INSTITUTO DE CIBERDEFENSA DE LAS FUERZAS ARMADAS

DIPLOMATURA UNIVERSITARIA EN GERENCIAMIENTO DE LA CIBERDEFENSA

TRABAJO FINAL INTEGRADOR

APORTES HACIA LA CREACIÓN DE UN SERVICIO AUXILIAR DE ESPECIALISTAS EN EL QUINTO DOMINIO PARA EL ESTADO ARGENTINO

Integrantes del Equipo Nro 3:

RAÚL OMAR ROLDAN

MARIANO HUMBERTO ILLANES

JUAN JOSÉ DELGADO

Títulos Profesionales / de grado

Técnico Universitario en Telecomunicaciones

Licenciado en Administración

Licenciado en Administración

21 de noviembre de 2023

Resumen

El ambiente ciberespacial de interés nacional requiere ser abordado de manera integral a nivel nacional para velar por los intereses de los argentinos, aunando los diferentes esfuerzos contra el accionar de actores indeseados que buscan afectar los sistemas e Infraestructuras Críticas (IICC) usando especialmente este dominio para el desarrollo de sus acciones.

El presente trabajo de investigación de diplomatura, que a su vez integra las diferentes materias y clases brindadas por los profesores, busca aportar ideas que contribuyan a la constitución de un servicio auxiliar de especialistas en el quinto dominio, para lo cual desarrollará las ventajas de contar con la mencionada estructura.

Para abordar esta temática, en la introducción y marco teórico se describen algunas de las acciones desarrolladas por países como España, Estonia, Francia y el Reino Unido de Gran Bretaña. Producto de la explotación de sus lecciones aprendidas o informes anuales de ciberseguridad, estos estados concluyeron en la creación y mantenimiento de estructuras similares a las propuestas por el Equipo de Trabajo que llevó adelante esta investigación.

En el primer capítulo se analizan las estructuras del Servicio Auxiliar de Radioperadores del Ejército y el Sistema Auxiliar de Radioaficionados de la Armada de manera tal de extraer conclusiones que permitan avizorar la posible conformación del Servicio Auxiliar de Especialistas Cibernéticos.

En el segundo capítulo, por un lado se desarrollan la posible estructura y composición del SAEC, para finalmente poder describir las principales ventajas de contar con el mencionado servicio.

Palabras Claves: servicio, auxiliar, especialista, ciberdefensa, dominio.

Índice General

Justificación / Fundamentación / Aportes

La evolución de las amenazas en el ciberespacio permite que tanto individuos como grupos de terroristas o Estados Nación lo utilicen para realizar ciberataques. Según García (2020) las guerras del siglo XXI se pelearán con ceros y unos, ya que los ciberataques serán un componente esencial del conflicto, lo que lleva a cuestionarnos si ¿estamos preparados para defender el ciberespacio?

En 2021, el Centro Nacional de Respuesta a Incidentes Informáticos de la Dirección Nacional de Ciberseguridad de la Jefatura de Gabinete de Ministros de la Nación Argentina registró 591 incidentes informáticos, un 261,50 % más que en 2022 (CERT.ar, 2022). Estos incidentes ponen de manifiesto el crecimiento de la problemática en cuanto a Seguridad Informática se trate, asimismo, la necesidad de multiplicar los esfuerzos para proteger las Infraestructuras y Activos Críticos tanto militares como civiles.

De acuerdo con Reale (2023) hay una proliferación cada vez mayor de delitos relacionados con la tecnología y ataques informáticos, y actualmente es moneda corriente. Según el mapa de ciber amenazas en tiempo real de la empresa antivirus Kaspersky, durante la última semana de marzo de 2023 Rusia fue el país más ciber atacado del mundo; Brasil, el segundo; Estados Unidos, el tercero y China, el cuarto (Cybermap Kaspersky, 2023).

Así como en la Armada de la República Argentina (ARA) existe el Servicio Auxiliar de Radioaficionados de la Armada (SARA) y en el Ejército Argentino (EA) encontramos a su homólogo, el Servicio Auxiliar de Radioaficionados del Ejército (SARE), se considera que el principal aporte del presente trabajo es sentar las bases para la creación de un Servicio Auxiliar, similar al SARE y el SARA, integrado por especialistas en el ámbito cibernético, que contribuyan y faciliten la protección de las IICC y AACC mencionados.

Estos especialistas deberán trabajar en estrecha colaboración con el Comando Conjunto de Ciberdefensa (CCCD) y en coordinación con las Direcciones de Ciberdefensa (DDC) de cada Fuerza como colaboradores externos y desde su pericia.

El personal que podría formar parte de este servicio debería poseer habilidades avanzadas en programación, análisis de sistemas y seguridad de redes, logrando estar altamente capacitados para mantener la seguridad de los sistemas de información críticos.

Planteamiento del Problema

Relacionado con el planteo del problema, y como se expresó adelantadamente en el resumen, el presente trabajo integrador final analizará la posibilidad de que el Estado Argentino cuente con un servicio auxiliar de especialistas en el quinto dominio, con la capacidad de apoyar desde diferentes perfiles profesionales a las operaciones que las Fuerzas Armadas desarrollan para hacer frente tanto a los ciberataques que reciben las IICC como aquellos objetivos de valor estratégico (OVE) que el poder ejecutivo determine para su

protección; del mismo modo, contrarrestar los ciberataques que pretendan obstaculizar las operaciones del instrumento militar en el caso de encontrarse en situación de conflicto.

Formulación del Problema

¿Cuáles son las ventajas para el Estado Argentino de contar con un servicio auxiliar de especialistas cibernéticos en apoyo a sus Fuerzas Armadas?

Solución Propuesta

Para dar respuesta al anterior interrogante, y dado el carácter y la diversidad de los ciberataques modernos, el equipo considera que es menester contar con recurso humano capacitado en diferentes áreas de competencia en el ambiente cibernético y que complementen las actividades que desarrollan las DDC y el COCOCIBER.

En términos concretos, al igual que existen el SARE y SARA, las FFAA pueden contar con el SAEC; cuya organización, distribución, alcance, exigencias y requisitos o perfiles de ingreso, aptitud y demás aspectos de detalle pueden ser estudiados en futuros trabajos finales de investigación.

Asimismo, para alcanzar dicha solución a la problemática planteada, el equipo pretende alcanzar los objetivos de acuerdo a cómo se detallan a continuación.

Objetivos

Principal o General

Evaluar las ventajas de crear una estructura de apoyo a las actividades que desarrollan las FFAA en el quinto dominio, similar a las del SARE y SARA.

Particulares o Intermedios

Objetivo Particular Nro 1

Analizar las estructuras del SARE y SARA para extraer conclusiones que permitan proyectar la creación del SAEC.

Objetivo Particular Nro 2

Determinar las ventajas de contar con una estructura en apoyo a las actividades de las FFAA en el quinto dominio.

Marco Teórico

Al investigar el estado del arte y el marco teórico del tema propuesto, se puede destacar que sólo se cuenta con información acerca de las misiones o funcionalidades del SARE y el SARA. Es por ello que se consideró el hecho de analizar algunas formas de ser implementados los sistemas de comunicaciones en caso de emergencia por parte de algunos países tomados como referencia.

España

Creación de un Cuerpo Especializado en Ciberdefensa

En la actualidad, Defensa estudia la creación de un cuerpo propio compuesto por expertos en ciberseguridad para proteger España en el ciberespacio, el cual pasaría de ser un Mando Conjunto del Ciberespacio a un Cuerpo Común.

Esto haría tener personal especializado de principio a fin de su carrera militar, con los beneficios que esto aporta. Además, los efectivos podrían ascender en el escalafón hasta llegar a general de división.

Por otra parte, la creación de un Cuerpo Común o cuarto Ejército permitiría captar a gente joven, nativos digitales. De esta forma se crearía un equipo de expertos permanentes para proteger a España en el ciberespacio.

Reserva Estratégica

El Mando Conjunto de Ciberdefensa es quien tiene la competencia para dirigir y coordinar las acciones de las Fuerzas Armadas en el ámbito de la ciberseguridad.

Con el fin de afrontar sus misiones cotidianas, las Fuerzas Armadas cuentan con un número de efectivo a los cuales se pueden sumar los reservistas: obligatorios y voluntarios.

Una de las actuaciones que podría requerir la intervención de una reserva de las Fuerzas Armadas como apoyar la labor de los efectivos de las distintas Administraciones Públicas sería un ataque cibernético calificado como situación de interés para la Seguridad Nacional.

Por ello, se propuso la creación de una reserva estratégica de talento en ciberseguridad que permita disponer de recursos humanos con los que reforzar los medios del Ministerio en apoyo de sus necesidades en cuanto a la ciberdefensa.

Sistema de Enlace en Caso de Emergencia

España cuenta con un sistema de emergencia tanto digitales como analógicos y a su vez, con una red tanto pública como privada.

Estos sistemas funcionan en forma coordinada con protección civil.

Sistema de Información de Emergencia (SIE). El SIE debe ser autorregulable y optimizable, es decir en permanente estado de adaptación al entorno de la organización de socorro en el que está instalado. La flexibilidad y facilidad de adaptación debe ser el punto fuerte de los sistemas de información para facilitar el flujo de información dentro de la organización.

Además, la información proporcionada por el sistema, debe cumplir con los siguientes requisitos ineludibles: veracidad, oportunidad, cantidad, relevancia, y debe ser completa.

Sistema de Integración Militar de Gestión de Emergencia (SIMGE). El SIMGE se diseñó sobre la base de las Operaciones Basadas en Efectos (EBAO) y una arquitectura orientada a servicios (SOA), con un protocolo estándar basado en servicios WEB denominado CESAR, que le permiten, a través de un nodo de interconexión entre la red WAN PG del Ministerio de Defensa y el mundo de Internet, interoperar y federarse con cualquier otro sistema de gestión de emergencias de otra organización.

Estonia

Este es un país que representa el paradigma de nación digital y consciente de la importancia estratégica que posee el ciberespacio para la seguridad nacional desde los sucesos de 2007.

Hace años que constituyó la Estonian Defence League Cyber Unit. Popularmente conocida como Cyber Defence League (CDL), esta unidad perteneciente a las Fuerzas Armadas cuenta con el apoyo y el soporte del Centro de Respuesta a Incidentes Informáticos del país (Estonian CERT). La CDL está compuesta por un conjunto heterogéneo de profesionales especialistas en ciberseguridad, ciberdefensa y operaciones de información, entre los que se hallan ingenieros, economistas, sociólogos, politólogos, psicólogos o abogados.

Francia

Recientemente se publicó en Francia la Revisión Estratégica de la Ciberdefensa, en la cual se indica que una de las prioridades es salvaguardar su soberanía digital. Por esta razón, la Ley de Programación Militar 2019/2025 prevé un incremento en el presupuesto para la lucha en el dominio cibernético.

Si bien el grueso se orientará a la industria de la ciberseguridad y ciberdefensa, como así también a la generación de ciber capacidades nacionales, una parte del presupuesto estará destinado a la remuneración, formación y adiestramiento de los futuros ciber reservistas. Se trabajó en un modelo de ciber reserva dual compuesto básicamente de dos modelos.

Por un lado, una reserva ciudadana con la misión de generar una cultura nacional de ciberseguridad y ciberdefensa mediante la formación y concienciación de todos los sectores – empresarial, académico o de usuario individual – de la sociedad civil del país;

Por el otro, na reserva operativa que tiene como objetivo asistir al Estado y a las FFAA en caso de que estalle una crisis cibernética importante. Sus integrantes colaborarían en la restauración de los sistemas atacados bajo la supervisión de especialistas del Ministerio de Defensa, el Ministerio del Interior o la Agencia Nacional de la Seguridad de los Sistemas de Información. Estas agencias también se encargarían de validar su acceso, proporcionar gratuitamente la formación complementaria y garantizar su alistamiento y preparación.

El gobierno pretende que, para 2019, Francia debía disponer de un cuerpo formado por 4.440 ciber reservistas organizados de la siguiente forma: 40 miembros permanentes, 400 pertenecientes a la reserva operativa (200 en territorio metropolitano y 200 en el extranjero) y 4.000 pertenecientes a la reserva ciudadana repartidos por todo el país.

Reino Unido de Gran Bretaña

En 2013, el Ministerio de Defensa británico anunció su interés por reclutar a varios centenares de expertos en ciberseguridad con el objetivo de constituir la Reserva Cibernética Conjunta o Joint Cyber Reserve Force, vinculada al Joint Forces Cyber Group de las Fuerzas Armadas.

Creada para proporcionar una "contribución esencial" a la seguridad nacional del país, esta unidad, eminentemente técnica y circunscrita al ámbito militar, está formada por individuos que abandonan la vida militar, miembros de la reserva activa e incluso sujetos sin experiencia militar previa y selecciona a sus miembros en base a sus conocimientos técnicos, habilidades, experiencia o aptitudes tecnológicas.

Aunque la misma jefatura de estado mayor de las FFAA reconoció que la ciber reserva debía ser un instrumento eminentemente civil y abrirse a otros ámbitos fuera del estrictamente tecnológico, en la actualidad ésta continúa teniendo una orientación militar y con un alcance limitado.

Así pues, la función principal de la Reserva Cibernética Conjunta es gestión y captura del talento bajo una óptica de habilidades técnicas y tácticas, sin dar peso a otras habilidades igualmente requeridas en el ámbito de la ciberdefensa, como podrían ser los conocimientos legales, políticos, estratégicos o psicológicos. Además, esta unidad circunscribe su ámbito de actuación a la protección de los activos del Ministerio de Defensa y las Fuerzas Armadas, dándole a la Reserva Cibernética Conjunta un alcance fundamentalmente militar.

Metodología

El método a emplear para desarrollar el trabajo de investigación será del tipo deductivo, con ciertas inferencias inductivas, para ello se realizarán distintos análisis y descripciones durante el desarrollo de cada capítulo a fin de obtener conclusiones parciales surgidas de cada uno de ellos y que permitan dar respuesta al objetivo general planteado por la investigación.

Capítulo 1

El SARE y SARA

Como se expresara en la introducción, en el presente capítulo se analizarán y las estructuras DEL SARE Y SARA con el objetivo de extraer conclusiones e identificar sus características distintivas como Servicios Auxiliares Independientes aplicables a la posible organización del SAEC.

Sección 1

El Sistema Auxiliar de Radioperadores del Ejército

Reglamentación

Por resolución del Jefe de Estado Mayor General del Ejercito de fecha 30 de noviembre de 1986, publicada en el BPE Nº 4547, se aprobó la directiva para el funcionamiento del Sistema Auxiliar de Radioaficionados del Ejercito (SARE) que asigna a la entonces Dirección de Comunicaciones la responsabilidad del control operacional y la de preparación e impartición de órdenes para la regularización y funcionamiento del Sistema.

Asimismo, el SARE debe cumplir con la siguiente documentación Rectora: Resolución E 3635/2017 del Ente Nacional de Comunicaciones (ENACOM); Ley Nacional de Telecomunicaciones Nro 19.798 y el Reglamento General de Radioaficionados.

Finalidad

Su finalidad es la de establecer redes radioeléctricas en apoyo de operaciones militares a desarrollar por la Fuerza Ejército dentro del marco de la Defensa Nacional.

Composición

El SARE está compuesto por personal especializado que se encarga de manejar y mantener la comunicación en apoyo a las operaciones militares.

Características

Conocimientos técnicos

Los radioperadores del ejército deben tener un profundo conocimiento de los principios de la radiocomunicación, así como de los equipos y tecnologías utilizadas en el campo.

Habilidades de comunicación

Es fundamental que los radioperadores sean capaces de comunicarse con claridad y precisión, transmitiendo información de manera efectiva tanto dentro del ejército como con otras unidades o fuerzas aliadas.

Capacidad para trabajar bajo presión

En situaciones de combate o emergencia, los radioperadores deben mantener la calma y la concentración para asegurar una comunicación eficiente, incluso en entornos hostiles o de elevados niveles de estrés.

Adaptabilidad y rapidez

Los radioperadores deben ser capaces de adaptarse rápidamente a diferentes situaciones y cambios en la comunicación, ajustando frecuencias, modos de transmisión y resolviendo problemas técnicos que puedan surgir.

Mantenimiento de equipos

Además de su función de comunicación, los radioperadores también deben ser capaces de realizar tareas de mantenimiento básico de los equipos de radio, asegurando su buen funcionamiento y disponibilidad en todo momento.

Trabajo en equipo

Los radioperadores suelen trabajar en estrecha colaboración con otros miembros del ejército, asumiendo responsabilidades conjuntas para garantizar una coordinación eficiente y segura de las comunicaciones.

Sección 2

El Servicio Auxiliar de Radioaficionados de la Armada

De acuerdo con lo descrito por Gaceta Marinera, el SARA, dependiente del Servicio de Comunicaciones Navales (SICO), fue creado el 21 de septiembre de 1961. El Servicio se inspiró en el Sistema de Radio Auxiliar Militar (MARS) de la Fuerza Aérea de los Estados Unidos. Al momento de su creación, la Estación Cabecera Buenos Aires (TB1) comenzó a funcionar en el Servicio de Hidrografía Naval; luego de numerosos traslados que incluyeron la Sede del Estado Mayor General de la Armada, desde 2015 se encuentra en el Centro Emisor Costanera Sur –que pertenece al SICO–.

En cada oportunidad se contó con la colaboración en la instalación y puesta en marcha de la estación de los radioaficionados voluntarios que lo integran, quienes además hacen guardias y cubren circuitos. Estos profesionales civiles de diferentes especificidades, junto a oficiales y suboficiales de la Armada, han logrado, a través de los años, volcar su experiencia adquirida en los radio clubes, colaborando en distintas ceremonias oficiales o celebraciones, representando a la Institución ante la comunidad de radioaficionados mundial, y conservando la tradición y su buen nombre.

Finalidad

Integrar a la Institución a aquellos radioaficionados que, con sus notables y valiosos servicios prestados a la comunidad, deseen sumarse voluntariamente y aportar aquello relacionado con las Radiocomunicaciones de interés para la Defensa Nacional.

Objetivo

El objetivo del SARA es participar en todas aquellas actividades relacionadas con las radiocomunicaciones que guarden vínculo con la Defensa Nacional, el cuidado de los recursos marítimos y la salvaguarda de la vida humana. Los radioaficionados remarcan que

más allá de tener sus obligaciones laborales, participar en este espacio de manera voluntaria es una manera de desarrollar su vocación de servicio.

Según lo expresado por Campoamor (2023) los integrantes del SARA “se nutren por la motivación de brindar apoyo, colaborando permanente con la preservación de la vida humana, desplegando sus enlaces y sus escuchas a lo largo de todo el litoral marítimo y continental de nuestro país. En estos 60 años de escucha participaron activamente para asegurar las comunicaciones vinculadas al bienestar de nuestros marinos; se destacan hitos y momentos históricos de mayor entrega y plena participación de sus integrantes. Evidencian un alto compromiso con la Institución y con los valores y tradiciones de la Armada Argentina”.

Características

Con adecuado entrenamiento y a requerimiento de la ARA, las estaciones del SARA pueden hacerse cargo del control de comunicaciones con estaciones del país y/o en el extranjero o móviles marítimos en los distintos modos de transmisión.

Las estaciones que integran el SARA llevan adelante numerosas actividades, la mayoría tienden a establecer un vínculo entre la sociedad civil y la ARA. Cabe mencionar: “llamadas de bienestar” entre la dotación de los buques y sus familiares; comunicaciones entre la Base Conjunta Antártica Orcadas y escuelas públicas; participación y apoyo en los casos SAR (Búsqueda y Rescate); entre otros.

Composición

Según detalla Luján (2023), actualmente el servicio cuenta con 26 integrantes militares –en actividad o retirados y de la Reserva Naval– y 75 integrantes voluntarios civiles, sumando un total de 101 integrantes radioaficionados distribuidos a lo largo de todo el país.

Conclusiones Parciales

En línea con la introducción del presente capítulo, se puede concluir que, en general, ambos servicios tienen una relación de apoyo directa con la misión de cada Fuerza ya sea que la misma se encuentre en operaciones, en emergencias o en tiempos de paz.

Asimismo, están compuestos por personal con un grado de especificidad considerable en lo que respecta a las técnicas radioeléctricas, sean estos civiles, reservistas, personal en situación de retiro o inclusive en actividad.

En ambos tipos de servicios, este personal se presenta en carácter voluntario para el cumplimiento de las tareas mencionadas en su finalidad y objetivo.

Teniendo en cuenta este capítulo y lo detallado en el marco teórico, también se puede concluir, parcial e inicialmente, que sería preciso que, en vistas hacia un SAEC, el personal que lo integre deberá ser reservista, de manera tal de cumplir las tareas con un mayor nivel de eficacia y con el grado de reserva que se precisa, a pesar que el trabajo sea remoto.

Capítulo 2

El Servicio Auxiliar de Especialistas Ciber y sus Ventajas

En este capítulo se describirán las ventajas de contar con un SAEC para el Estado Argentino que permita un apoyo permanente a las actividades de las FFAA en el quinto dominio.

Para ello, en una primera sección se esbozan las principales características y la posible estructura del mencionado servicio, siendo dicha descripción meramente teórica, inicial y optimizable, aspectos que pueden constituir un nuevo trabajo de investigación.

En la segunda sección se describirán las ventajas más relevantes, a criterio de los integrantes del Equipo, de contar con el mencionado SAEC, entendiendo que las mismas constituyen parte esencial del presente trabajo ya que forman parte de la solución al problema planteado.

Sección 1

Estructura y Características del SAEC

Estructura

Compatible con la distribución de la Red Técnica de Oficiales de Ciberdefensa, y sus Auxiliares, de acuerdo al despliegue territorial del Sistema Fijo del EA, el SAEC podría complementar el mismo desde sus cabeceras.

De manera tal de mantener el principio de unidad de comando, esta organización dependería orgánicamente de las DDC, en coordinación con el COCOCIBER, quien tiene canal técnico con la Subsecretaría de Ciberdefensa de la Nación, elemento que deberá interpelar al momento de proteger una IC que el poder ejecutivo ordene.

Composición Propuesta

Un servicio auxiliar especializado en ciberdefensa deberá estar compuesto de profesionales para diferentes áreas y equipos que trabajen de manera coordinada para garantizar la protección de las IICC y los AACC de las FFAA frente a posibles ciberataques.

Algunas de las áreas que pueden formar parte de este servicio son:

Equipo de Monitoreo de Seguridad

Este equipo se encarga de vigilar constantemente los sistemas de la organización, detectando cualquier actividad sospechosa o anómala que pudiera indicar un posible ataque.

Equipo de Respuesta a Incidentes

Este equipo es el encargado de actuar rápidamente ante cualquier incidente de seguridad, identificando el origen del problema y tomando las medidas necesarias para contenerlo y solucionarlo.

Equipo de Análisis de Riesgos

Este equipo se encarga de analizar las vulnerabilidades de los sistemas de la organización y de proponer medidas para mitigar los riesgos asociados a ellas.

Equipo de Pruebas de Penetración

Este equipo realiza pruebas de penetración para evaluar la capacidad de la organización para resistir posibles ataques externos o internos.

Equipo de Seguridad Física

Este equipo se encarga de garantizar la seguridad física de los equipos y sistemas de la organización, así como de controlar el acceso a las instalaciones y a los datos críticos.

Equipo de formación y concienciación de seguridad

Este equipo se encarga de mejorar la cultura de seguridad dentro de la organización, impartiendo formaciones y promoviendo buenas prácticas de seguridad entre los empleados.

Sección 2

Ventajas de contar con el SAEC

Una de las ventajas se refiere a que se puede contar con personas que han sido instruidas desde diferentes ámbitos, concluyendo con el castrense, lo que permitirá disponer de recursos humanos para reforzar los medios de las FFAA en apoyo de sus necesidades en cuanto a ciberdefensa.

Este servicio contara con un efectivo de reservistas y serán capaces de detectar cualquier posible fallo del sistema informático o ataque malicioso que pueda poner en riesgo la información, software o datos propios o de terceros.

Mientras están en apresto y cuando la institución no requiera sus servicios realizaran tareas de prevención ante la posibilidad de recibir un ataque cibernético, en la cual ayudaría a reaccionar rápidamente ante un ciberataque, corregirlo y responder de forma temprana a cualquier incidente de seguridad de la información.

Así mismo, es necesario destacar que en la actualidad las empresas que adquieren estos tipos de servicios acceden contratando a terceros sometiéndose a mantener un intercambio de información considerable con la empresa subcontratada y aceptar el riesgo de que, si la empresa tercerizada sufre una caída temporal o permanente de sus infraestructuras, esto afectara directamente a la empresa que ha subcontratado sus servicios.

Al contar con un SAEC, las instituciones del Estado Argentino no estarán expuestas a esas situaciones dado que por su naturaleza el servicio auxiliar garantiza permanencia en la estructura por formar parte de las fuerzas armadas en virtud de contar con un efectivo de reservistas.

Evitaría la rotación del personal en la cual incentiva la fuga de talentos y la reducción del efectivo capacitado para las tareas de competencia en ciberdefensa.

Conclusiones Finales

Como corolario del presente trabajo integrador y de investigación, se puede concluir que, en línea con lo expresado en el marco teórico, es necesario como Estado Nación que pretende proteger su soberanía digital, contar con un servicio auxiliar integrado por especialistas de diferentes perfiles profesionales tal como en su momento se decidió contar con el SARE y SARA.

Se concluye también que en principio deberían estar compuestos por personal con un grado de especificidad que pueda demostrarse de acuerdo a diferentes pruebas de ingreso.

Para cumplir con un formalismo acorde a los reglamentos militares y el marco legal actual, este personal deberá ser incorporado como Reservistas integrando fracciones desplegadas territorialmente a lo largo del país en las diferentes Compañías de Reserva.

Finalmente, este servicio contribuye a captar personal calificado y evitar la fuga definitiva de talentos especializados en el ambiente cibernético, asimismo, facilita el mantener efectivos formados en la defensa de las IICC y AACC de las FFAA y de la Nación.

Referencias

Arreola A. (2020). *Ciberespacio: quinto dominio de la guerra*. https://www.researchgate.net/publication/340819837_Ciberespacio_quinto_dominio_de_la_guerra.

Arroyo de la Rosa R. (2015). *El Enlace en las emergencias: fuerte y claro*. [Archivo PDF]. Secretaría General Técnica. Ministerio del Interior.

Centro de Racioaficionados Ciudad de Buenos Aires. *Sistema Auxiliar Radioperadores del Ejército*. https://www.lu5cba.org.ar/sistema-auxiliar-radioperadores-del-ejercito

ECD Confidencial Digital. *Defensa estudia crear un cuerpo propio de militares expertos en ciberdefensa*. https://www.elconfidencialdigital.com/articulo/defensa/defensa-estudia-crear-cuerpo-propio-militares-expertos-ciberdefensa/20211104170230299787.html

ENACOM. Ente Nacional de Comunicaciones. *Listado de Radioaficionados*. https://www.enacom.gob.ar/listado-de-radioaficionados_p316

Gaceta Marinera. Portal Oficial de Noticias de la Armada Argentina. El Servicio Auxiliar de Radioaficionados de la Armada cumple 60 años. https://gacetamarinera.com.ar/especiales/el-servicio-auxiliar-de-radioaficionados-de-la-armada-cumple-60-anos/

Radio Club Argentino. Sociedad Nacional. *Sistema Auxiliar de Radioperadores del Ejército*. https://www.lu4aa.org/wp/sare-rae2d/

Real Instituto Elcano Royal Instituto (2014). *Abriendo el debate sobre el ciber-reservismo*. https://www.realinstitutoelcano.org/blog/abriendo-el-debate-sobre-el-ciber-reservismo/

Reale J (2023). Los desafíos de la ciberguerra y la importancia de fortalecer la inteligencia estratégica militar en la Argentina. *Revista de la Escuela Nacional de Inteligencia · Número 2.*

Resolución N° 385 de 2013 (Ministerio de Defensa). Por la cual se establece la creación de las Direcciones de Ciberdefensa de las Fuerzas Armadas. 22 de octubre de 2013.

Resolución N° 343/2014 (Ministerio de Defensa). Por la cual se establece la creación de la Unidad de Coordinación Cibernética; y las Direcciones de Ciberdefensa del Ejército Argentino, de la Armada de la República Argentina y de la Fuerza Aérea Argentina. 14 de mayo de 2014.

S.A.R.A. Servicio Auxiliar de Radioaficionados. *Nuestro Servicio*. https://www.sara.ara.mil.ar/about.html

Thiber. The Cibersecurity Think Tank (2015). *Thiber Report Nº1: La necesidad de un Programa Nacional de Ciber - Reserva*. [Archivo PDF]. chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.thiber.org/wp-content/uploads/2018/03/Thiber-Report-N1-V3.pdf