavan cada año entre $ 500 mil millones y $ 1 billón en todo el mundo. El efecto global es asombroso en términos sociales, económicos y de seguridad".

El desarrollo vertiginoso de la tecnología en las últimas décadas, en particular de la Inteligencia Artificial, constituye una herramienta de extraordinaria utilidad tanto para los Estados y Fuerzas de Seguridad como para el Crimen Organizado, lo cual explica la pertinencia del tema elegido dentro del área de conocimiento de la Ciberdefensa. Por lo expuesto, resulta imperioso contar con instrumentos que, armonizando diferentes ciencias y técnicas, logren la capacidad de prevención de este delito a partir del entrenamiento en la detección de perfiles y patrones de comportamiento para anticiparse a su comisión. En lo inmediato, los algoritmos evolutivos basados en el funcionamiento de Redes Neuronales y Modelos Estadístico-Predictivos, como el que se plantea, parecen estarse posicionando entre los métodos más eficientes posibles encontrados hasta el momento.

El creciente desarrollo tecnológico de la última década ha favorecido el incremento exponencial y perfeccionamiento del blanqueo de activos hasta alcanzar niveles difíciles de determinar con precisión. En consecuencia, el efecto corrosivo generador de distorsiones económico-financieras a escala global derivadas del mencionado ilícito resulta complejo de cuantificar.

A los delitos precedentes se suman aquellos amparados en las nuevas tecnologías. Así por ejemplo, prácticas tradicionales como el micromecenazgo o aporte colectivo de donaciones online permite financiar diferentes proyectos de empresas emergentes en el ciberespacio fuertemente vinculadas con la tecnología, caracterizadas por ideas innovadoras para la producción de bienes y servicios a través de plataformas, al mismo tiempo que permiten a sus inversores quedar exceptuados de justificar legalmente el origen de sus fondos.

Tecnologías como la cadena de bloques e Inteligencia Artificial han favorecido la transferencia de importantes volúmenes de dinero en escasos minutos, y nada parecería obstar la triangulación con paraísos financieros y/o territorios de baja o nula tributación.

Reportes internacionales elaborados por organismos e instituciones de lucha contra el narcotráfico, pedofilia, prostitución, tráfico de armas, entre otros, dan cuenta del uso de criptomonedas en las mencionadas transacciones, lo mismo que ocurre con plataformas sociales de juego clandestinas que mueven sumas millonarias.

Paradójicamente, si bien los efectos del blanqueo de activos resultan adversos para el sistema económico-financiero global, y en esta investigación se hace hincapié en ello, también pueden generar algunos shocks reactivadores temporales de liquidez en ciertos mercados, los cuales verán incrementadas las inversiones y su capacidad de pago. Es por ello que estos patrones también requieren ser observados, dado que podrían ser indicadores de su práctica.

Si bien existen varios y variados modelos predictivos que permiten inferir patrones y perfiles en lo atinente a fraudes financieros y de seguros, evasión fiscal y riesgo crediticio, basados en algoritmos neuronales de aprendizaje automático a partir de técnicas de muestreo probabilísticas sobre casos concretos extraídos de repositorios miltiestructirales, no se han desarrollado hasta el momento algoritmos predictivos de inferencia sobre datos multiestructurales diseminados de manera desorganizada en el ciberespacio, usando técnicas no probabilísticas.

La ampliación de este tipo de investigación, es decir, el desarrollo de modelos cada vez más eficiente para la detección de patrones y perfiles que permitan inferir la comisión de delitos económico-financieros, dependerá de la solidez en el conocimiento sobre ciencia de datos con la que cuenten quienes decidan abordarla, tanto desde el punto de vista informático como técnico en disciplinas inherentes a las ciencias económicas.

Aportes a la ciberseguridad y la gestión de las Infraestructuras Críticas de la Información en Argentina (2011-2019)

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

Frente a ello, se hace énfasis en el análisis y revisión del plexo normativo relacionado con las funciones del Ministerio de Seguridad, Ministerio de Defensa, Secretaría de Modernización y la Agencia Federal de Inteligencia en lo que respecta a infraestructuras críticas de la información nacionales. Como resultado, surgirá como necesidad 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.

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 requiere un plan de prevención y protección a favor de conservar los servicios esenciales de la comunidad ya que, de lo contrario, la interrupción de los mismos ocasionaría consecuencias perjudiciales para la sociedad.

Considerando que las infraestructuras críticas han incorporado una gran cantidad de componentes informáticos, los ciber atacantes aprovechan 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. Estos atacantes emplean técnicas que se renuevan constantemente indicando que la prevención ya no es la única acción efectiva a realizar. Sin perjuicio de ello, y lejos de reemplazar las formas tradicionales de ataque, la ciberguerra, el ciberterrorismo, el ciberespionaje y el ciberdelito, en general conviven con estas y, frente a ello, los gobiernos han comenzado a trabajar en la ciberseguridad y ciberdefensa de sus países. Efectivamente, la estabilidad del país y la confianza del ciudadano en el Estado se verían comprometidas si ocurriera un ataque masivo y coordinado a alguno o varios de los sectores definidos como infraestructura crítica y, es por ello, que el Estado debe centrarse en medidas de prevención, protección y resiliencia de las mismas.

Ciertamente, "(…)la amplitud del concepto de infraestructura crítica y la multiplicidad de sectores afectados requiere afrontar la protección de dicha infraestructura de forma integral y multidisciplinaria" (Sanchez, 2012). Inclusive, desde el año 2004 la Organización de los Estados Americanos (OEA) enfatiza la importancia de desarrollar una estrategia comprensiva para proteger las infraestructuras críticas que adopte un enfoque integral, multidisciplinario e internacional (Organization of American States, Microsoft, 2018).

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

La investigación se centró principalmente en el desarrollo de tres temas: la investigación, desarrollo e innovación en ciberseguridad, 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 (ver tema 4 del presente artículo).

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 intrasectorial contemplando la dependencia e interdependencia de las distintas infraestructuras.

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

Posibilidad de empleo de X-ROAD para la interoperabilidad Nacional

La interoperabilidad es sumamente 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 con valor, incrementar la confiabilidad entre los sistemas y principalmente es la base que permite a los gobiernos beneficiarse del uso intensivo de las TIC.

Actualmente los sistemas de información implementados en el gobierno nacional trabajan de dos formas: por un lado, se tiene un sistema centralizado que contiene funcionalidades utilizadas por diferentes organizaciones llamado “Sistema de Gestión Documental Electrónica (GDE)” y por el otro se tienen sistemas propios de los organismos, con funcionalidades en general no contenidas en el GDE.

Es evidente que el GDE intenta elevar el nivel de calidad de los servicios prestados, pero dada su implantación, el mismo dispone de altos riesgos de baja de servicio que aún a la fecha siguen afectando a gran parte de los organismos, los cuales en su mayoría fueron encaminados a utilizarlo por medio de un decreto presidencial.

Para la integración de aplicaciones la normativa argentina permite utilizar un módulo del GDE o realizarla punto a punto teniendo en cuenta aspectos técnicos indicados como 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 de la interoperabilidad 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, 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.

La interoperabilidad o coordinación masiva de sistemas es necesaria como base núcleo de soporte para los diferentes mecanismos que permitan establecer un sistema integral de ciberdefensa-ciberseguridad, debido a que una de las principales necesidades de cualquier sistema integral es la comunicación de datos en tiempo real de forma segura. El flujo de información en tiempo real para la toma de decisiones puede ser considerado una infraestructura crítica lógica.

Durante la investigación se pudo detectar un patrón general que afectó a los diferentes países en los cuales la interoperabilidad fue considerada un tema estratégico. Este patrón puede ser descripto como etapas de evolución:

Etapa inicial: en donde no existe una gestión integral de la interoperabilidad, con fuerte presencia de islas de información, procesos disjuntos, normativa inicial. Se detecta la "OPCIONALIDAD" normativa como principal barrera que retrasa en gran medida la implementación de la interoperabilidad.

Etapa media: fuerte implementación de políticas de interoperabilidad, la información se relaciona y se establecen mecanismos fuertes de nivelación tecnológica a gran escala en conjunto con re implementación de procesos transversales y monitoreo de la evolución de las diferentes implementación y situación nacional y transnacional. Se detecta la "OBLIGATORIEDAD" e "INSTITUCIONALIZACIÓN" de la interoperabilidad como principal medida que doblega las barreras iniciales.

Etapa alta: Consolidación y mejora continua de la implementación. Inicio de un procesamiento masivo utilizando herramientas de big data e IA para obtención de conocimiento que permita agregar valor al esquema global.

También se pudo detectar la falencia técnica que aún restan por actualizar en la infraestructura de firma digital argentina, más específicamente en las relacionadas al componente de sello de tiempo y validación formal de los documentos firmados. Siendo estos últimos de gran importancia para el desarrollo y uso de una plataforma de interoperabilidad.

Con respecto a x-road, se pudo evidenciar la posibilidad de uso de dicha plataforma de interoperabilidad en el estado nacional. X-road se está expandiendo en gran medida, en varios continentes, aunque como con todo software de código abierto utilizado en sistemas importantes es recomendable disponer de equipos de revisión locales que permitan evaluar a un nivel técnico detallado su posible integración local.

Se recomienda seguir con una investigación más social sobre los factores que podrían afectar una implementación masiva de la interoperabilidad, como por ejemplo el aspecto político, en el cual durante cada mandato presidencial en general muchos cargos medios y altos son modificados sin posibilidad real de implementaciones a largo plazo. La instrumentación de mesas de coordinación multiperspectiva independientemente de la consideración de origen del poder, pero si enfocada en la visión a futuro del tema podrían otorgan la supervivencia de un proyecto a largo plazo. De igual manera, se recomienda analizar las posibles herramientas que permitan medir la madurez de la interoperabilidad en las diferentes regiones, si se puede medir quizás se pueda controlar y, si se puede controlar quizás se pueda mejorar. Un observatorio enfocado al tema de la interoperabilidad permitiría transparentar el estado actual.

La complejidad del tema delata la necesidad de una capacitación profesional, es ahí 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 en los niveles medios de mando que lo requieren, con el tiempo va generando una migración de los profesionales TIC al sector privado. Es necesaria una consulta general a los empleados TIC estatales, analizando su capacitación, si dispone de otros trabajos, etc. para detectar tendencias. Un análisis profundo de la "jerarquización" profesional granular debido al dinamismo propio de la evolución tecnológica permitiría una disminución de los tiempos de formación y especialización disminuyendo la brecha entre el formalismo de grado y las necesidades laborales reales.

Reflexiones finales

En los últimos años, la Defensa Nacional argentina viene reconociendo 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 entre otros aspectos surgieron diferentes ofertas de formación. Dentro de este marco, la formación en ciberdefensa y ciberseguridad aparece como un interrogante de interés tanto para actores y ámbitos políticos como académicos. Su abordaje lleva a preguntarnos sobre las necesidades y estrategias de formación que tanto el sector estatal como estratégico 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.

La formación en ciberdefensa y ciberseguridad constituye un nuevo campo del saber, incipiente, pero con un crecimiento vertiginoso, con interés estratégico para el sector público y privado. Al mismo tiempo presentan múltiples dimensiones, en proceso de normalización, construcción y definición. Pensar la investigación en este nuevo campo intelectual, de forma que aporte a su formación y consolidación de forma teórica y metodológica, será una necesidad no sólo de los ámbitos académicos sino también de aquellos que toman decisiones políticas.

Es en este sentido que el presente artículo brinda elementos orientadores para estudiantes, profesores, investigadores, planificadores de políticas públicas y decisores políticos del sector militar, civil y empresarial de modo de contribuir a la discusión teórica y metodológica que permitan una estructuración de futuras investigaciones. Cada uno de los temas trabajados presentan aportes a la investigación mediante la justificación del mismo en el marco de la ciberdefensa y ciberseguridad; resumiendo los principales hallazgos que su investigación fue develando; mencionando aquellos aspectos del mismo que conforman vacancias de investigación y brindando sugerencias para su continuidad.

La conformación de nuevos equipos de investigación inter y multidisciplinarios, donde se integren estudiantes, profesores, investigadores, como también personal con experiencia operativa y de gestión en las temáticas abordadas, documentando el proceso y resultados de tales investigaciones, aportará a las cátedras, carreras y planes de formación en el área, al igual que al proceso de toma de decisiones en todos los niveles y ámbitos involucrados con la ciberdefensa-seguridad. Para esto es necesario promover mayor intercambio y participación de tales equipos y sus miembros en actividades conjuntas interuniversidades, interagencial, e intersectorial que estimulen el debate, el intercambio, la confianza mutua y los vínculos académicos-políticos-productivos.

En el aspecto académico, la investigación en ciberdefensa y ciberseguridad, en Argentina, se encuentra dando sus primeros pasos. Tiene un largo camino por delante con una prolífica diversidad de temas y enfoques que aún esperan ser abordados y comunicados. No alcanza con el conocimiento personal o institucional, brindado en una cátedra o que circula en los mandos de conducción o es patrimonio de un agente en particular en su puesto laboral. 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

Arquilla, J. and Ronfeldt, D., "Cyberwar is Coming!" Comparative Strategy, Vol. 12, No. 2, Spring 1993, pp. 141–165. Copyright 1993 Taylor & Francis, Inc.

Arreola García, A. (2017). Ciberespacio, el campo de batalla de la era tecnológica. *Estudios en Seguridad y Defensa*, *11*(22), 109-138. https://doi.org/10.25062/1900-8325.212

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.

Bertranou, J. (2015). Planificación pública. Las exigencias de una adecuada problematización. En VV.AA., Aportes teóricos a la formación de líderes políticos y comunitarios (pp. 103-164). Neuquén: Casa de las Leyes.

Blasco, J. (7-02-2015). El más fuerte es el más vulnerable. Diario El País, España. Recuperado de http://internacional.elpais.com/internacional/2015/02/07/actualidad/1423330690_981628.html

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

Camilli, G. A. (2019). ¿Por qué leer a Clausewitz en el siglo XXI? Recuperado de http://190.12.101.91:80/jspui/handle/123456789/1243

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.

Contribuciones del software libre a la soberanía tecnológica y los desafíos futuros | Voces en el Fenix. (s. f.). Recuperado 4 de noviembre de 2019, de Voces en el Fénix website: http://vocesenelfenix.com/content/contribuciones-del-software-libre-la-soberan%C3%ADa-tecnol%C3%B3gica-y-los-desaf%C3%ADos-futuros

De 2010, 7 De Septiembre. (s. f.). El software libre es una «política de Estado». Recuperado 4 de noviembre de 2019, de Infobae website: https://www.infobae.com/2010/09/07/535445-el-software-libre-es-una-politica-estado/

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

Eissa, S.G; Gastaldi, S.; Poczynok, I. y Di Tullio, M. E. (2012). El ciberespacio y sus implicancias en la defensa nacional. Aproximaciones al caso argentino. Recuperado de http://sedici.unlp.edu.ar/bitstream/handle/10915/40210/Documento_completo.pdf?sequence=1

EJERCITO ARGENTINO. (1992). Reglamento de la Conducción para el Instrumento Militar Terrestre (1992.a ed.). Buenos Aires: IGM.

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

EMCO. (s. f.). Comando Operacional—Comando General Electoral. Recuperado 1 de noviembre de 2019, de https://cge2019.sytes.net/

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

Feliú Ortega, L. (2012). El espacio cibernético nuevo escenario de confrontación. Cuadernos del CESEDEN, febrero de 2012, pp. 42-43. Recuperado de http://www.defensa.gob.es/ceseden/Galerias/destacados/publicaciones/monografias/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.

Gnu.org. (s. f.). Recuperado 5 de noviembre de 2019, de https://www.gnu.org/distros/free-distros.en.html

Gobierno y Software Libre, una relación necesaria. (2011, septiembre 7). Recuperado 28 de octubre de 2019, de Artepolítica website: http://artepolitica.com/comunidad/gobierno-y-software-libre-una-relacion-necesaria/

González-Barahona, J. M. (2011). El concepto de software libre. Tradumàtica: tecnologies de la traducció, 0(9), 5-11. https://doi.org/10.5565/rev/tradumatica.10

Grant, T. J. (2014). On the Military Geography of Cyberspace. En Liles, S. (eds.), Proceedings, 9th International Conference on Cyber Warfare & Security (ICCWS 2014) (pp. 66-67). West Lafayette, USA: Purdue University, 24-25 March 2014.

Group, I. D. M. (2019, febrero 25). La OTAN quiere fomentar la colaboración en materia de ciberseguridad | Seguridad. Recuperado 4 de noviembre de 2019, de IT Trends website: https://www.ittrends.es/seguridad/2019/02/la-otan-quiere-fomentar-la-colaboracion-en-materia-de-ciberseguridad

Instituto Español de Estudios Estratégicos. (2017). Ciberseguridad: La cooperación público-privada. Madrid: Ministerio de Defensa, Secretaría General Técnica.

Levy, S. (2010). Hackers (1st ed). Sebastopol, CA: O'Reilly Media.

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

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

Los «hackers» españoles que vencen a todos en Europa (sin dinero ni ordenadores). (2017, noviembre 5). Recuperado 4 de noviembre de 2019, de El Confidencial website: https://www.elconfidencial.com/tecnologia/2017-11-03/hackers-campeonato-europa-ciberseguridad-espana_1471555/

MICHAEL N. SCHMITT. (s. f.). Manual de Tallin sobre el Derecho Internacional aplicable a la guerra cibernética.

Migrar a software libre es un asunto político – Radios Libres. (s. f.). Recuperado 4 de noviembre de 2019, de https://radioslibres.net/migrar-a-software-libre-es-un-asunto-politico/

Milla 10/09/2018 | 5:25, M. B. (2018, septiembre 7). El software libre se hace activista. Recuperado 3 de noviembre de 2019, de Elcano Blog website: https://blog.realinstitutoelcano.org/el-software-libre-se-hace-activista/

Nirenberg, O., Brawerman, J. y Ruiz, V. (2000). Evaluar para la transformación. Innovaciones en la evaluación de programas y proyectos sociales. Buenos Aires: Paidós.

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

Orciuoli, A. (2005). Citado por Stel, Enrique en “Guerra Cibernética”. Círculo Militar, 1ra Edición. Buenos Aires, 2005.

Organization of American States, Microsoft. (2018). Critical Infrastructure Protection in Latin America and the Caribbean 2018. Recuperado de https://www.oas.org/es/sms/cicte/cipreport.pdf

Ottis, R. y Lorents, P. (2012). “Cyberespace: Definition and Implications”. Coperative Cyber Defence Centre of Excelence, Tallinn, Estonia, 2012.

Raymond, E. (s. f.). La Catedral y el Bazar de Eric S. Raymond. Recuperado 28 de octubre de 2019, de https://biblioweb.sindominio.net/telematica/catedral.html

Sábato, J. A. (2011). El pensamiento Latinoamericano en la problemática Ciencia– Tecnología-Desarrollo-Dependencia. Argentina: Ediciones Biblioteca Nacional.

Sábato, J. A. y Botana, N. (1968). “La ciencia y la tecnología en el desarrollo futuro de América Latina”. El pensamiento latinoamericano en la problemática ciencia – tecnología – desarrollo – dependencia. Jorge A. Sábato. Argentina: Paidós, 1975.

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

Sheldon, J. (2011). Deciphering Cyberpower. Strategic Purpose in Peace and Ward.

Strategic Studies Quarterly. Summer Edition. Recuperado de http://www.airuniversity.af.mil/SSQ/

Sierra, D. (2015). Las dos caras de la tecnologíaO pinión Ciberelcano. Informe mensual de ciberseguridad. Abril 2015 / Nº2; p. 16.

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.

Strate, L. (2018). Eight Bits About Digital Communication. Razón y Palabra, 22 (1_100), pp. 589-618.

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

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

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

Why Open Source Software _ Free Software (OSS_FS, FOSS, or FLOSS)_ Look at the Numbers!.pdf. (s. f.).

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

Zanotti, A. (s. f.-a). Download citation of El software libre y su difusión en Argentina: Mercado, Estado, sociedad. Recuperado 4 de noviembre de 2019, de ResearchGate website: https://www.researchgate.net/publication/303866085_El_software_libre_y_su_difusion_en_Argentina_mercado_Estado_sociedad

Zanotti, A. (s. f.-b). El software libre y su difusión en la Argentina (2013.a ed., Vol. 1). Córdoba,Argentina: Editorial del Centro de Estudios Avanzados Centro de Estudios Avanzados, Facultad de Ciencias Sociales, Universidad Nacional de Córdoba,.

Ciberdefensa como campo intelectual: Aportes y propuestas de investigación en Ciberdefensa y Ciberseguridad para la realidad argentina.

Resumen

Este artículo presenta futuras líneas de investigación en relación a ciberdefensa y ciberseguridad a partir de miradas y abordajes heterogéneos vinculados a problemáticas de interés para el área. Pretende dar un marco académico y constituirse en antecedente a partir del cual luego encontrarán pertenencia las líneas de investigación propuestas. En el mismo se presenta el contexto argentino de lo "ciber" en cuanto a la normativa y lo conceptual; el lenguaje respecto a la definición conceptual de lo "ciber" a nivel global y la dificultad para su univocidad; la Ciberdefensa y el Triángulo Sabatino como relación y propuesta de análisis para una mirada desde lo tecnológico-productivo. Finalmente, el artículo da cuenta de los aspectos metodológicos más relevantes que orientan las once líneas de investigación presentadas.

Palabras Claves: CIBERDEFENSA – CIBERSEGURIDAD – INVESTIGACIÓN – CAMPO INTELECTUAL.

Ciberdefesa como campo intelectual: Contribuições e propostas de pesquisa em Ciberdefesa e Cibersegurança para a realidade argentina.

Resumo

Este artigo apresenta futuras linhas de pesquisa em relação à ciberdefesa e cibersegurança a partir de visões e abordagens heterogêneas vinculadas a problemas de interesse da área. Tem como objetivo fornecer uma estrutura acadêmica e se tornar um precedente no qual as linhas de pesquisa propostas serão posteriormente integradas. Nele se apresenta o contexto argentino de "cibernética" em termos de regulamentos e conceitos; linguagem quanto à definição conceitual de "ciber" em nível global e a dificuldade de sua univocidade; A ciberdefesa e o triângulo do sábado como proposta de relacionamento e análise para uma perspectiva tecnológico-produtiva. Por fim, o artigo dá conta dos aspectos metodológicos mais relevantes que norteiam as onze linhas de pesquisa apresentadas.

Palavras-chave: CIBERDEFESA - SEGURANÇA CIBERNÉTICA - INVESTIGAÇÃO - CAMPO INTELECTUAL.

Cyberdefense as an intellectual field: Contributions and research proposals in Cyberdefense and Cybersecurity for the Argentine reality.

Abstract

This article presents future lines of research in relation to cyber defense and cybersecurity based on heterogeneous perspectives and approaches linked to problems of interest to the area. It aims to provide an academic framework and to become a precedent from which the proposed lines of research will later find membership. In it, the Argentine context of "cyber" is presented in terms of the regulations and the conceptual; language regarding the conceptual definition of "cyber" at a global level and the difficulty of its univocity; Cyberdefense and the Sabbath Triangle as a relationship and analysis proposal for a technological-productive perspective. Finally, the article gives an account of the most relevant methodological aspects that guide the eleven lines of research presented.

Keywords: CYBERDEFENSE - CYBER SECURITY - INVESTIGATION - INTELLECTUAL FIELD.