PAZ CIBERESPACIAL Y RECURSOS HUMANOS: APORTES PARA PENSAR PUESTOS, PERFILES, FORMACIÓN Y RECLUTAMIENTO

Por DR. **ROQUE GUILLERMO RUTZ**

Palabras Clave:
> Ciberdefensa
> Recursos Humanos
> Educación
> Campo Intelectual

Introducción

La presente investigación se realizó durante el año 2020 en el marco del Proyecto UNDEFI Nº 693 "Paz y Guerra en el Ciberespacio", cuyo objetivo general era analizar los elementos y dinámica del conflicto en el ciberespacio para identificar sus impactos sobre la defensa nacional argentina. En dicho contexto, esta línea de investigación se centró en uno de los componentes esenciales de la ciberdefensa: los recursos humanos. Dado que en Argentina el campo es de reciente conformación y estructuración, no encontrándose en el ámbito académico civil investigaciones o producciones sobre el tema, el propósito de esta línea investigativa es presentar ejes prioritarios sobre los cuales puedan focalizarse futuros desarrollos que aporten al debate, al intercambio y a la transferencia académica. Para esto, los ejes analizados fueron: el contexto académico y productivo,

Podemos considerar que el campo de batalla futuro sucederá en tres ámbitos principales: el de la realidad, el virtual y de la información; los tres demandan entrenamiento y formación de los sujetos que en ellos se desenvolverán.

la necesidad de mapeos de puestos por sector y sus respectivos perfiles profesionales, las necesidades de capacitación para esos perfiles y dónde deben obtenerse.

Procesos sociales y culturales como la actual pandemia de COVID-19 aceleran los procesos de digitalización masiva de las poblaciones. Esta realidad, entre otros efectos, conlleva un gran impacto en el uso del tiempo que los sujetos le dedican a las tecnologías en el ciberespacio. En este contexto y siguiendo a Moresi podemos postular que *"ni las leyes, ni nuestras mentes, ni el sistema de aprendizaje se han adaptado al cambio, [...] estos cambios usan a nuestro cerebro como campo de batalla y será el ambiente donde se desarrollará el conflicto futuro"*[1]. En tal sentido, el argumento del artículo pasa por pensar el conflicto futuro que involucrará la formación de los recursos humanos para pensar en el cerebro, en sus adaptaciones y necesidades, en la nueva cultura digital y en cibernética como elemento central para dirimir los conflictos futuros.

Buscar y mantener la paz en el ciberespacio, en la actualidad y en el futuro, no alcanza con solo pensar en la protección de las infraestructuras críticas. Necesitamos mentes agudas, formadas y entrenadas que sean capaces de imaginar escenarios futuros complejos; donde este entrenamiento y formación requiere dar lugar a la investigación en educación vinculada a la ciberdefensa. Este artículo, busca contribuir en el marco del contexto descripto, proponiendo posibles líneas de investigación, diferentes herramientas que permitan pensar la formación y obtención de recursos humanos para el área. Porque *"el desafío es crear una nueva cultura de aprendizaje [...] ello requiere inicialmente comprender y conocer los desafíos que impone el ciberespacio para impedir ser dominados a través de él"*[2].

Pensar la paz desde el quinto dominio

Pensar la paz en el ciberespacio necesariamente lleva a prestarle atención estratégicamente al conflicto ciberespacial, para que conociéndolo se lo pueda prevenir o prepararse para enfrentarlo. Al respecto, en un reciente artículo publicado en la Revista *Visión Conjunta,* el ex comandante conjunto de Ciberdefensa expresa: *"a lo largo de los años [...] diversos documentos políticos han coincidido que relacionado a las amenazas cibernéticas resulta necesario abordarlo desde la perspectiva de la Defensa Nacional [...] para resguardar las Infraestructuras Críticas del Sistema de Defensa Nacional y aquellas otras asignadas a su protección"*[3].

Desde la perspectiva de pensar la paz en el quinto dominio, cabe preguntarse qué implican las amenazas cibernéticas y las respuestas vinculadas con los riesgos, donde el concepto riesgo está representado por la posibilidad de ataques a los objetivos estratégicos de un país. En tal sentido, Moyano nos dice: *"este riesgo debe focalizarse en las infraestructuras cuyo funcionamiento resulte crítico para el cumplimiento de las funciones vitales del Estado, su Defensa Nacional, el ejercicio de la soberanía y el resguardo de la vida y libertad de sus ciudadanos".* Bajo el amparo de esta definición, me permito un ejercicio de libre imaginación a partir del cual propongo diferentes escenarios hipotéticos, pero no imposibles.

Me pregunto si existe la posibilidad de pensar teóricamente situaciones en las cuales una persona, o un grupo de personas, una institución u organización, desde dentro o fuera del país, por motivos políticos, ideológicos, económicos, personal o el que fuere podría llevar a cabo alguna de las siguientes acciones: alterar mediante actividades en el ciberespacio, el funcionamiento de diques o centrales hidroeléctricas lo que provocaría inundaciones con nivel de catástrofe para la población, la economía y el Estado. Interrumpir el suministro eléctrico en un sector geográfico del país por un tiempo tal que perjudique al sistema de salud para provocar la muerte de pacientes. Alterar masivamente los datos bancarios

1. Moresi, 2020: 11.
2. Moresi, 2020: 13.
3. Moyano, 2020: 60.

para provocar desestabilización y conmoción en la población. Impedir las comunicaciones en los sistemas de navegación en el medio civil o militar de barcos, submarinos, aviones o radares, por un tiempo tal que pueda provocar la muerte de sus tripulantes o impedir la libertad de acción de una determinada operación en ejercicio de la soberanía del país. Alterar el proceso productivo de cualquier industria que provoque graves consecuencias a la economía del país y a la población (por ejemplo, impedir o retrasar la producción de una vacuna). Acciones de cibersabotaje o ciberespionaje en cualquier área estratégica del sector público o privado que limiten o impidan el ejercicio de la soberanía en dicha área. Estos y muchos otros escenarios (de posibles ataques a lo que podrían considerarse Infraestructuras con objetivos estratégicos para el país) podrían pensarse y desarrollarse con el nivel de complejidad que se quisiera para su abordaje y análisis estratégico de posibles soluciones, sin embargo, no es el objetivo de este trabajo.

Si bien el artículo no busca un análisis de escenarios de conflictos en el ciberespacio, mencionar los ejemplos anteriores nos remite a pensar en el conflicto como un elemento más a tener en cuenta si queremos buscar y mantener la paz en el quinto dominio. Para hacer frente a las situaciones de posibles conflictos cibernéticos, las agencias y organismos directa o indirectamente relacionados a su prevención, mitigación o resolución necesitan personal formado y capacitado para tal fin. Así lo reconoce el Comando Conjunto de Ciberdefensa al expresar que la *"capacitación, creación de competencias y sensibilización es un objetivo irrenunciable [...] La consecución de este objetivo debe basarse en la definición, implementación y continuo perfeccionamiento de una formación orientada hacia las funciones de cada uno de los puestos directamente relacionados con actividades de Ciberdefensa"*[5].

En tal sentido, dicho organismo dependiente del Estado Mayor Conjunto de las Fuerzas Armadas *"asumió la responsabilidad de definir, dirigir y coordinar la concientización, la formación y el adiestramiento especializado en materia de Ciberdefensa"*; para lo cual en un reciente artículo se presentó un plan de formación orientada al personal militar en sus distintos niveles e instituciones educativas. Además, considera que dicha formación de personal debe darse *"tanto en la conducción de Operaciones del Ciberespacio como en los aspectos técnicos y eminentemente operativos"*[6].

Otro aspecto que fundamenta la centralidad que tienen las miradas e investigaciones sobre aspectos educativos y de formación en temas de ciberdefensa es el propio diagnóstico realizado por el Comando Conjunto de Ciberdefensa, según el cual *"un análisis de la situación ha permitido determinar que, en la actualidad, la formación en este ámbito es escasa, parcialmente satisfecha con perfiles técnicos del área TIC, sin conocimientos profundos de las Operaciones Militares ni de Operaciones del Ciberespacio, no está debidamente estructu-*

rada ni homologada, y no garantiza la capacitación del personal para el acceso a formación de mayor nivel tecnológico ni para satisfacer las necesidades reales de las Fuerzas Armadas"[7].

Por ello este artículo busca contribuir al debate sobre un posible camino para pensar una política pública de formación y reclutamiento de personal según los perfiles profesionales que surjan de los puestos laborales requeridos por los organismos y las agencias involucradas.

Mapeos de puesto por sector

Habiendo relevado y conocido el contexto[8], lo que debemos hacer es un mapeo de puestos por sector. Téngase en cuenta que todo este proceso que estamos describiendo sobre los recursos humanos necesarios para afrontar el conflicto ciberespacial con el objetivo de conseguir la paz en el ciberespacio, es en definitiva pensar en una política educativa. Dicha política podrá tener diferente lineamiento y alcance según como lo piense una Universidad, el Ministerio de Defensa, un sector que represente una o varias Infraestructuras Críticas (sector nuclear, petrolero, bancario o el encargado de satélites, por ejemplo), o bien cada una de las Fuerzas Armadas u otras agencias del Estado que necesiten dichos recursos.

Para realizar este mapeo, es necesario un estudio o investigación de campo, pero no puede ser especulativo o teórico porque en ese caso se corre el riesgo de desvíos (por exceso o por defecto de cantidad) de recursos formados y sus especificaciones curriculares según los niveles y puestos a ocupar (tácticos, operativos o estratégicos), que entonces resultan de poca utilidad práctica. En tal sentido, el estudio deberá identificar los sectores que demandan estos recursos, sus características, sus puestos, las urgencias, las estrategias ya empleadas, los aspectos normativos y legales de contratación, ingreso y permanencia, entre otras cuestiones del diseño de investigación. Contando con este mapa o relevamiento de puestos por sector y nivel, puedo pasar a la elaboración técnica de cada perfil, para luego en base a ese perfil pensar en el diseño curricular de la formación.

Un ejemplo orientador sobre identificación de puestos por sector es lo publicado por el ex comandante conjunto de Ciberdefensa GB Moyano en la Revista *Visión Conjunta*. En dicho artículo el Comando Conjunto identifica para el área de su incumbencia los siguientes puestos: Operador de Ciberdefensa, Analista de Ciberdefensa, Supervisor de Ciberdefensa, Planificador de Ciberdefensa, Asesor de Ciberdefensa, Investigador de tecnologías del ciberespacio, Desarrollador de tecnologías del Ciberespacio, Conductor de Ciberoperaciones, Supervisor de SOC/CSIRT/CERT, Analista de amenazas, riesgos y vulnerabilidad, Asesor experto en ciberdefensa, Asesor en informática forense[9].

De igual modo podría servir de guía para identificar puestos por sector, el cuadro de procesos y subprocesos vinculados a la ciberdefensa publicado por el Comando Conjunto[10].

Mapa de perfiles profesionales

Este mapa presenta los siguientes elementos o áreas que deberán ser completadas por los responsables del diseño de los perfiles profesionales requeridos en cada organismo o área: Círculo rojo: (1)-áreas de la defensa dentro de la arquitectura institucional.

> Círculos verdes: (2)-objetivo de cada área de la defensa.
> Rectángulo marrón: (3)-conocimiento mínimo del profesional de acuerdo al objetivo del área.
> Rectángulo bordó: (4)-procesos o líneas de acción del objetivo.
> Rectángulo amarillo: (5)-actividades de cada proceso o línea de acción.
> Rectángulo morado: (6)-conocimientos, habilidades y competencias para realizar las actividades.
> Rectángulo rosado: (7)-tipos de puestos a ocupar para lograr el objetivo del área.
> Rectángulo celeste: (8)-disciplinas o áreas del conocimiento para la formación en el objetivo del área de la defensa.
> Rectángulos amarillo, verde y azul: (9)-perfil profesional especializado en defensa.

A continuación, se detalla qué comprenden conceptualmente cada uno de ellos. Una referencia gráfica a este mapa puede consultarse en Rutz (2017: Anexo III).

1. **Áreas de la defensa dentro de la arquitectura institucional:** hace referencia al área específica de la Defensa de acuerdo a la arquitectura organizacional del Ministerio de Defensa, pudiéndose pensar también las áreas propias de los Estados Mayores Generales y Conjunto de las Fuerzas Armadas, otras agencias del Estado o empresas del sector productivo. Por lo tanto, habrá tantos mapas de perfiles profesionales como áreas específicas se encuentren definidas en los organigramas del Ministerio de Defensa y los Estados Mayores Generales y Conjunto de las Fuerzas Armadas, otros organismos, agencias del Estado o empresas del sector productivo que busquen diseñar sus perfiles con este mapa.
2. **Objetivo de cada área de la defensa:** en ella se consignan los objetivos específicos del área particular de la Defensa a la que se refiera el mapa (en este caso sería la ciberdefensa), los cuales surgirán de las definiciones orgánicas y nor-

4. Moyano, 2020: 61.
5. Moyano, 2020: 56.
6. Moyano, 2020: 56-57. **7.** Moyano, 2020:57.
8. En Rutz (2019) se abordan los contextos para esta cuestión.
9. Moyano, 2020: 57.
10. Moyano, 2020: 61.

Se debe pensar en el conflicto como un elemento más a tener en cuenta si queremos buscar y mantener la paz en el quinto dominio. Para hacer frente a las situaciones de posibles conflictos cibernéticos, las agencias y organismos directa o indirectamente relacionados a su prevención, mitigación o resolución necesitan personal formado y capacitado a tal fin.

mativas determinadas técnica y políticamente por cada organismo de la Defensa, como los mencionados en el punto 1, de acuerdo a sus necesidades orgánicas funcionales, técnicas, administrativas y conceptuales. A su vez, a partir de esta se definirán las demás dimensiones del mapa.

3. **Conocimiento mínimo del profesional civil de acuerdo al objetivo del área:** en este apartado del mapa, un equipo técnico-político profesional debería establecer y delimitar los requerimientos de conocimientos específicos necesarios para poder cumplir con el objetivo del área según las definiciones del punto 2 y en el marco de requerimientos técnicos estratégicos, académicos y científicos definidos por una política de Defensa Sectorial. Estas necesidades de conocimientos serán la base para definiciones curriculares y de formación en el campo de la ciberdefensa.
4. **Procesos o líneas de acción del objetivo:** cada objetivo, según lo especificado en el punto 3, contará con determinados procesos o líneas de acción técnicas, administrativas o conceptuales, que serán necesarias realizar para dar cumplimiento al objetivo propuesto. Para poder desarrollar o hacer efectivas dichas líneas de acción se necesitará poseer determinados saberes prácticos y teóricos-conceptuales, como también competencias actitudinales, las cuales deberán ser definidas por un equipo técnico político profesional del área de referencia.
5. **Actividades de cada proceso o línea de acción:** cada línea de acción que surge del objetivo del área (2), queda especificada operativamente en un determinado número de actividades a desarrollar. Estas actividades operativas, que permiten la concreción de cada línea de acción, demandan determinados saberes prácticos y teóricos-conceptuales, como también competencias actitudinales, las cuales deberán ser definidas por un equipo técnico político profesional del área de referencia. Al mismo tiempo, este requerimiento de saberes y competencias serán insumos para las definiciones de otros mapas del campo, como el mapa curricular.
6. **Conocimientos, habilidades y competencias para realizar las actividades:** definidas las actividades que demandan los procesos (5), que permiten dar cumplimiento al objetivo del área específica, es posible deducir de ellas los conocimientos, las habilidades y las competencias requeridas para poder concretar dichas actividades. En esta dimensión del mapa, un equipo técnico político profesional del área debería especificar cuáles son esos conocimientos, esas habilidades y esas competencias que el perfil requiere, conforme al objetivo establecido y en el marco de las necesidades técnicas, estratégicas y políticas definidas a partir de una Política de Defensa Sectorial.
7. **Tipos de puestos a ocupar para lograr el objetivo del área:** a partir de las definiciones establecidas en los puntos anteriores, el área a la que se refiere el mapa, debería poder definir los tipos de puestos a ocupar de manera tal que permitan realizar las actividades planteadas, dentro de una línea de acción para la concreción del objetivo del área. Esta dimensión es una definición más orgánica funcional y laboral del mapa, que tiene estrecho vínculo con la definición del perfil profesional y que servirá de proyección futura para el desarrollo profesional dentro del campo.
8. **Disciplinas o áreas del conocimiento para la formación en el objetivo del área de la defensa:** esta parte del mapa toma las definiciones dadas en el punto 6 y a partir de ellas propone aquellas áreas del conocimiento o disciplinas científicas dentro de un área del conocimiento, que permitan formar a los futuros y posibles candidatos para ese perfil profesional buscado.
9. **Perfil profesional especializado en defensa:** finalmente, esta dimensión pretende orientar, a partir del análisis y definiciones

anteriores, sobre posibles carreras o titulaciones que debiera ofrecer el Sistema Universitario Nacional, en su nivel de formación básica, de grado, posgrado y especialización; como también en cuanto a experiencia necesaria requerida por el perfil, para poder realizar las actividades especificadas en el punto 5 y de acuerdo a los objetivos del área de la Defensa a la que se refiere el mapa en el punto 2.

¿Cómo capacito?

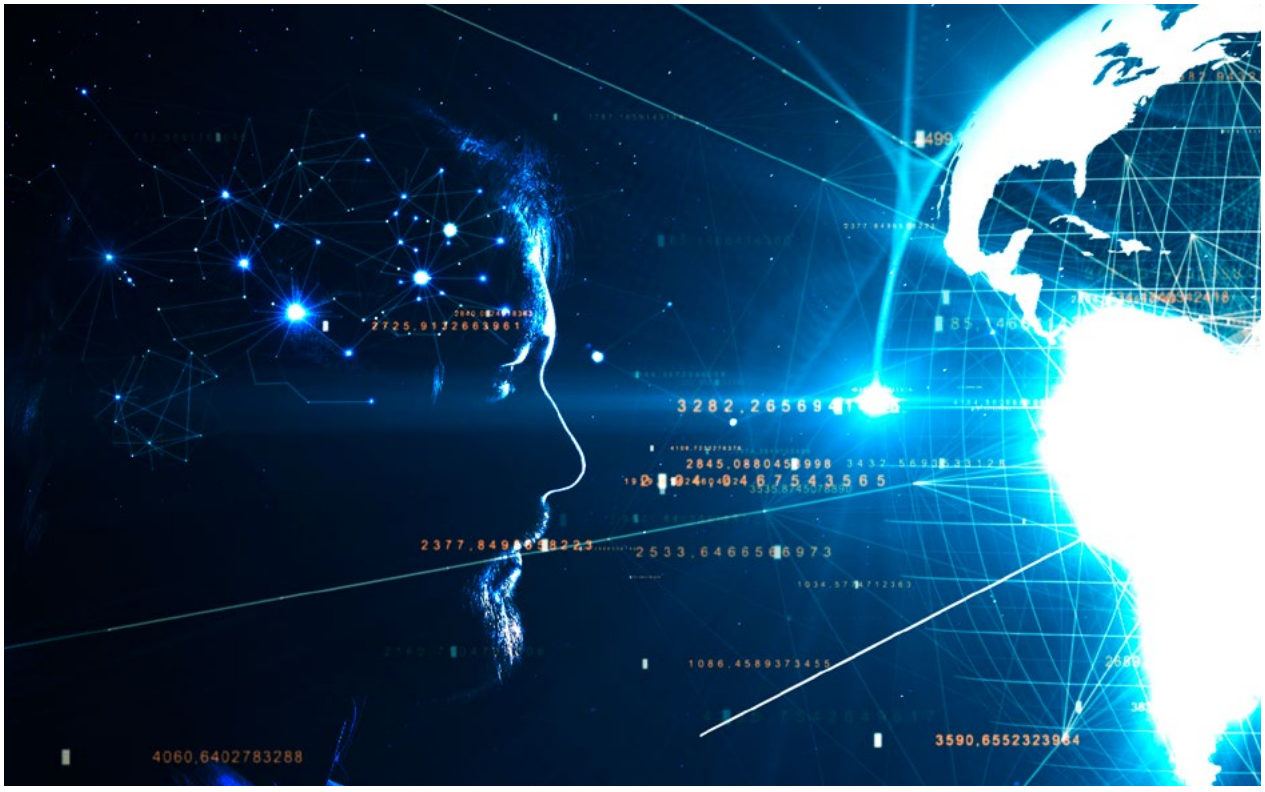
Una vez que cuento con los perfiles profesionales que necesito para los puestos que la estructura gubernamental o del sector productivo definió, cada organización individualmente o la autoridad política superior del área debería ponerse en contacto con los espacios académicos que considere pertinente para transmitirles la demanda o necesidad del área. Con esta demanda concreta, detallada, institucionalizada, producida en un documento (no informalmente transmitido como una charla), cada espacio académico debe pensar el mapa curricular para cada necesidad. En tal sentido presento en esta parte del artículo, lo que llamo "mapa curricular", como una de las tantas formas de pensar un currículum para un determinado perfil profesional o necesidad de un área, en este caso la ciberdefensa[11].

Las dimensiones que integran este mapa son:

> Círculo rojo: (1)-campo del conocimiento.
> Círculos verdes: (2)-posgrados (o niveles de formación) en ciberdefensa.
> Rectángulo lila: (3)-materias por áreas de conocimiento que aportan al posgrado.
> Rectángulo marrón: (4)-principales temas a abordar en cada materia.
> Rectángulo naranja: (5)-abordaje civil de los temas de la materia o disciplina.
> Rectángulo celeste: (6)-abordaje militar de los temas de la materia o disciplina.
> Rectángulo verde: (7)-perfil del profesor para cada materia o disciplina según tema y abordaje requerido.

1. **Campo del conocimiento:** el campo del conocimiento en el cual se espera que aporte este mapa, es el de la ciberdefensa. No obstante, podrían caber otros que refieran a distintos aspectos de la Defensa Nacional u otras áreas. Este mapa debe tener como fundamento teórico conceptual y empírico, el mapa de posgrados (no descrito en este artículo) y de perfiles profesionales, al mismo tiempo que

11. Una referencia gráfica a este mapa puede consultarse en Rutz (2017: Anexo III).



debe poder insertarse en el marco del mapa de disciplinas (no descrito en este artículo) que aportan al campo.

2. **Posgrados (o niveles de formación) en ciberdefensa:** en esta dimensión se indicarán los tipos de formación según niveles (por ejemplo: diplomatura, curso, licenciatura, maestría, doctorado, especialización) determinados para el área.
3. **Materias por áreas de conocimiento que aportan al posgrado:** en esta dimensión se repetirán las materias consideradas en el punto 7 del mapa de posgrados (no trabajado en este artículo)[12].
4. **Principales temas a abordar en cada materia:** en este apartado se debe dar cuenta, para cada una de las materias consideradas en el punto 3 de este mapa, de los principales temas imprescindibles a abordar desde el punto de vista técnico, académico y estratégico, para que la materia impartida marque un aporte y diferencia específica al campo particular y al área en general. Para ello deberá surgir un acuerdo técnico, político en base a una política sectorial de ciberdefensa en el marco de intereses estratégicos y necesidades reales de formación de los futuros profesionales del área.
5. **Abordaje civil de los temas de la materia o disciplina:** en esta dimensión un equipo de técnicos, profesionales y especialistas en el nivel académico referido, en la temática de la materia y en ciberdefensa; en conjunto con técnicos políticos del Ministerio de Defensa, en el marco de una política de Defensa Sectorial y de prioridades técnicas, políticas, académicas y estratégicas, deberían definir y describir los criterios rectores que debe tener el abordaje de las temáticas impartidas en cada materia consignada en el punto 4 de este mapa. Debería considerarse que este abordaje es el complemento desde una mirada, una teoría y una aplicación civil del mismo tema abordado militarmente en la misma materia.
6. **Abordaje militar de los temas de la materia o disciplina:** en ella, un equipo de técnicos, profesionales y especialistas en el nivel académico referido, en la temática de la materia y en ciberdefensa, en conjunto con técnicos políticos del Ministerio de Defensa, en el marco de una política de Defensa Sectorial y de prioridades técnicas, políticas, académicas y estratégicas, deberían definir y describir los criterios rectores que debe tener el abordaje de las temáticas impartidas en cada materia consignada en el punto 4 de este mapa. Debería considerarse que este abordaje es el complemento desde una mirada, una teoría y una doctrina militar del mismo

tema abordado civilmente en la misma materia.

7. **Perfil del profesor para cada materia o disciplina según tema y abordaje requerido:** en esta dimensión un equipo de técnicos, profesionales y especialistas en el nivel académico del posgrado, en la temática de la materia y en ciberdefensa; en conjunto con técnicos políticos del Ministerio de Defensa, en el marco de una política de ciberdefensa y de prioridades técnicas, políticas, académicas y estratégicas, deberían definir las características, condiciones y conocimientos necesarios del perfil de cada profesor para poder cumplir con los requerimientos de las materias conforme a las dimensiones de los puntos 5 y 6 de este mapa.

Este mapa permitiría definir las currículas de cada materia de los diferentes niveles y orientaciones de formación para la ciberdefensa tanto para civiles como para el personal de las Fuerzas Armadas, donde un ejemplo de plan de formación para el personal de las Fuerzas Armadas lo podemos encontrar en el cuadro que brinda el Comando Conjunto de Ciberdefensa[13].

¿De dónde los obtengo?

Finalmente, para concluir este recorrido propuesto en el artículo para pensar los recursos humanos de la Ciberdefensa que puedan abordar el conflicto ciberespacial buscando la paz en el quinto dominio, llegamos al interrogante ¿de dónde los obtengo?, sin desconocer la dificultad que tiene en la práctica resolver esta pregunta, considero oportuno plantear tres sectores como posibles semilleros donde encontrar personal en diferentes niveles de condiciones laborales, profesionales y de potencial técnico-profesional para la ciberdefensa.

El primero de estos sectores que propongo pensar en este artículo, son las Fuerzas Armadas (FF.AA). Al respecto se escuchan voces en todo el proceso de investigación, que se llevó a cabo desde fines de 2018 al presente, y son dos cuestiones. Por un lado, si este es un recurso humano de difícil obtención, alto costo de capacitación y permanencia, quizás habría que pensar en las políticas necesarias para permitir un mayor tiempo de permanencia y de carrera para los que ingresan o están en el área. De esta forma evitar que dicho personal sea desplazado a otros destinos, tareas o áreas. Por otra parte, si cuento escasamente con este recurso humano, quizás habría que revisar también la política de retiro del personal de las Fuerzas Armadas (destinado en el área de ciberdefensa), con el objetivo de retenerlo por mayor tiempo y que no esté obligado a retirarse si no asciende o no cumple algún otro requisito según la actual política de retiro del personal. O bien reconvertirlo en áreas técnicas, académicas o de investigación como personal de reserva que preste servicio, asesoría o apoyo a tiempo parcial. Esto es un tema a investigar y documentar académicamente en relación a la ciberdefensa.

Respecto a la Administración Pública Nacional (APN), en la actualidad existe un programa de movilidad interministerial (MOBI) sobre el cual gran parte de los empleados (y a veces los funcionarios) no tienen conocimiento, lo que debilita las posibilidades del Estado para la mejor utilización de sus recursos humanos según sus competencias, intereses y capacitación o formación. Por otra parte, no siempre el empleado público se halla en el puesto laboral para el cual está interesado o capacitado (ya sea por desconocimiento o interés específico del responsable jerárquico sobre dicho sector y empleado), en este sentido esto también es una práctica que debilita al Estado ya que en algunos casos tenemos un profesional que le costó millones al Estado en formación y desempeña una tarea operativa para lo cual no se requiere dicha formación; mientras que otras áreas que si requieren de tal nivel de formación no cuentan con dicho profesional. En tal sentido, desde la planificación estratégica es posible pensar que, mediante un relevamiento, una readecuación de tareas y un uso eficiente de puestos y recursos en la APN, el área de ciberdefensa podría disponer de personal potencialmente reconvertible. Esto también constituye una hipótesis de trabajo para futuros estudios académicos.

En la sociedad, en general, debemos pensar no solo en la universidad, sino en todos sus niveles educativos. La literatura nos dice que muchos hackers[14] son adolescentes; por otra parte, hemos visto en años recientes, como colegios[15] argentinos tuvieron éxitos e incluso ganaron concursos de robótica; cabe entonces preguntarse ¿debemos desestimar estos nichos de la población? ¿cómo y de qué forma podrían aportar al área? ¿de qué manera el Estado puede promover y desarrollar el interés y capacidad de este sector (los jóvenes) en relación a la ciberdefensa? También es válido afirmar que el sector de la población desocupada cuenta con personas (algunos profesionales y otros no) con conocimientos de programación y computación, donde muchos de ellos no pueden acceder a un puesto laboral formal porque no tienen un título universitario o terciario, aunque si una sólida experiencia en el

12. Rutz, 2017, Anexo III.
13. Moyano, 2020: 57.
14. https://www.elconfidencial.com/tecnologia/2015-11-30/jovenes-hackers-y-sobradamente-preparados-xxx_1108833/
https://www.bbc.com/mundo/noticias-46795226
https://www.elmundo.es/f5/2016/10/03/57f1917fe5fdeadf2d8b462e.html
15. https://www.infopico.com/2019/09/21/un-argentino-de-20-anos-fue-campeon-mundial-de-robotica-e-invento-una-app-para-ayudar-a-gente-con-problemas-de-audicion/
https://www.lanacion.com.ar/sociedad/maestros-argentinos-escuela-san-juan-gano-millon-nid2286092
https://www.lanacion.com.ar/tecnologia/un-colegio-argentino-llego-a-la-final-de-un-certamen-internacional-de-robotica-nid2112850/
https://www.colegiosanignacio.edu.ar/robotica-1-edicion-de-la-competencia-makex-argentina/

Para buscar y mantener la paz en el ciberespacio, en la actualidad y el futuro, no alcanza con sólo pensar la protección de las infraestructuras críticas. Necesitamos mentes agudas, formadas y entrenadas que sean capaces de imaginar escenarios futuros complejos.

CV

RUTZ ROQUE GUILLERMO

Doctor en Ciencias Sociales (FLACSO). Magíster en Estrategia y Geopolítica (ESG). Magíster en Defensa Nacional (FADENA). Magíster en Educación y Ciencias Sociales (FLACSO). Especialista en Políticas Educativas (FLACSO). Licenciado en Bibliotecología y Documentación (UNMDP). Investigador por la Universidad de la Defensa (UNDEF: FADENA – FIE) en las áreas Defensa Nacional, Educación y Ciberdefensa. Profesor invitado en temas de ciberdefensa en la Maestría de Ciberdefensa y Ciberseguridad (UBA-ENI), Maestría en Defensa Nacional (FADENA).

tema. Algunos de los que no cuentan con un título formal, son ocupados temporalmente por el sector privado; entonces quizás el Estado también deba aprender del sector privado y pensar políticas que posibiliten el acceso de este personal según las necesidades. Este, como los mencionados con anterioridad, es un tema de interés para estudios académicos sobre recursos humanos y ciberdefensa.

Con lo expuesto quiero decir, que quizás haya que revisar los planes y políticas de reclutamiento y acceso para determinados puestos de interés estratégico para el Estado. Pero primero hay que pensarlo, investigarlo, consensuar posturas y en base a los datos de estudios empíricos y no meramente especulativos, tomar la decisión política para luego llevarlas a la práctica. Lo cual también demanda de la habilidad para consensuar estrategias, planes y programas de largo plazo, que no cambien con cada director, coordinador de área o coalición-grupo político que asuma el gobierno. Para un resultado positivo se deben pensar políticas públicas en materia educativa vinculada a la ciberdefensa que mediante el consenso puedan ser mantenidas en el tiempo.

Trabajar sobre un plan de reclutamiento que no solo piense en la inmediatez, sino que contemple las necesidades y dificultades actuales, como también las posibilidades futuras y, logre propuestas a mediano y largo plazo, para que desde la educación primaria se comience a preparar el terreno de potenciales expertos en el tema, debería ser un objetivo de investigación académica, lo cual este estudio no ha podido identificar que existiera. De igual modo, pensar y poner en práctica un trabajo conjunto e interministerial entre, por ejemplo, el Ministerio de Defensa, el Ministerio de Seguridad, el Ministerio de Educación y las Universidades; e interjurisdiccional: nación y provincias para desarrollar un programa de formación y desarrollo del talento con objetivos a corto plazo, pero también con desarrollos a largo plazo que se conviertan en políticas de Estado, debería estar en las agendas de investigación y formación.

Conclusiones

Para algunos autores del ámbito militar, pensar el conflicto futuro implica pensar en el cerebro, sus adaptaciones al cambio, la nueva cultura digital y cibernética, en definitiva, pensar en la educación del sujeto social como elemento central para dirimir los conflictos. En tal sentido podemos considerar que el campo de batalla futuro sucederá en tres ámbitos principales: el de la realidad, el virtual y el de la información; los tres demandan entrenamiento y formación de los sujetos que en ellos se desenvolverán.

Este contexto y visión respecto a la búsqueda de paz ciberespacial, se correlaciona con la necesidad de políticas de largo alcance dado que adquirir ciertas capacidades conceptuales, técnicas y procedimentales en el ámbito educativo y con la mente como protagonista, no es un producto que se pueda bajar de una estantería o adquirir en un comercio de ramos generales cuando se quiera y en la cantidad que uno desee.

De tal manera, podemos afirmar que buscar y mantener la paz en el ciberespacio, en la actualidad y en el futuro no alcanza, con solo pensar (en los términos y alcances actuales) la protección de las infraestructuras críticas. Necesitamos mentes agudas, formadas y entrenadas que sean capaces de imaginar escenarios futuros complejos; donde este entrenamiento y formación requieren de un lugar para la investigación en educación vinculada a la ciberdefensa.

Aceptada la realidad de las miradas, esfuerzos, políticas e investigaciones puestas en la educación para la ciberdefensa, se presenta un reto adicional. El propio Comando Conjunto de Ciberdefensa, quien en el presente se erige como autoridad en el tema, determina que en la actualidad la formación en este ámbito es escasa, parcialmente satisfecha con perfiles técnicos del área TIC, sin conocimientos profundos de las Operaciones Militares ni de Operaciones del Ciberespacio; además no está debidamente estructurada ni homologada y no garantiza la capacitación del personal para el acceso a formación de mayor nivel tecnológico ni para satisfacer las necesidades reales de las Fuerzas Armadas.

Las conclusiones mencionadas precedentemente justifican por sí mismas la centralidad y necesidad de un espacio para la investigación en todos los temas vinculados a la educación-formación de los recursos humanos orientados a la ciberdefensa. Este artículo propone un camino para tal fin. Dicho proceso contempla el contexto actual de la ciberdefensa desde la perspectiva política, académica y científico-productiva que abonan y coinciden con las necesidades antes mencionadas. El proceso incluye, además, la necesidad de mapear los puestos por sector, la definición de perfiles profesionales para dichos puestos, el desarrollo de planes curriculares basados en los perfiles profesionales antes definidos y, finalmente, el desarrollo de un plan de reclutamiento de personal.

Los elementos, pasos y herramientas de este proceso presentado como propuesta para la definición de una política pública en tema de formación para la ciberdefensa, pueden conformar un plan de investigación en ciencias sociales con el aporte de miradas interdisciplinarias e interagencial, de manera que aporte a la toma de decisiones, al conocimiento del campo, a la formación de investigadores y profesores del área. Es necesario reconocer que tanto desde el ámbito académico, el político como también el militar se están llevando a cabo acciones que demuestran el interés y el esfuerzo por construir conocimiento en el terreno de la ciberdefensa. Sin embargo, pareciera que faltan miradas estructurantes y vínculos comunicantes para potenciar los esfuerzos que se vienen realizando, particularmente en temas de educación y sus subtemas derivados: políticas, planes, programas, actividades académicas, aspectos curriculares, recursos humanos, entrenamiento, cooperación, investigación, entre otros.

BIBLIOGRAFÍA

Bourdieu, P. (2002). Campo de poder, campo intelectual. Itinerario de un concepto. Editorial Montressor.

–

Bourdieu, P. (1996). Cosas dichas. Barcelona: Editorial Gedissa.

–

Moresi, A. A. (2020). "El conflicto futuro" en: *Visión Conjunta*, año 12, número 22-2020, pp. 10-13.

–

Moyano, T. R. (2020). "La República Argentina y sus esfuerzos en ciberdefensa: el compromiso con las buenas prácticas como parte de su ideario" en: *Visión Conjunta*, año 12, número 22- 2020, pp. 50-63.

–

Rodriguez, L. G. y Soprano, G. (2018). *Profesionales e intelectuales de Estado: análisis de perfiles y trayectorias en la salud pública, educación y las fuerzas armadas*. Rosario: Prohistoria Ediciones.

–

Rutz, G. (2019). Ciberdefensa y formación de posgrado en Argentina. Indagaciones preliminares para un aporte al desafío ciber de la defensa nacional. En: Defensa Nacional, n° 3-2019. pp. 272-274. Disponible en https://www.undef.edu.ar/wp-content/uploads/2020/06/DEFENSA-NACIONAL-REVISTA-CIENTIFICA-n%C2%B03-para-la-web.pdf

–

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. Disponible en http://repositorio.flacsoandes.edu.ec/handle/10469/12727

–

Sabato, 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. Sabato. Argentina: Paidós, 1975.