Facultad del Ejército
Escuela Superior de Guerra
"Tte Grl Luis María Campos"

TRABAJO FINAL INTEGRADOR

Título: "El Estado de Ciberseguridad de los sistemas informáticos logísticos del Ejército Argentino y su influencia en el sostenimiento de la Fuerza en operaciones".

Que para acceder al título de Especialista en Planificación y Gestión de RRMM de OOMMTT presenta el Mayor DAVID ALBERTO NARVAEZ.

Director de TFI: Teniente Coronel Aníbal Exequiel RODRIGUEZ.

Ciudad Autónoma de Buenos Aires, 22 de enero de 2024.

Resumen o Abstract

El presente trabajo aborda el estado de ciberseguridad en los sistemas informáticos logísticos del Ejército Argentino, y de qué manera su vulnerabilidad podría afectar al sostenimiento de la fuerza, ya sea en la paz o en operaciones.

Con este propósito, en una primera parte se analizan los antecedentes de cómo han sido afectados los sistemas logísticos en el ámbito civil, seguida de una segunda parte, la cual consta de un análisis de los sistemas informáticos civiles y los empleados en la fuerza, la influencia de la ciberseguridad en el sostenimiento y una comparación con la ciberseguridad de otras fuerzas armadas, finalmente una tercera parte en la que se indaga sobre las acciones y perspectiva futura en materia de ciberseguridad en el ámbito de la fuerza.

El marco referencial teórico considerado es la doctrina básica específica vigente en nuestra fuerza, como así también aquellos documentos legales publicados por el Ministerio de Defensa de la República Argentina, antecedentes y otros artículos relacionados directamente con la logística y la ciberdefensa.

La ciberdefensa en los últimos años se ha posicionado en el mundo como un desafío permanente para aquellas naciones que intentan proteger y conservar su espacio cibernético lo más seguro y confiable posible, aplicando ciertos principios, a fin de lograr la libertad de acción adecuada, buscando un grado de iniciativa y sostenimiento, que permita al comandante conducir las operaciones en el campo de combate.

Palabras Clave

Ciberespacio- Ciberseguridad- Logística- Operaciones- Sostenimiento

Índice

Glosario

Dado que el área de ciberdefensa posee un vocabulario específico y se utilizan términos que no son de uso frecuente, para la presente investigación se ha desarrollado un glosario, el cual se confeccionó con definiciones de diversas fuentes, y se detalla a continuación.

Adware. Es un software no deseado diseñado para mostrar anuncios en su pantalla, normalmente en un explorador. es un precursor de los Programas Potencialmente No Deseados (PUP) de hoy en día, también supervisa su comportamiento online para ofrecerle anuncios específicos. (Dirección de Educación Operacional. Escuela de Comunicaciones, 2022).

Antivirus. Es un programa informático específicamente diseñado para detectar, bloquear y eliminar código malicioso (troyanos, gusanos, etc. así como proteger los equipos de otros programas peligrosos). (Escuela Superior de Guerra, 2022).

Armas cibernéticas o ciberarmas. Es una acción cibernética destinada a realizar funciones ofensivas o defensivas que se materialicen en un ataque y tengan por finalidad un daño intencional, con resultado de destrucción de las cosas, violencia en las personas, disfuncionalidad o disrupción, temporal o permanente, de redes, sistemas, equipos, funciones, servicios o instalaciones, o atente contra intereses, derechos o libertades. (Dirección de Educación Operacional. Escuela de Comunicaciones, 2022).

Bases de datos. Hace referencia a una gran cantidad de información que ha sido sistematizada para su correcto almacenamiento, de forma tal que los datos que allí están contenidos puedan ser utilizados cuando se considere necesario, pudiendo ser posteriormente ordenados u organizados. (Escuela Superior de Guerra, 2022).

Cadena de suministros (SCM). Se refiere a las herramientas y métodos cuyo propósito es mejorar y automatizar el suministro a través de la reducción de las existencias y los plazos de entrega. (Escuela Superior de Guerra, 2022).

Ciberamenaza. Amenaza a los sistemas y servicios presentes en el ciberespacio o alcanzables a través de éste. (Escuela Superior de Guerra, 2022).

Ciberataque. Acción producida en el ciberespacio que compromete la disponibilidad, integridad y confidencialidad de la información mediante el acceso no autorizado, la modificación, degradación o destrucción de los sistemas de información y telecomunicaciones o las infraestructuras que los soportan. (Escuela Superior de Guerra, 2022).

Ciberdefensa. Conjunto de acciones que se desarrollan en el ciberespacio para prevenir, detectar, identificar, anular, impedir, evitar, contrarrestar, contener o repeler una amenaza o agresión cibernética, sea esta inmediata, latente o potencial, a fin de permitir el empleo del Instrumento Militar de la Nación. (Escuela Superior de Guerra, 2022).

Ciberguerra. La ciberguerra o guerra tecnológica hace referencia al uso de ataques digitales por parte de un país para dañar los sistemas informáticos más esenciales de otro país. Tiene como objetivo encontrar vulnerabilidades técnicas y tecnológicas en los sistemas informáticos del enemigo para atacarlas. La ciberguerra es llevada a cabo por hackers que ataquen las infraestructuras críticas del enemigo a través de medios tecnológicos. (Escuela Superior de Guerra, 2022).

Ciberespacio. Es el ambiente complejo que resulta de la interacción de personas, software, y servicios en internet por medio de dispositivos y redes conectadas. No posee existencia física, sino que es un dominio virtual que engloba todos los sistemas. (Dirección de Educación Operacional. Escuela de Comunicaciones, 2022).

Ciberesiliencia. Es la capacidad que tiene una organización de recuperarse rápidamente tras haber sido víctimas de un ataque por parte de ciberdelincuentes. Su objetivo es disminuir los impactos y las consecuencias negativas que estos puedan traer para la organización, como, por ejemplo, interrupciones en la operación o prestación de servicios, afectaciones económicas,

daños a la reputación, a la infraestructura e incluso, afectación a la continuidad de esta. (Mónica Maria Jimenez, 2022).

Ciberseguridad. Es la preservación de la confidencialidad, integridad y disponibilidad de la información en el ciberespacio. (Escuela Superior de Guerra, 2022)

Firewall o cortafuegos. Son sistemas de seguridad compuesto o bien de programas software o de dispositivos hardware situados en los puntos limítrofes de una red que tienen el objetivo de permitir y limitar el flujo de tráfico entre los diferentes ámbitos que protege sobre la base de un conjunto de normas y otros criterios La funcionalidad básica es asegurar que todas las comunicaciones entre la red e Internet se realicen conforme a las políticas de seguridad de la organización o corporación Estos sistemas suelen poseer características de privacidad y autentificación. (Escuela Superior de Guerra, 2022).

Función de sostenimiento. Es la función relacionada con las tareas, sistemas e infraestructura que proveen el sostén y los servicios para asegurar la libertad de acción, extender el alcance operacional y prolongar la resistencia de las fuerzas terrestres.

Incluye a todos los subsistemas, medios y personal necesarios para sostener a las fuerzas terrestres, sea en sus asientos de paz, en su movimiento hacia la Zona de Combate y durante las operaciones militares. (Escuela Superior de Guerra, 2022).

Herramientas informáticas. Es un software, programa o solución digital que facilita y mejora la eficiencia de todo el proceso de la cadena de suministros. (Escuela Superior de Guerra, 2022).

Infraestructuras críticas. Son aquellas que resultan indispensables para el adecuado funcionamiento de los servicios esenciales de la sociedad, la salud, la seguridad, la defensa, el bienestar social, la economía y el funcionamiento efectivo del Estado, cuya destrucción o perturbación, total o parcial, los afecte y/o impacte significativamente. (Dirección de Educación Operacional. Escuela de Comunicaciones, 2022).

Infraestructuras críticas de información. Son tecnologías de información, operación y comunicación, así como la información asociada, que resultan vitales para el funcionamiento o la seguridad de las infraestructuras críticas. (Escuela Superior de Guerra, 2022).

Ingeniería social. Conjunto de técnicas psicológicas y habilidades sociales (tales como: la influencia, la persuasión y la sugestión). Busca directa o indirectamente que un usuario revele información sensible, sin estar consciente de los riesgos que esto implica. Es bastante similar al hacking normal, con la única diferencia que no se interactúa con una máquina, sino con una persona, puede estar basada en computadoras o en contacto humano. (Dirección de Educación Operacional. Escuela de Comunicaciones, 2022)

Logística. Es el conjunto de actividades destinadas a brindar sostén a las fuerzas, proporcionando recursos con la aptitud adecuada, en cantidad, calidad, tiempo y lugar oportuno. Incluye el apoyo logístico de personal, de material, de finanzas y de asuntos territoriales. (Ejército Argentino, 2004).

Malware. O "software malicioso" es un término amplio que describe cualquier programa o código malicioso que es dañino para los sistemas. El malware hostil, intrusivo e intencionadamente desagradable intenta invadir, dañar o deshabilitar ordenadores, sistemas informáticos, redes, tabletas y dispositivos móviles. (Dirección de Educación Operacional. Escuela de Comunicaciones, 2022).

Phishing o suplantación de identidad. Los autores del phishing no tratan de explotar una vulnerabilidad técnica en el sistema operativo de su dispositivo, sino que utilizan ingeniería social, es la forma más sencilla de ciberataque y, al mismo tiempo, la más peligrosa y efectiva. (Dirección de Educación Operacional. Escuela de Comunicaciones, 2022).

Ransomware. El malware de rescate o ransomware, es un tipo de malware que impide a los usuarios acceder a su sistema o a sus archivos personales y que exige el pago de un rescate

para poder acceder de nuevo a ellos. (Dirección de Educación Operacional. Escuela de Comunicaciones, 2022).

Sistemas de información logística. Los sistemas de información logística son soluciones digitales que se encargan de extraer y procesar información de distintas actividades logísticas para facilitar la toma de decisiones, la resolución de problemas, la planificación estratégica y la gestión de la cadena de suministro, ya sea en su totalidad o solo en algunas de sus etapas (aprovisionamiento, almacenamiento, despacho, distribución, transporte, etc.). (Escuela Superior de Guerra, 2022).

Sistemas de informática y comunicaciones. Son todas aquellas herramientas y programas que tratan, administran, transmiten y comparten la información mediante soportes tecnológicos. (Escuela Superior de Guerra, 2022).

Spyware. Es un término genérico para denominar al software malicioso que infecta su ordenador o dispositivo móvil y recopila información sobre usted, su navegación y su uso habitual de Internet, así como otros datos. (Dirección de Educación Operacional. Escuela de Comunicaciones, 2022).

Tecnologías de la información y la comunicación (TIC). Son el conjunto de tecnologías desarrolladas en la actualidad para una información y comunicación más eficiente, las cuales han modificado tanto la forma de acceder al conocimiento como las relaciones humanas. (Caterina Chen, 2022)

Troyano. Los ataques de tipo caballo de Troya, o simplemente troyanos, utilizan el engaño y la ingeniería social para engañar a los usuarios desprevenidos y hacer que ejecuten programas aparentemente inofensivos que ocultan una carga maliciosa. (Dirección de Educación Operacional. Escuela de Comunicaciones, 2022).

Introducción

Presentación del Problema.

En relación con el tema.

El presente trabajo de investigación se vincula con las Materias Apreciación de Situación de Materiales. Gestión en Recursos Materiales y Operaciones Logísticas de Material.

Tema específico de investigación.

El Estado de Ciberseguridad de los sistemas informáticos logísticos del Ejército Argentino y su influencia en sostenimiento de la Fuerza en operaciones.

Sobre el problema a investigar.

Planteo del problema.

De acuerdo a la Directiva del Subjefe del Estado Mayor del Ejército Nº 829-21 Directiva Anual de Ciberdefensa, para realizar un ciberataque no es necesario desplazarse, moverse o tener que pasar una frontera, ya que en el ciberespacio no hay límites, es anónimo y asimétrico.

Las amenazas cibernéticas están consideradas como uno de los principales riesgos por la alta probabilidad de que ocurran y por el impacto que podrían tener. Existen variados y constantes intentos de intrusión en los sistemas, que el hombre común no ve y que incluso a veces al especialista también le cuesta ver, como así también hay amenazas muy sofisticadas que se caracterizan por el sigilo.

Actualmente tampoco es necesario tener grandes conocimientos técnicos para agredir los sistemas de información, ya que hasta en internet se pueden encontrar gran cantidad de herramientas ofensivas y observar el intercambio de instrumentos de hacking en foros dedicados a esta materia.

Por lo expresado, resulta necesario considerar que es de vital importancia, tener en cuenta la importancia de la ciberseguridad en los sistemas informáticos logísticos, los antecedentes e incidentes ocurridos en el ámbito civiles los cuales afectaron las cadenas

logísticas y tomado como referencia estos hechos, apreciar de qué manera puede afectar al sostenimiento logístico del Ejército Argentino en los diferentes escenarios en los que actúe, sea en la paz o en operaciones.

Antecedentes.

En el año 2021 la Comisión Económica para América Latina (CEPAL) realizó un informe respecto al Estado de ciberseguridad en la logística de América Latina y el Caribe en el ámbito civil y de qué manera se vieron afectadas las cadenas logísticas.

Desde el año 2020 el Ejército Argentino, a través del Programa Anual de Carreras y Cursos (PACC) y en coordinación con la Dirección de Educación Operacional (DEOP), se designó a la Escuela de Comunicaciones para que programe e imparta el Curso Básico y Avanzado de Ciberdefensa, al personal del Arma de Comunicaciones, curso que continúa siendo impartido hasta el día de la fecha.

Relacionado con la doctrina del Arma de Comunicaciones, se inició la actualización de los reglamentos que actualmente se encuentran en uso, incorporando el área de ciberdefensa dentro de las Unidades y Subunidades del Arma.

Así también la empresa Cuatro Ochenta (Entidad española especialista en ciberseguridad) publicó un artículo en referencia a lo ocurrido durante el año 2020, en el cual el área de logística y transporte ocuparon el tercer lugar en importancia en lo que se refiere a ciberataques.

También se puede mencionar que la Escuela Superior de Guerra (ESG) impartió un seminario sobre ciberseguridad, ciberguerra y ciberespacio, tomando como centro de gravedad los acontecimientos ocurridos entre la guerra entre Rusia y Ucrania.

Otro aspecto a tener en cuenta en lo relacionado con la pandemia, lo cual incrementó un mayor uso de la informática, internet, el comercio electrónico y obligó a las diferentes organizaciones a que sus empleados ejecuten su actividad laboral desde sus hogares. Esto

provocó una saturación de los servicios de internet, como así también género que las organizaciones como usuarios individuales se vieran más propensos a ser víctimas de ciberataques, al no tener los conocimientos básicos de seguridad informática que les brinde una adecuada protección contra los ciberataques y robo de información de importancia.

Relacionado a la situación actual, existe falta de conciencia en seguridad informática en gran parte del personal, lo que a veces dificulta tomar medidas eficaces, y teniendo en cuenta que en los conflictos actuales como ser el caso de Ucrania, las primeras operaciones se realizaron en el ámbito del ciberespacio.

Delimitación del problema.

En el presente trabajo se buscará analizar particularmente el estado actual de ciberseguridad de los sistemas informáticos logísticos del Ejército Argentino y de qué manera pueden afectar el sostenimiento logístico de la fuerza tanto en la paz como en operaciones tomando como antecedentes los incidentes ocurridos en la logística del ámbito civil.

Primeros elementos surgidos del rastreo bibliográfico.

Los sistemas informáticos logísticos son herramientas digitales que se encargan de extraer y procesar información de distintas actividades logísticas para facilitar la toma de decisiones, la resolución de problemas y otras actividades que, permiten dar velocidad y rapidez al manejo de la información, poseen vulnerabilidades que pueden perjudicar a las cadenas logísticas, tanto en el ámbito civil como en el militar. (Escuela Superior de Guerra, 2022)

Si se aplican estos sistemas informáticos al ámbito militar, y teniendo en cuenta los nuevos escenarios en los conflictos actuales, donde ha surgido una nueva dimensión en el combate moderno (el ciberespacio), ya no solamente existen los enfrentamientos en el terreno, sino también que se busca el dominio del este, incluso antes del inicio de las hostilidades.

Por ello, es necesario tratar la temática de la ciberseguridad y su relación con la logística, teniendo en cuenta unos de los criterios básicos para el sistema logístico cuyo enunciado es

“Máximo empleo de las herramientas informáticas” (Logística de Material - ROD-19-02, 2004) y de qué manera puede influir un ciberataque en el sostenimiento logístico de la fuerza, ya sea en la paz o durante el desarrollo de operaciones de naturaleza variable.

Objetivos del Trabajo Final Integrador.

Objetivo general. Determinar el estado de ciberseguridad de los sistemas informáticos logísticos del Ejército Argentino y de qué manera puede influir para el desarrollo del sostenimiento logístico en operaciones

Objetivo Específico N.º 1. Describir el marco legal y los aspectos doctrinarios relacionados con la ciberseguridad de los sistemas informáticos logísticos del Ejército Argentino, antecedentes y su relación con los incidentes ocurridos en la logística en el ámbito civil.

Objetivo Específico N.º 2: Comparar y analizar el estado de ciberseguridad de los sistemas informáticos logísticos del Ejército Argentino desde el año 2020, en su asiento de paz y su relación con el sostenimiento logístico en operaciones.

Objetivo Específico N.º 3. Evaluar y analizar qué acciones y perspectivas se están llevando a cabo actualmente en los sistemas informáticos logísticos de la fuerza en la paz y si estas acciones evitarían que el sostenimiento logístico se vea afectado en operaciones.

CAPÍTULO I. Antecedentes y descripción de aspectos relacionados con la ciberseguridad en el Ejército Argentino

Introducción

En el presente capítulo se busca describir el marco legal y los aspectos doctrinarios relacionados con la ciberseguridad de los sistemas informáticos logísticos del Ejército Argentino, antecedentes y su relación con los incidentes ocurridos en la logística en el ámbito civil. Se hará referencia al marco jurídico en nuestro país, incidentes que afectaron las cadenas logísticas en el contexto civil, la situación actual en Argentina y el estado de la doctrina vigente.

Sección I. Antecedentes en Latinoamérica y marco legal argentino

Para iniciar con el presente capítulo, en lo que respecta a documentos relacionados con operaciones en el ciberespacio, se puede hacer mención a lo siguiente:

> El Convenio de Budapest que se firmó el 23 de noviembre de 2001 y entró en vigencia el 1° de julio de 2004, en la ciudad de Budapest, República de Hungría, siendo este el primer tratado internacional creado con el objetivo de proteger a la sociedad frente a los delitos informáticos y los delitos en Internet, mediante la elaboración de leyes adecuadas, la mejora de las técnicas de investigación y el aumento de la cooperación internacional, inicialmente en el marco de la Unión Europea, y posteriormente extendiéndose al resto del planeta, para la creación de las leyes nacionales de protección contra el ciberdelito. En la actualidad, el Convenio ha sido ratificado por más de 50 naciones de todo el mundo y en particular en lo que respecta a Latinoamérica forman parte de este convenio, Argentina, Chile, Colombia, Costa Rica, Panamá, Paraguay, Perú y República Dominicana. (Diaz, 2021, pág. 9)
>
> La pandemia reciente, afectó la producción, las exportaciones e importaciones, no solamente de América Latina y el Caribe, sino en el resto del mundo. Al

mismo tiempo que este fenómeno se transformó en un impulsor de la digitalización, acelerando el proceso de transición y logrando así, mantener las operaciones durante el aislamiento, reduciendo la interacción entre las personas. Para lograr mantener la base operativa, las organizaciones han abierto filiales virtuales en los hogares para continuar el trabajo en modalidad home office. (Diaz, 2021, pág. 5)

El COVID-19 dio un impulso importante al proceso de transformación digital, acelerando los tiempos de adopción y aumentando las escalas, respondiendo a la necesidad de mantener a las organizaciones en operación durante el aislamiento ocurrido a partir del mes de marzo 2020 en el mundo, en algunos casos, y en otros, ha permitido continuar operando bajo protocolos estrictos, con el fin de reducir los contagios. Pero además de los cambios que se han experimentado durante estos meses, se está observando un cambio estratégico en las organizaciones respecto a la tecnología. (Diaz, 2021, pág. 8)

En este contexto, las amenazas a la ciberseguridad preexistentes ya son una realidad. Desde el inicio de la pandemia, además de los problemas operativos de los centros logísticos, los ciberataques fueron en aumento y las actividades logísticas siguen estando entre los sectores económicos más afectados. La evidencia muestra un incremento de los ciberataques en los últimos años, a pesar de no contar con toda la información sobre la infraestructura crítica, y las cadenas logísticas. (Diaz, 2021, pág. 5)

Este escenario emergente encontró a diferentes países del mundo con diferentes grados de maduración en ciberdefensa, registrándose este efecto tanto en el ámbito privado como público. Es de destacar que el fenómeno de la cibercriminalidad impone en las comunidades un proceso complejo que nace con

> la toma de conciencia ante la evidencia contundente del alcance y poder de daño de los ciberataques. Para dar tratamiento orgánico a esta problemática, en el año 2018 la Unión Internacional de Telecomunicaciones (UIT), división de Naciones Unidas, en conjunto con otras organizaciones, redactaron la "Guía para la elaboración de una estrategia nacional de ciberseguridad" donde se define el rol del estado en la elaboración de una Estrategia Nacional de Ciberseguridad (NCS por sus siglas en inglés). (Diaz, 2021, pág. 9)

El marco legal y las políticas de seguridad de las operaciones en el ciberespacio en nuestro país. Dentro de la legislación de la República Argentina existe una marcada diferencia entre lo que es la Defensa Nacional y la Seguridad Interior, según las siguientes leyes: la ley 23.554 y la ley 24.059, las cuales marcan lo siguiente:

> Estas leyes sirvieron para dar los lineamientos básicos para la formulación de la Directiva Estrategia de Ciberseguridad, la cual es de particular interés para esta investigación. El concepto de seguridad nacional, que la mayoría de los países del mundo, emplea de manera integrada, no se aplica de la misma manera en nuestro país. Este aspecto adquiere suma importancia cuando se requieren determinar los aspectos jurídicos, debido a las características particulares de la actividad, sumando a esto, las operaciones que se ejecutan en el ciberespacio. (Cabrera, 2019, pág. 6)

Ley de Defensa Nacional 23.554. La Ley 23.554, promulgada en el año 1988, establece "las bases jurídicas, orgánicas y funcionales para la preparación, ejecución y control de la defensa nacional". (Cabrera, 2019). La mencionada ley menciona que:

> En su artículo 2, la ley establece claramente que "la defensa nacional es la integración de la acción coordinada de todas las fuerzas de la Nación para la solución de aquellos conflictos que requieren el empleo de las Fuerzas Armadas,

> en forma disuasiva o efectiva para enfrentar las agresiones de origen externo. Tiene por finalidad garantizar de modo permanente la soberanía e independencia de la Nación Argentina, su integridad territorial y capacidad de autodeterminación; proteger la vida y libertad de sus habitantes". (Honorable Congreso de la Nación, 1988, pág. 1)

Así también, el artículo 4 de esta ley establece que:

> Para dilucidar las cuestiones pertinentes a la defensa nacional, se deberá tener permanentemente en cuenta la diferencia fundamental que separa la defensa nacional de la seguridad interior, y que, por lo tanto, la seguridad interior será regida por una ley especial (Honorable Congreso de la Nación, 1988, pág. 1)

Esta ley, en el artículo 5, define que:

> La defensa nacional abarca los espacios continentales, Islas Malvinas, Georgias y Sándwich del Sur, y demás espacios insulares, marítimos y aéreos de la República Argentina", así como el sector antártico argentino, con los alcances asignados por las normas internacionales, y los tratados suscritos o por suscribir por la Nación esto sin perjuicio de lo dispuesto por el artículo 28. (Honorable Congreso de la Nación, 1988)

Por su parte el artículo 28 de dicha ley, establece que para el caso de guerra o conflicto armado internacional "el Presidente de la Nación podrá establecer teatros de operaciones, delimitando las correspondientes áreas geográficas" (Honorable Congreso de la Nación, 1988, pág. 1)

De la ley anteriormente mencionada, es de particular interés, el concepto de:

> Un espacio definido, con límites geográficos, comprendidos dentro de un teatro de operaciones, los cuales tendrán una clara incidencia a la hora de determinar los efectos de las ciberoperaciones que ejecute nuestro sistema de ciberdefensa

> y de qué manera puede verse afectado el sostenimiento logístico. (Cabrera, 2019, pág. 7)

Decreto 703/2018. Directiva Política de Defensa Nacional (DPDN). Este decreto ha originado modificaciones en las políticas de defensa nacional las cuales se mencionan a continuación.

> Los cambios que enfrenta la Defensa de la República Argentina, provocaron la necesidad de la creación y posterior aprobación de una nueva Directiva de Política de Defensa Nacional (DPDN) que se adapte a las amenazas que afectan a los estados en la actualidad. En este marco, la República Argentina debe desarrollar la capacidad para anticiparse, disuadir y superar cualquier riesgo o amenaza que afecten la seguridad de sus infraestructuras críticas las cuales son el principal blanco para la ejecución de ciberataques. (Cabrera, 2019, págs. 7-8)
>
> En lo que respecta al ciberespacio el desarrollo tecnológico incrementó los riesgos vinculados con organizaciones militares. La disuasión se ha extendido al ámbito cibernético, donde no solo los estados cobran gran importancia en su desarrollo sino también diferentes entes privados y organizaciones están desarrollando capacidades en este espacio. Por tal razón, diariamente surgen nuevos desafíos producto de la existencia y evolución hacia una mayor conectividad, alterando la privacidad y los derechos de la ciudadanía. (Cabrera, 2019, pág. 8)
>
> Es por eso que, tanto los estados como los actores no estatales diseñan y crean medios cibernéticos para explotar las vulnerabilidades vinculadas a los sistemas de comando, control, comunicaciones, computadoras, inteligencia, vigilancia, reconocimiento y logística entre otros, tanto de organizaciones militares como civiles. De igual forma, las redes empleadas por entidades terroristas explotan el

ciberespacio para reclutar miembros, recaudar fondos y difundir su propaganda. (Cabrera, 2019, pág. 24)

El ciberespacio es un ambiente donde prevalece el anonimato, sin embargo, las amenazas cibernéticas, pueden ser originadas desde organizaciones militares y agencias de inteligencia de otros estados. De esta manera los estados con mayor desarrollo tecnológico, explotan sus ventajas en comparación con el resto de los países, mediante el desarrollo de ciberoperaciones, las cuales también están al alcance de actores secundarios o con tecnología y capacidades menos desarrolladas. Esta problemática requiere adoptar medidas para armar sistemas lo suficientemente seguros y resilientes en lo que respecta a la ciberseguridad, permitiendo de esta manera neutralizar cualquier amenaza o riesgo que atente contra nuestras infraestructuras críticas y la información de ellas por medio de la Defensa Nacional. (Cabrera, 2019, págs. 8-9)

Por tal razón el sistema de Defensa Nacional debe orientar sus esfuerzos a generar las capacidades que permitan proteger de manera eficiente los objetivos estratégicos e infraestructuras críticas que puedan ser objeto de una agresión de origen externo. Además, se debe contemplar lo que establece el marco jurídico vigente con respecto a los ciudadanos argentinos y bienes nacionales en el exterior. (Cabrera, 2019, pág. 9)

El ciberespacio se ha instalado como un dominio que cruza transversalmente a los otros dominios, por tal razón configura una amenaza de interés estratégico para la defensa nacional. Por esto, las fuerzas armadas, como parte integrante del Ministerio de Defensa deben desarrollar capacidades que permitan fortalecer las capacidades de vigilancia y control del ciberespacio. Esto permite anticipar y prevenir ciberataques y ciberexplotación de las redes nacionales que puedan

> afectar el Sistema de Defensa Nacional, como así también acciones contra la infraestructura crítica del país o que posibiliten el acceso a los activos digitales estratégicos adjudicados a su custodia, a fin de garantizar la seguridad de sus infraestructuras informáticas críticas o estratégicas. (Cabrera, 2019, págs. 9-10)
>
> Las Fuerzas Armadas en general y el Ejército Argentino en particular, deben adecuar sus elementos, al impacto que ocasionan estos nuevos riesgos. La política de ciberdefensa debe orientarse al desarrollo de capacidades en materia de ciberseguridad, de tal manera que permitan tener un sistema capaz de resistir ciberataques, ya que ser invulnerable es imposible en esta área en la actualidad. Esta tarea debe contemplar la cooperación con otras áreas del Estado, y diferentes organismos públicos y privados que tengan responsabilidad en la política de ciberseguridad nacional y así poder trabajar en forma coordinada e integrada. (Cabrera, 2019, pág. 10)

Resolución 829 (2019) Estrategia Nacional de Ciberseguridad. El 24 de mayo de 2019 se emitió a través de la resolución mencionada, los lineamientos de la Estrategia Nacional de Ciberseguridad:

> Relacionado con la problemática de la ciberseguridad, la República Argentina se rige por lo que marca el Comité de Ciberseguridad dentro de la Secretaría de Gobierno de Modernización. Es este Comité del Estado Argentino que tiene la responsabilidad de desarrollar la Estrategia Nacional de Ciberseguridad y hacer cumplir los principios y objetivos que marca el Poder Ejecutivo Nacional en el ciberespacio. (Cabrera, 2019, pág. 10)
>
> La constante evolución de las tecnologías de la información y la comunicación (TIC), han permitido mejorar las estructuras económicas a logística a nivel mundial, por tal motivo hoy constituyen uno de los principales motores del

progreso y del bienestar humano. Esto modificó el mundo actual, ya que no es posible prescindir de ellas, ni concebir un futuro próspero, ya que su evolución es constante. Por ello, el contexto actual ubica al ciberespacio como un elemento esencial en la vida de las personas y las organizaciones, proyectando en este gran parte de su actividad, no habiendo aspecto de la vida que no se pueda desarrollar en este dominio. Sin embargo, esto implica graves riesgos a la seguridad de las personas, las organizaciones y los gobiernos, estando el entorno digital amenazado por nuevas formas de delitos, la acción de grupos terroristas y la confrontación entre los Estados que día tras día se encargan de fomentar la confianza, empleando el ciberespacio. Por la complejidad que plantea este nuevo escenario, la Estrategia Nacional de Ciberseguridad establece los principios esenciales y los objetivos centrales de la República Argentina en torno a su proyecto para la protección del ciberespacio. Entre los principios esenciales se destaca, el respeto por los derechos y las libertades individuales, el liderazgo en ciberseguridad, la fomentación de capacidades y el fortalecimiento individual. Otros principios se desarrollan bajo el concepto de cooperación como la integración internacional y la cultura de ciberseguridad y responsabilidad compartida. El último principio es el fortalecimiento del desarrollo socioeconómico, ya que el ciberespacio genera posibilidades para el progreso económico y social de la nación, a su vez la economía tiene una estrecha relación con la logística de un país. También entre los objetivos podemos destacar la concientización del uso seguro del ciberespacio, la capacitación y educación del uso seguro de este campo, el desarrollo del marco normativo y el fortalecimiento de las capacidades en ciberseguridad. También se destacan la protección y recuperación de los sistemas del sector público, fomentar la industria de

> ciberseguridad, la cooperación internacional y la protección de las infraestructuras críticas nacionales de información. (Cabrera, 2019, pág. 11)

Sección II. Ciberseguridad y logística en el medio civil

La ciberseguridad en la logística de España. Un informe presentado por la empresa CuatroOchenta (Entidad española especialista en seguridad informática) en el año 2022, plantea lo siguiente:

> El año 2020 va a ser recordado por muchísima gente como el año de la pandemia de COVID 19, pero también como un año en el que las empresas y trabajadores han tenido que cambiar sus modos de trabajo adaptándose a esa nueva realidad impuesta. Los cambios han sido muchos, desde habilitar el trabajo remoto desde sus domicilios, donde ha sido posible, mejorar la infraestructura de servicios, los cambios en espacios físicos para garantizar la seguridad de los trabajadores, a la transformación digital. Sin embargo, muchas empresas van a recordar el 2020 como un año bien complicado en el que no sólo han tenido que sortear los problemas de la pandemia, sino también los problemas relacionados con la ciberseguridad. (CuatroOchenta, 2022, pág. 3)
>
> El sector logístico y de transporte español, fue durante el año 2020, el tercero más afectado por los ciberataques, con un 43% de ellos dirigidos a las pequeñas y medianas empresas, según se mencionó en una serie de conferencias realizadas sobre la ciberseguridad en la logística y el transporte. Esto se debió principalmente a su importancia y vinculación con los diferentes sectores y actividades de la economía, por tanto, despertó el interés de los hackers informáticos. (CuatroOchenta, 2022, pág. 4)
>
> Entre los ciberataques que más complicaciones provocó en la logística de España, se puede hacer mención al hecho ocurrido en junio de 2017, cuando se

detectó que el virus “Petya” fue el causante de multitud de problemas, desde el cierre temporal de operaciones de TNT Express (filial de FedEx), hasta los problemas de la naviera Maersk, cuya valoración de los daños superó los 255 millones de dólares. Si bien esta última fue de las primeras, no fue la única empresa naviera afectada, sino todo lo contrario, la lista de empresas afectadas continuó en aumento. (CuatroOchenta, 2022, pág. 4)

El interés de los ciberdelincuentes por el sector logístico y de transporte está claro: las empresas de logística tienen información que podría ser sensible por el material que transportan o por los datos propios de sus clientes. Además, provocar el cierre de operaciones también tiene un impacto directo en otros sectores, con lo que el daño global aún es mayor. Existen factores adicionales como la transformación digital y la habilitación del trabajo remoto, que generan un mayor interés en los ciberdelincuentes. No todas las empresas han sabido adaptarse de forma segura a este cambio de paradigma en el modo de trabajo y sin querer, han generado nuevas vías de entrada para los ciberataques. Este último aspecto es especialmente crítico, pues alrededor del 80% de las organizaciones han sido víctimas de ataques como consecuencia del aumento de empleados que trabajan en forma remota. (CuatroOchenta, 2022, pág. 4)

Respecto a los riesgos, si bien en la actualidad existen algunos comunes a cualquier sector, en logística y transporte hay riesgos adicionales a considerar de forma especial. El primero de los riesgos está relacionado con la integridad de la información, pues una fuga o secuestro de información podría ser crítica para la continuidad de negocio. El secuestro de los equipos podría estar en segundo lugar, pues él no disponer de información en tiempo real de los envíos de efectos o saber a dónde se debe recoger o enviar la mercadería produce una interrupción

> de las operaciones. Si además la mercadería es perecedera, el problema se acrecienta aún más. Por último, se puede destacar las tecnologías de la información y la comunicación (TIC). Se tratan de sistemas que están pensados para ofrecer funcionalidades concretas y de fácil integración en el primer caso, y de robustez y fiabilidad en el segundo. En cualquier caso, representan un riesgo de ciberseguridad porque un ciberdelincuente podría tomar el control de este ámbito de forma bastante fácil y rápida. A partir de aquí, se abren nuevos riesgos, desde acceso a información privilegiada, hasta usarlos a modo de dispositivos comprometidos y lanzar ataques a la propia u otras empresas. (CuatroOchenta, 2022, pág. 5)

La ciberseguridad en el conflicto entre Rusia y Ucrania. Según algunos artículos utilizados durante el Seminario de Ciberdefensa impartido por el curso de primer año en la Escuela Superior de Guerra durante el 2022, antes de que Ucrania sufriera la invasión de Rusia, "ya había sido atacada de forma silenciosa". (Escuela Superior de Guerra, 2022)

Los ataques cibernéticos se han convertido en un arma muy poderosa y Rusia lo está utilizando contra los puntos más vulnerables de Ucrania como complemento a la "incursión militar sobre el terreno". (Escuela Superior de Guerra, 2022)

De esta manera, el presidente Volodímir Zelenski hizo frente al gigantesco poder militar y de inteligencia ruso, mientras los hackers intentaban "paralizar las infraestructuras en los servicios de agua, electricidad o telecomunicaciones, efecto que en los inicios del conflicto fue logrado parcialmente". (Escuela Superior de Guerra, 2022), asimismo se dijo lo siguiente:

> Este conflicto es denominado por los expertos como "guerra híbrida" y modifica considerablemente el panorama bélico conocido hasta ahora. Porque al mismo tiempo que los tanques, misiles o portaaviones invaden un país, los hackers trabajan contra objetivos políticos, económicos o sociales que acaben o

> deterioren la confianza y la gobernabilidad de ese país. (Escuela Superior de Guerra, 2022)
>
> La línea que separa estos ataques cibernéticos de una "ciberguerra" es sumamente fina, ya que esta última es un combate bélico en el que los adversarios pretenden destruir las comunicaciones e infraestructuras críticas de su enemigo, pero, en vez de bombardear líneas de ferrocarril, cadenas de suministros de alimentación o infraestructuras hospitalarias, buscan anular la infraestructura conectada a los sistemas informáticos. (Escuela Superior de Guerra, 2022)

La ciberseguridad en la logística marítima de la Unión Europea. Una investigación expuesta en Helsinki, durante el año 2020, denominada "La preparación para amenazas cibernéticas en la industria de la logística marítima", analizó el impacto que tiene la ciberseguridad en a la logística marítima y cómo debe prepararse para minimizar sus efectos, algunos de los cuales se detallan a continuación.

El transporte marítimo es uno de los elementos clave para el comercio mundial y la economía de la Unión Europea, "ya que el 80 % del comercio mundial y el 74 % del comercio de la Unión Europea se realiza por mar". (Harri Pyykköa, Jarkko Kuusijärvib Bilhanan Silverajanc, Ville Hinkkaa, 2020). Asimismo, esta investigación resalta lo siguiente respecto al empleo del transporte marítimo:

> El comercio mundial depende del transporte marítimo, que es una parte operativa integral de sistemas portuarios cada vez más complejos y grandes. Los sistemas marítimos y portuarios están más predispuestos a diversos tipos de amenazas tanto físicas como tecnológicas. Existe una demanda en evolución para desarrollar y aplicar metodologías e instrumentos con el fin de evaluar los riesgos generales que ocurren en la industria de la logística marítima. Debido al

hecho de que los puertos son parte de la infraestructura crítica, una interrupción de las operaciones portuarias puede llegar a ser muy costosa y la seguridad portuaria sigue siendo de vital importancia ya que las amenazas hacia los puertos afectan no solo a los actores dentro del área física, sino que también causan graves daños financieros en las cadenas de suministro existentes. Además de los peligros naturales, existen fuentes de riesgo intencionales y no intencionales creadas por el hombre que tienen el potencial de causar pérdidas financieras o incluso daños físicos a organizaciones o personas. (Harri Pyykköa, Jarkko Kuusijärvib Bilhanan Silverajanc, Ville Hinkkaa, 2020, pág. 1)

Como se destacó anteriormente, los puertos son una parte vital de las cadenas de suministro globales y los riesgos no son solo para los puertos en sí mismos, sino también a las otras partes que integran la cadena de suministros, desde el fabricante hasta el usuario final de la carga. Existen varios tipos de riesgos que afectan a los puertos que, en el peor de los casos, pueden conducir al cierre de este, como la falla de los sistemas de seguridad, el robo de carga o datos, el contrabando de material ilícito que pasa por las aduanas y las pérdidas financieras. Incluso una debilidad menor en los sistemas portuarios o en las bases de datos críticas crea un potencial para ataques cibernéticos, que es un hecho que no puede ser ignorado por las partes interesadas de la industria de la logística marítima. Debido a la creciente tendencia de digitalización que afecta a todas las cadenas de suministros, los sistemas de información marítima son cada vez más vulnerables a las amenazas cibernéticas y, como la industria marítima depende cada vez más de diferentes sistemas de tecnologías de la información y la comunicación (TIC), la ciberseguridad debe actualizarse a un nivel adecuado

> para cumplir con los requisitos de seguridad para el futuro. (Harri Pyykköa, Jarkko Kuusijärvib Bilhanan Silverajanc, Ville Hinkkaa, 2020, pág. 1)
>
> La industria marítima es una parte integral de la mayoría de las cadenas de suministros, ya que gran parte del comercio a nivel mundial se realiza por mar. Por lo tanto, los problemas en los transportes marítimos afectarán en gran medida a la gestión de toda la s de suministro. Sin embargo, es un desafío construir un modelo para una cadena de suministros segura de extremo a extremo para la logística marítima, ya que cualquiera de sus partes individuales puede ser afectada En ausencia de soluciones, los profesionales cibernéticos, los operadores y los manipuladores de carga tienen, en muchos casos, sistemas informáticos poco seguros, que los hacen vulnerables a ciberataques. Para evitar estas acciones, deben intentar construir sistemas más confiables y seguros, a partir de los sistemas informáticos disponibles. Esta es la filosofía detrás de gran parte de la industria de la ciberseguridad hoy en día: sistemas que se observan entre sí, buscan vulnerabilidades y signos de ataque. A corto plazo, sin embargo, la gestión del riesgo cibernético sigue siendo una faceta importante para la preparación cibernética, que debería convertirse en un inherente parte de las operaciones de logística marítima. (Harri Pyykköa, Jarkko Kuusijärvib Bilhanan Silverajanc, Ville Hinkkaa, 2020, págs. 1-2)

Ciberseguridad y logística empresarial. Un estudio realizado por la Universidad Bowling Green de Estados Unidos, abordó la problemática de la ciberseguridad y su impacto en la logística, y de qué manera las empresas deben enfrentar este desafío.

> La ciberseguridad es la capacidad de prevenir, defenderse y recuperarse de las interrupciones causadas por ciberataques de adversarios. Los ciberataques han sido clasificados en ataques activos y ataques pasivos. Los ataques pasivos son

difíciles de detectar y se utilizan principalmente en datos confidenciales. Estos ataques son clasificados básicamente en dos tipos: escucha y análisis de tráfico. Los ataques activos son clasificados como enmascarados, repetitivos, modificatorios y aquellos que niegan el acceso a un servicio determinado. Los hackers utilizan malware para penetrar en un sistema y violar los datos críticos como pueden ser el pago de los clientes y datos personales. Las violaciones cibernéticas aumentan cada año afectando la confidencialidad, la integridad, y disponibilidad de datos. Los sistemas de manipulación de carga y cadena de suministros se han convertido en un objetivo rentable para la ejecución de ciberataques. Con el tiempo, los dispositivos de manipulación de carga se conectan con redes informáticas, para que puedan integrar y compartir información entre las empresas. Esto es de utilidad para las empresas, ya que contribuye para monitorear y administrar las operaciones de forma remota, pero también aumenta las posibilidades de ciberataques. Cuando el sistema está ampliamente conectado en red, un malware puede acceder a él. La mayoría de las empresas administran proveedores externos donde el intercambio y acceso a la información es constante, lo que puede generar vulnerabilidades, especialmente si los procesos están automatizados. (Haschak M. S., 2019, págs. 1-2)

La ciberseguridad se ha convertido en una parte esencial de la vida empresarial. Plantea un desafío dinámico para empresas y amenazan su buen funcionamiento y su ventaja competitiva. Los ciberataques han ido en aumento, lo que ha puesto de manifiesto que la mayoría de las empresas no están bien equipados para abordar el problema de la ciberseguridad. A pesar de la importancia que ha adquirido esta temática y sus amenazas, sigue existiendo una brecha entre la

> conciencia de las empresas sobre ciberseguridad, las consecuencias de los ciberataques y la preparación de la empresa para abordarlo. Estos ataques causan un gran impacto financiero, obligando a las empresas a ser resilientes, realizar inversiones para incrementar la seguridad informática, y abordar esto desde una perspectiva sistémica y no por partes. (Haschak M. S., 2019, pág. 17)
>
> Las empresas enfrentan desafíos críticos de ciberseguridad a medida que adoptan nuevas tecnologías, operando con aplicaciones móviles y basadas en la web, trabajando con socios internos y externos, operando en un entorno competitivo. Estos desafíos también incluyen la falta de mano de obra calificada y escasez de compromiso del personal. Si bien estos desafíos son difíciles, las empresas pueden minimizar el impacto al desplegar tácticas y estrategias, como puede ser la aplicación de una estrategia de defensa de múltiples capas, técnicas de encriptación, asegurar puntos de acceso, crear acuerdos de nivel de servicio con terceros e invertir en tecnologías de seguridad. Abordar los desafíos de ciberseguridad no solo disminuirán las interrupciones del negocio, sino que también otorga ventajas competitivas. (Haschak M. S., 2019, pág. 17)
>
> Las empresas deben tomar medidas como supervisar el flujo de datos en la cadena de suministros y realizar un análisis de riesgo integral. De esta manera se podrá disminuir la afectación en las cadenas de suministros y demás infraestructuras logísticas y de sostenimiento. (Haschak M. S., 2019, pág. 17)

La importancia de la ciberseguridad en las operaciones logísticas. La empresa chilena Symmetrics Lab, entidad que se dedica al desarrollo de aplicaciones móviles y web, publicó el 10 de octubre de 2023, en su blog de Linkedin, un artículo donde hace referencia a la importancia de proteger las operaciones logísticas mediante la ciberseguridad.

En los tiempos actuales donde la inmediatez es la norma y los clientes tiene una amplia gama de canales de comunicación con los proveedores de productos y servicios, poder cumplir con los estándares de calidad esperados y destacar en un mercado saturado de ofertas, resulta de vital importancia el uso de la tecnología, ya que las empresas se ven en la necesidad de optimizar y automatizar sus operaciones para poder cumplir con la demanda de productos y contar con el componente tecnológico necesario para desarrollar eficientemente las operaciones La implementación de la tecnología en las operaciones logísticas otorga una gran ventaja pero también conlleva a asumir grandes riesgos, siendo el de mayor importancia el de sufrir posibles ciberataques. (Symetrics Lab, 2023)

La ciberseguridad se ha convertido en una prioridad para las empresas de todas las industrias y el sector logístico no escapa de ello, pues la misma tecnología que les ayuda a lograr cumplir con grandes números de entregas, mejorar la trazabilidad de sus operaciones y reducir costos operativos es la misma que puede ayudar a vulnerar la seguridad de datos confidenciales de clientes, proveedores, empleados e inclusive de productos y los piratas informáticos o ciberdelincuentes se han dedicado a perfeccionar sus habilidades para encontrar y explotar esas vulnerabilidades con la finalidad de interrumpir operaciones, redes o sistemas y exponer información confidencial. (Symetrics Lab, 2023)

Parte del éxito del funcionamiento de una cadena de suministro es la comunicación y conexión en tiempo real con las partes involucradas (proveedores, productor y consumidores) pero si alguna de las partes involucradas no cuenta con un buen sistema de seguridad para proteger sus sistemas, esto se convierte en la puerta de entrada para el ataque, pues una de las

> formas para los piratas electrónicos de vulnerar un sistema es a través del socio laboral más pequeño, ya que es más probable que su presupuesto de ciberseguridad sea más reducido y sus sistemas no estén del todo actualizados y una vez que logran entrar al sistema tienen acceso a toda la información almacenada. Para evitar que la empresa u organización y sus sistemas sean víctima de un ciberataque es necesario que todas las partes cuenten con las medidas técnicas y organizativas necesarias para estar protegidos ante cualquier ataque. (Symetrics Lab, 2023)
>
> La vulnerabilidad de las operaciones logísticas ante un ataque cibernético radica en el gran volumen de información de valor que manejan, ya que en cada operación se almacena una gran cantidad de datos confidenciales, información personal, financiera y detalles sobre los bienes que se transportan que así como los operadores logísticos usan esta información para mejorar sus operaciones y prever problemas, en las manos incorrectas esta información puede usarse para estafas, manipulación, chantajes y en algunos casos hasta puede poner en riesgo la cadena de producción al alterar los sistemas, es por esto que aunque contar con diferentes niveles de acceso y control de usuarios es de gran ayuda, es necesario tomar todas las previsiones necesarias para evitar y afrontar cualquier ataque. (Symetrics Lab, 2023)

A continuación, se mencionan algunos de los "aspectos que deben ser tenidos en cuenta en materia de ciberseguridad por parte de las empresas que ejecutan operaciones logísticas". (Symetrics Lab, 2023)

> - **Identificación y evaluación de amenazas cibernéticas:** las operaciones logísticas deben poder detectar y evaluar las amenazas cibernéticas a sus sistemas y datos. Esto incluye amenazas externas, como piratas informáticos, y

amenazas internas, como la negligencia de los empleados. Con la creciente sofisticación de los ataques cibernéticos, cada vez es más difícil para las operaciones logísticas detectar amenazas antes de que causen daños. (Symetrics Lab, 2023)

- **Gestión de vulnerabilidades:** con tantas partes involucradas en las operaciones logísticas, puede ser difícil gestionar las vulnerabilidades en toda la red, esto implica mantener el software actualizado y garantizar que se implementen los protocolos de seguridad adecuados, es necesario dejar en claro con las otras empresas la importancia y el valor que aporta mantener todos los sistemas al día, ya que cualquier sistema que no se encuentre actualizado es más propenso a ser atacado. (Symetrics Lab, 2023)

- **Gestión y protección de datos:** las operaciones de logística deben cumplir con las leyes de protección de datos que corresponda al país donde están operando, como por ejemplo la Ley Orgánica de Protección de Datos (LOPD) y el Reglamento General de protección de Datos (RGPD) y garantizar que se implementen procedimientos de protección y cifrado adecuados. Las operaciones logísticas también deben garantizar que los datos se transfieran de forma segura entre las partes a lo largo de la cadena de suministro. (Symetrics Lab, 2023)

- **Complejidad de la cadena de suministro:** con tantos entes externos involucrados en las operaciones logísticas, puede ser complejo mantener controles de seguridad adecuados en toda la cadena de suministro, sin embargo sabemos que la comunicación es clave en este tipo de situaciones establecer un estándar de seguridad entre las partes puede ser beneficioso ya que los socios de la cadena de suministro pueden diferir en su nivel de preparación de seguridad,

lo que genera vulnerabilidades potenciales en la red general. (Symetrics Lab, 2023)

- Errores humanos: los empleados y los proveedores externos pueden exponer datos confidenciales sin darse cuenta si sus equipos no cuentan con los sistemas de seguridad adecuados. Esto puede conducir a filtraciones de datos que comprometan toda la operación logística. (Symetrics Lab, 2023)

Para reducir los riesgos de las amenazas a la ciberseguridad, “las operaciones logísticas deben tomar medidas que les ayude a protegerse y así evitar cualquier riesgo que pueda generar un ataque”. (Symetrics Lab, 2023)

Algunas de las acciones que pueden realizarse son las siguientes:

- **Desarrollar una estrategia de seguridad cibernética:** comience por identificar y evaluar los riesgos cibernéticos y las vulnerabilidades presentes en su operación logística, luego, desarrolle una estrategia de ciberseguridad que abarque medidas de prevención, detección, respuesta y recuperación, asigne roles y responsabilidades a varios empleados y socios. (Symetrics Lab, 2023)

- Implementar controles de acceso estrictos: contar con controles de acceso estrictos para garantizar que solo las personas autorizadas tengan acceso a datos, sistemas y redes confidenciales es indispensable para la protección del sistema, implemente herramientas como la autenticación multifactor (por ejemplo, biométrica y huellas digitales), políticas de contraseñas y controles de acceso basados en roles para minimizar el riesgo de filtraciones de datos. (Symetrics Lab, 2023)

- Actualizar regularmente el software y los sistemas: mantenga todos los software y sistemas actualizados con los últimos parches y actualizaciones para

reducir el riesgo de vulnerabilidades en los sistemas que los piratas informáticos pueden explotar. (Symetrics Lab, 2023)

- Llevar a cabo capacitaciones regulares para los empleados: mantener a tu equipo educado y al día sobre las mejores prácticas de seguridad cibernética, enseñarlos a identificar correos electrónicos de phishing, ataques de ingeniería social y reportar cualquier actividad sospechosa, será de gran ayuda al momento de protegerse de ciberataques. (Symetrics Lab, 2023)

- Transferir datos de forma segura a lo largo de la cadena de suministro: asegúrese de que los datos se transfieran de forma segura entre las partes a lo largo de la cadena de suministro utilizando tecnologías de encriptación y protocolos de comunicación seguros. (Symetrics Lab, 2023)

- Identificar y administrar los riesgos de terceros: comprenda los riesgos asociados que implica la interacción con proveedores externos y asegúrese de que existan contratos adecuados que estipulen sus responsabilidades de seguridad, incluida la planificación de respuesta a incidentes y la protección de datos. (Symetrics Lab, 2023)

- Evaluar y probar periódicamente los controles de seguridad: evaluar y probar periódicamente la eficacia de los controles y las políticas de seguridad. Esto incluye realizar escaneos de vulnerabilidades y pruebas de penetración para identificar y abordar posibles debilidades de seguridad. (Symetrics Lab, 2023)

Al implementar estas medidas las empresas pueden aumentar su seguridad, proteger sus datos y reducir sus riesgos de potenciales ataques, lo esencial en esto es mantenerse al día la actualización de sistemas y tomar todas las medidas necesarias para proteger y resguardar tus sistemas de cualquier tipo de ataque. (Symetrics Lab, 2023)

> Como conclusión de este artículo, la ciberseguridad es fundamental para el buen funcionamiento de cualquier empresa, en el caso de las empresas logísticas se hace indispensable contar con un buen sistema que resguarde y proteja no solo los sistemas sino también la información de los clientes, invertir en equipo e infraestructuras necesarias para para resguardar y garantizar el buen funcionamiento de las operaciones. (Symetrics Lab, 2023)

La ciberdefensa y la ciberseguridad de las infraestructuras críticas y de la información en Argentina. Las infraestructuras críticas no están exentas de ser afectadas por ciberataques, por lo que resulta necesario tener en cuenta que:

> La infraestructura de la información para diseñar y mejorar tanto la ciberdefensa como la ciberseguridad constituye un nuevo campo del saber, que crece a paso vigoroso y que implica un sector de interés para el dominio público y privado. Al mismo tiempo, presenta múltiples dimensiones a desarrollar: lo económico, tecnológico, educativo, político, normativo, militar. Para cada una de estas áreas implicadas en los procesos de sistematización y puesta en marcha de una infraestructura de la información existen y existirán necesidades específicas, comunes y diferenciadas. En ese aspecto, uno de los intereses primordiales estará relacionado con los recursos humanos, con el patrimonio material y con las características organizativas. Para esto, será una necesidad, no solo del ámbito académico, sino también de los sectores políticos, pensar en la información y en la ciberdefensa a partir de bases comunes, pero con perfiles diferenciales. (Taberna Agostina ; Rutz Guillermo, 2021, pág. 3)
>
> El ciberespacio, al igual que los espacios terrestres, marítimos, aéreo y espacial, es objeto de análisis por parte de numerosas instituciones públicas y privadas, tanto nacionales como internacionales. En los últimos años, y especialmente

> luego del ataque cibernético a Estonia en 2007, este interés se ve reflejado en instituciones globales y regionales, como la Organización de las Naciones Unidas, la Organización de Estados Americanos, la Organización del Tratado del Atlántico Norte o la organización para la Seguridad y Cooperación en Europa, tanto en la producción escrita como en la incorporación a sus estructuras institucionales de organismos especializados en el tema. Del mismo modo diversos países han incluido la problemática en sus agendas de estrategia nacional de seguridad. (Taberna Agostina ; Rutz Guillermo, 2021, pág. 3)

Sección III. La Doctrina sobre ciberdefensa en el Ejército Argentino

La ciberdefensa comprende:

> Medidas técnicas, políticas y organizativas que protegen los sistemas y redes militares de ciberataques, como así también la capacidad de reacción y ataque propios de un conflicto armado. Desde un fundamento concreto, la Ciberdefensa se sustenta mayoritariamente en tecnología de ciberseguridad ampliamente probada, y desplegada en el sector civil". (Anca, Luis Javier, 2015, pág. 33)

El reglamento ROB-00-01, "Conducción de las Fuerzas Terrestres", menciona la Ciberdefensa, en el marco de las Operaciones Complementarias, y la define como:

> El conjunto de acciones que se desarrollan en el ciberespacio para prevenir, detectar, identificar, anular, impedir, evitar, contrarrestar, contener o repeler amenazas o agresión cibernética, sea esta inmediata, latente o potencial, a fin de permitir el empleo del Instrumento Militar de la Nación. (Ejército Argentino, 2015)

Asimismo, en referencia a la finalidad, refiere dos modalidades:

- "Ciberdefensa directa, con la finalidad de vigilar y controlar las redes y sistemas en los ámbitos específico y conjunto". (Ejército Argentino, 2015)

- Ciberdefensa indirecta, cuya finalidad es la de “disputar el control del ciberespacio necesario para el accionar de las fuerzas militares”. (Ejército Argentino, 2015)

Por lo anteriormente mencionado es necesario tener en cuenta:

> Que la doctrina rectora mencionada en el ámbito de la fuerza, es obsoleta, escasa y restrictiva en cuanto a las tareas que enumera. Asimismo, es contradictoria en cuanto a su objetivo último, en lo que respecta a la ciberdefensa indirecta, ya que, si se pretende disputar el control del ciberespacio como lo marca la última Directiva Política de Defensa Nacional (DPDN) del 2018 o los lineamientos dados en la directiva estratégica de ciberseguridad de 2019, no basta con medidas de carácter pasivo. Por tal razón, es necesario incorporar medidas de carácter activo que permitan mantener la iniciativa. (Cabrera, 2019, pág. 19)
>
> El marco doctrinario, el cual se encuentra en proceso de actualización, es escaso ante la naturaleza de las actividades en el ciberespacio, como una nueva dimensión de los conflictos armados. También, la diferencia que hace nuestro país en cuanto a la separación en materia legal, de Defensa y Seguridad, es determinante en cuanto al ámbito de empleo de las fuerzas armadas. La aparición de una dimensión con características particulares propias, que no responde a reglas obsoletas, plantea una larga lista de interrogantes al momento de enfrentar estas nuevas amenazas de forma integral y eficiente. (Cabrera, 2019, pág. 19).

En función de los elementos de juicio analizados en este primer capítulo, se pueden determinar las siguientes conclusiones.

La legislación de la República Argentina para el empleo de las Fuerzas Armadas, la cual se encuentra enmarcada por la Ley de Defensa Nacional 23.554, junto con la Directiva Política de Defensa Nacional, establecen que “conflictos que requieren el empleo de las Fuerzas Armadas, en forma disuasiva o efectiva serán empleadas para enfrentar las agresiones de origen

externo" (Honorable Congreso de la Nación, 1988); no así la Estrategia Nacional de Ciberseguridad. Esta no hace mención en forma taxativa, que las Fuerzas Armadas "sólo deben actuar exclusivamente ante agresiones de origen externo, en el ámbito del ciberespacio". (Secretaria de Gobierno de Modernización de la Jefatura del Gabinete de Ministros, 2019)

En cuanto al desarrollo de capacidades en el ámbito de la ciberdefensa, la resolución 1380/2019, promulgada en octubre de 2019 permitió la creación del Centro Nacional de Ciberdefensa en el ámbito de la Subsecretaría de Ciberdefensa. Este centro reúne a diferentes áreas relacionadas con la protección y seguridad de infraestructuras críticas de vital importancia para la Defensa Nacional.

El entorno del ciberespacio es incierto, ambiguo y complejo, dónde detectar a quienes actúan en él no es tarea fácil, y por lo tanto se hace difícil determinar cuáles son sus objetivos e intereses. Estos podrían ser empresas, fuerzas armadas, e incluso países, dificultando el desarrollo de capacidades que permitan anticipar, mitigar o neutralizar las amenazas ante posibles ciberataques.

En la República Argentina, la ciberdefensa es un área que ha comenzado a tenerse en cuenta recientemente y la cual es aplicada en forma defensiva ante un ciberataque, a esto se agrega el marco legal, el cual separa Defensa de Seguridad Interior y la ausencia de una legislación particular para las acciones de carácter ofensivo en el ciberespacio, dan como resultado que sea vea dificultado el desarrollo de capacidades para la proporcionar seguridad y dar protección a las infraestructuras críticas, sean civiles o militares.

En cuanto al análisis sobre los incidentes ocurridos en las cadenas logísticas del medio civil, se puede observar que los ciberataques, no discriminan países ni fronteras, ni entidades, por lo que resulta necesario tener en cuenta estos aspectos ya que la ciberdefensa es puesta a prueba en la paz, afectando empresas, cadenas de suministros, transporte, entre otros.

Otro aspecto de importancia es lo relacionado con la protección de las operaciones logísticas que realizan las empresas civiles, las cuales marcan la importancia de proteger una de las partes más importante de las operaciones logísticas, la cadena de suministros, la cual guarda información de vital importancia no solamente de la empresa sino también de proveedores, efectos transporte, finanzas e información confidencial de los clientes.

Por lo mencionado en el párrafo anterior resulta necesario que no solamente en el ámbito civil sino también en el militar, invertir en equipamiento e infraestructura de ciberdefensa, así como capacitar y concientizar al personal en materia de ciberdefensa y ciberseguridad, y de esta manera evitar o neutralizar incidentes y evitar daños mayores.

Por ello resulta necesario actualizar la doctrina rectora utilizada en el ámbito de la fuerza, capacitar al personal militar en esta área, sobre todo a aquellos que utilizan las herramientas informáticas logísticas, de tal manera que puedan detectar y reaccionar ante hechos que afecten la vulnerabilidad de los sistemas informáticos logísticos empleados.

CAPÍTULO II. Situación de la ciberseguridad en el Ejército Argentino y su influencia en el sostenimiento logístico en operaciones

Introducción

Continuando con la investigación del presente trabajo, en el capítulo II, el cual tiene como objetivo comparar y analizar el estado de ciberseguridad de los sistemas informáticos logísticos del Ejército Argentino desde el año 2020, en su asiento de paz y su relación con el sostenimiento logístico en operaciones. Se dará una explicación de los sistemas de información logística empleados en el ámbito civil y en la fuerza, seguidamente se dará una síntesis de cómo se ha desarrollado la ciberseguridad en otras fuerzas armadas del mundo, y para finalizar de qué manera puede afectarse el sostenimiento logístico y las conclusiones del presente capítulo.

Sección I. Aspectos de relevancia relacionados con los Sistemas de Información Logística

La importancia de los sistemas de gestión en empresas y organizaciones se debe, en cierta parte, a la evolución producto de la globalización del comercio, que da como resultado un aumento de la competencia de los mercados. (Escuela Superior de Guerra, 2022)

Ante esta situación las empresas “deben responder rápidamente ante las distintas situaciones que se pueden presentar en su entorno”. (Escuela Superior de Guerra, 2022)

En este contexto, se debe tener en cuenta que:

> La fluidez en el intercambio de información entre las distintas partes de la empresa juega un papel fundamental para la toma de decisiones. Desde esta perspectiva, los nuevos sistemas de gestión apuestan por la utilización de herramientas que permitan conectar los distintos departamentos a través de los datos derivados desde sus correspondientes actividades, con el objetivo de obtener una visión global de la situación de la empresa. (Escuela Superior de Guerra, 2022)

Los sistemas de información logística son soluciones digitales que se encargan de extraer y procesar información de distintas actividades de abastecimiento para facilitar la toma de decisiones, la resolución de problemas, la planificación estratégica y la gestión de la cadena de suministros, ya sea en su totalidad o solo en algunas de sus etapas (aprovisionamiento, almacenamiento, despacho, distribución, entre otros.). Entre sus características podemos mencionar:

- Parte fundamental en el proceso de digitalización de las empresas modernas.
- Ayuda en el flujo de información efectivo para la toma de decisiones.
- Evitar la incertidumbre.

Cuando se utilizan sistemas de información logística, los flujos de información "se convierten en datos de importancia crucial para la toma de decisiones". (Escuela Superior de Guerra, 2022), como así también lo siguiente:

> Al integrar los Sistemas de Información Logística dentro de las tecnologías de la información y la comunicación (TIC) en las empresas logísticas, "estas logran ser más productivas y competitivas, al manejar la información de forma eficiente y precisa, se puede gestionar correctamente la cadena de suministros, minimizar los errores, ahorrar tiempo y dinero, optimizar las entregas, aumentar la calidad del servicio al cliente, entre otros". (Escuela Superior de Guerra, 2022)

Utilidad de los sistemas de información logística. Entre las utilidades que brindan los sistemas de información logística, se puede mencionar que:

- Habilitan la reunión de datos relacionados con una o varias actividades en la cadena de suministros, justo en el momento y oportunidad en la que acontecen.
- Otorgan información útil en tiempo real.

- Permiten tomar decisiones inmediatas o realizar planes a corto, mediano o largo plazo.
- Conceden la obtención de informes, facilitando información útil a proveedores, distribuidores, clientes e inversionistas logísticos. (Escuela Superior de Guerra, 2022)

Tipos de sistemas de información logística. Los principales sistemas de información logística que tienen mayor empleo en la logística civil y empresarial son:

> *Programas ERP (Enterprise Resource Planning):* los ERP son programas integrales y horizontales. Ofrece soluciones para distintas áreas de la empresa, sin especializarse en una en particular. Por lo general, un ERP tiene módulos para la gestión de pedidos, de clientes y proveedores, de ventas, cobranza, marketing, logística, producción, abastecimiento, entre otros. (Escuela Superior de Guerra, 2022)
>
> *Programas "best of breed":* son aplicaciones verticales. Es decir, se especializan en un tipo de actividad específica. En el caso del sector de logística, estas actividades específicas pueden ser la gestión de almacenes o la administración del transporte de productos. (Escuela Superior de Guerra, 2022)

Herramientas informáticas para la gestión logística. Estas herramientas han permitido a la gestión logística optimizar sus recursos, teniendo en cuenta que:

> A través de los años, la logística ha sufrido importantes transformaciones no sólo en términos conceptuales sino también cómo ha evolucionado a lo que conocemos hoy día como e-logística, con lo cual se incorpora la utilización de una herramienta fundamental como es internet. Debido a este avance, las organizaciones han determinado un cambio en su manejo de inventarios, almacenes y cadena de suministros. Esto da como resultado la implementación

de ciertos sistemas de apoyo como WMS, SCM, ERP y CRM, cuyo detalle será explicado a continuación. (Escuela Superior de Guerra, 2022)

Warehouse Management System o Sistema de Administración de Almacenes (WMS). El WMS es un "sistema de gestión y optimización mediante el uso de aplicaciones de informática para el inventario y el almacén, así como los factores más importantes que se deben considerar para la administración eficiente". (Escuela Superior de Guerra, 2022)

Supply Chain Management o Gestión de la Cadena de Suministros (SCM).

SCM, se refiere a las herramientas y métodos cuyo propósito es mejorar y automatizar el suministro a través de la reducción de las existencias y los plazos de entrega. Los sistemas SCM incluyen vendedores, instalaciones de manufactura, proveedores de logística, centros de distribución interna, distribuidores, mayoristas y otras entidades que conducen al usuario final. (Escuela Superior de Guerra, 2022)

Customer Relationship Management o Administración de la Relación con el Cliente (CRM).

Un sistema CRM es definido como la mejora al tratamiento de información, tomando en cuenta todos los procesos por la cual cursa para así poder obtener resultados relevantes, los cuales ayudan en el desarrollo de gestión de negocios en la empresa, permitiendo una debida atención a requerimientos al cliente. (Escuela Superior de Guerra, 2022)

Enterprise Resources Planning o Planificación de Recursos Empresariales (ERP).

Es un sistema de información, el cual es responsable de la administración y planificación de tareas específicas de la empresa, que ayuda a mejorar el rendimiento y manipulación de los datos que esta maneje. Los ERP son sistemas

> que integran el manejo de la información para que sea más precisa, rápida y de fácil acceso a la organización. (Escuela Superior de Guerra, 2022)

Sección II. Los Sistemas de Información Logística en el Ejército Argentino.

Herramientas informáticas logísticas en el Ejército Argentino. De acuerdo a lo visto en las clases referidas a herramientas logísticas se puede decir que:

> En el ámbito de la fuerza, en lo que refiere al empleo de herramientas y sistemas informáticos para la gestión logística, actualmente se encuentra en uso el SIGILEA (Sistema de Gestión e Información Logística del Ejército Argentino), el cual agrupa una serie de herramientas que serán detalladas a continuación. (Escuela Superior de Guerra, 2022)

Sistema Digital de Gestión de efectos de Arsenales (SIDIGEA). Es una herramienta informática de empleo de Arsenales, para gestionar información sobre el estado de situación de Abastecimiento y Mantenimiento de los efectos de Arsenales, siendo esta la única base de datos Logística de Material de Arsenales con "utilidad para todos los niveles de comando." (Leonardo Anibal Belizon, 2014, pág. 9), como así también:

> El sistema dispone de variadas consultas agrupadas de utilidad para los distintos niveles de comando. Permite realizar el circuito completo de las órdenes, sin necesidad inmediata del documento de registro impreso y es de utilidad para responder "requerimientos de los usuarios desde el Estado Mayor Conjunto, hasta las Unidades y Subunidades Independientes". (Leonardo Anibal Belizon, 2014, pág. 9)
>
> El SIDIGEA es un sistema de datos centralizado que opera en tiempo real, por cuanto cualquier alta, baja o modificación que el usuario realice, es inmediatamente puesta a disposición de otro usuario. Además, es necesario que en esta herramienta los datos de origen sean cargados donde son generados de

manera de mantener actualizado los estados y datos de los efectos. (Leonardo Anibal Belizon, 2014, pág. 9)

Sistema de tarjeta electrónica precargable (Visa Flota).

El sistema de tarjeta electrónica Visa Flota es una herramienta que simplifica el control de combustible y se limita a los fondos acreditados en cada uno de los centros de costos centralizadores por parte del escalón superior y de estos a las tarjetas magnéticas precargables. (Ejército Argentino, 2015)

La tarjeta magnética precargable permite dos modalidades de emisión: la tarjeta conductor o nominal (emitida a nombre de una persona física) y la tarjeta vehículo (emitida con la identificación del vehículo y la patente). (Ejército Argentino, 2015)

Este sistema, mediante el empleo de una tarjeta proporciona una solución de pago para administrar todos los gastos generados por la operación de los vehículos de guarnición o campaña, incluidos el combustible, el mantenimiento y las reparaciones. (Visa Argentina, 2022)

El programa Visa Flota proporciona un método de pago seguro y accesible. También ofrece a los administradores un sistema simple y confiable para supervisar y proyectar los gastos de los vehículos empleados. (Visa Argentina, 2022)

Con el programa de tarjeta Visa Flota, la organización podrá:

- Asignar tarjetas por vehículo o conductor.
- Acceder a la información de transacciones para controlar mejor los gastos y desarrollar un presupuesto más preciso.
- Límites preestablecidos para cada tarjeta para controlar, por ejemplo, la frecuencia de uso y los montos de transacción. (Visa Argentina, 2022).

Sistema de Capacidades de Mantenimiento de las Fuerzas Armadas II (SICAMAN II).

> Este sistema prescripto por la Resolución MD 123/2011 vincula operativamente entre las tres fuerzas armadas las infraestructuras de mantenimiento de material de cada una de ellas. De esta manera, se procura optimizar el aprovechamiento de la capacidad instalada total tanto en cuanto a recursos humanos y tecnológicos, como a medios e instalaciones. El SICAMAN II promueve la prestación de servicios entre las fuerzas armadas que resulten a priori menos onerosos que los disponibles en el mercado comercial. Este sistema fomenta la integración de las capacidades de mantenimiento de las fuerzas armadas, facilita su aprovechamiento conjunto y coadyuva a fortalecer aquellas capacidades que permitan sostener sistemas comunes. Su implementación ha permitido a las tres fuerzas ejecutar tareas de mantenimiento y recuperación de medios en instalaciones de las otras, generando un creciente proceso de empleo sinérgico de tales capacidades. Asimismo, como consecuencia de la evolución del sistema y con el objeto de extender sus alcances, se han incorporado como prestadores de servicios, el Servicio de Hidrografía Naval, el Instituto de Investigaciones Científicas y Técnicas para la Defensa (CITEDEF), el Servicio Meteorológico Nacional, Fabricaciones Militares, el Instituto Geográfico Nacional, la Fábrica Argentina de Aviones ***(***FAdeA) y el Complejo Industrial Naval Argentino (CINAR). (Presidencia de la Nación. Ministerio de Defensa, 2015, pág. 134)

Portal de Compras Públicas de la República Argentina COMPR.AR.

> También se puede hacer mención que para la adquisición de efectos para el uso de la fuerza se emplea el sistema COMPR.AR el cual es utilizado en todo el ámbito de la administración pública nacional, como así también la herramienta

> GEDO (Gestión Electrónica de Documentos Oficiales), la cual permite el envío y recepción de documentación con diferente clasificación de seguridad de manera ágil, rápida y segura. (Escuela Superior de Guerra, 2022).

Como puede observarse, las herramientas informáticas utilizadas dentro de la fuerza son similares a las empleadas en el medio civil, y como se mencionó en el primer capítulo, no están exentas de ser afectadas por ciberataques que reduzcan o anulen el apoyo logístico o la capacidad de sostenimiento.

En la actualidad la ciberdefensa ha adquirido suma importancia, no solamente en el ámbito militar, sino que también en el civil. En lo que respecta a las herramientas informáticas aplicadas a la logística, estas se encuentran mucho más desarrolladas y son más utilizadas en el campo empresarial, que en el militar. En el caso del Ejército Argentino la herramienta de mayor uso es el SIDIGEA, la cual es utilizada en todo el ámbito de la fuerza, puede ser utilizada en la paz, sino también en operaciones y no es de uso exclusivo en unidades logísticas, como pueden ser los Batallones de Intendencia, Batallones de Arsenales y Bases de Apoyo Logístico.

Influencia de la ciberseguridad en el sostenimiento logístico de la fuerza. Por todo lo expuesto anteriormente, se debe tener especial atención a que tanto la ciberseguridad como el sostenimiento logístico, su ámbito de aplicación, sea en la paz, como así también en la guerra y conflictos de otra índole, como ser emergencias, desastres naturales o catástrofes, pueden verse afectados. Realizando un análisis comparativo entre las herramientas utilizadas en el ámbito civil y las que utiliza el Ejército Argentino, ambas poseen características similares en cuanto a su forma de empleo. Así también tomando como referencia lo expuesto en el primer capítulo de los incidentes acontecidos en el medio civil, sobre la afectación de las cadenas logísticas, no solamente en nuestro país sino también en el exterior, junto con la aplicación de sistemas y herramientas de información logística, que si bien facilitan y agilizan la gestión de efectos, son vulnerables a las acciones de ciberataques, con la finalidad de reducir o anular la

capacidad de gestión de efectos, sustracción de información vital, lo cual ocasionará serias dificultades para el sostenimiento logístico, no solamente en la paz, sino que también en operaciones de diferente tipo.

> En el caso del Ejército Argentino, el especialista en ciberdefensa ha pasado de ser una figura opcional en cualquier organización a convertirse en un elemento imprescindible. Pero también juega un papel preponderante el usuario de la red informática, ya que el principal vector de intrusión en las redes procede de la falta de conciencia en seguridad informática y de las violaciones a las políticas de seguridad. Esta situación dificulta tomar medidas eficaces en tiempo y forma. (Ejército Argentino, 2022, pág. 1).

Por lo expuesto, es una responsabilidad de comando "lograr la máxima capacitación técnica profesional del personal que opera los medios del subsistema informático, tanto del usuario común como de los especialistas". (Ejército Argentino, 2022)

Es así que resulta necesario instruir y capacitar al personal que sea usuario de las herramientas informáticas logísticas de la fuerza, para de esta manera minimizar los incidentes que puedan afectar el sostenimiento logístico de la fuerza, ya sea en la paz o en la guerra.

Sección III. La ciberdefensa en el ámbito militar y su aplicación en otros países

En relación a la ciberdefensa en las organizaciones militares, en esta parte del presente capítulo se volcará a continuación parte de un informe final correspondiente al Proyecto de Investigación denominado "La Defensa Cibernética. Alcances estratégicos, proyecciones doctrinarias y educativas", presentado en mayo del año 2017, donde remarca la importancia de la ciberseguridad, su relación con la Defensa Nacional y la responsabilidad que conlleva para las Fuerzas Armadas.

Estados Unidos y la ciberdefensa.

Los Estados Unidos, en el año 2003, modificaron su doctrina militar, dejando solamente el de Operaciones de Información, este concepto abarca el empleo integral de capacidades de la guerra electrónica, operaciones de redes de computadoras, operaciones psicológicas, operaciones de velo y engaño y operaciones de seguridad, en conjunto con las capacidades de soporte, con la finalidad de influenciar, interrumpir, corromper o usurpar los sistemas de comando y control del adversario, a su vez que se protegen los sistemas propios. (Ortiz, Javier Ulises; Fonseca Claudia; Ansorena Gratacos Miguel; Perdomo Luz Ivone, 2017, pág. 68)

En mayo de 2010 Estados Unidos crea su primer comando de ciberdefensa (U.S. Cyber Command - USCYBERCOM). Su misión es planear, coordinar, integrar, sincronizar y conducir "actividades para: dirigir las operaciones y defender las redes de información especificadas por el Departamento de Defensa y; prepararse para, cuando sea oportuno, llevar a cabo una amplia variedad de operaciones militares en el ciberespacio a fin de llevar a cabo acciones en todos los dominios, asegurar la libertad de acciones a los Estados Unidos y sus aliados en el ámbito del ciberespacio e impedir lo mismo a sus adversarios". (Ortiz, Javier Ulises; Fonseca Claudia; Ansorena Gratacos Miguel; Perdomo Luz Ivone, 2017, pág. 68)

Ese mismo año el Ejército de los Estados Unidos, creó el Cibercomando del Ejército (U.S. Army Cyber Command- ARCYBER), como componente dependiente del USCYBERCOM. Tiene por misión planificar, coordinar, integrar, sincronizar, dirigir y conducir operaciones y defensa de la red de todas las redes del Ejército y conducir operaciones en el ciberespacio, en apoyo a las

> operaciones militares para asegurar la libertad de acción de las fuerzas terrestres y proteger los sistemas propios. (Ortiz, Javier Ulises; Fonseca Claudia; Ansorena Gratacos Miguel; Perdomo Luz Ivone, 2017, pág. 68)
>
> En apoyo las operaciones militares, la Estrategia de Estados Unidos, establece que el Departamento de Defensa dirige un rango de actividades "fuera del ciberespacio" como la cooperación "con agencias del gobierno, con el sector privado, y socios internacionales (Canadá, Gran Bretaña, Australia y Nueva Zelanda) para buscar información, construir alianzas y socios, y fomentar normas de conducta responsable para mejorar la estabilidad estratégica global" (Ortiz, Javier Ulises; Fonseca Claudia; Ansorena Gratacos Miguel; Perdomo Luz Ivone, 2017). Esta estrategia, plantea abiertamente que Estados Unidos, podrá realizar actividades de ciberguerra al afirmar que el país "debe ser capaz de recurrir a las ciberoperaciones para destruir las redes de comando y control, infraestructuras críticas o sistemas de armas de los potenciales adversarios del país" (Ortiz, Javier Ulises; Fonseca Claudia; Ansorena Gratacos Miguel; Perdomo Luz Ivone, 2017). También recuerda que las ciberoperaciones se integrarán plenamente en el planeamiento y conducción de las operaciones militares. (Ortiz, Javier Ulises; Fonseca Claudia; Ansorena Gratacos Miguel; Perdomo Luz Ivone, 2017, pág. 68)

La ciberdefensa de la República Popular China.

En lo que respecta en el ámbito de ciberdefensa, la Academia de Ciencias Militares de China, la Universidad Nacional de la Defensa China, la Academia de Comando de Comunicaciones de Wuhan "han desarrollado en los últimos años estudios sobre la ciberguerra". (Ortiz, Javier Ulises; Fonseca Claudia; Ansorena Gratacos Miguel; Perdomo Luz Ivone, 2017, pág. 73)

> Los expertos militares de las entidades mencionadas anteriormente, han indicado que el uso de Internet en las revueltas desarrolladas en 2011 en el mundo árabe, están asociadas a acciones gubernamentales desde el exterior de esos países, por lo cual China debe construir, una "frontera de Internet" (Ortiz, Javier Ulises; Fonseca Claudia; Ansorena Gratacos Miguel; Perdomo Luz Ivone, 2017) y "defender su soberanía de internet" (Ortiz, Javier Ulises; Fonseca Claudia; Ansorena Gratacos Miguel; Perdomo Luz Ivone, 2017), indicando que "igual que la guerra nuclear fue la guerra estratégica de la era industrial, la ciberguerra se ha convertido en la guerra estratégica de la era de la información y se ha convertido en una forma de batalla que es muy destructiva y concierne a la vida y la muerte de las naciones". (Ortiz, Javier Ulises; Fonseca Claudia; Ansorena Gratacos Miguel; Perdomo Luz Ivone, 2017, pág. 73)

Los expertos de este país, incluyen nuevos conceptos dentro de las denominadas ciberactividades como "cibermovilización, cibermanipulación, cibereclutamiento que no conforman lo que entendemos por la guerra (ataque y defensa)". (Ortiz, Javier Ulises; Fonseca Claudia; Ansorena Gratacos Miguel; Perdomo Luz Ivone, 2017, pág. 73)

> Un informe publicado por el New York Times en el año 2013, indicó que unidades militares secretas de China atacan a Estados Unidos diariamente. Este informe indica que los denominados Primer, Segundo, Tercer y Cuarto Departamentos, dependientes del denominado Departamento General de Personal (DGP) del Ejército Popular de Liberación realizan dichas ciberoperaciones. Asimismo, el informe señala que el Departamento General de Personar también supervisa las regiones militares de China, la Armada, la Marina, la Fuerzas Aérea y la Segunda Artillería, lugar donde se encuentran las

armas nucleares chinas. (Ortiz, Javier Ulises; Fonseca Claudia; Ansorena Gratacos Miguel; Perdomo Luz Ivone, 2017, pág. 73)

Las organizaciones militares de la Federación de Rusia y el Ciberespacio.

Rusia, en el año 2012, a través del Ministerio de Defensa publicó un documento titulado *"*Criterios conceptuales sobre la actividad de las Fuerzas Armadas de la Federación de Rusia en el espacio informático", el cual establece las tendencias que adoptaran sus fuerzas para el control, la prevención y la solución de conflictos cibernéticos. (Ortiz, Javier Ulises; Fonseca Claudia; Ansorena Gratacos Miguel; Perdomo Luz Ivone, 2017, pág. 75)

El documento mencionado no hace mención alguna sobre la gestión por parte de Rusia de acciones bélicas ofensivas en el ciberespacio. La concepción estratégica se resume en tres acciones fundamentales: contención, prevención y autorización de los conflictos bélicos en el campo digital. En el documento también se expone que "en condiciones de escalada de un conflicto en el espacio informático y de su paso a una situación de crisis, hacer uso del derecho de autodefensa individual o colectiva mediante el empleo de cualquier procedimiento y medio elegido, que no sean contrario a las normas reconocidas universalmente y a los principios de las leyes internacionales". (Ortiz, Javier Ulises; Fonseca Claudia; Ansorena Gratacos Miguel; Perdomo Luz Ivone, 2017, pág. 75)

Posteriormente, en febrero de 2013, el Ministerio de Defensa de Rusia ordenó al Estado Mayor Conjunto de las FFAA, acelerar el plan para la creación de un cibercomando militar. Este cibercomando integra esfuerzos militares junto al Ministerio del Interior, responsable en investigar delitos informáticos, y el Centro de seguridad informática del Servicio Federal de Seguridad

(Inteligencia), área responsable del accionar contra grupos extremistas, organizaciones criminales y servicios secretos extranjeros que puedan atentar contra los intereses rusos. (Ortiz, Javier Ulises; Fonseca Claudia; Ansorena Gratacos Miguel; Perdomo Luz Ivone, 2017, pág. 75)

Las Fuerzas de Defensa de Israel (FDI) y la ciberdefensa.

Desde 2010, el Gobierno Israelí cuenta con una "Ciber Iniciativa Nacional", a cargo de la Autoridad Nacional de Seguridad de la Información. Posteriormente, en el año 2012, ministro de Defensa. indicó que Israel desarrolla acciones tanto la defensa como el ataque en el ciberespacio, expresando que "a diferencia de la guerra convencional, en este tipo de lucha es más importante invertir en la defensa que atacar al enemigo" (Ortiz, Javier Ulises; Fonseca Claudia; Ansorena Gratacos Miguel; Perdomo Luz Ivone, 2017). Asimismo, indicó que *"*debemos cambiar a un sistema proactivo, en que no solo reaccionemos ante ataques *"* (Ortiz, Javier Ulises; Fonseca Claudia; Ansorena Gratacos Miguel; Perdomo Luz Ivone, 2017), agregando que la ciberdefensa *"*es más importante y más difícil*"* (Ortiz, Javier Ulises; Fonseca Claudia; Ansorena Gratacos Miguel; Perdomo Luz Ivone, 2017) que los ciberataques, señalado que Israel desde aspirar a convertirse en líder mundial en ciberdefensa, a niveles militar y civil. (Ortiz, Javier Ulises; Fonseca Claudia; Ansorena Gratacos Miguel; Perdomo Luz Ivone, 2017, pág. 78)

El Gobierno israelí estableció a mediados de 2012 un Comité Nacional para desarrollar la defensa de las infraestructuras críticas, sistemas financieros y otros activos. Por su parte, las FDI cuentan con componentes específicos frente a ataques tecnológicos contra su país. En abril de 2012, las FDI finalizaron el primer curso de ciberdefensa. Este curso fue desarrollado para brindar

capacidades para prevenir los ciberataques contra las redes propias. En el mencionado curso se implementó un nuevo sistema de simulación de ciberguerra. Este simulador, desarrollado para el gobierno, instalaciones militares e instalaciones civiles de infraestructura crítica, permite la formación personal y grupal de los diferentes usuarios en la localización, manejo y gestión de diversos eventos de la guerra cibernética y los ataques que esta trae aparejados. Asimismo, ofrece capacitación en prevención de los episodios de guerra cibernética, mediante la simulación de escenarios de redes de protección. (Ortiz, Javier Ulises; Fonseca Claudia; Ansorena Gratacos Miguel; Perdomo Luz Ivone, 2017, pág. 78)

Las Fuerzas Armadas de Irán y el ciberespacio.

Irán, en el año 2011, anunció, que para contrarrestar posibles amenazas externas sobre sus instalaciones nucleares, había puesto en marcha un "cibercomando" dedicado a luchar contra posibles ataques de piratas informáticos contra las redes del país, que tendría como misión "vigilar, identificar y contraatacar cuando se produzcan amenazas informáticas contra las infraestructuras nacionales" (Ortiz, Javier Ulises; Fonseca Claudia; Ansorena Gratacos Miguel; Perdomo Luz Ivone, 2017, pág. 79)

También indicó que "los Estados Unidos está reduciendo el tamaño de su Ejército para poder tener una infraestructura de defensa cibernética más grande. Pues, países como Irán tienen que instalar y modernizar sus organizaciones de defensa cibernética e incluso construir un Ejército cibernético" (Ortiz, Javier Ulises; Fonseca Claudia; Ansorena Gratacos Miguel; Perdomo Luz Ivone, 2017). Asimismo, el director del Sistema de Defensa Pasiva de Irán, expresó que Irán es uno de los países que más ha sido objeto de ciberataques a lo largo de los

últimos años. En este sentido, también recalcó que los centros atacados no salieron afectados y de momento Irán es en gran medida inmune a este tipo de ataques. A principios de marzo de 2012, el líder iraní anunció la creación del Consejo Superior del Ciberespacio, conformado por el presidente del país y los jefes del Parlamento y el Poder Judicial, el secretario del Consejo Supremo de Seguridad Nacional, varios ministros y mandos militares y policiales. (Ortiz, Javier Ulises; Fonseca Claudia; Ansorena Gratacos Miguel; Perdomo Luz Ivone, 2017, pág. 78)

La ciberdefensa en el Reino Unido de Gran Bretaña (RUGB).

En julio de 2010, el director del Centro de Comunicaciones Gubernamental (GCHQ) presentó al Parlamento Británico un informe donde indicaba que las amenazas cibernéticas son reales y creíbles y que el RUGB "debe prepararse para participar en una serie de operaciones ofensivas cibernéticas para proteger sus intereses". (Ortiz, Javier Ulises; Fonseca Claudia; Ansorena Gratacos Miguel; Perdomo Luz Ivone, 2017, pág. 80)

Posteriormente, en octubre de 2010, fue publicada la Estrategia de Seguridad Británica, donde coloco a la amenaza cibernética, en el mismo nivel que las acciones del terrorismo internacional, desastres naturales, una pandemia o una crisis militar internacional que precisa una respuesta nacional. (Ortiz, Javier Ulises; Fonseca Claudia; Ansorena Gratacos Miguel; Perdomo Luz Ivone, 2017, pág. 80)

En tal sentido, el RUGB cuenta con el Programa Nacional de Seguridad Cibernética, tendiente a ampliar los sistemas de protección de la seguridad cibernética, asegurar la información, mejorar la detección y análisis de los ataques cibernéticos; aumentar la cooperación con países aliados; y en la

creación de una unidad cibernética conjunta en colaboración con el Ministerio de Defensa para desarrollar nuevas tácticas, técnicas y planes relativos a las operaciones militares. (Ortiz, Javier Ulises; Fonseca Claudia; Ansorena Gratacos Miguel; Perdomo Luz Ivone, 2017, pág. 80)

La ciberdefensa en Francia.

En lo que respecta a la ciberdefensa en Francia, este país incluyó en su Libro Blanco sobre Defensa y Seguridad Nacional, al ciberespacio, centrándose en la seguridad de los "sistemas de información, centros nerviosos reales de nuestra sociedad" (Ortiz, Javier Ulises; Fonseca Claudia; Ansorena Gratacos Miguel; Perdomo Luz Ivone, 2017), donde "todos los sectores de actividades, ya sean estatales, industrial, financiero o comercial, dependen más de la tecnología y redes de comunicaciones electrónicas". (Ortiz, Javier Ulises; Fonseca Claudia; Ansorena Gratacos Miguel; Perdomo Luz Ivone, 2017, pág. 81)

Frente a esta amenaza creciente y aún más insidiosa, este libro destacó la necesidad de dotar a Francia con una capacidad de defensa activa, capaz de detectar y contrarrestar los ataques, recomendando crear una agencia nacional responsable de este ámbito. Así, a mediados de 2009 se crea la Agencia Nacional para la Seguridad de Sistemas de Información (ANSSI) con la misión de proteger los sistemas nacionales de información y proponer las normas que deben aplicarse para la protección de los sistemas estatales y verificar la aplicación de las medidas adoptadas. Por medio del Centro Operacional de la Seguridad de Sistemas de Información (COSSI), se detectan y responden ataques y se vigilan las redes más sensibles de la administración y se desarrollan nuevas capacidades defensivas. (Ortiz, Javier Ulises; Fonseca Claudia; Ansorena Gratacos Miguel; Perdomo Luz Ivone, 2017, pág. 81)

Por su parte, la Secretaria General de la Defensa de la Seguridad Nacional (SGDS) mantiene dos planes de trabajo: el Plan Vigipirate, el cual incluye vigilancia, prevención y protección, y cuyo principal objetivo es la preparación del Estado para la protección de la población, su infraestructura y sus instituciones, El otro plan, el Plan de Piranet,, es complementario del anterior, es para dar respuesta a amenazas o ataques a gran escala utilizando medios específicos de agresión o que afectan a los entornos particulares, donde se requiere la intervención del estado en una grave crisis, constituyéndose así en uno de los pilares de la estrategia de esa defensa. Cabe destacar que en 2012 se anunció que en la Escuela Interarmas del Ejército francés se estableció un centro de conocimientos de ciberdefensa. (Ortiz, Javier Ulises; Fonseca Claudia; Ansorena Gratacos Miguel; Perdomo Luz Ivone, 2017, pág. 81)

En 2013, el Gobierno francés dio a conocer su actualización del Libro Blanco sobre Defensa y Seguridad Nacional y la Ley de Programación Militar, documentos los cuales determinan la orientación estratégica del sistema de defensa del país para el periodo 2014 a 2019. Como amenazas y riesgos consecuentes de la globalización: aprecian los movimientos de bienes, mercancías y/o personas, los riesgos para la seguridad marítima en el marco del aumento de la piratería, los riesgos terroristas y, entre otros “el incremento exponencial de los riesgos mediante ciberataques contra las infraestructuras digitalizadas y las amenazas que pueden dirigirse contra el espacio extra-atmosférico”. (Ortiz, Javier Ulises; Fonseca Claudia; Ansorena Gratacos Miguel; Perdomo Luz Ivone, 2017, pág. 81)

La ciberdefensa en Alemania.

Este país, desde el año 2006, posee una unidad militar de operaciones de red de computadoras (Computer Network Operations Unit - CNO) que está subordinada al comando estratégico de inteligencia militar, centrada en la guerra cibernética, con capacidad para operar en redes hostiles y desarrollar simulaciones de ataques cibernéticos. El desarrollo de la capacidad alemana de ciberdefensa y ciberataque, debe ser considerado, teniendo en cuenta los antecedentes de ataques realizados contra redes gubernamentales durante los últimos años y que el país procura estar al nivel de otros países de la OTAN, como Estados Unidos, Francia y Gran Bretaña. (Ortiz, Javier Ulises; Fonseca Claudia; Ansorena Gratacos Miguel; Perdomo Luz Ivone, 2017, pág. 83)

En 2011, el Gobierno alemán dio a conocer su Estrategia de Ciberseguridad**.** Por medio de esta, se crea el Centro Nacional de Ciberdefensa (CNA), el cual analiza los ataques recibidos por la Red de Internet y asiste al Gobierno sobre la mejor forma de combatirlos. Posteriormente, en el año 2016, Alemania dio a conocer su nuevo Libro Blanco de la Defensa, el cual realiza recomendaciones para mejorar las capacidades de ciberdefensa y mejorar la resiliencia de la población civil frente a crisis de seguridad. (Ortiz, Javier Ulises; Fonseca Claudia; Ansorena Gratacos Miguel; Perdomo Luz Ivone, 2017, pág. 83)

La ciberdefensa en España.

El 28 de enero de 2010 se aprueba el documento “Visión de la Ciberdefensa Militar", el cual orientará la definición, desarrollo y empleo de las capacidades militares del país para garantizar la eficacia en el uso del ciberespacio en las operaciones militares. Resultado de ello, en julio de 2011 se aprobará el “Concepto de Ciberdefensa Militar”, que definirá principios, objetivos y retos

de la ciberdefensa en el ámbito militar y un año después de anunciará el "Plan de Acción para la Obtención de la Capacidad de Ciberdefensa Militar", el cual comenzará la coordinación de los esfuerzos entre el ámbito conjunto y específicos a partir del aprovechamiento de las estructuras existentes. (Ortiz, Javier Ulises; Fonseca Claudia; Ansorena Gratacos Miguel; Perdomo Luz Ivone, 2017, pág. 84)

El 19 de febrero de 2013, el Ministro de Defensa establece la creación del Mando Conjunto de Ciberdefensa de las Fuerzas Armadas (MCCD) el cual es el responsable de realizar el planeamiento y la ejecución de las acciones relativas a la ciberdefensa militar en las redes y sistemas de información y telecomunicaciones de las Fuerzas Armadas u otros que pudiera tener encomendados, así como contribuir a la respuesta adecuada en el ciberespacio ante amenazas o agresiones que puedan afectar a la Defensa Nacional. Asimismo, el MCCD dirige y coordina la actividad de los centros de respuesta a incidentes de seguridad de la información del Ejército de Tierra, del Ejército del Aire y de la Armada, y el centro de operaciones de seguridad de la información del Ministerio de Defensa. (Ortiz, Javier Ulises; Fonseca Claudia; Ansorena Gratacos Miguel; Perdomo Luz Ivone, 2017, pág. 84)

Define como objetivo global en el ámbito de la ciberseguridad "Garantizar un uso seguro de las redes y los sistemas de información a través del fortalecimiento de nuestras capacidades de prevención, detección y respuesta a los ciberataques" (Ortiz, Javier Ulises; Fonseca Claudia; Ansorena Gratacos Miguel; Perdomo Luz Ivone, 2017), para lo cual se requerirá una actualizada Política de Ciberseguridad Nacional. (Ortiz, Javier Ulises; Fonseca Claudia; Ansorena Gratacos Miguel; Perdomo Luz Ivone, 2017, pág. 84)

> En materia de Defensa expone la necesidad de "ampliar y mejorar permanentemente las capacidades de Ciberdefensa de las Fuerzas Armadas que permitan una adecuada protección de sus Redes y Sistemas de Información y Telecomunicaciones, así como de otros sistemas que afecten a la Defensa Nacional" (Ortiz, Javier Ulises; Fonseca Claudia; Ansorena Gratacos Miguel; Perdomo Luz Ivone, 2017), consolidando la implantación del Mando Conjunto de Ciberdefensa y potencializando su cooperación con los diferentes órganos con capacidad de respuesta ante incidentes cibernéticos en aspectos de común interés así como las capacidades militares y de inteligencia para ejercer la respuesta oportuna, legítima y proporcionada en el ciberespacio ante amenazas o agresiones que puedan afectar a la Defensa. (Ortiz, Javier Ulises; Fonseca Claudia; Ansorena Gratacos Miguel; Perdomo Luz Ivone, 2017, pág. 84)

Como puede observarse en la información volcada precedentemente, el área de ciberseguridad dentro de algunas de las principales potencias militares, viene desarrollándose hace desde hace más de una década, no solamente en lo referido al ámbito militar o civil, sino también incluye el marco normativo, como puede observarse en la actualización de los libros blancos de la defensa de algunos de los países nombrados precedentemente

Otro aspecto relacionado con la ciberseguridad, es que además del marco jurídico y la creación de organismos militares especializados en esta temática, el ámbito de la educación y capacitación adquiere suma importancia, como el caso de Israel y Francia, los cuales cuentan con centros de capacitación especializados en operaciones en el ciberespacio, lo que demuestra la importancia que ha tomado el ciberespacio en el ámbito militar.

En comparación con lo ocurrido dentro de las organizaciones militares de nuestro país en general y en particular del Ejército Argentino, el desarrollo es mucho más reciente, tanto en lo militar, el marco legal, los aspectos doctrinarios y de capacitación. A pesar de esto, las

perspectivas son positivas, lo que demuestra un avance para mejorar las capacidades actuales en materia de ciberdefensa.

En función del análisis comparativo de las diferentes fuentes bibliográficas consultadas, se pueden extraer las siguientes conclusiones, correspondientes al segundo capítulo.

La pérdida de la iniciativa y el control en el ciberespacio dificultará el planeamiento del apoyo logístico para el sostenimiento, entorpeciendo el asesoramiento al comandante para el desarrollo de las operaciones militares.

La dependencia de los medios militares a las tecnologías de la información y comunicación (TIC) y sistemas de información y gestión logística, constituye un objetivo rentable a los ciberataques. Este aspecto se puede comprobar en la actualidad, ya que algunas que las principales potencias dentro de sus fuerzas armadas, le han dado suma importancia al ciberespacio, creando centros de capacitación o modificando sus organizaciones militares, para incluir a la ciberdefensa como un ámbito vital para el desarrollo de las operaciones. Comparando con lo ocurrido en el Ejército Argentino, el desarrollo en materia de ciberdefensa es mucho más reciente.

Desarrollar organizaciones especializadas en ciberseguridad permite tener una visión más detallada de las principales causas y consecuencias de las operaciones en el ciberespacio y como puede verse afectado el sostenimiento logístico. Esto contribuye a entender que, la obtención de la superioridad en el ciberespacio es un requisito para la efectividad de las operaciones militares

Tanto el conocimiento de los efectos de las ciberoperaciones, como el desarrollo de las capacidades de ciberseguridad, permitirán diseñar y desarrollar un sistema seguro y eficaz ante las acciones en el ciberespacio que puedan afectar el sostenimiento logístico, pudiendo establecer medidas para mitigar sus efectos y garantizar el apoyo.

Si bien se puede afirmar que la problemática relacionada con la ciberdefensa ha tomado relevancia en los últimos años en el ámbito de las Fuerzas Armadas en general, y del Ejército

Argentino en particular, resulta sumamente necesario continuar evolucionando en materia de ciberdefensa, aplicada a los sistemas logísticos empleados en la actualidad.

Teniendo en cuenta no solo las dificultades presentadas por el marco legal y doctrinario; sino también por la complejidad del ambiente y la diversidad de enfoques existentes.

CAPÍTULO III. Análisis de las Acciones de ciberseguridad para garantizar el sostenimiento logístico

Introducción

Para dar cierre a esta investigación, en este último capítulo el cual se planteó el siguiente objetivo evaluar y analizar qué acciones y perspectivas se están llevando a cabo actualmente en los sistemas informáticos logísticos de la fuerza en la paz y si estas acciones evitarían que el sostenimiento logístico se vea afectado en operaciones. Este capítulo reúne lo concerniente a infraestructuras críticas de la información en Argentina, las acciones llevadas a cabo por la fuerza, las particularidades de los sistemas informáticos logísticos empleados en el Ejército Argentino, sus perspectivas y las respectivas conclusiones.

Sección I. La gestión de las infraestructuras críticas de la información en Argentina

Las infraestructuras críticas en nuestro país han ido cambiando a lo largo del tiempo, por lo que resulta necesario mencionar lo siguiente:

> El concepto de infraestructura crítica de la información ha ido evolucionando junto con el crecimiento de la tecnología hasta convertirse en un activo esencial para cualquier sociedad. En la actualidad, dichas infraestructuras de un país se encuentran en el plano terrestre, marítimo, aéreo, espacial o el ciberespacio, y requieren de un plan de prevención y protección para conservar los servicios esenciales de la comunidad ya que, de lo contrario, la interrupción de estos ocasionará consecuencias perjudiciales para la sociedad. (Taberna Agostina ; Rutz Guillermo, 2021, pág. 8)
>
> Considerando que las infraestructuras críticas han incorporado una gran cantidad de componentes informáticos, los responsables de ejecutar ciberataques, aprovechan sus puntos débiles para generar impacto en el funcionamiento de un Estado (salud, seguridad, defensa, logística, bienestar social y economía),

empleando técnicas que se renuevan constantemente, indicando que la prevención ya no es la única acción efectiva a realizar. Lejos de reemplazar las formas tradicionales de ataque como son la ciberguerra, el ciberterrorismo, el ciberespionaje y el ciberdelito, los gobiernos han comenzado a trabajar en la ciberseguridad y ciberdefensa de sus países. Efectivamente, la estabilidad del país y la confianza del ciudadano en el Estado se verían comprometidas si ocurriera un ataque masivo y coordinado a alguno o varios de los sectores definidos como infraestructura crítica, y es por ello que el Estado debe centrarse en medidas de prevención, protección y resiliencia de estas. (Taberna Agostina ; Rutz Guillermo, 2021, pág. 8)

El abordaje de los Sistemas de Protección de Infraestructuras Críticas de la República Argentina desarrolla la idea respecto a que el auge de las ciberamenaza y los ciberataques ocurridos contra infraestructuras críticas en el mundo obliga a la Argentina a estar preparada para anticipar, prevenir, proteger y defender aquellas infraestructuras que brindan servicios esenciales. El Estado debe garantizar el normal y continuo funcionamiento de dichos servicios, y para ello es indispensable trabajar y desarrollar conceptos como inteligencia, ciberinteligencia, ciberamenazas, ciberataques, ciberseguridad y ciberdefensa en torno a la protección de las infraestructuras críticas, con el fin de decidir qué camino deberá tomar la Argentina con relación a la ciberseguridad. (Taberna Agostina ; Rutz Guillermo, 2021, pág. 10)

El Sistema de Protección de Infraestructuras Críticas de la República Argentina (SIPICRA) permite coordinar todos los sistemas institucionales ya existentes para brindar protección de la sociedad y los servicios que son esenciales mediante el empleo de un esquema innovador y multisectorial. El SIPICRA,

> junto al Sistema de Inteligencia Nacional, no solo brinda más capacidades para la identificación, detección y mitigación de ciberamenazas y ciberataques, sino también la obtención de un lenguaje común para entender el fenómeno y aplicar las técnicas necesarias con el fin de gestionar las contramedidas que garanticen la resiliencia de las infraestructuras críticas de la Nación y sus valores democráticos. (Taberna Agostina ; Rutz Guillermo, 2021, págs. 10-11)
>
> Otro tema de importancia al cual debe hacerse referencia, es a la importancia en el uso y práctica consistente de simuladores de ciberseguridad como medio de ejercitación de los operadores críticos de las infraestructuras críticas. El aumento del uso de las tecnologías de la información y la comunicación (TIC) debido a la crisis surgida de la pandemia, provocó un aumento de la compleja interrelación entre sistemas en infraestructuras críticas. Esto, a su vez, generó nuevas vulnerabilidades de seguridad y ciberamenazas que podrían afectar a la sociedad. Además, las simulaciones en forma de ciberejercicios se consideran herramientas para proporcionar una comprensión de cómo se realizan los ciberataques y cómo pueden afectar las infraestructuras críticas nacionales. Estos métodos sobre cómo protegerlos a escala mundial desde un único punto de vista remoto pueden convertirse en una ventaja estratégica. A medida que los especialistas realizan simulacros para adquirir experiencia de primera mano antes de enfrentarse a la realidad, los ciberejercicios buscan imitarlos para responder de forma eficaz contra determinadas crisis cibernéticas y, por tanto, defender la infraestructura crítica. (Taberna Agostina ; Rutz Guillermo, 2021, pág. 11)

Como puede observarse, las infraestructuras críticas y de la información incluyen el área de defensa, por lo que resulta necesario no descuidar esta temática dentro de las fuerzas

armadas, ya que estas poseen información sensible e importante. Para esto es importante proteger a estas infraestructuras, que, en el caso de ser afectadas, no solo causarían inconvenientes, a las organizaciones militares como el Ejército Argentino, la Armada o la Fuerza Aérea, sino que podrían ocasionar daños de importancia e incluso anular el sistema de defensa nacional de nuestro país.

Sección II. La ciberseguridad en el Ejército Argentino y su perspectiva futura

La Dirección de Ciberdefensa del Ejército Argentino. De acuerdo a lo publicado en su página oficial, la Dirección de Ciberdefensa del Ejército fue inaugurada en el año 2014. La mencionada dirección depende de la Dirección General de Comunicaciones e Informática y "trabaja en conjunto con las direcciones de Ciberdefensa de las otras Fuerzas Armadas, el Comando Conjunto de Ciberdefensa y la subsecretaria de Ciberdefensa del Ministerio de Defensa" (Teniente Coronel Juan Carlos Guerra, 2023, pág. 35) . La Dirección de Ciberdefensa del Ejército Argentino realiza una importante cantidad de actividades referidas a la Ciberdefensa, que son de suma importancia para la fuerza.

Entre sus objetivos se encuentran la prevención, el tratamiento, la identificación y la resolución de incidentes de seguridad sobre los sistemas informáticos que conforman la infraestructura crítica del Ejército Argentino., como así también:

> La Dirección de Ciberdefensa del Ejército Argentino mediante su página Web, a la cual se accede mediante el Portal Ejército Argentino, brinda capacitación, publicaciones de interés y alertas en todo lo vinculado a la ciberdefensa, actualizaciones e incidentes que ocurren dentro del ámbito de los sistemas informáticos de la fuerza. (Ejército Argentino, 2022)

Diferentes acciones realizadas en el ámbito de la fuerza. Como se menciona en el apartado anterior la creación de la Dirección de Ciberdefensa del Ejército es bastante reciente, como así también el Comando Conjunto de Ciberdefensa.

Ambas organizaciones, son el principal elemento para prevenir y neutralizar las acciones que se ejecuten en el ciberespacio, contra las infraestructuras críticas del Ejército y de las otras Fuerzas Armadas.

Esta nueva amenaza obligó a la fuerza a actualizar su doctrina, incluyendo a la ciberdefensa dentro de sus organizaciones, particularmente en la unidades y subunidades independientes del arma de comunicaciones

Dentro de las acciones de importancia, junto con la actualización de doctrina dentro de la fuerza, se está teniendo en cuenta la necesidad de agregar a personal especialista en ciberdefensa dentro de los cuadros de organización, inicialmente en las Unidades y Subunidades independientes del arma de comunicaciones.

En cuanto a instrucción y capacitación dentro del Ejército Argentino, la Dirección de Educación Operacional, en coordinación con la Escuela de Comunicaciones, inició en el año 2019, la impartición de los cursos básico y avanzado de ciberdefensa para el personal del arma de comunicaciones y del sistema de computación y datos (SCD), y de esta manera contar con personal especialista dentro de los cuadros de organización de nivel unidad y subunidad, e incluso hasta el nivel Gran Unidad Combate.

Relacionado con el párrafo anterior, en el marco del desarrollo de los ejercicios de alumnos ejecutados en la Escuela Superior de Guerra, se incluyen actividades de ciberdefensa, mostrando así la inclusión de esta temática como parte de la formación académica.

Otro dato de interés es la modificación del cuadro de organización del Batallón Operaciones Electrónicas 601, al cual se le agregó una fracción con capacidades en materia de ciberdefensa; integrando de esta manera la guerra electrónica y la ciberdefensa. Posteriormente, en el mes de septiembre de 2022, mediante el financiamiento del Fondo Nacional de la Defensa (FONDEF), se lo equipó, con cabinas y material específico, para conformar la primera compañía de ciberdefensa táctica.

En lo que respecta a las acciones realizadas por la Dirección de Ciberdefensa del Ejército, desde su página Web, ha determinado una serie de normas y recomendaciones para mitigar los efectos sobre la ciberdefensa de la fuerza, las cuales serán detalladas a continuación.

Aspectos troncales sobre ciberseguridad. En el ámbito del Ejército Argentino hay muchas variables y aspectos que debemos considerar a la hora de prevenir posibles incidentes de ciberseguridad. Estos son sólo 7 de los más importantes:

1. Asegurarse de proteger los datos, especialmente aquellos sensibles, impidiendo el acceso indebido, negando todos los permisos que no estén explícitamente autorizados.
2. Evitar contraseñas comunes y utilizar contraseñas fuertes y robustas lo más larga posible, al menos ocho caracteres, que combine caracteres alfanuméricos, utilizar mayúsculas y minúsculas y que incluyan caracteres especiales; asimismo conviene cambiar de contraseña con cierta periodicidad.
3. Ser conscientes de la posibilidad de sufrir un ciberataque, el personal debe estar advertidos de los riesgos de un ataque, es necesario evitar que comentan errores comunes. Los Oficiales de ciberdefensa guarnicionales contarán con un plan de comunicación para actuar en situaciones de crisis, como por ejemplo sufrir una amenaza.
4. Realizar análisis periódicos internos en el servidor, de ser posibles diarios y también monitorear y revisar la actividad que se realiza en la red.
5. Restringir el acceso a los equipos, restringir acceso a aquella información que no necesiten, así como inhabilitar los accesos desde varios sistemas, porque puede ser la puerta de acceso de un hacker. No permitir que personas ajenas utilicen los equipos.

6. Proteger todos los dispositivos conectados con herramientas eficaces y mantenerlas actualizadas periódicamente.
7. Realizar copias de seguridad de todo para prevenir ataques cibernéticos y poder restaurar en caso de vulneración del sistema. (Ejército Argentino, 2022)

Sección III. Particularidades de la ciberseguridad de los sistemas informáticos logísticos del Ejército Argentino.

La Directiva del Subjefe del Estado Mayor General del Ejército N°842/ 22 define lo siguiente:

> Las amenazas cibernéticas están consideradas como uno de los principales riesgos por la alta probabilidad de que ocurran y por el impacto que podrían tener. Existen variados y constantes intentos de intrusión en los sistemas, que el hombre común no ve y que incluso a veces al especialista también le cuesta ver. Hay amenazas muy sofisticadas que se caracterizan también por el sigilo. (Ejército Argentino, 2022, pág. 1).
>
> Actualmente tampoco es necesario tener grandes conocimientos técnicos para agredir los sistemas de información, ya que hasta en internet se pueden encontrar gran cantidad de herramientas ofensivas y observar el intercambio de instrumentos de hacking en foros dedicados a esta materia. (Ejército Argentino, 2022, pág. 1).

Por lo expuesto anteriormente resulta necesario concientizar y capacitar al personal que opera los sistemas informáticos logísticos, permitiendo de esta manera mejorar la eficacia del sistema de seguridad de la información y producir capacidades y habilidades en materia seguridad informática, de tal manera que los operadores cuenten con los recursos necesarios para enfrentar las amenazas que puedan afectar el sostenimiento logístico de la fuerza, ya sea en la paz o en operaciones.

Para lograr esto, durante el año 2023 se inició un plan de concientización sobre ciberdefensa para el personal de la fuerza, el cual permitirá reducir las violaciones a las políticas de seguridad informática, a nivel Usuario y mejorar la capacitación del personal especialista. Este plan será de aplicación para todo el Ejército Argentino, en particular para las fracciones del arma de comunicaciones que trabajen en materia de ciberdefensa, Para ello todos los niveles de Comando serán responsables de conocer, cumplimentar y controlar todos aquellos aspectos que establezca el mencionado plan.

La ciberseguridad y los sistemas informáticos logísticos de la fuerza. Como se mencionó anteriormente el sistema informático más utilizado en la logística de la fuerza es el SIDIGEA, la cual permite el manejo de inventarios de efectos de arsenales dentro de la fuerza. El mencionado sistema puede ser utilizado tanto en la paz como en operaciones, ya que la información de la misma puede ser actualizada en tiempo real.

En cuanto a la ciberseguridad del SIDIGEA, se accede a la misma a través del portal informático del Ejército Argentino, el cual permite el acceso a la intranet de la fuerza. Esto presenta una dificultad ya que en el caso de que el portal de la fuerza sea afectado por un incidente de seguridad informática, no se tendría acceso a la misma, lo cual causaría dificultades e incluso impediría proporcionar la información necesaria para dar un adecuado sostenimiento y apoyo logístico.

Otro detalle a tener en cuenta es que los usuarios y operadores de esta herramienta, no poseen los conocimientos necesarios en materia de ciberseguridad, lo que provocaría que el sistema sea vulnerable ante una amenaza que afecte la seguridad informática.

En el caso de las Unidades que tienen relación con el sostenimiento logístico de la fuerza, como es el caso de Batallones de Intendencia, Batallones de Arsenales y Bases de Apoyo Logístico, algunas de ellas no cuentan con personal capacitado en materia de ciberdefensa, lo que provoca que los mencionados elementos sean vulnerables y puedan ser víctima de

incidentes que afecten su seguridad informática, y en algunos casos puedan ser anulados ocasionando serios inconvenientes a la logística de la fuerza, no solamente en su asiento de paz sino también durante el desarrollo de operaciones militares.

Existen otras herramientas de información logística empleadas dentro de la fuerza como son el sistema COMPR.AR, VISA FLOTA y GEDO, pero dichos sistemas no son de uso exclusivo militar, sino que también son utilizadas en el ámbito civil y no solamente en sectores relacionados con la logística.

Para ello resulta necesario capacitar a los usuarios de los sistemas informáticos logísticos de las unidades mencionadas, para de esta manera minimizar los efectos que puede ocasionar un incidente que afecte la seguridad informática del elemento y de esta manera evitar que el sostenimiento y apoyo logístico se vea afectado.

La Perspectiva hacia el futuro del Ejército Argentino en el ámbito de la ciberdefensa. En referencia a las acciones futuras que van a desarrollarse dentro del Ejército Argentino, se puede mencionar que:

> Los nuevos planes de campaña, expuestos durante el mes de agosto del presente año los cuales van a tener un carácter conjunto y en donde no solamente serán de ejecución en el ámbito terrestre, naval o aéreo, sino que también tendrán aplicación en el ciberespacio, ya que es un entorno no físico y donde las amenazas iniciaran sus ataques en este ámbito, siendo denominadas operaciones multimodales y de multidominio; para esto, resulta necesario contar con los recursos humanos, materiales y financieros, para poder vigilar y controlar el ciberespacio. Dichos planes de campaña son de suma importancia para la actualización y el planeamiento de las Fuerzas Armadas, ya que desde el año 2010 no había un plan sólido en materia de capacidades y que el empleo de

> fuerzas según la situación geopolítica que se estuviera desarrollando en el escenario internacional que se daba por esos años. (Mariano Lacroix, 2022).

El Teniente Coronel Juan Carlos Guerra en un artículo publicado en la Revista Soldados en diciembre de 2023, menciona la importancia del desarrollo de la Ciberdefensa en el Ejército Argentino:

> El ciberespacio es un ámbito más donde se desarrollan las operaciones militares. Es por ello que las Fuerzas Armadas de todo el mundo cuentan con organizaciones especialmente equipadas e instruidas para llevar adelante operaciones en el ciberespacio. Nuestros sistemas están cada vez más informatizados y, aun sin darnos cuenta, al hacer uso de ellos nos movemos en el ciberespacio. Protegernos y estar en capacidad de influir en el oponente y sus oponentes y sus redes es la razón de ser de la Ciberdefensa. (Teniente Coronel Juan Carlos Guerra, 2023, págs. 35-37)

Para dar un cierre a este tercer capítulo y en relación con el objetivo planteado, y el análisis realizado, se pueden determinar las siguientes conclusiones, las cuales se detallan a continuación.

Las infraestructuras críticas de la información, las cuales abarcan al ámbito de defensa, deben ser protegidas ante acciones de ciberataques, de tal manera que sean lo menos vulnerables posibles. Para el caso del sostenimiento logístico, el cual es vital para el desarrollo de las operaciones, antes, durante y después del desarrollo de estas, resulta necesario un estricto complimiento de las normas y procedimientos establecidos, los cuales no solamente deben ser tenidos en cuenta en la paz, sino que también en operaciones

Para lograr esto, es necesario desarrollar capacidades de ciberseguridad que permitan responder ante un ciberataque y estar en capacidad de contrarrestarlo de forma inmediata. Por ello, la instrucción y capacitación de los operadores y usuarios, permitirá conformar un sistema

capaz de volver a su estado inicial en corto tiempo, tras ser atacado. Esto permitirá ser efectivos en cuanto a la ciberesiliencia en las estrategias de ciberseguridad y estar en capacidad de recobrar la iniciativa.

Contar con equipamiento de ciberdefensa en el nivel táctico adquiere un papel preponderante para el logro de los objetivos que se impongan durante el desarrollo de una operación militar.

Resulta necesario la capacitación del personal que opera las aplicaciones para la información y gestión logística, en todo lo referido a ciberdefensa y no solamente limitarlo a al personal del arma de comunicaciones

La actualización de los planes de la fuerza y la incorporación de equipo específico para ciberdefensa es un primer paso muy alentador en esta área, ya que el dominio del ciberespacio es un ámbito de rápida evolución que no debe ser descuidado y debe ser tenido en cuenta en la actualidad.

La implementación de un plan de concientización de ciberdefensa dentro de la fuerza, permitirá concientizar y capacitar al personal que opera herramientas informáticas logísticas y reducir las violaciones a las políticas de seguridad informática

Las organizaciones que actúan en el ciberespacio en la actualidad pueden ejecutar operaciones, que en muchos casos pueden ocasionar daños de mayor impacto e importancia, que las realizadas de manera convencional, sin tener en cuenta si son organizaciones, instituciones civiles, militares o si es en la paz o en un conflicto armado.

Conclusiones Finales

Los antecedentes respecto a los incidentes ocurridos en el área logística civil, relacionados con la ciberseguridad y ciberdefensa, es un aspecto que debe ser tenido en cuenta para el fortalecimiento de la ciberseguridad dentro del sostenimiento y la logística de la fuerza, ya que los ciberataques no discriminan organizaciones ni fronteras.

El marco legal en materia de ciberseguridad es bastante nuevo en cuanto a su implementación, en comparación con algunas potencias del primer mundo, en lo que respecta al ciberespacio. Si a esto le agregamos el marco jurídico de la República Argentina, el cual separa claramente el área de Defensa del área de Seguridad Interior, junto con la escasez de una legislación particular para las acciones en el ciberespacio, da como resultados inconvenientes para el desarrollo de capacidades para la defensa de las infraestructuras críticas y logísticas, sean civiles o militares.

La doctrina vigente en materia de logística y ciberdefensa en el ámbito de la fuerza, se encuentra en proceso de actualización ya que esta es obsoleta y escasa en lo que respecta a ciberdefensa. Así también la creación de organizaciones especializadas en ciberdefensa es bastante reciente, en comparación con países del primer mundo, los cuales poseen capacidades mucho más desarrolladas y actualizadas que en nuestro país, no solamente en lo operacional, sino también en el ámbito educativo.

La pérdida del control y el dominio del ciberespacio puede ocasionar la carencia de información confiable y exacta, lo cual puede provocar inconvenientes para el planeamiento del apoyo logístico para el sostenimiento y un asesoramiento equivocado al comandante para el desarrollo de las operaciones.

La dependencia de la informática y el uso de sistemas informáticos en todos los ámbitos de la fuerza, y particularmente para el sostenimiento logístico, ya sea en la paz o en operaciones,

ha provocado que las ciberoperaciones y la ciberseguridad adquieran un papel preponderante en el campo de batalla actual y futuro

La impartición de cursos de capacitación para el personal que utiliza sistemas informáticos logísticos, la actualización de los planes y la incorporación de tecnología específica para ciberdefensa en el ámbito de la fuerza, otorga una perspectiva positiva hacia el futuro en esta área.

La implementación de un plan de concientización de ciberdefensa dentro de la fuerza, permitirá concientizar y capacitar al personal que opera sistemas informáticos logísticos y reducir las violaciones a las políticas de seguridad informática

De acuerdo al presente trabajo, y en función del análisis realizado se puede observar que el estado de ciberseguridad de los sistemas informáticos logísticos de la fuerza, registra un avance positivo en cuanto a su desarrollo presente.

En cuanto a la perspectiva hacia el futuro, la inclusión de la ciberdefensa en el planeamiento logístico, otorga un panorama alentador hacia el desarrollo de capacidades de ciberdefensa en un futuro próximo.

Por lo expuesto anteriormente se considera necesario no descuidar la ciberdefensa en el área logística del Ejército Argentino, siendo necesario para ello, contar con personal altamente capacitado, no solamente en el área logística, sino que también en aspectos relacionados con la ciberdefensa, los que le proporcionarán al comandante un ciberespacio seguro y confiable, la libertad de acción necesaria para el desarrollo de las operaciones y un sostenimiento logístico ininterrumpido a las tropas empeñadas.

Referencias

Anca, Luis Javier. (18 de Agosto de 2015). La conducción de las operaciones de ciberdefensa: Principios básicos en el campo de combate moderno. (Trabajo Final Integrador de Especialización). *Escuela Superior de Guerra, Facultad del Ejército*. Ciudad Autónoma de Buenos Aires, Buenos Aires, Argentina.

Cabrera, C. I. (Diciembre de 2019). Empleo de las redes informáticas en Ciberoperaciones en el marco de la Gran Unidad de Batalla. (Trabajo Final Integrador de Especialización). *Escuela Superior de Guerra, Facultad del Ejército.* Ciudad Autónoma de Buenos Aires, Buenos Aires, Argentina.

Caterina Chen. (14 de Septiembre de 2022). *Significados*. https://www.significados.com/tic/

CuatroOchenta. (2022). *Claves para gestionar la ciberseguridad en logística y transporte.* España.

Diaz, R. M. (2021). *Estado de la ciberseguridad en la logística de América Latina y el Caribe*. https://hdl.handle.net/11362/47240

Dirección de Ciberdefensa del Ejército Argentino. (2023). Clases- Capacitación para Oficiales de Ciberdefensa. Salta, Salta, Argentina.

Dirección de Educación Operacional. Escuela de Comunicaciones. (2022). Clases- Curso de Ciberdefensa. Campo de Mayo, Buenos Aires, Argentina.

Ejército Argentino. (2004). *Logística de Material - ROD-19-02.* Buenos Aires: Dirección de Organización y Doctrina.

Ejército Argentino. (2015). *Conducción para las Fuerzas Terrestres- ROB 00- 01.* Dirección de Organización y Doctrina.

Ejército Argentino. (2015). *Régimen Funcional de Intendencia. Tomo I Efectos I y III de Intendencia- RFD-21-01-I.* Dirección de Organización y Doctrina.

Ejército Argentino. (29 de Junio de 2020). Directiva del SubJefe del Estado Mayor General del Ejército N° 03/G/20. *Normas y Procedimientos de Ciberdefensa*. Ciudad Autónoma de Buenos Aires, Buenos Aires, Argentina: Estado Mayor General del Ejército.

Ejército Argentino. (05 de Abril de 2021). Directiva del Subjefe del Estado Mayor del Ejército Nº 829-21. *Directiva Anual de Ciberdefensa*. Ciudad Autónoma de Buenos Aires, Buenos Aires, Argentina: Estado Mayor General de Ejército.

Ejército Argentino. (11 de Noviembre de 2022). Directiva del Subjefe del Estado Mayor General del Ejército N°842/ 22. *Plan de Concientización de Ciberdefensa*. Ciudad Autónoma de Buenos Aires, Buenos Aires, Argentina: Estado Mayor General del Ejército.

Ejército Argentino. (27 de Agosto de 2022). *Portal Ejército Argentino*. Direccion de Ciberdefensa del Ejército Argentino: https://portal.ejercito.mil.ar/proxy/4d07afa5/https/www.ciber.ea.mil.ar/

Escuela Superior de Guerra. (2022). *Clases- Logística Conjunta*. Ciudad Autónoma de Buenos Aires, Argentina.

Escuela Superior de Guerra. (2022). *Clases- Sistemas de Información Logística*. Ciudad Autónoma de Buenos Aires, Argentina.

Escuela Superior de Guerra. (2022). Seminario de Ciberdefensa. Ciudad Autónoma de Buenos Aires, Buenos Aires, Argentina.

Harri Pyykköa, Jarkko Kuusijärvib Bilhanan Silverajanc, Ville Hinkkaa. (27-30 de Abril de 2020). Proceedings of 8th Transport Research Arena. *The Cyber Threat Preparedness in the Maritime Logistics Industry*. Helsinki, Finlandia: Rethinking Transport.

Haschak, M. S. (Febrero de 2019). *Cyber Security and Its Implication on Material Handling and Logistics*. Estados Unidos: College Industry Council on Material Handling Education.

Haschak, M. S. (Febrero de 2019). Cyber Security and Its Implication on Material Handling and Logistics. Estados Unidos.

Honorable Congreso de la Nación. (1988). Ley de Defensa Nacional Nª 23.554. Publicado en Boletín Oficial Nª 26.375. Ciudad Autónoma de Buenos Aires, Buenos Aires, Argentina.

Leonardo Anibal Belizon. (Octubre de 2014). Herramienta informática de empleo en la Logístico de Material del Componente Ejército del Teatro de Operaciones para el registro integral de los efectos de Arsenales e Intendencia. (Trabajo Final Integrador de Especialización). *Escuela Superior de Guerra, Facultad del Ejército*. Ciudad Autónoma de Buenos Aires, Buenos Aires, Argentina.

Mariano Lacroix. (25 de Agosto de 2022). *Zona Militar*. https://www.zona-militar.com/2022/08/25/nuevo-hito-para-el-ciclo-de-planeamiento-militar-argentino/

Mayor Bryan J. Quinn, E. d. (Cuarto Trimestre de 2022). Military Review. *La competencia logística en el teatro de operaciones. Fundamental para ganar el combate moderno*. Fort Leavenworth, Kansas., Estados Unidos: Army University Press.

Mónica Maria Jimenez. (23 de Marzo de 2022). *Blog Pirani*. Ciber resiliencia: que es y por que es tan importante.: https://www.piranirisk.com/es/blog/ciber-resiliencia-que-es-y-su-importancia

Ortiz, Javier Ulises; Fonseca Claudia; Ansorena Gratacos Miguel; Perdomo Luz Ivone. (Marzo de 2017). Informe Final de Proyecto de Investigación.La Defensa Cibernetica. Alcances estratégicos, proyecciones doctrinarias y educativas. *Escuela Superior de Guerra, Facultad del Ejército*. Ciudad Autónoma de Buenos Aires, Buenos Aires, Argentina.

Poder Ejecutivo Nacional. (9 de Mayo de 2019). *Directiva Estratégica de Ciberseguridad de la República Argentina*. Ciudad Autónoma de Buenos Aires, Buenos Aires, Argentina.

Presidencia de la Nación. Ministerio de Defensa. (2015). *Libro Blanco de la Defensa.* Ministerio de Defensa.

Secretaria de Gobierno de Modernización de la Jefatura del Gabinete de Ministros. (24 de Mayo de 2019). Estratégia Nacional de Ciberseguridad.

Symetrics Lab. (10 de Octubre de 2023). *Logística y ciberseguridad, ¿Cómo la ciberseguridad protege tus operaciones logísticas?* https://es.linkedin.com/pulse/log%C3%ADstica-y-ciberseguridad-c%C3%B3mo-la-protege-tus-operaciones

Taberna Agostina ; Rutz Guillermo. (Diciembre de 2021). Aportes a la ciberdefensa y ciberseguridad para la gestión de las infraestructuras críticas de la información en Argentina. *Revista Defensa Nacional N° 6,* 171-186.

Teniente Coronel Juan Carlos Guerra. (Diciembre de 2023). Revista Soldados. *La Ciberdefensa en el Ejército Argentino*. Ciudad Autónoma de Buenos Aires, Buenos Aires, Argentina: Fundación Soldados.

Visa Argentina. (7 de Septiembre de 2022). *Visa*. https://www.visa.com.ar/empresas/soluciones-comerciales/tarjetas-corporativas/visa-flota.html