LA CIBERDEFENSA Y LA CIBERINTELIGENCIA MILITAR

Por CR (R) **PATRICIO GABRIEL CASARINO Y DR. JAVIER ULISES ORTIZ**

Palabras Clave:
> Tecnología de la información
> Ciberguerra
> Operaciones militares
> Ciberespacio

ARTÍCULO CON REFERATO

Resumen
Por los constantes cambios que presentan el ciberespacio y sus actores, en un mundo cada vez más tecnológicamente integrado y dependiente, se requieren más capacidades para adaptarse y, de manera constante, se deben actualizar las doctrinas para prevenir operaciones e incorporar tecnología y capacitación. En Defensa Nacional, los Estados y la ciberdefensa encuentran en la ciberinteligencia militar una respuesta reciente para asegurar acciones que puedan prever, detectar y enfrentar, neutralizando los desafíos y las ciber amenazas.

Introducción
Los conflictos bélicos evolucionaron rápidamente respecto al pasado y derivan, actualmente, en los que corresponden a esta era de la globalización, que se caracteriza por los avances de las tecnologías de la información y comunicación (TIC). Con la aparición del ciberespacio para la confrontación de intereses, aparece también un nuevo ámbito para el desarrollo de los conflictos que podrían

Conforme al pensamiento militar ruso actual sobre las "guerras de nueva generación", la guerra híbrida se basa en el uso combinado de medios militares y no militares, para emplear básicamente todo el espectro del inventario de políticas de un Estado, incluidos diplomáticos, económicos, políticos, sociales, información y también medios militares.

ser considerados como otra variante de las guerras modernas, pero que reúne todas las características para tener una categoría propia: la "guerra cibernética" o "ciberguerra".

Norbert Winer, profesor del *Massachussets Institute of Technology,* fue quien en 1964 creó el término "cibernética" al designar la disciplina que estudia el problema del control y la comunicación en general. Por otra parte, William Gibson, autor de obras de ciencia ficción, fue quien desarrolló en 1984 el término "ciberespacio" como un lugar indefinido en el mundo que existe y donde millones de personas viven a diario[1].

Asimismo, François Huyghe, especialista francés en ciencias de la información estratégica, amplió la distinción entre Ciberguerra *(cyberwar – information warfare),* que se orienta estrictamente a la conducción de operaciones militares según los principios relativos de los canales de información, tendientes a destruir o controlar los sistemas de comunicación del adversario y; Netguerra (*netwar*), que corresponde a los conflictos de gran escala entre naciones o sociedades comerciales. En este caso el agresor buscará modificar o pervertir lo que una población civil (consumidores, opinión pública, electores, clientes, etc.) sabe o cree de ella misma o del mundo que lo rodea[2].

Esta distinción es coincidente con la perspectiva estadounidense de la *RAND Corporation,* uno de los principales centros de desarrollos militares donde inicialmente se analizó la agenda de los conflictos por desarrollarse en el ciberespacio, producto de la globalización y los necesarios cambios organizacionales que se requerirán para enfrentarlos, y que asignarán una especial importancia a la defensa de las *"infraestructuras tecnológicas"* que las soportan[3].

En concordancia con ello, asesores de la Defensa del gobierno de EE.UU. han definido a la ciberguerra como "una acción hostil en el ciberespacio cuyos efectos amplían o son equivalentes a una violencia física importante. En el mundo físico, los gobiernos ejercen prácticamente un monopolio en el uso de fuerza a gran escala, el defensor tiene un conocimiento íntimo del terreno y los ataques terminan como consecuencia del desgaste o del agotamiento. Tanto los recursos como la movilidad son costosos", donde países como los miembros del Consejo de Seguridad de la ONU (Estados Unidos, Rusia, Gran Bretaña, Francia y China) tienen una capacidad mayor que otros Estados y actores no estatales para controlar el mar, el aire o el espacio, pero requieren desarrollar nuevas capacidades frente a las vulnerabilidades que se les presentan en materia cibernética[4].

Así, "la ciberguerra irrumpió en nuestras sociedades para incrustarse en todos los campos, desde el militar hasta el civil. Las redes informáticas provocaron una suerte de extensión de los campos de batalla hacia un mundo virtual en plena interacción con la realidad [...] la ciberguerra pone en tela de juicio los fundamentos mismos de la forma de hacer la guerra. La ciberguerra obtiene resultados importantes a bajo costo. Es más barato movilizar 10.000 computadoras que 10.000 soldados. La tecnología de las redes reequilibra la geopolítica". Existe evidencia de esto y fue cuando insurgentes iraquíes el 18 de diciembre de 2009 hackearon sistemas de operaciones militares de los aviones Predator de Estados Unidos mediante un *software* que costaba alrededor de 26 U$S[5].

En abril de 2007, Estonia recibió el primer ataque masivo de la guerra cibernética, cuando redes de robots informáticos, conocidos como *botnets,* enviaron cantidades masivas de mensajes basura *(spam)* y pedidos automáticos *online* para saturar los servidores, las páginas web de bancos, medios de prensa y organismos gubernamentales colapsándolos debido a niveles sin precedente de tráfico de datos, para provocar que la población de Estonia se quedara sin accesos a cajeros automáticos o al *homebanking,* y el gobierno perdiera la comunicación entre sus organismos y la capacidad de funcionamiento del país.
Estos ataques duraron varias semanas produciéndole al país inmensas pérdidas económicas.
En este caso, si bien la agresión

fue supuestamente interestatal, no existió el uso de armas de ninguna clase, pero los efectos fueron traumáticos para la Nación.

Otro ejemplo de este tipo de conflictos es el ataque en 2010 del gusano informático llamado *Stuxnet*, que atacó las centrifugadoras de uranio de Irán. Este gusano afectó a los equipos con Windows y fue capaz de reprogramar controladores lógicos ocultando esta acción y afectando a los sistemas de monitorización y control de procesos (SCADA). Es importante destacar que actualmente toda central eléctrica o de distribución de energía, planta potabilizadora de agua, red ferroviaria de subterráneos o el funcionamiento de los semáforos de una gran ciudad es controlada por los SCADA *(Supervisory Control And Data Acquisition)*.

Dentro de este nuevo escenario, genéricamente se pueden establecer cuatro tipos de eventos que se distinguen por su finalidad u objetivos en el ciberespacio: el cibercrimen, activismo cibernético, ciberguerra/ciberdefensa, espionaje y sabotaje cibernético. Si bien esta clasificación es arbitraria, muchas de estas formas se combinan con uno o más fines, asimismo las variantes que existen en ellas son múltiples y excederían el objetivo de este trabajo.

En cuanto a la ciberguerra, el objetivo buscado es afectar de manera sustancial el potencial de una Nación, llevándola al borde del colapso y de ese modo imponer la voluntad del agresor, sea de manera abierta o encubierta, para realizar operaciones en todos los niveles: táctico, operacional y estratégico. Por su parte, el espionaje o sabotaje cibernético tiene por finalidad u objetivo principal obtener información o producir un daño que le genere una ventaja cualitativa al agresor. Frente a ello, las Fuerzas Armadas deben afrontar el constante cambio del ámbito operacional y dar respuestas, primeramente doctrinarias.

Enseñanzas de las ciberoperaciones militares

Durante los últimos años, en el marco del planeamiento militar, las FFAA a nivel internacional han iniciado las acciones del desarrollo orgánico, doctrinario y tecnológico de la capacidad de ciberdefensa militar para disponer de un conjunto de aptitudes que le permitan operar en esta nueva dimensión de los conflictos armados (el ciberespacio), llamada por algunos países como "capacidad de ciberguerra". Estas aptitudes dependen, no solo del conocimiento y habilidades del personal organizado, equipado e instruido especialmente para realizar operaciones militares en el ciberespacio, sino de todo personal que opere medios TIC en el ciberambiente militar o en el ciberespacio, aun por motivos particulares.

A modo de ejemplo, son de destacar las acciones ejecutadas en el ciberespacio por parte de Rusia contra Ucrania entre 2014 y 2015, que han sido caracterizadas como inmersas en una "Guerra Híbrida". Esta nueva forma de guerra tuvo como objetivo derrotar al oponente rompiendo su capacidad de resistencia sin lanzar un ataque militar a gran escala. Conforme al pensamiento militar ruso actual sobre las "guerras de nueva generación", la guerra híbrida se basa en el uso combinado de medios militares y no militares, para emplear básicamente todo el espectro del inventario de políticas de un Estado, incluidos diplomáticos, económicos, políticos, sociales, información y también medios militares[6]. La evolución de este conflicto, aún latente, tuvo diferentes acciones de Rusia y respuestas de Ucrania que dieron lugar al empleo por ambas partes de acciones y medios cibernéticos como lo ocurrido el 23 de diciembre de 2015, cuando tres empresas de distribución regional de energía de Ucrania recibieron un ataque cibernético sin precedentes, que causó cortes de energía masivos y provocó el "apagón" que afectó a 225.000 clientes en el país.

Un análisis del Instituto Español de Estudios Estratégicos del Ministerio de Defensa valorizó las operaciones del ciberespacio en ese conflicto

1. Arpagian, 2009.
2. Huyghe, 2001.
3. Arquila, J. y Ronfeldt; 2001.
4. NYE, 2012.
5. Apagian, 2010.
6. Rácz, 2015.

al señalar que los "acontecimientos en Ucrania han hecho saltar las alarmas en determinados ámbitos ante el paradigma de conflicto empleado por Rusia. La real o aparente combinación de diferentes medios, militares o no, de manera abierta o encubierta, en el marco de un plan bien orquestado han incrementado las voces que señalan que nos encontramos –una vez más– en una era que presenta una nueva tipología de conflictos. Esta nueva modalidad de conflicto se llama guerra híbrida y está generando un amplio debate que permita su comprensión plena"[7].

Estos ataques fueron realizados por acciones remotas de agresores cibernéticos que aprovechan la manipulación de credenciales digitales legítimas obtenidas a través de diferentes procedimientos, y así desconectar de manera sincronizada y coordinada los sistemas de energía. Mientras las empresas de energía aplicaban sus planes de contingencia, los servicios solo pudieron restaurarse de manera limitada. Consecuencia de ello, la OTAN (Organización del Tratado del Atlántico Norte) proporcionó un apoyo de equipos "ciber" especializados en la evaluación de daños al gobierno de Ucrania, del mismo modo que lo ocurrido en Estonia en 2007. En particular, cabe destacar algunas de las conclusiones elaboradas por el *Departament of Homeland Security* de Estados Unidos[8]. En el mismo, se concluye que este ciberataque explotó vulnerabilidades comunes y conocidas, pero que tomó de sorpresa a usuarios desprevenidos acerca de los riesgos que ocasionarían por el uso inadecuado de los sistemas y componentes TIC de las centrales de energía operadas por empresas ucranianas.

Luego, el gran objetivo de este nuevo tipo de guerra "no guerra"[9] fue la destrucción de las capacidades informacionales y las infraestructuras críticas. Esta concepción de la guerra se desarrolla en EE.UU, Europa, India, Rusia y China donde comenzaron a conceptualizar estratégicamente sobre el tema y generar acciones. De este modo el espacio informacional y la infraestructura crítica que los soporta, se encuentran en una concepción amplia que las interrelaciona estratégicamente[10].

En el ámbito militar, las medidas de seguridad de contrainteligencia contemplan todas las acciones necesarias de prevención para el uso seguro de los medios informáticos y de comunicaciones, la seguridad física de las instalaciones y la protección de los diferentes medios de soporte de la información.

La ciberdefensa en la Defensa Nacional

La Ley 23.554 de 1988 define a la Defensa Nacional como la integración y la acción coordinada de todas las fuerzas de la Nación para la solución de aquellos conflictos que requieran 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 la libertad de sus habitantes. La responsabilidad primaria de las Fuerzas Armadas es la defensa ante agresiones militares estatales contra la soberanía e integridad territorial de la Nación. Se destaca que la Ley 24.059 de Seguridad Interior determina el empleo de las fuerzas policiales y de seguridad

AÑO	PRINCIPALES CONCEPTOS REFERIDOS A LA CIBERDEFENSA
Libro Blanco 2010	Se requiere una "estrategia de carácter defensivo" de ciberdefensa "frente a una eventual agresión militar estatal externa, y para desarrollar eficazmente la conducción de las operaciones militares y repeler con éxito dicha agresión" en una nueva dimensión operacional, asegurando el "ciberespacio específico de los componentes del Sistema de Defensa Nacional, y aquellos ámbitos de interés estratégico asociados ante agresiones externas contra el ciberespacio nacional (ciberguerra)".
Libro Blanco 2015	El ciberespacio "se convirtió en un nuevo dominio, creado por el hombre, en donde ocurren cada vez con mayor frecuencia interacciones sociales y donde el conflicto armado internacional, como fenómeno social, podría desarrollarse". "No es un ámbito militar operacional específico, sino que es una dimensión operacional transversal a los ambientes operacionales tradicionales en el que pueden desarrollarse operaciones de naturaleza militar, lo cual requiere un planeamiento militar conjunto". Adquiere importancia "para el desarrollo de operaciones militares, este ámbito artificial y sin precisa locación física no constituye un ambiente operacional específico sino otro, con medios y reglas propias, que atraviesa a los espacios terrestres, marítimos y aeroespaciales. Pudiendo afectar infraestructuras críticas se requiere una "adaptación de los sistemas de defensa y el desarrollo de capacidades específicas".

La Estrategia define como principios rectores de la ciberseguridad: el respeto por los derechos y libertades individuales, el liderazgo, la construcción de capacidades y fortalecimiento federal, la integración internacional, la cultura de ciberseguridad, la responsabilidad compartida y el fortalecimiento del desarrollo socioeconómico.

de la Nación frente a acciones de naturaleza delictiva y establece que las Fuerzas Armadas solo pueden eventualmente, y cuando lo requiera el sistema de seguridad interior, enfrentar amenazas de naturaleza no militar.

Desde 1998, el Ministerio de Defensa ha publicado y actualizado el *libro Blanco de la Defensa Nacional* donde a lo largo de los últimos años incorporó una visión estratégica sobre el "quinto espacio" (el ciberespacio) como ámbito de las operaciones militares (ver tabla).

La estrategia de ciberseguridad Nacional

Por su parte, el Decreto 577/17 establece las respectivas competencias ministeriales en orden a conformar una Estrategia de Ciberseguridad Nacional según cada Ministerio o Subsecretaría, asignándole al Ministerio de Defensa la determinación de los objetivos y políticas del área de su competencia y la realización de estudios y trabajos técnicos en la formulación y ejecución de las políticas nacionales en lo que hace específicamente a la Defensa Nacional.

Asimismo, el Ministerio de Modernización, mediante la Secretaría de Gobierno de Modernización, lleva adelante la responsabilidad de presidir el Comité de Ciberseguridad, que es integrado por representantes del Ministerio de Modernización, de Defensa y de Seguridad Interior para desarrollar la referida estrategia en coordinación con las áreas de la Administración Pública Nacional y elaborar el plan de acción.

El Decreto 557/17 define al objetivo de la estrategia como: "el desarrollo de las previsiones en materia de protección del ciberespacio, destinado a implementar en forma coherente y estructurada acciones de prevención, detección, respuesta, defensa y recuperación frente a las amenazas cibernéticas, conjuntamente con el desarrollo de un marco normativo acorde" y; Ciberespacio como: "el dominio global y dinámico compuesto por las infraestructuras tecnológicas –incluida Internet–, las redes y los sistemas de información y de telecomunicaciones, plantea renovadas oportunidades a la sociedad en su conjunto, a la par de importantes desafíos en cuanto a su protección y seguridad".

La Subsecretaría de Ciberdefensa del Ministerio de Defensa

Fue establecida en 2016 sobre la base de otras áreas preexistentes y es dependiente de la Secretaría de Ciencia, Tecnología y Producción para la Defensa. En el marco de la actualización de la Administración Pública Nacional (Decreto 174/2018) tiene como funciones, entre otras, la de asistir al Secretario en el planeamiento, diseño y elaboración de la política de ciberdefensa de acuerdo a lo establecido en el Ciclo de Planeamiento de la Defensa Nacional en coordinación con la Subsecretaría de Planeamiento Estratégico y Política Militar y ejercer el control funcional sobre el Comando Conjunto de Ciberdefensa de las Fuerzas Armadas.

El Comando Conjunto de Ciberdefensa del EMCO

Se creó el 14 de mayo de 2014 (Res. 343/14) y tiene como misión ejercer la conducción de las Operaciones de Ciberdefensa en forma permanente a los efectos de garantizar las operaciones militares del Instrumento Militar de la Defensa Nacional en cumplimiento de su misión principal y de acuerdo a los lineamientos establecidos en el Planeamiento Estratégico Militar. Son sus funciones, entre otras, coordinar las acciones con los centros de ciberdefensa de las Fuerzas Armadas y establecer los criterios rectores a nivel del Instrumento Militar para la determinación de infraestructuras críticas a ser protegidas. Asimismo, el Comando entiende en los estándares y procedimientos de Ciberdefensa, criptografía e informática forense y la supervisión de los

7. Sanchez Herraez, 2014.
8. ICS-CERT, 2016.
9. RToffler, 1994.
10. Ortiz, Gratacos, Fonseca, 2016.

La ciberinteligencia militar constituirá un conocimiento indispensable para un adecuado planeamiento y ejecución de todas las operaciones y actividades que deberán realizar las tropas en todos los niveles de conducción.

CV

PATRICIO GABRIEL CASARINO

Coronel (R) del Arma de Ingenieros del Ejército Argentino. Oficial de Estado Mayor y de Inteligencia. Licenciado en Estrategia y Organización (ESG-IESE). Docente e investigador del Instituto de Inteligencia de las FFAA (IIFA). Investigador acreditado por la UNDEF. Se desempeñó como Jefe de Estado Mayor y luego Comandante del Comando Conjunto de Ciberdefensa (EMC).

JAVIER ULISES ORTIZ

Doctor en Ciencia Política, Licenciado y Profesor Universitario en Relaciones Internacionales (USAL). Posdoctorado en la UNCuyo. Posgraduado en Estrategia I-II (ESG-IESE) y en Política y Estrategia de Defensa (US National Defense University). Docente e investigador del IIFA y profesor en la ESGC, Maestría en Estrategia Militar y en la ESG-EA. Investigador acreditado por la UNDEF y por los Ministerios de Educación y de Defensa.

centros de respuesta de cada Fuerza y capacitación de personal propio. Además, interviene en la elaboración, revisión y experimentación de la Doctrina de Ciberdefensa.

La ciberdefensa en la nueva Directiva de Política de Defensa Nacional

Mediante el Decreto 703/18, la DPDN (Directiva de Política de Defensa Nacional) dedica varios ítems de la Defensa Nacional a la ciberdefensa y, al realizar la Apreciación del Escenario Global y Regional - Diagnóstico Global (Ministerio de Defensa, 2018) establece modificaciones a su antecesora en 2014 y define nuevos escenarios, riesgos, amenazas y medidas a adoptar.

En su Capítulo I Apreciación del Escenario Global y Regional respecto al Diagnóstico Global, entre otros, indica que: "el desarrollo tecnológico incrementó los riesgos asociados a la militarización del ciberespacio. La disuasión se ha extendido al ámbito cibernético, al tiempo que han surgido nuevos desafíos producto de las tensiones entre una mayor conectividad, la privacidad y los derechos de la ciudadanía. Tanto los Estados como los actores no estatales están desarrollando medios cibernéticos para explotar las vulnerabilidades inherentes a los sistemas de comando, control, comunicaciones, inteligencia, vigilancia y reconocimiento. De igual forma, las redes terroristas explotan el ciberespacio para reclutar miembros, recaudar fondos y difundir su propaganda. Las amenazas cibernéticas sofisticadas provienen de organizaciones militares y agencias de inteligencia de otros Estados. Si bien los gobiernos tecnológicamente avanzados explotan sus ventajas comparativas con relación al resto de los países, el despliegue de operaciones disruptivas en el ciberespacio también está al alcance de las naciones menos desarrolladas. El abordaje de esta problemática desde la perspectiva de la Defensa Nacional requiere adoptar medidas y acciones tendientes a resguardar la seguridad cibernética de las infraestructuras críticas del Sistema de Defensa Nacional y de aquellas que sean designadas para su preservación, independientemente del origen de la agresión [...]".

Además, como posicionamiento estratégico del país indica que: "La consolidación del ciberespacio como un ambiente operacional militar configura una amenaza de interés estratégico para la Defensa Nacional. El desarrollo de las nuevas tecnologías de información y comunicaciones, junto con la extensión global de la conectividad, han convertido al ciberespacio en un ámbito en el que los Estados despliegan operaciones de agresión e influencia sobre las naciones adversarias. La tendencia hacia una mayor competencia estratégica internacional en el ciberespacio ha llevado a numerosos países a

desarrollar capacidades cibernéticas de vanguardia, a fin de garantizar la seguridad de sus infraestructuras informáticas críticas o estratégicas". Frente a ello, refiere que el país "debe adecuar sus organizaciones militares al impacto que emerge de estos nuevos riesgos" y "la política de ciberdefensa debe orientarse a la reducción gradual de las vulnerabilidades que emergen de la informatización de los activos estratégicos de interés para la Defensa Nacional. Esta tarea debe contemplar la cooperación con otras áreas del Estado que tengan responsabilidad en la política de ciberseguridad nacional [...]".

En cuanto a la vigilancia y control del ciberespacio, el Ministerio de Defensa "deberá fortalecer las capacidades de vigilancia y control del ciberespacio a fin de 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 [...]".

Finalmente, dentro de las instrucciones para la reforma del sistema de Defensa Nacional, ordena al Ministerio de Defensa proponer "un plan para reformar el Instrumento Militar de la Nación a fin de recuperar la capacidad de cumplir su misión principal". Para lo cual, el Estado Mayor Conjunto deberá elevar los planes que estime necesarios para el cumplimiento de los siguientes objetivos, destacándose el "Fortalecimiento de la arquitectura del Sistema de Comando, Control, Comunicaciones, Computación, Inteligencia, Vigilancia y Reconocimiento (C4ISR) de los niveles Estratégico Militar, Operacional y Táctico [...]".

La Estrategia Nacional de Ciberseguridad de la República Argentina

El 24 de mayo de 2019, la Secretaría de Gobierno de Modernización de la Jefatura de Gabinete de Ministros de la Nación emitió la Resolución N° 829/2019, a través de la cual establece la Estrategia Nacional de Ciberseguridad y crea la Unidad Ejecutiva del Comité de Ciberseguridad, enmarcada en el Decreto N° 577/2017. La estrategia establece acciones que brindan un espacio seguro para las actividades en el ciberespacio de carácter público o privado que desarrollarán a partir de la coordinación y cooperación de la Administración Pública Nacional; de otros poderes nacionales; de las administraciones y poderes de las jurisdicciones provinciales, de la Ciudad Autónoma de Buenos Aires y municipales; del sector privado; de las organizaciones no gubernamentales y de las entidades académicas. Como objetivo, la estrategia establece: concientizar el uso seguro del ciberespacio, capacitar y educar en el uso seguro del ciberespacio, desarrollar un marco normativo, fortalecer capacidades de prevención, detección y respuesta, proteger y recuperar los sistemas de información del sector público, fomentar la industria de la ciberseguridad y la cooperación internacional y proteger las infraestructuras nacionales de información.

De esta manera, define como principios rectores de la ciberseguridad: el respeto por los derechos y libertades individuales, el liderazgo, la construcción de capacidades y fortalecimiento federal, la integración internacional, la cultura de ciberseguridad, la responsabilidad compartida y el fortalecimiento del desarrollo socioeconómico.

En lo concerniente al ámbito militar, la estrategia indica que "el escenario internacional presenta fuertes antagonismos y tensiones. Un número importante de países están haciendo un uso militar creciente del Ciberespacio, para generar inestabilidad y desconfianza entre las naciones y temores en las sociedades. En este marco, la República Argentina promoverá en todos los foros en los que participe el uso pacífico del Ciberespacio y apoyará toda iniciativa que tenga por fin la instauración de valores como la Justicia, el respeto al Derecho Internacional, el equilibrio y la disminución de la brecha digital entre las naciones, para impulsar el diálogo y la cooperación. El Ciberespacio debe constituirse en un dominio en el

que impere la paz, sustrayéndolo de posibles conflictos armados"[11].

La ciberinteligencia militar para la ciberdefensa

La Ley 23.544/88 de Defensa Nacional en la producción de Inteligencia Estratégica Militar define como responsabilidad "proporcionar información e inteligencia" para contribuir a la Defensa Nacional, asegurando la ejecución de operaciones militares conjuntas y combinadas.

Por su parte, la Ley 25.520/01 de Inteligencia Nacional y sus respectivas reglamentaciones define a la Inteligencia Estratégica Militar como "la parte de la Inteligencia referida al conocimiento de las capacidades y debilidades del potencial militar de los países que interesen desde el punto de vista de la Defensa Nacional, así como el ambiente geográfico de las áreas estratégicas operacionales determinadas por el planeamiento estratégico militar". De este modo, establece que "los organismos de inteligencia de las Fuerzas Armadas tendrán a su cargo la producción de inteligencia estratégica operacional y la inteligencia táctica necesaria para el planeamiento y conducción de operaciones militares".

En materia doctrinaria el Reglamento de Doctrina Básica para la Acción Militar Conjunta del EMCO (RC 00-01.2005), entiende que en el sistema de inteligencia militar operacional "debe prevalecer como signo distintivo la creatividad para innovar en la búsqueda permanente de nuevos puntos de vista, nuevas fuentes de información, nuevos medios, procedimientos y técnicas, un sistema de inteligencia creativo es el primer instrumento para evitar la sorpresa, la creatividad en inteligencia es la capacidad de visualizar tempranamente los cambios en el pensamiento enemigo e inferir sus nuevos paradigmas"[12].

En ese marco, la ciberinteligencia será entendida como el conocimiento resultante del proceso a que es sometida la información.

La revista *New York Magazine* expresó, en 1996, que "Ciber" era un prefijo perfecto, porque puede ser insertado en cualquier palabra antigua para que parezca nueva, fresca y, por lo tanto, extraña.

Así, frente a ello, surgen distintas interpretaciones del término "ciberinteligencia" (CYBINT):

> Es entendido como el resultado del análisis forense del código informático empleado por un atacante.
> Se considera en tanto que su único objetivo es generar información que sirva para mejorar desde un punto de vista técnico la arquitectura de ciberseguridad de una empresa o institución.
> Es percibido como la proyección en el ciberespacio de las funciones tradicionales de captación de datos que lleva a cabo un servicio de inteligencia, situándola en el mismo plano que otras actividades de obtención como, por ejemplo, la inteligencia de señales (SIGINT) o la inteligencia de fuentes abiertas (OSINT)[13].
> Determinado desde lo organiza-

cional como "todos los esfuerzos realizados por una organización de inteligencia para prevenir que adversarios, organizaciones de inteligencia enemigas u organizaciones criminales puedan acceder y recopilar información digital sensible o inteligencia a través de ordenadores, redes y equipamientos asociados"[14].

> Considerado desde lo operacional como "operaciones de ciberinteligencia, vigilancia y reconocimiento (ciber IVR) que comprenden actividades en el espacio cibernético para reunir inteligencia activa de los sistemas del blanco y del adversario requeridos para apoyar las operaciones militares. Las misiones cibernéticas ISR para la defensa pueden ser apoyadas por las capacidades nacionales o de cada una de las fuerzas armadas. Por su parte, las operaciones cibernéticas de preparación operacional del ambiente (ciber OPE) son todas las actividades que realizan para preparar y posibilitar la ciberinteligencia, vigilancia y reconocimiento, y las operaciones defensivas y ofensivas. Estas son las operaciones típicas del nivel operacional de guerra"[15].

Sin embargo, expertos en informática entienden a la ciberinteligencia como "el producto obtenido tras aplicar a la información del ciberespacio distintas técnicas de análisis que permitan su transformación en conocimiento, de forma que resulte útil a la hora de tomar decisiones con el menor nivel de incertidumbre posible"[16].

Por último, ambos expertos resaltan la importancia del componente humano como factor clave dada la carencia de "cultura de ciberinteligencia" y que las organizaciones que abordan esta nueva cultura son recientes, que en tiempo real posibilita "mantener la visibilidad del panorama de amenazas y permite que su equipo de seguridad pueda responder con más rapidez. Esto incluye detectar actividades maliciosas que ya están dentro de su red, analizarlas y comprender los objetivos de los atacantes"[17].

Asimismo, surge una interpretación dual del mismo concepto ciberinteligencia:

> En el sentido restringido, "como fuente específica de información que puede alertar sobre peligros a la seguridad en cualquier dominio o ambiente en el cual se producen relaciones e interacciones sociales que, tal como se indicó anteriormente, pueden corresponder a tierra, mar, aire, espacio y ciberespacio"[18].

> En el sentido amplio, se refiere al "conjunto de actividades que apuntan a obtener conocimiento previo de amenazas y vulnerabilidades a los sistemas de comunicación de información a través de una variedad de medios técnicos", para lo cual se requiere de instituciones y servicios profesionales específicos en la materia, que incluyen la ciberinteligencia[19], ya que el ciberespacio es "la mayor fuente de obtención (de datos) entre las denominadas abiertas" donde "las redes sociales representan una fuente fundamental de obtención, tanto por la relativa facilidad con la que es posible explotar sus vulnerabilidades, como por la información que es publicada en ellas por sus usuarios (datos personales, filiaciones, posturas políticas e incluso información sensible)", así como en las cerradas y en la *Deep Web*[20].

Luego, una visión integradora de ambas interpretaciones (amplia y restringida) "permitiría entender la ciberinteligencia como el resultado de un ambiente en el cual se producen interacciones sociales –el ciberespacio–, el cual es usado por las personas, organizaciones e instituciones para la generación, almacenamiento y transmisión de información, donde ante la necesidad de ofrecer ciberseguridad y anticipar los peligros que pueden afectarla es necesario contar con una capacidad de ciberinteligencia"[21].

Luego, la ciberinteligencia militar constituirá un conocimiento indispensable para un adecuado planeamiento y ejecución de todas las operaciones y actividades que deberán realizar las tropas en todos los niveles de conducción. Tendrá responsabilidad primaria en el estudio del ambiente cibernético para establecer la influencia que ejercerán sus distintos componentes sobre las actividades propias y del enemigo.

Proporcionará las capacidades y debilidades asignadas al enemigo en el ambiente cibernético, necesarias para la adopción de resoluciones adecuadas por parte del comandante. Contribuirá a la seguridad a través de operaciones de medidas de seguridad en el ambiente cibernético y promoverá las medidas de seguridad de contra inteligencia a aplicarse para disminuir el riesgo generado en este nuevo ambiente.

Conclusiones

La situación actual del ciberambiente militar y las amenazas conocidas o potenciales a las cuales están expuestas las FFAA y los sistemas del Instrumento Militar obligan a iniciar un proceso de concientización en ciberseguridad, que pongan a cada integrante de las FFAA y a las autoridades responsables en las diferentes funciones involucradas, frente a las necesidades de prevención, reducción de riesgos,

11. Jgm, 2019.
12. Doldán Estrada, 2014.
13. Torres, Soriano, 2017.
14. Insa, 2011.
15. de Vergara, E. y Trama, G., 2017.
16. Rufián Albarrán y Burgos, 2017.
17. Peñaranda, 2019.
18. Sancho Hirane, 2018.
19. Gruszczak, 2016.
20. Cubeiro, 2016.
21. Sancho Hirane, 2018.

alerta temprana, descubrimiento de vulnerabilidades, detección de incidentes y respuestas eficaces para, al menos, mitigar los efectos inmediatos y recuperar los activos e infraestructuras críticas de información ante ciberagresiones o ciberataques. Allí surge la necesidad de entender a la ciberinteligencia en general y la militar en el campo estratégico militar como una actividad necesaria para enfrentar esos desafíos a la Defensa Nacional en materia de ciberdefensa. Las FFAA tienen establecidas normas y procedimientos de seguridad informática que requieren una actualización permanente para hacer frente a nuevas amenazas cibernéticas, que se propagan con rapidez y producen efectos dañinos o tienen un potencial daño oculto. Estas acciones crean las condiciones necesarias que requieren la conducción y ejecución de operaciones del ciberespacio por parte de los organismos de Ciberdefensa, así como la formación y capacitación de todo el personal de las FFAA para operar en el ciberespacio de manera segura.

BIBLIOGRAFÍA

ARQUILA, J., y RONDFELD, D. (2003). *Redes y guerras en red*. El futuro del terrorismo, el crimen. Alianza Editorial, España.

-

ARPAGIAN, N. (2009). *La Cyberguerre, la guerre numérique a comencé*. Ed Magnard-Vouibert. París y reportaje (2010) en: http://www.pagina12.com.ar/diario/elmundo/4-145379-2010-05-09.html

-

CASARINO, P. (2018). Ciberdefensa una opinión personal, Gabriel Manual de Informaciones. Diciembre de 2018 N° 4 Vol LX, Buenos Aires.

-

CUBEIRO, Enrique (2016). Ciberinteligencia. DIAZ, Antonio (Ed). *Conceptos Fundamentales de Inteligencia*. Tirant lo Blanch, España, pág 50.

-

de VERGARA, E. y TRAMA, G. (2017). *Operaciones militares cibernéticas: Planeamiento y Ejecución en el Nivel Operacional*. Buenos Aires: Escuela Superior de Guerra Conjunta. Disponible en: http://www.cefadigital.edu.ar

-

DPDN (2018), Directiva de Política de Defensa Nacional, Ministerio de Defensa de la República Argentina, DECTO-2018-703-APN-PTE

-

DOLDÁN ESTRADA, F. (2014). *Diseño de un subsistema de inteligencia conjunto para el apoyo meteorológico en el nivel operacional*. Buenos Aires: Escuela Superior de Guerra Conjunta. Disponible en http://www.cefadigital.edu.ar/

-

GRUSZCZAK, A. (2016). *New Security Challenges*. Polonia, Palgrave Macmillian. Referido en

-

HUYGHE, F. (2001) *L'ennemi à l'ère numérique: Chaos, information, domination*. Broché, Defense, Paris.

-

ICS-CERT (2016). *Alert (IRALERT H1605601) CyberAttack Against Ukrainian Critical Infrastructure. The Industrial Control Systems Cyber Emergency Response Team. Departament of Homeland Security*, EEUU: https://ics-cert.us-cert.gov/alerts/IR-ALERT-H-16-056-01.

-

INSA (2011). *Cyber Intelligence: Setting the Landscape for an Emerging Discipline*. The Intelligence and National Security Alliance. Cyber Intelligence White Paper (July). https://images.magnetmail.net/images/clients/INSA/attach/INSA_CYBER_INTELLIGENCE_2011.pdf

-

JGM (2019) Estrategia Nacional de Ciberseguridad, Res. 829,19, Jefatura de Gabinete de Ministros, Secretaría de Gobierno de Modernización. https://www.boletinoficial.gob.ar/detalleAviso/primera/208317/20190528

-

NYE, J. (2012). Ciberguerra y ciberpaz. Proyecto Syndicate. 2012 : http://www.project-syndicate.org/commentary/cyber-war-and-peace/spanish

-

ORTIZ, J.U.; GRATACOS, M. y FONSECA, C. (2016). La Defensa Cibernética. Buenos Aires: Escuela Superior de Guerra, Ejército Argentino. Disponible en: http://www.cefadigital.edu.ar/

-

RÁCZ, A. (2015). *Russia's Hybrid War in Ukraine. Breaking the Enemy's Ability to Resist*. FIIA, Helsinski.

-

PEÑARANDA, A. (2019). La tendencia clave 2019: la ciberinteligencia. Thrive, 19 de febrero de 2019, España:https://thrive.dxc.technology/es/2019/02/16/la-tendencia-clave-de-2019-la-ciberinteligencia/

-

SANCHEZ HERRAEZ, Pedro (2014). La Nueva guerra Híbrida: un somero análisis estratégico. Instituto Español de Estudios Estratégicos, Nº 54/2014. España, 29 de octubre de 2014.

-

TOFFLER, A. y H. (1994). Las Guerras del Futuro, la supervivencia en el alba del siglo XXI. Barcelona. Plaza & Janes, Madrid.

-

TORRES SORIANO, M. (2017) Concepto y niveles de la ciber-inteligencia, Revista de Aeronáutica y Astronáutica, Ejército del Aire, España. Nº 862 (abril)(pp. 316-320). http://www.ejercitodelaire.mde.es/stweb/ea/ficheros/pdf/C2993F28850C8BD1C12580FB00283DCC.pdf

-

RUFIÁN ALBARRÁN, M. (2017). Ciberinteligencia: conocer para decidir correctamente. InnoTec, Madrid.https://www.innotecsystem.com/documentos/medios/2017marzo_cuadernos.pdf

-

SANCHO HIRANE, C. (2018). Ciberinteligencia. Contextualización, aproximación conceptual, características y desafíos. Centro de Investigaciones y Estudios Estratégicos de la ANEPE, Ministerio de Defensa Nacional de Chile, CT Nº1/18. https://www.anepe.cl/wp-content/uploads/Cuaderno-Trabajo-N%C2%B01-2018.pdf