Ciberdefensa como campo intelectual:
aproximaciones a los desafíos de la acción pedagógica relativa a sus dominios[1]

Por Guillermo Rutz

Resumen: Este artículo busca reflexionar sobre la ciberdefensa como campo intelectual en el marco de la teoría de Bourdieu. Para ello realiza un recorrido por los siguientes elementos que constituyen un campo: estructura, interés, lucha por la distribución de capital, actores en juego, mercado específico, búsqueda de autonomía y arbitrio de la acción pedagógica. De este modo, el artículo busca distinguir indicios que acerquen o no a la ciberdefensa a las condiciones para constituirse como tal y dentro del cual surjan tanto desarrollos teóricos como debates conceptuales. A partir de las reflexiones, en cada elemento considerado 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 estos dominios en particular y dentro del ámbito de la Defensa Nacional.

Palabras Clave: ciberdefensa, campo intelectual, dominios, educación, política

[1] Pertenencia institucional: proyecto "Ciberdefensa y Educación. Aspectos curriculares, políticos-estratégicos y estratégicos-productivos vinculados a la Formación Ciber para los intereses de la Defensa y Soberanía Nacional", presentado por la unidad académica Facultad de Ingeniería del Ejército en la convocatoria UNDEFI 2019 de la Universidad de la Defensa Nacional (Resolución UNDEF 432/19, Proyecto Nro 722), sin financiamiento.

Introducción

Se suele señalar el incidente ocurrido en Estonia en 2007 como el hito que marca precedente en las acciones llevadas adelante por los gobiernos y Estados en relación a políticas de ciberdefensa y ciberseguridad. En Argentina, las fuentes periodísticas dan cuenta que a partir de 2013 comienzan a aparecer algunos artículos de poca profundidad académica o política sobre el tema. En cuanto a políticas de Estado, podemos decir que los documentos públicos evidencian el inicio de marcos normativos a partir del año 2011 con la creación del Programa Nacional de Infraestructuras Críticas de Información y Ciberseguridad, y luego en 2014 la creación del Comando Conjunto de Ciberdefensa. Sin embargo, recién en 2019 se dicta la Estrategia Nacional de Ciberseguridad (Rutz, 2019).

La Universidad Nacional de la Defensa, a través de la Facultad de la Defensa Nacional, en el año 2019 da continuidad al Proyecto de investigación UNDEFI: "Soberanía nacional y ciberdefensa. Elementos teóricos y político-estratégicos del desafío ciberespacial para la Defensa Nacional", comenzado el año anterior. En el mismo, se abre una nueva línea de investigación: "Ciberdefensa y formación de posgrados en Argentina. Aproximaciones desde una perspectiva social y de políticas públicas". Como resultado de esta línea de investigación se publicaron dos artículos: "Ciberdefensa y formación de posgrado en Argentina. Indagaciones preliminares para un aporte al desafío ciber de la Defensa Nacional" (Rutz, 2019) y "Ciberdefensa y formación de posgrados en Argentina: reflexiones a partir de perspectivas políticas y sociales para el interés de la Soberanía Nacional" (Rutz, 2020), los cuales detallan los hallazgos y perspectivas futuras. La investigación respondió a un enfoque metodológico cualitativo basado en tres aspectos: la indagación en la agenda periodística local de publicaciones en línea, para lo cual se consideraron aquellas de mayor publicación en idioma español; realización de entrevistas semiestructuradas a directores de carrera de formación de posgrado (tanto maestrías como cursos de especialización) en ciberdefensa y ciberseguridad, como también a decisores de políticas públicas expresamente vinculadas a la temática; análisis de la normativa vigente y marcos teóricos relativos al aspecto social y de políticas públicas.

"Ciberdefensa y formación de posgrado en Argentina. Indagaciones preliminares para un aporte al desafío ciber de la Defensa Nacional". En este artículo se expone el aporte, de la formación de posgrado en ciberdefensa y ciberseguridad a los elementos teóricos y político-estratégicos, en un contexto de desafío ciberespacial para la Defensa Nacional. Para ello analiza siete ejes: aspectos curriculares, vínculos entre currículum y contexto normativo, cooperación entre actores y estructuras, desafíos y dilemas actuales, posgrados y perfiles profesionales, políticas públicas referidas a la formación, y por último incentivos a la

formación, investigación e innovación. La investigación permitió identificar, en los cinco primeros ejes, doce categorías de análisis con cuarenta y dos hallazgos, mencionados en esa publicación. Tales categorías y hallazgos dieron lugar a la estructura de una nueva línea de investigación dentro del área ciber: formación en ciberdefensa y ciberseguridad. Ambas constituyen un nuevo campo del saber, con interés estratégico para el sector público y privado, el cual presenta múltiples dimensiones a ser estudiadas y desarrolladas, como por ejemplo las dimensiones económica, tecnológica, educativa, política, normativa, militar, entre otros aspectos o enfoques posibles (Rutz, 2019).

"Ciberdefensa y formación de posgrados en Argentina: reflexiones a partir de perspectivas políticas y sociales para el interés de la Soberanía Nacional". La publicación reflexiona desde un abordaje social, educativo, de políticas públicas y cuestiones curriculares sobre los hallazgos respecto a la formación de posgrado en Ciberdefensa para Argentina en 2019. En dichas aproximaciones se presentan miradas que buscan interpelar respecto a la realidad local a partir de recorridos comparativos de las agendas latinoamericanas y española sobre las siguientes cuestiones: criterios curriculares, estructura y marco curricular, orientación de la formación, inclusión de Políticas, Doctrinas y Directivas, vínculos o cooperación con universidades, empresas y Estado, ejercicios de simulación, reconocimiento de otros actores, planteos que los posgrados se hacen frente a los desafíos, forma de abordar la cuestión curricular, dependencia curricular y tecnológica, desafíos y dilemas que se reconocen, orientaciones y demandas sobre perfiles a formar, perfiles profesionales a los que se orientan los posgrados (Rutz, 2020).

A partir de lo investigado y las producciones académicas antes mencionadas, se da continuidad a la línea de investigación "Ciberdefensa y formación de posgrados en Argentina. Aproximaciones desde una perspectiva social y de políticas públicas" del proyecto UNDEFI con pertenencia a FADENA, mediante un nuevo proyecto llevado a cabo por la Facultad de Ingeniería del Ejército, en el marco de la Universidad de la Defensa Nacional: "Ciberdefensa y Educación. Aspectos curriculares, políticos-estratégicos y estratégicos-productivos vinculados a la Formación Ciber para los intereses de la Defensa y Soberanía Nacional". Como parte del mismo, surge este artículo donde se busca reflexionar sobre la ciberdefensa como campo intelectual, siguiendo la teoría de Bourdieu. Para ello realiza un recorrido por los siguientes elementos que constituyen un campo: estructura, interés, lucha por la distribución de capital, actores en juego, mercado específico, búsqueda de autonomía y arbitrio de la acción pedagógica. Busca de este modo distinguir indicios que la acerquen o no a las condiciones para constituirse como tal y dentro del cual surjan tanto desarrollos teóricos como debates conceptuales. A partir de las reflexiones en cada elemento considerado, toma el sentido de la acción pedagógica como elemento central de análisis para este caso y en función del mismo mirar, sociológicamente y con criterios de política educativa, 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. Esta publicación busca pensar qué desafíos se le presentan a este campo en construcción, desde lo pedagógico y conceptual sobre estos dominios en particular y dentro del ámbito de la Defensa Nacional, para hacer visibles probables líneas de debates como también posibles aportes académicos tanto para políticas educativas, desarrollos curriculares y fortalecimiento en general del área a partir de la discusión académica.

Ciberdefensa como campo intelectual[2]

La teoría de los campos de Bourdieu se fundamenta en la idea de que existen leyes generales de funcionamiento de la sociedad que se pueden analizar independientemente de las características particulares de los individuos. Desde la perspectiva teórica de Bourdieu, un campo es un espacio social estructurado y estructurante compuesto por instituciones, agentes y prácticas. Está estructurado en la medida en que posee formas más o menos estables de reproducción del sentido. Es decir, los sujetos se hallan inscritos en espacios sociales estructurados y dinámicos, a los que responden y son capaces de modificar. Así, podemos hablar del campo científico, del campo de la política, del campo religioso, del campo del arte, etc. (Bourdieu, 2000).

De este modo, un campo está constituido por la existencia de capitales comunes y por un conjunto de estrategias de lucha que tienden a la apropiación de los mismos. Cada campo elige y jerarquiza las formas de expresión y desarrollo del conflicto, fija los roles, además de los niveles de participación de los actores en la estructura social y establece los mecanismos de confrontación de individuos y grupos. Así, tanto al interior como al exterior de cada campo, las diferentes estrategias de actores y grupos en pugna responden a la desigual disposición de recursos, movilidad, acceso a diversos medios, influencia sobre otros contingentes, capacidad de establecer alianzas, de legitimar argumentos y visiones (Bourdieu, 1990).

La estructura de cada campo pone en evidencia el estado de la relación de fuerzas entre los actores y grupos internos que intervienen en la lucha, pero también entre los distintos campos de la sociedad en un contexto más amplio. Asimismo, podemos atestiguar las diversas alianzas, los pactos o los acuerdos estratégicos para la existencia de los mismos y la reorientación permanente de la tensión social (Bourdieu, 2002).

[2] Sobre análisis del campo intelectual de la Defensa Nacional en Argentina, véase Rutz (2017).

La fortaleza de cada campo estriba en la capacidad de producción, difusión y preservación de determinados capitales que solo tendrán valor dentro de los límites de este espacio. En consecuencia, la posición de los individuos en un campo específico está determinada por su volumen de capital económico (dinero, propiedades, inversiones), capital social (relaciones, contactos, parentescos) y capital cultural (información, saberes, conocimiento socialmente validado). Asimismo, por el volumen de capital cultural objetivado (libros, archivos, bases de datos, música, objetos de arte), de capital cultural subjetivado (consumo, apropiación, interiorización de la cultura) y de capital cultural institucionalizado (títulos, constancias, certificados, diplomas y toda acreditación institucional).

Sin embargo, cada campo elige las formas de valoración, reproducción, transmisión y conservación de su propio capital. De este modo, cierto tipo de bienes, relaciones sociales o saberes tendrán valor específico en campos concretos. Aun así, la teoría de los campos concibe a estos espacios de interacción social como estructuras dinámicas cuyos grados de desarrollo y autonomía están en función de su propia historia y, al mismo tiempo, de las funciones sociales que desempeñan al interior de estructuras de dominación más amplias.

En el contexto del marco conceptual descripto y de la investigación desarrollada dentro del Proyecto "Ciberdefensa y Educación. Aspectos curriculares, políticos-estratégicos y estratégicos-productivos vinculados a la Formación Ciber para los intereses de la Defensa y Soberanía Nacional", analizaremos para el caso de la ciberdefensa los siguientes elementos de un campo: estructura, interés, lucha por la distribución de capital, actores en juego, mercado específico, búsqueda de autonomía y arbitrio cultural de la acción pedagógica.

Estructura[3]

Distribución en un momento histórico de un capital específico: Desde el 2014 a la fecha, la ciberdefensa en Argentina ha surgido y cobrado un interés particular y progresivo logrando acumular capital simbólico, político y económico. Al mismo tiempo, se evidencia una distribución de capital específico a través de la generación de marcos normativos, estructuras burocráticas estatales, creación de posgrados, actividades académicas, entre otras. *Relaciones de fuerzas entre agentes y estructuras*: Para el caso argentino se evidencia la presencia de diversos

[3] "La estructura de un campo es un estado de la distribución, en un momento dado del tiempo, del capital especifico que allí está en jugo. Se trata de un capital que ha sido acumulado en el curso de luchas anteriores, que orienta las estrategias de los agentes que están comprometidos en el campo y que puede cobrar diferentes formas, no necesariamente económicas, como el capital social, el cultural, el simbólico y cada una de sus subespecies. En ese sentido puede decirse también que la estructura de un campo es un estado de las relaciones de fuerza entre las instituciones y/o agentes comprometidos en el juego" (Bourdieu, 2014:12), citado en Rutz (2015).

actores civiles, militares, académicos y políticos que tienen sus propios ámbitos de acción, lo cual directa o indirectamente genera vínculos, posturas y relaciones de poder tanto a nivel institucional como individual. *Agentes comprometidos en el juego*: Con la creación de la Secretaría de Ciberdefensa en el Ministerio de Defensa, el Comando Conjunto de Ciberdefensa en el ámbito del Estado Mayor Conjunto, equipos de investigación en diferentes facultades de la Universidad Nacional de la Defensa, tres maestrías y diversas ofertas de posgrados en universidades públicas y privadas, todo esto evidencia una masa crítica de agentes involucrados en el tema que a priori demostraría un compromiso en el juego interinstitucional, político y académico de la ciberdefensa.

Interés [4]

Engendra el interés que le es propio: Las acciones en el ámbito de diversas agencias del Estado, a nivel político y en las universidades, en particular en los últimos tres años, pone de manifiesto que la ciberdefensa como campo en Argentina se propuso y logró engendrar un interés incluso mayor al evidenciado por la defensa nacional. *No reduce los fines de la acción a fines económicos*: Las acciones llevadas a cabo en los diferentes ámbitos y por distintos actores hacen referencia a fines que trascienden lo estrictamente económico, así lo demuestra la generación de normativas, estructuras operativas y burocráticas en el Estado, creación de ofertas de posgrados, eventos académicos entre otros. *Acordar a cierto juego social un interés y beneficio simbólico*: Este aspecto del campo, en el caso de la ciberdefensa en Argentina, se puede apreciar en las orientaciones de los artículos publicados por diferentes investigadores, en los aspectos curriculares de las ofertas de posgrados existentes, en los lineamientos políticos de las normativas generadas en el ámbito del Estado nacional.

[4] Cada campo engendra así el interés (illusio) que le es propio, que es la condición de su funcionamiento. La noción de interés o de illusio se opone no solo a la de desinterés o gratuidad, sino también a la de indiferencias (Bourdieu, 2014:11). Al no reducir los fines de la acción a fines económicos, esta noción de illusio —y también de inversión o de libido— implica acordar a cierto juego social que él es importante, que vale la pena luchar por lo que allí se lucha, que es posible tener interés por el desinterés —en sentido estrictamente económico— y obtener beneficios de ello —en especial simbólicos— como en el caso de aquellos universos sociales que se explican por la economía de los bienes simbólicos (Bourdieu, 2014:12), citado en Rutz (2015).

Luchas por la distribución de capital [5]

Luchas destinadas a conservar o transformar la relación de fuerzas: Si bien no hay estudios actuales que revelen o evidencien luchas por la distribución de capital (simbólico, político, social, económico) en el ámbito de la ciberdefensa argentina, es de esperar, en función de lo dicho respecto de los elementos anteriores, que estas surjan en relación a las diferentes agencias del Estado (por ejemplo, entre el Ministerio de Seguridad y el de Defensa, entre diferentes posturas ideológicas de los investigadores, asesores políticos y teóricos futuros del tema). Actualmente es posible inferir algunas de estas posturas respecto a la distinción normativa, legal, operativa, agencial, entre ciberdefensa y ciberseguridad.

Actores en juego [6]

Necesidad de gente dispuesta a jugar el juego: Esta necesidad se halla satisfecha con pronóstico alentador cuando se observa la matrícula de la Maestría en ciberdefensa y ciberseguridad de la UBA, como también en la Maestría de ciberdefensa, de la Facultad de Ingeniería del Ejército, en el ámbito de la Universidad de la Defensa Nacional; o en las diferentes ofertas de posgrado en el ámbito universitario privado. *Gente dotada del hábitus, del conocimiento y reconocimiento de las leyes del juego*: En cuanto al conocimiento, el campo tiene asegurado sus actores en función de los estudiantes, docentes e investigadores del ámbito universitario actualmente existente. Respecto al reconocimiento de las leyes del juego, estas se irán desarrollando y consolidando como habitus a medida que se consoliden los cargos operativos, de mandos medios y alto en los diferentes organismos del Estado y en la producción académica de los investigadores y estudiantes en el ámbito universitario. *Creencia en el valor de lo que está en juego*: Este componente del campo, en el caso de la ciberdefensa argentina, se halla más visible y exponencialmente en desarrollo y consolidación cuando observamos el despliegue normativo, la creación de agencias y estructuras del Estado, la creación de ofertas

[5] Además de un campo de fuerzas, un campo social constituye un campo de luchas destinadas a conservar o transformar ese campo de fuerzas. Es decir, es la propia estructura del campo, en cuanto sistema de diferencias, lo que está permanentemente en juego. En definitiva, se trata de la conservación o de la subversión de la estructura de la distribución del capital específico, que orienta a los más dotados del capital específico a estrategias de ortodoxia y a los menos capitalizados a adoptar estrategias de herejía (Bourdieu, 2014:12), citado en Rutz (2015).

[6] Para que un campo funcione es necesario que haya gente dispuesta a jugar el juego, que esté dotada de los habitus que implican el conocimiento y el reconocimiento de las leyes inmanentes al juego, que crean en el valor de lo que allí está en juego. La creencia es, a la vez, derecho de entrada a un juego y producto de la pertenencia a un espacio de juego (Bourdieu, 2014: 13), citado en Rutz (2015).

de posgrados, equipo de investigación y participación en congresos o conferencias académicas.

Mercado específico [7]

El mercado específico para el caso de un campo del conocimiento, en los términos sociológicos de Bourdieu, tiene que ver con la producción académica, esto es: artículos, ponencias, investigaciones, tesis, congresos, entre otros; y a los consumidores y productores de tales bienes. En el corto tiempo desde que la ciberdefensa aparece en la agenda política y académica de Argentina, la producción académica muestra un crecimiento progresivo con miras a consolidarse. En tal sentido se puede decir que la ciberdefensa como campo intelectual está construyendo su propio mercado específico.

Búsqueda de autonomía [8]

Explicitación y sistematización de los principios de la legitimidad propia. En el caso argentino de ciberdefensa, se evidencia una clara voluntad de búsqueda de autonomía respecto a otros campos cuando observamos artículos, papers, congresos, tesis de maestría, generación de normativa específica, convocatorias y aprobación de equipos de investigación propios. Todo esto da cuenta de un interés particular, de una necesidad concreta y de la búsqueda genuinamente académica y política por diferenciarse de otras áreas del conocimiento, aún dentro de la propia área de la defensa nacional.

[7] El surgimiento del mercado específico señala históricamente el surgimiento del campo específico, con sus posiciones y sus relaciones entre posiciones. Podría decirse entonces que, a mayor desarrollo del mercado propio, mayor autonomía del campo respecto de los demás, o que la influencia de los otros campos varía según el grado de complejidad o de desarrollo del campo como campo específico, que posee leyes de funcionamiento propias, que actúan mediatizando la incidencia de otros campos (Bourdieu, 2014:13-14), citado en Rutz (2015).

[8] El grado de autonomía de un campo de producción restringida se mide según el grado en el cual puede funcionar como un mercado específico, generador de un tipo de rareza y de valor irreductibles, entre otras cosas, a la rareza y al valor económico de los bienes considerados, a saber, la rareza y el valor propiamente culturales. Dicho de otro modo, mientas el campo esté en mejores condiciones de funcionar como el lugar de una competencia por la legitimidad cultural, la producción puede y debe orientarse, en mayor medida, hacia la búsqueda de las distinciones culturalmente pertinentes en un estado dado de un campo determinado, es decir, hacia los temas, las técnicas o los estilos que están dotados de valor en la economía propia del campo, porque son capaces de conferir a los grupos que los producen un valor propiamente cultural, afectándolos con marcas de distinción que el campo reconoce como culturalmente pertinentes y por lo tanto susceptibles de ser percibidas y reconocidas como tales (Bourdieu, 2014:93), citado en Rutz (2015).

Arbitrio cultural de la acción pedagógica [9]

Sistema de enseñanza que cumple una función de legitimación cultural: En relación a esto, la ciberdefensa en Argentina rápidamente logró instrumentarlo mediante la creación de tres maestrías y diversas ofertas de posgrados, evitando así quedar sólo como una materia o subespecialidad de otras carreras. *Delimitación de lo que merece ser transmitido y adquirido y de lo que no lo merece*: Tanto desde el ámbito civil con la Maestría de la UBA, como en el ámbito militar con la Maestría de la FIE o mediante las ofertas de posgrado en universidades privadas, el campo de la ciberdefensa argentina ha decidido qué se transmite y qué no, tanto a los postulantes que buscan ingresar al campo como también para el conocimiento y divulgación de sus investigaciones y estudios mediante las tesis, los artículos y papers académicos, la organización de congresos y seminarios, entre otros. *Distinción entre las obras legítimas e ilegítimas, como también entre la manera legítima e ilegítima de abordar las obras legítimas*: Si bien en este estadio de construcción del campo no hay grandes restricciones al respecto de obras legítimas e ilegítimas (en materia de discusiones teóricas, académicas, metodológicas, políticas, doctrinarias o ideológicas) todo está dado para que este aspecto del arbitrio cultural suceda más temprano que tarde mediante el accionar de las instituciones académicas, organismos del Estado que provean puestos técnicos, empresas privadas, políticas públicas y todos los agentes intervinientes en dichos ámbitos.

Ciberdefensa: desafíos de la acción pedagógica en relación a sus dominios

De acuerdo a la investigación llevada a cabo por Trama y Vergara (2017), si bien se han realizado seminarios y simposios a nivel regional latinoamericano en torno al *ciberespacio* [10] y la defensa, "existe un vacío en lo que se refiere a la influencia en las *operaciones militares* [11]" (Trama y Vergara, 2017: 18). De acuerdo a los autores, esto puede vincularse al riesgo que implica para los países revelar sus debilidades, dejando expuestas así vulnerabilidades estratégicas. Sin embargo, este estudio remarca la necesidad de publicaciones que investiguen aspectos estratégicos militares relacionados con los Comandos Conjuntos de *Ciberdefensa* [12] "en toda la gama de operaciones militares".

[9] Toda acción pedagógica se define como un acto de imposición de un arbitrio cultural que se disimula como tal y que disimula lo arbitrario de lo que inculca. El sistema de enseñanza cumple, inevitablemente, una función de legitimación cultural al convertir en cultura legítima, por este único efecto de disimulación, el arbitrio cultural que una formación social plantea por su existencia misma, y, más precisamente, reproduciendo, a través de la delimitación de lo que merece ser transmitido y adquirido y de lo que no lo merece, la distinción entre las obras legítimas e ilegítimas y, al mismo tiempo, entre la manera legítima y la ilegítima de abordar las obras legítimas (Bourdieu, 2014:104), citado en Rutz (2015).

El mencionado estudio (el primero en su tipo), devela la dificultad entre las Fuerzas, a la hora de simular la planificación de *operaciones conjuntas* [13], debido a que los participantes carecen de precisión en los conceptos implícitos en las *operaciones cibernéticas militares* [14]. Se le suman como limitaciones actuales la escasa bibliografía en español y la falta de antecedentes en el tema. Lo mencionado marca con precisión la necesidad de ahondar y extender la investigación en relación a las miradas pedagógicas o de políticas educativas referidas a la formación de cuadros estratégicos, operativos y tácticos de la ciberdefensa. Sin embargo, esta dificultad no es privativa de las Fuerzas a nivel local. De manera similar y a modo de ejemplo se puede decir que a nivel internacional no hay acuerdo o un consenso general sobre qué debe considerarse como operaciones cibernéticas que afectan a la Defensa Nacional, entre otras múltiples cuestiones a considerar.

Conforme a la investigación referida, las operaciones cibernéticas son las que conllevan la interrupción, negación, degradación o destrucción de la información existente en computadoras y redes. De tal manera, se puede decir que son ofensivas, defensivas y de exploración, donde se incluyen la inteligencia, la vigilancia, reconocimiento y preparación del ambiente operacional (Trama y Vergara, 2017: 88). Para estos autores, las capacidades militares a desarrollar en torno a la ciberdefensa tiene que ver con aquellas herramientas, acciones, conocimientos que permitan ejercer el mando y control de las fuerzas en dichas operaciones, además de poder "retener la libertad de acción en el ciberespacio y prevenir sorpresas estratégicas" (Trama y Vergara, 2017: 89).

De acuerdo a las conclusiones del trabajo citado en los párrafos precedentes y, en el marco del Proyecto "Ciberdefensa y Educación. Aspectos curriculares, políticos-estratégicos y estratégicos-productivos vinculados a la Formación Ciber para los intereses de la Defensa y Soberanía Nacional", desde una perspectiva social y educativa, es necesario conocer cuáles son los dominios de la ciberdefensa (en el sentido estrictamente vinculado al ámbito militar y de incumbencia de la Defensa Nacional) y su abordaje curricular en las instancias de formación. Para esto, en primera instancia tomaremos el mapa de dominios propuesto por Henry Jiang, según el cual podemos identificar nueve: 1-Operaciones de seguridad, 2-Desarrollo de carrera, 3-Arquitectura de seguridad, 4-Seguridad física, 5-Estándares de Seguridad, 6-Evaluación de riesgos, 7-Gobernanza, 8-Inteligencia de amenazas y 9-Educación del usuario. A continuación, veremos qué aspectos aborda cada uno de ellos.

> 1-*Operaciones de seguridad*. [16] Este dominio comprende la defensa activa, fuga de datos, gestión de vulnerabilidad, sistema de gestión de información y eventos de seguridad, prevención, protección, detección, plan de recuperación de desastre, plan de continuidad de negocio, centro de operaciones de seguridad, respuesta a incidentes:

notificación de incumplimiento, contención, erradicación, investigación y dentro de ella, forencia.

2-*Desarrollo de carrera*. [17] El segundo dominio abarca cuestiones de autoestudio, grupo de pares, formación, certificaciones, conferencias, definición de roles, perfiles, funciones, competencias y puestos en los niveles estratégicos, operativos y tácticos.

3-*Arquitectura de seguridad*. [18] En este caso, el dominio aborda el desarrollo seguro de aplicaciones, diseño de red, protección de datos, criptografía, construcción segura del sistema: configuración de línea de base, ingeniería de seguridad, seguridad en la nube: identidad federada y Cloud Access Security Broker, control de acceso, gestión de identidad mediante la gestión de acceso privilegiado y gestión de identidad y acceso.

4-*Estándares de Seguridad*. [19] Los estándares de seguridad tienen que ver con los protocolos y normativas desarrollados por distintos organismos como el Instituto Nacional de Estándares y Tecnologías (NIST), las Normas ISO/IEC, el control de objetivos para tecnologías de información (COBIT), los controles de seguridad críticos para ciberdefensa (SANS / CSC).

5-*Evaluación de riesgos*. [20] La evaluación de riesgos comprende el análisis de vulnerabilidad, inventario de activos, riesgos de terceros y de la tercera parte, evaluación de riesgos de la central de datos, control del mapa de flujos de datos, escaneo de códigos fuente mediante caja blanca y caja negra, texteo de penetración mediante equipo azul y equipo rojo: usando ingeniería social, aplicaciones e infraestructura.

6-*Gobernanza*. [21] Comprende las auditorías, leyes y regulaciones del Estado de aspectos federales y de la industria específica, participación en la gestión ejecutiva: riesgos informados, informes y puntuaciones, procedimientos de supervisión escritos de la compañía: sus políticas, procedimiento, estándares, cumplimiento y aplicación.

7-*Inteligencia de amenazas*. [22] Este dominio se ocupa de la inteligencia externa e interna, la inteligencia compartida, la inteligencia contextual, los indicadores de compromiso en la gestión de riesgos (IOCs) y del control de amenazas en todos ellos.

8-*Educación del usuario*. [23] La educación de usuarios comprende el refuerzo de la conciencia o concientización de riesgos, amenazas y usos de los entornos ciber, la formación de nuevas habilidades, el entrenamiento en herramientas específicas.

> 9-*Seguridad física*. [24] La seguridad física, en el marco de la ciberdefensa/ciberseguridad, está dada principalmente en el hardware (puertas traseras), seguridad física de los centros de datos, cables de fibra óptica troncales y locales, contramedidas electrónicas, entre otros aspectos.

A su vez, Trama y de Vergara plantean dos modelos de "objetivos estratégicos y líneas de acción de una *Política de Ciberdefensa* [25]", de los cuales se tomarán, para el recorte de investigación que este tema requiere, algunos de ellos, dada la pertinencia temática y la pertenencia institucional de dicho estudio. En tal sentido, del Modelo 1 los objetivos estratégicos: "3. Promover la capacitación del personal en materia de ciberdefensa, y 4. Reforzar el sistema de Investigación y Desarrollo … en materia de ciberdefensa" (Trama y Vergara, 2017: 291) constituyen interesantes puntos de referencia para indagar respecto tanto del campo intelectual como de los dominios de la ciberdefensa. Mientras que del Modelo 2 los objetivos estratégicos "1. Formar Fuerzas Armadas conscientes de los riesgos derivados de las *amenazas cibernéticas [26]* …, y 5. Alcanzar y mantener los conocimientos, habilidades, experiencias y capacidades tecnológicas que se necesiten para sustentar todos los objetivos de la defensa cibernética" (Trama y Vergara, 2017: 295-6) aportan en el mismo sentido.

En relación a lo expresado, cabe preguntarse respecto a los desafíos de la acción pedagógica en términos de elementos de un campo, para lograr alcanzar y sostener determinadas habilidades, conocimientos y experiencias relativas a la ciberdefensa. Para tal fin, es necesario definir los perfiles del personal necesario para el área y en función de ello diagramar curricularmente las carreras de formación.

Reflexiones provisorias

Al reflexionar sobre la ciberdefensa como campo intelectual desde el marco dado por la teoría de campos de Bourdieu podemos decir que existen indicios concretos que permiten considerar a la ciberdefensa como un campo intelectual en construcción. Sin embargo, es necesario investigar, reflexionar y documentar en mayor profundidad respecto a cada uno de los componentes o elementos mencionados que conforman un campo intelectual. No sólo para ver su tendencia, desarrollo y comportamiento, sino también para determinar su influencia y significación para otros campos intelectuales o para las políticas públicas, instituciones y actores vinculados a la ciberdefensa. En este sentido, se puede decir que el estudio de la ciberdefensa como campo intelectual y su implicancia social, política, académica, científica-tecnológica y específicamente civil o militar, constituyen en la actualidad un área de vacancia para la investigación y producción académica en Argentina.

En el marco teórico referido, los sujetos se hallan inscritos en espacios sociales estructurados y dinámicos, a los que responden y son capaces de modificar. En tal sentido, y

para los propósitos de este artículo, debemos pensar respecto a todas las variables posibles –que necesitamos conocer o serían de utilidad en el campo político, académico o científico-productivo-, de tales espacios sociales estructurados vinculados a la ciberdefensa, como por ejemplo: las instancias académicas donde se enseñan, debaten o investigan; los espacios institucionales donde se ponen en juego sus prácticas operativas, como también las interacciones que permiten o no acuerdos y consensos para futuras definiciones políticas.

Dado que la fortaleza de cada campo estriba en la capacidad de producción, difusión y preservación de determinados capitales que solo tendrán valor dentro de los límites de este espacio, resulta de interés para este estudio y en particular para el proyecto en el cual se inscribe el presente artículo, poder plantear líneas de investigación que den cuenta de aquellos indicadores. Esto permitirá ir evaluando dicha fortaleza a través de, por ejemplo: capacidad de producción y difusión académica, tipo de producción y difusión, qué capitales culturales e intelectuales se preservan y de qué modo, a qué se da valor y el ranking que se les otorga; o qué límites actuales tiene el campo y cuáles impone por voluntad de sus actores.

La ciberdefensa como campo intelectual, en relación a cuestiones estratégicas militares ya tiene diagnosticada la necesidad de investigaciones y publicaciones que aporten datos empíricos, reflexiones críticas o propuestas prácticas sobre las operaciones militares en todos sus alcances y sentidos, como también aquellas que tomen a los Comandos Conjuntos de Ciberdefensa como objeto de estudio. Las investigaciones existentes también dan cuenta de la necesidad de pensar sobre la dificultad entre las distintas fuerzas armadas a la hora de poner en práctica diferentes etapas de lo que se denominan operaciones conjuntas; o cómo se resuelve la adquisición, entre la diversidad de actores, para que manejen con precisión conceptos que hacen al lenguaje propio del campo. Para todo esto será necesario generar vínculos de confianza y cooperación entre proyectos de investigación y sus objetos de estudio, instituciones y actores del ámbito académico y militar, creando todos los protocolos de confidencialidad que fueran necesarios. Algunas de las limitaciones actuales con las que cuenta este campo en construcción es la falta de antecedentes en los diferentes temas y objetos de estudios que le competen, como también la escasa bibliografía en español, en particular sobre reflexiones locales o regionales vinculadas a lo estrictamente militar y de la defensa nacional.

En cuanto a políticas de ciberdefensa que tengan que ver con el ámbito de la educación, existe en la producción académica local existente 4 propuestas: 1. Promover la capacitación del personal en materia de ciberdefensa; 2. Reforzar el sistema de Investigación y Desarrollo en materia de ciberdefensa; 3. Formar Fuerzas Armadas conscientes de los riesgos derivados de las amenazas cibernéticas; y 4. Alcanzar y mantener los conocimientos, habilidades, experiencias y capacidades tecnológicas que se necesiten para sustentar todos los objetivos de la defensa cibernética. Sin embargo, de acuerdo a los alcances de esta

investigación, pareciera que faltan debates y estudios que permitan dar cuenta sobre aspectos políticos, científico-tecnológicos, metodológicos que dialoguen con las necesidades tácticas y operacionales de la defensa nacional y sus elementos actuantes, a efectos de definir planes y programas curriculares y académicos que puedan satisfacer esas demandas de política educativa en relación a la ciberdefensa.

En lo particular esta investigación se plantea ahondar sobre los desafíos que se le presentan al sentido de la acción pedagógica frente a los dominios de la ciberdefensa. Para ello tomó una clasificación –no quiere decir que sea la única o la correcta- que comprende: 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. Al respecto se propone indagar sobre las percepciones y reacciones de dos tipos de sujetos vinculados a esta categoría –dominios de ciberdefensa- los alumnos y profesores que transitaron por instancias de formación de posgrado en ciberdefensa. A partir de esto, determinar qué desafíos se les presentan tanto desde lo pedagógico, lo conceptual como dentro del ámbito de la defensa nacional, es el objetivo a desarrollar en futuras publicaciones.

Para comprender el arbitrio cultural de la acción pedagógica en lo que a ciberdefensa concierne es necesario comprender y develar las características del sistema de enseñanza que cumple una función de legitimación cultural, respecto a los contenidos investigados; a qué y quienes responde la delimitación de lo que merece ser transmitido y adquirido, de lo que no lo merece y qué implicancias para la defensa nacional (sus políticas, sus instituciones, sus actores y acciones operativas) tienen dichas delimitaciones respecto a, en este caso particular sus dominios. Por último, este arbitrio de la acción pedagógica se comprende cuando es posible hacer visible la distinción entre las obras legítimas e ilegítimas, como también entre la manera legítima e ilegítima de abordar las obras legítimas, es decir, qué de lo que se escribe y piensa se acredita o desacredita y qué tipo de interpretaciones se aceptan sobre lo escrito. En tal sentido, será parte de futuras publicaciones dar cuenta de esto en cuanto a los dominios de la ciberdefensa.

Bibliografía

BOURDIEU, P. (2002). Las reglas del arte. Barcelona: Anagrama.

BOURDIEU, P. (2000). Cosas dichas. Barcelona: Gedisa.

BOURDIEU, P. (1990). Algunas propiedades de los campos. En P. Bourdieu, Sociología y cultura, pp. 135-142. México: Grijalbo.

RUTZ, R. G. (2020). Ciberdefensa y formación de posgrados en Argentina: reflexiones a partir de perspectivas políticas y sociales para el interés de la Soberanía Nacional. (en prensa).

RUTZ, R. G. (2019). Ciberdefensa y formación de posgrado en Argentina. Indagaciones preliminares para un aporte al desafío ciber de la Defensa Nacional. Revista Científica, Defensa Nacional, número 3.

RUTZ, R. G. (2017). Aportes para la discusión sobre organización intelectual y social del Campo de la Defensa vinculada a las ciencias sociales, en la formación de posgrados (Tesis Doctoral). FLACSO, Buenos Aires, Argentina.
http://repositorio.flacsoandes.edu.ec/handle/10469/12727

RUTZ, R. G. (2015). Universidad y Defensa: vínculos, aportes y tensiones del Sistema Universitario Argentino a la formación de posgrados orientados a civiles para la Defensa Nacional (Tesis Maestría en Estrategia y Geopolítica). ESG-IUE, Buenos Aires, Argentina.

http://repositorio.flacsoandes.edu.ec/handle/10469/12751

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.

Bibliografía de referencia

[10] Ciberespacio

Llongueras Vicente Adrianna (2013). La Guerra Inexistente, La Ciberguerra. Editorial Academia Española, España.

La estrategia internacional para el ciberespacio (DIEEEI21-2011). Instituto Español de Estudios Estratégicos: IEEE. Recuperado de http://www.ieee.es/Galerias/fichero/docs_informativos/2011/DIEEEI21-2011EstrategiaInternacionalCiberespacio.pdf

Conflicto en el ciberespacio. Centro de Estudios Estratégicos de La Haya. Ministerio de Asuntos Exteriores y Defensa de los Países Bajos. Recuperado de https://www.hcss.nl/pub/2019/strategic-monitor-2019-2020/conflict-in-cyberspace/

[11] Operaciones militares.

Scott Jasper. PhD thesis U.S. Strategic Cyber Deterrence Options. UNIVERSITY OF READING.

Recuperado de http://centaur.reading.ac.uk/79976/1/22839264_Jasper_thesis.pdf

[12] Ciberdefensa

Aimar, Gago Edgardo (2017). El enfoque argentino sobre ciberseguridad y ciberdefensa (Trabajo Final de Licenciatura). Escuela Superior de Guerra Tte Grl Luis María Campos. Ciudad Autónoma de Buenos Aires. Recuperado de https://repositoriosdigitales.mincyt.gob.ar/vufind/Record/CEFADIG_5519b9c4e1ec7a8b75b0db195f286944

Parly, Florence (2019). Fuerzas de defensa cibernética de los ejércitos franceses. Doctrina de ciberdefensa de la República Francesa. Discurso - Estrategia cibernética del ejército - 18 de enero de 2019. Recuperado de https://www.defense.gouv.fr/content/download/557384/9657762/Discours%20Florence%20Parly%20-%20Strat%C3%A9gie%20cyber%20des%20Arm%C3%A9es%20-%2018%20janvier%202019.pdf

Francia. Doctrina militar del control informático ofensivo. Recuperado de https://www.defense.gouv.fr/content/download/557386/9657778/Doctrine%20militaire%20de%20lutte%20informatique%20offensive.pdf

DELERUE, François. Instituto de Investigación Estratégica de la Escuela Militar (IRSEM). República Francesa. Recuperado de https://www.irsem.fr/equipe/delerue.html

La defensa nacional de China en la nueva era. Recuperado de http://eng.mod.gov.cn/news/2019-07/24/content_4846443.htm

Ciberguerra, los escenarios de confrontación. Instituto Español de Estudios Estratégicos: IEEE

Recuperado de http://www.ieee.es/Galerias/fichero/docs_opinion/2014/DIEEEO18-2014_Ciberguerra_EscenariosConfrontacion_EguskineLejarza.pdf

Robert Vargas Borbúa, Rolando P. Reyes Chicango y Luis Recalde Herrera. Ciberdefensa y ciberseguridad, más allá del mundo virtual: modelo ecuatoriano de gobernanza en ciberdefensa. Universidad de las Fuerzas Armadas ESPE, Ecuador. Recuperado de

DOI: https://doi.org/10.17141/urvio.20.2017.2571

https://revistas.flacsoandes.edu.ec/urvio/article/view/2571/1605

CIBERSEGURIDAD: RETOS Y AMENAZAS A LA SEGURIDAD NACIONAL EN EL CIBERESPACIO.

Instituto Español de Estudios Estratégicos - Instituto Universitario "General Gutiérrez Mellado". Recuperado de https://publicaciones.defensa.gob.es/media/downloadable/files/links/c/e/ce_149.pdf

[13] Operaciones conjuntas

Anca, Luis Javier. TRABAJO FINAL INTEGRADOR. La ciberdefensa: hacia el desarrollo de una interoperabilidad conjunta del teatro de operaciones. Recuperado de http://www.cefadigital.edu.ar/bitstream/1847939/478/1/TFI%2001-2015%20ANCA.pdf

Defensa cibernética: CIOC por primera vez en el ejercicio conjunto de Joint Stars. Ministero della Difesa. República Italiana. Recuperado de https://www.difesa.it/InformazioniDellaDifesa/periodico/Periodico_2017/Documents/Numero3/ID-3_2017_ridotto.pdf
http://www.difesa.it/SMD_/Eventi/Pagine/cyber_defence_debutto_cioc_esercitazione_joint_stars.aspx

[14] Operaciones cibernéticas militares

Operaciones militares cibernéticas. Escuela Superior de Guerra Conjunta. Recuperado de http://www.esgcffaa.edu.ar/pdf/ESGCFFAA-2016_pdf-49.pdf

Cyber war in perspective: russian aggression against ukraine. Centro de Excelencia Cooperativo de Ciberdefensa de la OTAN. Recuperado de https://ccdcoe.org/uploads/2018/10/CyberWarinPerspective_full_book.pdf

Ciberseguridad, contrainteligencia y operaciones encubiertas en el programa nuclear de irán: de la neutralización selectiva de objetivos al "cuerpo ciber" iraní. Resultados de búsqueda

Instituto Español de Estudios Estratégicos: IEEE. Recuperado de http://www.ieee.es/Galerias/fichero/docs_opinion/2013/DIEEEO42-2013_Inteligencia_Iran_XSertvija.pdf

Daniel Cohen y Ofir Bar'el. The Use of Cyberwarfare in Influence Operations. Centro de Investigación Cibernética Interdisciplinaria de Blavatnik (CICR), Universidad de Tel Aviv. Israel. Recuperado de https://icrc.tau.ac.il/sites/cyberstudies-english.tau.ac.il/files/media_server/cyber%20center/cyber-center/Cyber_Cohen_Barel_ENG.pdf

Giles, Keir. Monografía 9: "Manual de la guerra de información rusa". NATO, Defense College. Recuperado de http://www.ndc.nato.int/download/downloads.php?icode=506

[17] Desarrollo de carrera

HM Gobernment (2014). Cibersecurity Skill: a guide for business. Recuperado de https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/386248/bis-14-1276-cyber-security-skills-a-guide-for-business.pdf

Universidad Técnica de Tallin (Tallinna Tehnikaülikool). Recuperado de https://www.ttu.ee/studying/tut_admission/programmes-in-taltech/masters/cyber-security/#overview-24

https://ois.ttu.ee/portal/page?_pageid=37,674560&_dad=portal&_schema=PORTAL&p_action=view&p_fk_str_yksus_id=50001&p_kava_versioon_id=50439&p_net=internet&p_lang=EN&p_rezhiim=0&p_mode=1&p_from=

Escuela de Ingeniería Cibernética (SCE) de la Universidad Xidian. Recuperado de https://en.xidian.edu.cn/info/1003/1371.htm

SEGURIDAD CIBERNÉTICA Y DELITO CIBERNÉTICO. Universidad de Bolonia. Recuperado de https://www.unibo.it/en/teaching/course-unit-catalogue/course-unit/2019/446835

La Dirección General de Seguridad Exterior de la República Francesa está buscando aprendices que sean expertos en Fortnite. Recuperado de https://etudiant.lefigaro.fr/article/la-dgse-recherche-des-stagiaires-experts-en-fortnite_84f02360-1322-11e9-830d-78e7d5526521/

Natural Language Processing for Social Media: Second Edition. Recuperado de https://ieeexplore.ieee.org/document/8239762

Laboratorio de Sistemas de Información Avanzados, Departamento Computación Facultad de Ingeniería, Universidad de Buenos Aires. Recuperado de http://sedici.unlp.edu.ar/bitstream/handle/10915/46107/Documento_completo.pdf?sequence=1&isAllowed=y

[18] Arquitectura de seguridad

ENISA (2006). Como crear un csirt paso a paso. Recuperado de file:///C:/Users/Docente/AppData/Local/Temp/CSIRT_setting_up_guide_ENISA-ES-1.pdf

Itil v3. Recuperado de https://docs.supersalud.gov.co/PORTALWEB/PLANEACION/ADMINISTRACIONSIG/GSDE01.PDF

ONTI (2005). Modelo de política de seguridad de la información para organismos de la administración publica nacional. Recuperado de http://servicios.infoleg.gob.ar/infolegInternet/anexos/240000-244999/242859/norma.htm

Seguridad informática en las instalaciones nucleares. Organismo Internacional de Energía Atómica. 2.3.3. Defensa en profundidad, pagina 13. Recuperado de https://www-pub.iaea.org/MTCD/Publications/PDF/Pub1527s_web.pdf

[19] Estándares de seguridad

ISO 27001 (2005). Sistemas de gestión de seguridad de la información. Recuperado de

https://www.isotools.org/pdfs-pro/iso-27001-sistema-gestion-seguridad-informacion.pdf

ISO 27032 (2012). Gestión de la ciberseguridad ciberseguridad.

BS7799,1998 199 (2005). Gestión de la seguridad de la información y riesgos.

DoD 8570.01-M. Certificación del personal que realiza funciones de Aseguramiento de la información (IA) dentro del Departamento de Defensa (DoD) de los Estados Unidos de América. Recuperado de https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodm/857001m.pdf

Oficina del Subsecretario de Defensa para Adquisiciones y Sostenibilidad de los Estados Unidos de América. Recuperado de https://www.acq.osd.mil/dpap/dars/dfars/html/current/252204.htm

Almacenamiento seguro de la información. Una guía de aproximación para el empresario.

Instituto Nacional de Ciberseguridad. Reino de España. Recuperado de https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_ciberseguridad_almacenamiento_seguro_metad_0.pdf

Proyecto de trabajo de grado. Guía para la implementación de la norma ISO 27032. Sandra Liliana Guzmán Solano. UNIVERSIDAD CATÓLICA DE COLOMBIA - FACULTAD DE INGENIERÍA. Recuperado de https://repository.ucatolica.edu.co/bitstream/10983/23385/1/Proyecto%20Guia%20ISO%2027032.pdf

Framework for Improving Critical Infrastructure Cybersecurity. National Institute of Standards and Technology. Recuperado de https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

[20] Evaluación de riesgos

ISO 27005 (2018). Gestión de riesgos de la seguridad de la información.

ISO 31000 (2009). Gestión de riesgos.

Vásquez, Miguel Darío (2016). TESIS DE POSGRADO: Técnicas anti-forenses informáticas. Universidad Nacional de Córdoba. Facultad de Matemática, Astronomía, Física y Computación. Recuperado de https://rdu.unc.edu.ar/bitstream/handle/11086/2849/TI%20CAPce_Vasquez_2016.pdf?sequence=1&isAllowed=y

[21] Gobernanza

IT gobernance institute, Information security gobernante. Guía para gestión de los sistemas de información.

Piorun, Daniel. Normas y marcos relacionados con la implementación de esquemas de Gobierno de la Tecnología de la Información. Recuperado de http://bibliotecadigital.econ.uba.ar/download/tpos/1502-1042_PiorunD.pdf

Procesos habilitadores de COBIT 5. Objetivos de control para la información y tecnologías relacionadas. ISBN 978-1-60420-285-4

[22] Inteligencia de amenazas

La Cámara de Diputados de la Nación Argentina ha publicado el Primer Informe de Ciberterrorismo y Ciberseguridad basado en la metodología de UK POST (United Kingdom Parliamentary Office of Science and Technology) del Parlamento Británico. Recuperado de https://www.b1nary0.com.ar/wp-content/uploads/2019/12/Ciberterrorismo-y-ciberseguridad-informe-parlamentario.pdf

Evaluación de amenazas espaciales 2019. Centro de Estudios Estratégicos e Internacionales. Recuperado de https://csis-prod.s3.amazonaws.com/s3fs-public/publication/190404_SpaceThreatAssessment_interior.pdf?fzHArWoAPB93dlIqxJnYxYPaoP4wScdT

Satellite Network Hacking & Security Analysis. International Journal of Computer Science and Security (IJCSS). Recuperado de https://www.cscjournals.org/manuscript/Journals/IJCSS/Volume10/Issue1/IJCSS-1200.pdf
Son vulnerables los sistemas de comunicación satelitales. Universidad Nacional Autónoma de México. Recuperado de https://www.seguridad.unam.mx/son-vulnerables-los-sistemas-de-comunicacion-satelitales

Ciberataque por brecha de aire (air-gap). Universidad Ben-Gurión del Néguev -, Estado de Israel. Recuperado de https://cyber.bgu.ac.il/air-gap/

Synesthesia: Detecting Screen Content via Remote Acoustic Side Channels. Recuperado de https://www.cs.tau.ac.il/~tromer/synesthesia/synesthesia.pdf

Inyección de audio basada en láser en sistemas controlables por voz. The University of Electro-Communications - University of Michigan - University of Michigan. Recuperado de https://lightcommands.com/

https://lightcommands.com/20191104-Light-Commands.pdf

Echelon. Universidad de Buenos Aires. IX Congreso Iberoamericano de Seguridad Informática. Recuperado de http://www.criptored.upm.es/descarga/Actas_cibsi2017_UBA.pdf

Compañía de vigilancia Hacking Team. CONSEJO DE SEGURIDAD DE LAS NACIONES UNIDAS - República del Sudán. Venta al Gobierno de programas informáticos de intrusión con capacidad de inteligencia electrónica y determinó que podían calificarse de "equipo militar". El proveedor del equipo, Hacking Team. Recuperado de https://www.undocs.org/es/S/RES/1591%20(2005)

https://www.hcdn.gob.ar/proyectos/proyectoTP.jsp?exp=4055-D-2015

The EP and the global interception system 1998 – 2002. EUROPEAN PARLIAMENT. Recuperado de https://www.europarl.europa.eu/EPRS/EPRS_STUDY_538877_AffaireEchelon-EN.pdf

[23] Educación del usuario.

Hall, Anthony. No hay balas de plata. Esencia y accidentes de la ingeniería de software. University of North Chapel Hill. Recuperado de https://www.u-cursos.cl/ingenieria/2008/1/CC31B/1/material_docente/bajar?id_material=163224

Vilca, Stella Maris. Trabajo Final de Posgrado: Los desafíos de la concientización en las organizaciones actuales. Recuperado de http://bibliotecadigital.econ.uba.ar/download/tpos/1502-1061_VilcaSM.pdf

Taddeo, Mariarosaria. Son la ética digital, la filosofía de la tecnología, la ética de los conflictos cibernéticos y la ciberseguridad. Oxford Internet Institute: OII - Universidad de Oxford. Recuperado de https://www.oii.ox.ac.uk/people/mariarosaria-taddeo/?publications

[24] Seguridad física

Hansche, Susan. Oficial (ISC) 2 guia para el examen CISSP. Recuperado de https://www.academia.edu/4903488/Official_ISC2_Guide_to_the_CISSP-ISSEP_CBK

Garcia, Mary Lynn (2007). Design and Evaluation of Physical Protection Systems. Butterworth-Heinemann

Patterson, David G. (2005). Implementación De Sistemas De Protección Física: Guía Práctica. ASIS International.

[25] Políticas de ciberdefensa

Pessino, Mauro. Trabajo Final de Grado: LAS POLÍTICAS EN CIBERSEGURIDAD DE LA ORGANIZACIÓN DEL TRATADO DEL ATLÁNTICO NORTE (OTAN) PERÍODO 2008-2013. Recuperado de https://repositorio.uesiglo21.edu.ar/bitstream/handle/ues21/13842/PESSINO%20MAURO.pdf?sequence=1&isAllowed=y

Camila Hernández Sánchez. Control a las exportaciones de cibertecnologías: Un análisis del Arreglo de Wassenaar y sus implicancias para la ciberseguridad. Recuperado de https://scielo.conicyt.cl/pdf/rchdt/v7n1/0719-2584-rchdt-7-01-00061.pdf

Wassenaar: Cybersecurity and Export Control. Naval Postgraduate School, Center for Homeland Defense and Security. Recuperado de https://www.hsdl.org/?view&did=795893

Ingreso de la REPUBLICA ARGENTINA al WASSENAAR ARRANGEMENT. Recuperado de http://servicios.infoleg.gob.ar/infolegInternet/anexos/60000-64999/63378/norma.htm

[26] Amenaza cibernética

Robles Carrillo, Margarita. Amenaza y uso de la fuerza a través del ciberespacio: un cambio de paradigma. Revista Latinoamericana de Derecho Internacional.

Robles Carrillo, Margarita. El ciberespacio: presupuestos para su ordenación jurídico-internacional. Recuperado de DOI: 10.7770/rchdcp.v1i1.1025

PRESENTACIÓN

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), Licenciado en Bibliotecología y Documentación (UNMDP). Docente y bibliotecario de nivel Primario. Cuenta con numerosas capacitaciones en Administración Pública Nacional (INAP).

Co-Dirige el Proyecto de investigación UNDEFI-FIE: "Ciberdefensa y Educación". También participa como Investigador académico del Proyecto UNDEFI-FADENA: "Soberanía nacional y ciberdefensa". Desde el 2009 investiga sobre diferentes aspectos académicos y educativos de la Defensa Nacional tales como: "Organización intelectual y social del Campo de la Defensa vinculada a las ciencias sociales", "Vínculos y aportes del Sistema Universitario Argentino a la formación para la Defensa", "Características y Fundamentos políticos, doctrinarios y experiencias de implementación en diferentes niveles de formación para la Defensa" sobre los cuales ha escrito 5 tesis de posgrados, libros y artículos académicos en revistas especializadas.

Participó como Profesor invitado en la Maestría de Ciberdefensa y Ciberseguridad (UBA), la Maestría en Defensa Nacional (FADENA) y la Diplomatura en Gestión de la Ciberdefensa (ESGCFFAA). Fue Tutor Académico de Cadetes del Colegio Saint Cyr, en el marco de cooperación Franco-Argentina entre UNDEF-FADENA con Embajada de Francia. Se desempeñó como Jurado en Concursos docentes de posgrados de la ESG, Evaluador externo y Jurado de Tesis de posgrados en varias Universidades. Actualmente Dirige Tesis en Defensa y Ciberdefensa.

Fue Director de Escuelas Rurales por 10 años. Ha dictado cursos de formación docente entre 2003-2008. Cuenta con 19 años de experiencia en la Administración Pública. Se desempeña en el Ministerio de Educación de la Nación, habiendo sido jurado y veedor de concursos de empleo público entre 2013-2017. Ha colaborado en la elaboración de perfiles para cargos de empleo público. Se desempeñó como Referente Federal (2012-2017) entre el Ministerio de Educación de la Nación y todos los Ministerios de Educación Provinciales coordinando, gestionando y monitoreando circuitos administrativos-legales-contables de Convenios, Actas, Transferencias y Rendiciones de fondos siendo por ello evaluado anualmente en auditorias ISO; recibiendo el área el Premio Nacional a la Calidad de Jefatura de Gabinete de Ministros. Desde 2014 es Miembro Paritario de la Comisión de Igualdad de Oportunidades y Trato (CIOT) ejerciendo como enlace político-administrativo entre el Ministerio de Educación, la Unión del Personal Civil de la Nación y la Comisión Central CIOT.