Eissa, Sergio G.

El ciberespacio y sus implicancias para la defensa nacional : aproximaciones al caso argentino

Sergio G. Eissa / Sol Gastaldi /
Iván Poczynok / Elina Zacarías Di Tullio

El ciberespacio y sus implicancias para la defensa nacional

Aproximaciones al caso argentino

Introducción

En la última década, numerosos estudios e investigaciones han caracterizado al *ciberespacio* como un dominio de naturaleza militar. En esta línea, la conveniencia de desarrollar capacidades militares de *ciberdefensa* por parte de los Estados ha pasado a ocupar cada vez más espacios en los debates sobre la defensa nacional y el diseño de las fuerzas militares.

Sin embargo, a diferencia de los tradicionales escenarios de batallas –la tierra, el mar, el aire y el espacio–, este nuevo dominio militar no es físico, sino *virtual* (Joyanes Aguilar, 2010). Esta caracterización abre un abanico de interrogantes desde el punto de vista de la defensa nacional: pensar el ciberespacio como un entorno con sus propios medios y reglas, con la particularidad de no poseer locación física específica, implicaría un cuestionamiento a la utilidad de las categorías tradicionales con las que abordamos la *guerra real*.

En relación con este punto, algunos autores entienden que la revolución informática causará cambios en cómo las sociedades pueden entrar en conflicto y en la forma en que sus fuerzas armadas librarán las guerras (Arquilla y Ronfeldt, 1993). Sin embargo, a la hora de precisar los alcances de estos ajustes y los efectos físicos que podrían derivarse de la utilización del ciberespacio con fines militares, los acuerdos se diluyen. Así, las preguntas más recurrentes entre los analistas refieren, por ejemplo, a si es posible que una guerra se desarrolle fuera de ambientes físicos, a la conveniencia de analizar el ciberespacio como un escenario militar y a la capacidad de los Estados de proteger militarmente este ámbito.

En este artículo presentaremos algunos elementos generales que atraviesan el debate actual sobre la utilización del ciberespacio con fines militares. En particular, intentaremos responder a la pregunta sobre si existe una dimensión específicamente militar del ciberespacio. La clarifi-

cación de estas cuestiones nos permitirá analizar su impacto en la defensa nacional y, posteriormente, establecer bajo qué condiciones el Estado debería desarrollar capacidades militares para desenvolverse en él. Finalmente, consideraremos la legislación nacional en materia de defensa, para evaluar el rol que el sistema de defensa nacional podría asumir en torno a esta problemática.

Globalidad e información, ¿nuevas reglas?

El carácter novedoso y contemporáneo de los fenómenos vinculados al ciberespacio constituye el principal obstáculo a la hora de dilucidar sus implicancias para la defensa nacional. En la actualidad, existen diversas formas de entender la ciberseguridad, la ciberguerra o la guerra de la información; y conceptos como *operaciones cibernéticas* y *ataques cibernéticos* se confunden constantemente. Si bien en determinadas ocasiones estas definiciones parecen complementarse, la mayoría de las veces resultan contradictorias y obligan a una revisión constante de los términos.

La ausencia de consensos a la hora de definir las operaciones cibernéticas reproduce sus efectos en el nivel político, y obstaculiza la atribución de responsabilidades y la toma de decisiones. De este modo, la falta de acuerdos conceptuales y la dispersión terminológica son elementos centrales a tener presentes para abordar el estudio de la ciberdefensa.

Si bien el núcleo del ciberespacio lo constituye la producción y transferencia de información, es un saber común que esta trasferencia y producción ocupa un lugar central en el diseño de estrategias militares desde los orígenes de la teoría militar.[1] Entonces, lo que diferencia el ciberespacio de otras formas de transferencia y producción de información es el carácter global del medio por el cual esta circula. De esta forma, la globalidad es un rasgo que distingue la transferencia de información en el ciberespacio del resto de los espacios físicos tradicionales.

En líneas generales, podemos decir que la globalidad expresa la interdependencia cada vez más estrecha entre las transformaciones de carácter local y global. El desarrollo de los sistemas de comunicación, tecnología y transporte ocupó un papel central en este proceso, lo que posibilita el distanciamiento entre el tiempo y el espacio (Giddens, 2000). Esta expansión tuvo como consecuencia directa la multiplicación de la magnitud de la información transferida de un lugar a otro. Por esta razón, algunos autores se han referido a las sociedades contemporáneas como *sociedades de la información*, y señalan que la aceleración de las comunicaciones impactó en todas las formas de interacción humana, en las reglas de vida de los hombres, en la forma en que se producen las mercancías, en los modos de ejercer el poder e, incluso, en las dinámicas de la guerra y la paz (Castells, 2006).

De este modo, la globalidad como fenómeno reviste importancia por su

[1] Cabe recordar la conocida máxima de Sun Tzu en su obra *El arte de la guerra*: "Si te conoces a ti mismo y conoces a tu enemigo, no necesitas temer al resultado de un centenar de batallas. Si te conoces a ti mismo pero no conoces a tu enemigo, por cada victoria que ganes sufrirás también una derrota. Si no te conoces ni a ti mismo ni a tu enemigo, sucumbirás en cada batalla".

impacto en el espacio físico, ya que es allí donde se manifiesta la vida social de los hombres. En consecuencia, podemos afirmar que este nuevo ámbito de circulación de información no constituye un espacio en sí mismo, sino más bien una dimensión superpuesta, que atraviesa a los espacios físicos tradicionales. En esta misma dirección, Sheldon indica que los dominios clásicos generan efectos estratégicos en cada uno de los otros, pero el ciberpoder[2] genera efectos en todos los espacios de forma absoluta y simultánea (Sheldon, 2011). Si bien esta distinción es de carácter analítico, resulta de vital importancia para comprender las implicancias del ciberespacio en el ámbito de la defensa, ya que las operaciones virtuales –entendidas como operaciones de información– resultan de interés para los Estados por su capacidad de producir alteraciones o modificaciones en el mundo físico.

El ciberespacio como nuevo dominio militar

A mediados de 2010, el subsecretario de Defensa de los Estados Unidos, William Lynn, señaló que el ciberespacio "debe ser reconocido como un territorio de dominio igual que la tierra, el mar y el aire en lo relativo a la guerra" (Pellerin, Ch., 2010). En este mismo sentido, en la Cumbre de la OTAN en Lisboa en mayo de 2010, el general norteamericano Keith Alexander indicó que el ciberespacio debía *militarizarse* para proteger el derecho a la privacidad de los ciudadanos estadounidenses (Joyanes Aguilar, 2010).

Parece absolutamente entendible que estos llamamientos a la militarización despierten cuestionamientos, sobre todo cuando el ciberespacio es declarado como un ámbito donde no existen límites entre lo público y lo privado. En un espacio de estas características, que atraviesa el resto de los dominios tradicionales, ¿cómo establecer los alcances de la militarización? Al respecto, Sierra Caballero advierte que lo que subyace por detrás en este tipo de lecturas es la concepción de una estrategia militar "total y permanente, sin límites y distancias territoriales […] en la que la seguridad es consagrada en principio rector de la vida pública" (Sierra Caballero, 2003, p. 258).

En torno a estas objeciones, algunos analistas sostienen que la militarización de la red

> no debe ser entendida como una ocupación de la red por fuerzas militares con el objetivo de controlar los movimientos en ella, sino como el derecho de las naciones a disponer de ciberarmamento en defensa de sus legítimos intereses. Nuestros enemigos las poseen y las usan. Una percepción mal entendida que confine la capacidad militar a los medios convencionales nos pondría en una cla-

2 Joseph Nye (2010, p. 4) define al ciberpoder como "la capacidad de obtener resultados preferidos a través del uso de los recursos de información interconectados electrónicamente del dominio cibernético", mientras que Daniel Kuehl (citado por Nye, 2010, p. 4) lo define como "la capacidad de usar el ciberespacio para crear ventajas e influenciar eventos en otros medios operacionales y a través de los instrumentos de poder" (la traducción es propia). De esta forma, el ciberpoder puede ser utilizado para obtener resultados deseados dentro del ciberespacio o para utilizar los instrumentos cibernéticos con el fin de producir resultados en otros dominios fuera de él.

> ra y peligrosa situación de desventaja (Ganuza Artiles, 2010, p. 169).

Según un artículo publicado en 2011 en la revista de la OTAN, varios países están desarrollando cada vez más "capacidades de ciberdefensa", ya que "una buena ciberdefensa puede hacer que estas amenazas sean manejables hasta el punto de que los riesgos remanentes resulten aceptables, como ocurre con las amenazas clásicas" (Theiler, 2011). En esta misma dirección, Torres Soriano advierte que alrededor de treinta países ya han creado en el ámbito de sus fuerzas armadas unidades especializadas en ciberguerra, las cuales poseen como misión "desarrollar las capacidades necesarias para combatir en una nueva dimensión del conflicto bélico donde el objetivo es penetrar en las computadoras y redes del enemigo para causar daños y alterar sus sistemas informáticos" (Torres Soriano, 2011, p. 14).

En relación con estas observaciones, debemos tener presente, como indica Ernesto López, que la perspectiva estratégica de la OTAN "se funda en una noción amplia de seguridad, en la que se destacan la complejización y la multidimensionalidad como asuntos centrales, y en un concepto de indivisibilidad de aquella" (López, 2004, p. 70). Esta dimensión ampliada de la seguridad incluye a las genéricamente denominadas *nuevas amenazas*, razón por la cual no sería aconsejable que los criterios adoptados para este desarrollo de capacidades militares se trasladen acríticamente y directamente al sistema de defensa argentino. Al respecto, cabe recordar los señalamientos de Saint-Pierre, para quien "existe cierta tendencia a transformar todas las amenazas en cuestiones de seguridad, lo cual no hace sino generalizar el concepto de seguridad a todos los ámbitos de la vida". Por esta razón, continúa el autor, "muchas veces se apela al vector militar para resolver problemas que podrían abordarse desde otras políticas públicas" (Saint Pierre, 2004, pp. 50-51).

Un reflejo de esta tendencia a la militarización de las cuestiones públicas se observa en el hecho de que la mayoría de los llamamientos al desarrollo de capacidades de ciberdefensa se sustentan en una *advertencia* sobre lo que podría pasar en un futuro cercano. Esto significa que no están basados en el conocimiento práctico de los efectos reales de las operaciones cibernéticas. Por esta razón, el artículo previamente citado de la Revista de la OTAN afirma que "aún no ha habido un acto de ciberterrorismo con daños físicos y efectos materiales, pero la tecnología de los ciberataques está evolucionando claramente desde una simple molestia a una amenaza seria contra la seguridad de la información e incluso contra infraestructuras nacionales esenciales" (Theiler, 2011).

En este mismo sentido, Richard Clarke analiza las operaciones de ciberguerra atribuidas a Rusia –primero en Estonia y luego en la guerra con Georgia de 2008– y señala que "los rusos […] mostraron moderación en el uso de sus ciberarmas en los episodios de Estonia y Georgia. Probablemente los rusos están guardando sus mejores ciberarmas para cuando verdaderamente las necesiten, en un conflicto donde la OTAN o los Estados Unidos estén involucrados" (Clarke, 2010, p. 21).

Estas cuestiones ponen en duda la identificación de una dimensión específicamente militar del ciberespacio,

en tanto no es posible –al menos en la actualidad– establecer cuáles son los *alcances reales* de las operaciones cibernéticas. Por esta razón, parecería que los llamamientos a militarizar el ciberespacio son más una reacción ante la incertidumbre que el resultado de análisis estratégicos pormenorizados, sustentados empíricamente.

La militarización prematura se observa incluso en los términos utilizados en la mayor parte de la bibliografía para dar cuenta de las llamadas "operaciones cibernéticas". Al respecto, un analista del Comité Internacional de la Cruz Roja advierte que la utilización del término "ataque" para referirse a cualquier acción cibernética que es inadecuada, ya que la amplia mayoría de las operaciones cibernéticas no se dan en el contexto de un conflicto armado o guerra (Droege, 2011). Estos factores, entre otros, contribuyen a adoptar una acepción bélica del término, lo cual colabora con la confusión general y con los llamamientos a la militarización, aun sin saber bien cuáles serían las responsabilidades de los militares al respecto.

Partiendo de lo expuesto, creemos que el análisis debe centrarse en la identificación y clarificación de las condiciones en que una operación cibernética requiere la intervención del sistema de defensa nacional y, particularmente, del instrumento militar. En este sentido, el marco normativo vigente en la Argentina presenta una ventaja comparativa en relación con los escenarios analizados previamente, y establece un freno a la posibilidad de militarizar asuntos públicos.

En búsqueda de nuevos conceptos

En la revisión bibliográfica realizada, es común encontrar la utilización de distintas expresiones para referirse a la ciberguerra o al desarrollo de capacidades de ciberdefensa. Entre las expresiones más usadas, destacamos las de "guerra cibernética", "guerra informática", "guerra de la información", "guerra comunicacional", entre otras. Como señalamos al comienzo del trabajo, la variedad de términos utilizados revela la ausencia de consensos teóricos o acuerdos jurídicos sobre las implicancias militares del ciberespacio. De este modo, a la hora de analizar ciertos documentos desarrollados en otros países sobre la temática, debemos tener especial cuidado respecto de las definiciones y las expresiones empleadas; caso contrario, caeríamos en el error de extraer conclusiones de la comparación de fenómenos cualitativamente distintos.

Como consecuencia, las imprecisiones en la definición de los fenómenos vinculados a la ciberdefensa se trasladan también al ámbito de las definiciones operacionales. De esta forma, las funciones de ciberdefensa se asemejan a veces a las responsabilidades de inteligencia o de guerra electrónica. Al respecto, Richard Clarke sostiene que los análisis sobre el ciberespacio y la ciberguerra están influenciados por las viejas estrategias y por la doctrina de la inteligencia (Clarke, 2010). En el mismo sentido se pronuncia Enrique Stel, para quien la ciberguerra no debe confundirse "con guerra electrónica, acción psicológica, mando y control, C4-IT,[3] Operaciones Especia-

3 C4-IT hace referencia a los términos en inglés "Comando", "Control", "Comunicaciones", "Computación" y "Tecnologías de la Información".

les de Inteligencia o Inteligencia Electrónica" (Stel, 2003, p. 59).

Tal como hemos expuesto, la mayoría de los artículos y trabajos vinculados al ciberespacio desde el ámbito de la defensa coinciden en la centralidad otorgada a la información. Por esta razón, algunos autores se refieren de forma indistinta a las *guerras cibernéticas* y a las denominadas *guerras de la información*. Así, por ejemplo, según un artículo publicado en el año 2010 en la revista *Military Review*,

> la ciberguerra puede ser entendida como una agresión promovida por un Estado y dirigida a dañar gravemente las capacidades de otro para tratar de imponerle la aceptación de un objetivo propio o, simplemente, para sustraerle información, cortar o destruir sus sistemas de comunicación, alterar sus bases de datos, es decir, lo que habitualmente hemos entendido como guerra, pero con la diferencia de que el medio empleado no sería la violencia física, sino un ataque informático que le permita obtener una ventaja sobre el enemigo para situarse en superioridad, o incluso para derrocarle (Sánchez Medero, 2010, p. 21).

Por otro lado, la Fuerza Aérea de los Estados Unidos define al ataque informático como "cualquier acción dentro del medio informático llevada a cabo para negar, explotar, corromper o destruir la información de un adversario, los sistemas de información y las operaciones de información, a la vez que se protege a las fuerzas aliadas de acciones similares".[4] La definición de *operaciones informáticas* elaborada por los Estados Unidos en la Publicación Conjunta para Operaciones Informáticas 3-13 del año 1998, apunta en esta misma dirección. Allí se las define como aquellas acciones encaradas para lograr la superioridad en la información en apoyo a la estrategia militar nacional, afectando la información del adversario y los sistemas de información, a la vez que se defienden la información y los sistemas de información propios (U.S. Department of Defense, 1998).

De las definiciones expuestas, se desprende una cuestión que resulta de utilidad para precisar en qué ocasiones una operación cibernética requiere la intervención de la jurisdicción Defensa. La caracterización de una operación como de guerra refiere a su vinculación con un enfrentamiento armado presente, donde existe un oponente claramente identificado. Con esto queremos decir que una operación de guerra cibernética es reconocible por su vinculación con un estado de guerra. Esto impide, en consecuencia, catalogar apriorísticamente las operaciones informáticas como *operaciones de guerra*. En tanto y en cuanto estas no tengan un objetivo específicamente militar, correspondería caracterizarlas como operaciones delictivas que exceden el ámbito de la defensa nacional, y deben ser tratadas por otros organismos del Estado.

Operaciones cibernéticas que afectan la defensa nacional

Llegados a este punto, estamos en condiciones de delimitar a qué nos re-

4 Citado en Stein, G. (1996). La traducción es nuestra.

ferimos cuando hablamos de amenazas a la seguridad cibernética. Como recuerda Saint Pierre (2004, p. 21), el concepto de seguridad refiere a un estado de cosas estático, y "como objetivo de la actividad de la defensa, es tan general, vago y ambiguo que resulta inútil desde el punto de vista práctico". Por esta razón, añade Bulcourf (2004, p. 129), si entendemos como una amenaza a la seguridad –en este caso ciberespacial– a cualquier operación que incide en la política estatal e internacional, "el concepto es tan amplio que pierde toda utilidad desde el punto de vista cognitivo, lo que puede conducir a analizar cualquier fenómeno que posea una arista conflictiva como una nueva amenaza".

En relación con este punto, a continuación proponemos algunos lineamientos generales para el abordaje de las denominadas amenazas cibernéticas. En primer término, debemos tener presente que las amenazas son "percepciones de situaciones sociopolíticas de riesgo, construidas por los actores sociales de acuerdo con sus visiones, concepciones y perspectivas, condicionadas por el escenario histórico en el que actúan" (Sain, 2004, p. 217). Por esta razón, cuando hablamos de amenazas a la seguridad cibernética, nos referimos a la percepción, por parte de un actor político históricamente situado, de escenarios de riesgo que pueden alterar un *estado de cosas deseable* desde el punto de vista de la circulación de la información en el ciberespacio.

En cuanto a las operaciones cibernéticas, pueden ser definidas como acciones realizadas contra un ordenador, o mediante un ordenador o un sistema informático, utilizando para ello el flujo de datos. El Departamento de Defensa de los Estados Unidos se refiere a ellas como "el empleo de capacidades cibernéticas donde el propósito primario es alcanzar objetivos dentro o a través del espacio. Semejantes operaciones incluyen operaciones de red de computadoras y actividades para operar y defender la red global de información" (U.S. Department of Defense, 2010). La forma más habitual o recurrente de operación cibernética es la denominada "ataque de denegación de servicio" (*Denegation of service*, DOS), que consiste en sobrecargar los recursos informáticos o computacionales del sistema de la víctima a partir del aumento del tráfico de información. Como resultado, este recurso o servicio pierde la conectividad y se hace inaccesible para sus usuarios. Para que este ataque sea rápido y efectivo, suelen utilizarse las denominadas *botnets,* robots informáticos que envían solicitudes de acceso de manera continua y automática.

Esta definición amplia de operación cibernética nos permite distinguir entre operaciones que pueden alterar un estado de cosas deseable en el ámbito de la defensa nacional, y operaciones cibernéticas que afectan a la *seguridad* en un sentido general (de carácter público o privado, colectivo o individual) y que deben ser abordadas desde los organismos y agencias estatales que hacen a la seguridad pública (Chabrow, 2009).

Ahora bien, ¿qué tipo de operaciones cibernéticas requieren la participación del sistema de defensa nacional? Para Enrique Stel (2003), son aquellas operaciones orientadas a "causar daño a los sistemas militares de un Estado". Al respecto, Colin S. Gray sostiene que

las operaciones de ciberguerra refieren al empleo de los medios cibernéticos por las fuerzas armadas en un contexto de enfrentamiento bélico contra un actor relevante en términos de seguridad (citado por Stel, 2003). Siguiendo esta línea argumental, el autor define a las operaciones cibernéticas que afectan a la defensa nacional como aquellas operaciones realizadas por un Estado cuyo objetivo básico es "afectar la red para entorpecer o destruir la capacidad militar de otro Estado".

En un sentido similar, aunque insuficiente desde nuestro punto de vista, Richard Clarke define a la ciberguerra como "acciones realizadas por un Estado para penetrar en las computadoras o redes de otro Estado, con el propósito de causar daño" (Clarke, 2010, p. 6). Este autor se refiere a la guerra entre Rusia y Georgia iniciada en agosto de 2008 como ejemplo de una acción de ciberguerra, donde presumiblemente Rusia acompañó sus acciones militares con ataques de denegación de servicio a los sitios web gubernamentales y medios de comunicación de Georgia. Según Clarke,

> precisamente al mismo momento en que el ejército ruso se movió, también lo hicieron los ciberguerreros. Su objetivo fue impedir que los georgianos pudieran tener información sobre lo que sucedía, y para ello lanzaron ataques DOS en los sitios web gubernamentales de Georgia y en sus medios de comunicación. El acceso de Georgia a la CNN y la BBC también fue bloqueado (Clarke, 2010, p. 18).

Partiendo de estas definiciones, y ofreciendo una perspectiva analítica anclada en el ordenamiento argentino, *caracterizamos a los ataques cibernéticos que afectan a la defensa nacional como ciberoperaciones conducidas por actores estatales en un escenario de guerra, orientadas a afectar las capacidades militares de otros Estados*. Esta definición toma en consideración que una operación cibernética solo puede ser caracterizada como una operación militar a partir de su vinculación con un escenario de enfrentamiento bélico. En este sentido, la ciberguerra afecta a la defensa y a su instrumento militar dependiente, porque se refiere a la interrupción o destrucción de sistemas de información y comunicación en un contexto de guerra (Arquilla y Ronfeldt, 1993).

En rigor, consideramos que los ataques cibernéticos que afectan a la defensa nacional están orientados hacia alguno/s de los siguientes objetivos:

- quebrantar la infraestructura del enemigo, la logística y las cadenas de suministro;
- distraer, confundir e inhabilitar el sistema C4IVR del enemigo (Comando, Control, Comunicaciones, Computación, Inteligencia, Vigilancia y Reconocimiento);
- negar capacidades similares del enemigo;
- crear oportunidades para ataques estratégicos en las infraestructuras del enemigo.

Este conjunto de objetivos evidencia la relación de superposición que observa el ámbito del ciberespacio respecto de los espacios físicos tradicionales: los efectos de este tipo de operaciones no se restringen al mundo virtual, sino que impiden, interfirieren o anulan el fun-

cionamiento de las capacidades militares del enemigo en el espacio físico. Por esta razón, si bien las acciones de ciberguerra poseen su origen en un ámbito virtual –el de las redes de comunicación y sistemas informáticos–, sus efectos impactan sobre el mundo físico y podrían afectar el tráfico aéreo y terrestre, el control de las infraestructuras críticas, el abastecimiento energético y de agua, entre otros.[5]

Recapitulando lo dicho hasta aquí, hemos definido las ciberoperaciones como el amplio conjunto de acciones realizadas contra un ordenador, o mediante un ordenador o un sistema informático, utilizando el flujo de datos con el fin de alcanzar objetivos en o a través del ciberespacio. Dentro de este conjunto de operaciones, constituyen ataques cibernéticos que afectan a la defensa nacional aquellos orientados a afectar las capacidades militares de otros Estados. En este mismo sentido, consideramos que lo que denominamos *ciberguerra* corresponde al nivel militar porque se refiere a la interrupción o destrucción de sistemas de información y comunicación en un contexto bélico.

En suma, de estas consideraciones se desprende que las operaciones cibernéticas en sentido amplio –sean de carácter público o privado, individual o colectivo– corresponden al ámbito de la ciberseguridad, en tanto la ciberdefensa debe abocarse exclusivamente a aquellos ataques cibernéticos cuyo objetivo es afectar las capacidades militares de los Estados.

La ciberseguridad en la legislación nacional

En nuestro país, la legislación en torno a la ciberseguridad está en pleno proceso de conformación. A los fines de nuestro trabajo, nos referiremos a tres normativas que delimitan el ámbito de la ciberseguridad y que constituyen el puntapié inicial sobre el cual considerar la atribución de responsabilidades al sistema de defensa nacional.

El Decreto Nº 624/03 y sus modificatorios (estructura organizativa de la Jefatura de Gabinete de Ministros) establecieron que la Subsecretaría de Gestión Pública (SSGP) de la Jefatura de Gabinete de Ministros es el organismo responsable del diseño, implementación y seguimiento de la política de modernización del Estado y de la definición de estrategias sobre tecnologías de la información, comunicaciones asociadas y otros sistemas electrónicos de tratamiento de información en la Administración Pública Nacional.

En esta misma dirección, el Decreto Nº 1.028 de ese mismo año estableció que la Oficina Nacional de Tecnologías de Información (ONTI) –dependiente de la SSGP– es el organismo encargado de:

- proponer una estrategia de optimización, tanto en lo referente a los recursos aplicados como a nivel de prestación, de las subredes que componen la Red Nacional de Información Gubernamental, que establezca normas para el control técnico y administración;

5 Entre las operaciones de este tipo, podemos mencionar el bombardeo producido en septiembre de 2007 por parte de la aviación israelí contra un reactor nuclear en construcción en territorio sirio, posible gracias a una acción previa de ciberguerra que *cegó* los sistemas antiaéreos de Siria.

• participar en todos los proyectos de desarrollo, innovación, implementación, compatibilización e integración de las tecnologías de la información en el ámbito del sector público, cualquiera fuese su fuente de financiamiento;
• mantener actualizada la información sobre los bienes informáticos de la Administración Nacional;
• elaborar lineamientos y normas que garanticen la homogeneidad y pertinencia de los distintos nombres de los dominios de los sitios de internet del Sector Público, a través de la intervención junto con el Ministerio de Relaciones Exteriores, Comercio Internacional y Culto en el otorgamiento de los mismos.

En relación con estas atribuciones, la Resolución de la Jefatura de Gabinete de Ministros Nº 580/11[6] instituyó, en el ámbito de la ONTI, el "Programa Nacional de Infraestructuras Críticas de Información y Ciberseguridad". En su articulado se establece que este programa tiene por objetivos:

• elaborar "un marco regulatorio específico que propicie la identificación y protección de las infraestructuras estratégicas y críticas de las entidades y jurisdicciones definidas en el artículo 8 de la Ley Nº 24.156 y sus modificatorios, los organismos interjurisdiccionales, y las organizaciones civiles y del sector privado";
• fomentar "la cooperación y colaboración de los mencionados sectores con miras al desarrollo de estrategias y estructuras adecuadas para un accionar coordinado hacia la implementación de las pertinentes tecnologías";
• "administrar toda la información sobre reportes de incidentes de seguridad en el Sector Público Nacional que hubieren adherido al Programa y encauzar sus posibles soluciones de forma organizada y unificada";
• "establecer prioridades y planes estratégicos para liderar el abordaje de la ciberseguridad, y asegurar la implementación de los últimos avances en tecnología para la protección de infraestructuras críticas".

En cumplimiento de estas responsabilidades, el Programa deberá "dictar las normas que resulten necesarias para su implementación" y "coordinar las actividades con las entidades y jurisdicciones del Sector Público Nacional".

Esta última atribución es de gran importancia para analizar la contribución que el sistema de defensa nacional podría hacer a la estrategia de ciberseguridad de la nación en su conjunto. Al respecto, cabe destacar que, por medio del artículo 5, esta resolución invita a todas las entidades y jurisdicciones (incluyendo al Ministerio de Defensa y su dependiente instrumento militar) a adherir a este Programa. Por otro lado, en el artículo 6 se afirma que la implementación del Programa no supondrá la interceptación ni la intervención en conexiones o redes de acceso privado de acuerdo con lo "estatuido por la Ley Nº

6 La Resolución N° 580/2011 sustituyó a la Resolución SGP N° 81/99 por la cual se había creado la Coordinación de Emergencias de Redes Teleinformáticas de la Administración Pública Nacional (ARCERT).

25.326 de Protección de Datos Personales y su Decreto Reglamentario Nº 1.558 del 29 de noviembre de 2001".

Según lo expuesto, queda establecido que la ONTI es la entidad responsable de fijar los criterios de seguridad de las redes de la administración pública nacional. Es decir que ello forma parte del ámbito de la ciberseguridad entendida en un sentido amplio, lo cual se traduce en una restricción de la participación del sistema de defensa nacional, en correspondencia con la separación entre los ámbitos de la seguridad interior y la defensa.

La distinción categórica entre las responsabilidad de la defensa y la seguridad interior no se basa únicamente en la experiencia histórica argentina, sino que tiene un fuerte respaldo consensual. Los ejes centrales de esta separación prohíben expresamente que fuerzas armadas realicen tareas de inteligencia criminal, al tiempo que suprimen las hipótesis de conflicto con los países vecinos, y apuntan hacia el efectivo gobierno civil de la política de defensa nacional. En suma, esta delimitación permite establecer también los límites de acción para el sistema de defensa nacional en lo estrictamente referido a la ciberdefensa.

La contribución del sistema de defensa nacional a la defensa del ciberespacio

Ahora bien, ¿cuál es el rol del sistema de defensa frente a la problemática del ciberespacio y la ciberdefensa en el marco de la actual legislación? Para dar respuesta a este interrogante, es imprescindible tener presentes las normas que regulan las responsabilidades del sistema de defensa nacional y, específicamente, la participación del instrumento militar en él.

La Ley Nº 23.554 de Defensa Nacional identifica las agresiones estatales de origen externo como criterio primordial para el empleo del instrumento militar. Este concepto se ve esclarecido por la definición contenida en su Decreto Reglamentario Nº 727/06: "se entenderá como 'agresión de origen externo' el uso de la fuerza armada por un Estado contra la soberanía, la integridad territorial o la independencia política de nuestro país, o en cualquier otra forma que sea incompatible con la Carta de las Naciones Unidas".

Por su parte, el Decreto Nº 1.691/06, Directiva de Organización y Funcionamiento de las fuerzas armadas, sostiene que la estructuración –tanto orgánica como funcional– de las fuerzas armadas debe realizarse a partir de la misión principal del instrumento militar, cual es la de conjurar y repeler toda agresión externa perpetrada por fuerzas armadas de otro Estado. Esta misión, por lo tanto, constituye el principal criterio ordenador de todo el diseño de fuerzas, en tanto que toda misión subsidiaria del instrumento militar no debe afectar las capacidades requeridas para el cumplimiento de aquella misión primaria y esencial.

Por otro lado, la Ley Nº 24.948 de Reestructuración de las Fuerzas Armadas, reconoce otros supuestos de empleo del instrumento militar, definidos como subsidiarios por el Decreto Nº 1.691/06. Estos son:

- operaciones en el marco de las Naciones Unidas;

• operaciones en apoyo de la seguridad interior, encuadradas en la Ley Nº 24.059;
• operaciones en apoyo a la comunidad nacional o de países amigos; y
• participación de las fuerzas armadas en la construcción de un sistema de defensa subregional.

En el caso de operaciones de apoyo de la seguridad interior, deben tenerse en cuenta varios criterios. En primer lugar, el artículo 27 de la Ley de Seguridad Interior expresa que, a requerimiento del Comité de Crisis, el Ministerio de Defensa dispondrá que

> las Fuerzas Armadas apoyen las operaciones de seguridad interior mediante la afectación […] de sus servicios de arsenales, intendencia, sanidad, veterinaria, construcciones y transporte, así como de elementos de ingenieros y comunicaciones, para lo cual se contará en forma permanente con un representante del Estado Mayor Conjunto en el Centro de Planeamiento y Control de la Subsecretaría de la Seguridad Interior.

En segundo lugar, el artículo 28 establece que "todo atentado en tiempo de paz a la jurisdicción militar, independientemente de poner en forma primordial en peligro la actitud defensiva de la Nación, constituye asimismo una violación de la seguridad interior". En este caso, es una "obligación primaria de la autoridad militar la preservación de la fuerza armada y el restablecimiento del orden dentro de la aludida jurisdicción, de conformidad con las disposiciones legales vigentes en la materia".

El tercer supuesto a tener en cuenta surge de los artículos 31 y 32 de la norma. El primero de ellos dispone que "las Fuerzas Armadas serán empleadas en el restablecimiento de la seguridad interior dentro del territorio nacional, en aquellos casos excepcionales en que el sistema de seguridad interior […] resulte insuficiente a criterio del Presidente de la Nación para el cumplimiento de los objetivos establecidos en el artículo 2". Por su parte, el artículo 32 expresa que "a los efectos del artículo anterior, el Presidente de la Nación, en uso de las atribuciones contenidas en el artículo 86, inciso 17 de la Constitución Nacional, dispondrá el empleo de elementos de combate de las Fuerzas Armadas para el restablecimiento de la normal situación de seguridad interior, previa declaración del estado de sitio".

En los supuestos excepcionales precedentemente aludidos, el empleo de las fuerzas armadas se ajustará, además, a las siguientes normas (artículo 32):

> a) La conducción de las Fuerzas Armadas, de seguridad y policiales nacionales y provinciales queda a cargo del Presidente de la Nación, asesorado por los comités de crisis de esta ley y la Ley N° 23.554;
> b) Se designará un comandante operacional de las Fuerzas Armadas y se subordinarán al mismo todas las demás fuerzas de seguridad y policiales exclusivamente en el ámbito territorial definido por dicho comando;
> c) Tratándose la referida en el presente artículo de una forma excepcional de empleo, que será desarrollada únicamente en situaciones de extrema gravedad, la misma no incidirá en la doctrina, organización, equipamiento y capacitación de las Fuerzas Armadas, las que

> mantendrán las características derivadas de la aplicación de la Ley N° 23.554.

En este contexto, cabe señalar que el sistema de seguridad interior y el sistema de defensa nacional "atienden supuestos de hechos distintos, y se excluyen mutuamente en su aplicación" (Dapena, 2007, p. 46). Por lo tanto, la prevención y persecución del terrorismo, el narcotráfico, el crimen organizado y, por supuesto, del ciberterrorismo, no son hipótesis de empleo del instrumento militar; y en los casos de interacción con el sistema de seguridad interior, "no existen otras hipótesis que permitan la utilización del instrumento militar", más allá de las establecidas en la Ley Nº 24.059.

Por último, cabe mencionar que el Decreto 1.714/09, por el cual se aprueba la Directiva de Política de Defensa Nacional, sostiene que la República Argentina adopta

> un modelo de defensa de carácter "defensivo", de rechazo y oposición a políticas, actitudes y capacidades ofensivas de proyección de poder hacia terceros Estados, en el cual la concepción y la disposición estratégica, la política de defensa y su consecuente política militar, diseño de fuerzas y previsión de empleo y evolución del instrumento militar, se encuentra estructurada según el principio de legítima defensa ante agresiones de terceros Estados.

De esta forma, la ciberdefensa debería descansar exclusivamente en el desarrollo de capacidades defensivas en su ámbito de competencia.

En función de lo expuesto en este apartado, ¿qué podríamos inferir respecto de la actuación del instrumento militar frente a potenciales ataques a través del ciberespacio? ¿Cómo delimitar los ámbitos de actuaciones cuando es *casi* imposible identificar quién es el agresor? Considerando como punto de partida la legislación y doctrina vigentes en la materia, creemos que debe adoptarse un enfoque basado en efectos. Es decir, la intervención del sistema de defensa en el ciberespacio debe estar definida no por quien produce el ataque, sino sobre la base de qué infraestructura o sistema están siendo afectados.

Consideraciones finales

A la luz del análisis realizado, creemos pertinente hacer algunas consideraciones finales en torno a las implicancias del ciberespacio en la defensa nacional.

En primer término, debemos señalar que la caracterización del ciberespacio como un *ámbito global* no debe confundirse con la inexistencia de límites geográficos y geopolíticos en el espacio físico. La globalidad del ciberespacio no puede equipararse con la ausencia de límites geográficos, debido a que estamos comparando dos planos analíticos distintos. El ciberespacio no constituye un espacio en sí mismo, sino una dimensión que atraviesa los espacios físicos. Este "equívoco interesado", en palabras de Ernesto López, no se distingue demasiado de aquellos análisis que –interesados en aprovechar el debilitamiento de las unidades políticas individuales– declararon el fin de los Estados nacionales a mediados de la década de 1990.

En relación con este punto, se observa que detrás de la consideración del ciberespacio como una amenaza a la seguridad de los Estados subyace la su-

perposición de los ámbitos de la seguridad interior y la defensa externa. Por esta razón, creemos de vital importancia recuperar las recomendaciones de Saint Pierre en torno al abordaje de la seguridad como un "estado de cosas deseable", definido por la percepción históricamente situada de las unidades políticas. En el caso que nos compete, las operaciones cibernéticas constituyen amenazas a la ciberseguridad en un sentido general o ampliado, lo que afecta un "estado de cosas deseable" en referencia a los sistemas informáticos de un Estado.

Sin embargo, solo una porción de estas operaciones afecta específicamente el ámbito de la defensa nacional. En este sentido, entendemos que dentro de la amplia gama de operaciones cibernéticas, únicamente son de interés para la defensa nacional aquellas que persiguen objetivos militares, es decir, que poseen la intención de alterar e impedir el funcionamiento de las capacidades del sistema de defensa nacional. Por lo tanto, aquellas agresiones que afecten toda otra infraestructura que no pertenezca al sistema de defensa nacional son responsabilidad, en primera instancia, de otras agencias del Estado.

En este contexto, proponemos avanzar en una dirección que permita al sistema de defensa nacional, a partir de sus competencias jurisdiccionales, contribuir a la ciberseguridad en un sentido general o ampliado, que coordine su accionar con otras entidades y jurisdicciones del sector público nacional, a la vez que permita desarrollar y fortalecer las capacidades de ciberdefensa.

Bibliografía

Arquilla, J. y D. Ronfeldt (1993), "Cyberwar is Coming!", *Comparative Strategy*, vol. 12, Nº 2, primavera, pp. 141-165.

Balaguer Prestes, R. (s/f), "¿Ágora electrónica o Time Square? Una revisión de consideraciones sociales sobre Internet", *Revista Textos de la Cibersociedad*, Nº 1, <http://www.cibersociedad.net>.

Bulcourf, P. (2004), "Continuidad, cambio y reconceptualizaciones en torno de las nuevas amenazas", en López, E. y M. Sain (comps.), *Nuevas amenazas. Dimensiones y perspectivas. Dilemas y desafíos para la Argentina y el Brasil,* Bernal, Editorial de la Universidad Nacional de Quilmes.

Castells, M. (2006), *La era de la información,* Buenos Aires, Siglo XXI.

Clarke, R. y R. Knake (2010), *Cyberwar. The next Threat to National Security and What to Do about It,* Washington, Ed. Harper Collins.

Dapena, N. (2007), "La diferencia entre seguridad interior y defensa nacional. Conceptos, competencias, y una propuesta facultades, límites, prohibiciones e interacciones", *Revista de la Defensa Nacional*, N° 1, Buenos Aires, Ministerio de Defensa de la Nación.

Ganuza Artiles, N. (2010), "La situación de la ciberseguridad en el ámbito internacional y en la OTAN", en Joyanes Aguilar, L. *et al.* (comps.), *Ciberseguridad, retos y amenazas a la seguridad en el ciberespacio*, Madrid, Instituto Español de Estudios Estratégicos.

Giddens, A. (2000), *Un mundo desbocado. Los efectos de la globalización en nuestras vidas,* Madrid, Taurus.

Joyanes Aguilar, L. (2010), "Introducción. Estado del arte de la ciberseguridad", en Joyanes Aguilar, L. *et al.* (comps.), *Ciberseguridad, retos y amenazas a la seguridad en el ciberespacio,* Madrid, Instituto Español de Estudios Estratégicos.

Kuehl, D. (2009), "From Cyberspace to Cyberpower: Defining the Problem", en Franklin, D. *et al.* (eds.), *Cyberpower and National Security,* Washington, National Defense UP.

Libicki, M. (2009), *Cyberdeterrence and Cyberwar,* RAND Corporation, <http://www.rand.org>.

López, E. (2004), "Nueva problemática de seguridad y nuevas amenazas", en López, E. y M. Sain (comps.), *Nuevas amenazas. Dimensiones y perspectivas. Dilemas y desafíos para la Argentina y el Brasil,* Bernal, Editorial de la Universidad Nacional de Quilmes.

Nye, J. (2010), "Cyber Power", en *Belfer Center for Science and International Affairs,* Harvard Kennedy School, <http://belfercenter.ksg.harvard.edu/files/cyber-power.pdf>.

Puime Maroto, J. (2009), "El ciberespionaje y la ciberseguridad", en CEDESEN, *La violencia en el siglo XXI. Nuevas dimensiones de la guerra,* Madrid, Ministerio de Defensa Nacional.

Sain, M. (2004), "Nuevos horizontes, nuevos problemas. Las fuerzas armadas argentinas frente a las nuevas amenazas (1990-2001)", en López, E. y M. Sain (comps.), *Nuevas amenazas. Dimensiones y perspectivas. Dilemas y desafíos para la Argentina y el Brasil,* Bernal, Editorial de la Universidad Nacional de Quilmes.

Saint Pierre, H. (2004), "Una reconceptualización de las nuevas amenazas: de la subjetividad de la percepción a la seguridad cooperativa", en López, E. y M. Sain (comps.), *Nuevas amenazas. Dimensiones y perspectivas. Dilemas y desafíos para la Argentina y el Brasil,* Bernal, Editorial de la Universidad Nacional de Quilmes.

Sánchez Medero, G. (2010), "Internet: una herramienta para las guerras en el siglo XXI", *Military Review: The professional Journal of the U.S. Army*, Edición Hispanoamericana, julio-agosto.

Sheldon, J. (2011), "Deciphering Cyberpower. Strategic Purpose in Peace and War", *Strategic Studies Quarterly*, verano, <http://www.au.af.mil/au/ssq/2011/summer/sheldon.pdf>.

Sierra Caballero, F. (2003), "La guerra en la era de la información: propaganda, violencia simbólica y desarrollo panóptico del sistema global de comunicación", *Revista de Ciencias Sociales y de la Comunicación*, Nº 3, Murcia.

Stein, G. (1996), *Information Attack: Information Warfare in 2025, Research Paper Presented to Air Force 2025,* Air War College, <http://csat.au.af.mil/2025/volume3/vol3ch03.pdf>.

Stel, E. (2003), *La guerra cibernética. El ciberespacio - La Cuarta Fuerza*, Buenos Aires, Dunken.

Theiler, O. (2011), "Nuevas amenazas: el ciberespacio", *Revista digital de la OTAN*, septiembre, <http://www.nato.int/docu/review/2011/11-september/Cyber-Threads/ES/index.htm>.

Torres Soriano, M. (2011), "Los dilemas estratégicos de la ciberguerra", *Ejército,* Nº 839, Madrid, Ministerio de Defensa Nacional.

U.S. Department of Defense (1998), *Joint Doctrine for Information Operations,* Washington, Joint Chiefs of Staff, <http://www.c4i.org/jp3_13.pdf>.

——— (2010), *Joint Publication*, *DoD Dictionary of Military Terms*, Washington, Joint Staff, Joint Doctrine Division, J-7, <http://ra.defense.gov/documents/rtm/jp1_02.pdf>.

Fuentes periodísticas

"Cyberwar. The threat from the Internet" (3-9 de julio de 2010), *The Economist Magazine*, vol. 396, N° 8.689.

Droege, C. (16 de agosto de 2011), "No hay lagunas jurídicas en el ciberespacio", <http://www.icrc.org>.

Chabrow, E. (9 de noviembre de 2009), "Conventional War Strategy Doesn't Work in Cyberspace", *GovInfo Security*, <http://www.govinfosecurity.com>.

Pellerin, Ch. (18 de octubre de 2010), "Cyberspace is the New Domain of Warfare", Ministerio de Defensa de los Estados Unidos de América, <http://www.defense.gov/news/newsarticle.aspx?id=61310>.

Normativa de la República Argentina

Decreto Nº 624/03.
Decreto Nº 1.028/03.
Decreto Nº 727/06. Reglamentación de la Ley de Defensa Nacional.
Decreto Nº 1.691/06. Directiva sobre Organización y Funcionamiento de las Fuerzas Armadas.
Decreto 1.714/09. Directiva de Política de Defensa Nacional.
Ley Nº 23.554 de Defensa Nacional.
Ley Nº 24.059 de Seguridad Interior.
Ley Nº 24.948 de Reestructuración de las Fuerzas Armadas.
Resolución de la Jefatura de Gabinete de Ministros Nº 580/11.

(Recibido el 22 de julio de 2013.)
(Evaluado el 5 de septiembre de 2013.)

Autores

Sergio Gabriel Eissa es licenciado en Ciencias Políticas de la Universidad de Buenos Aires (UBA). Maestro en Ciencias Sociales con mención en Relaciones Internacionales (FLACSO) y candidato a doctor en Ciencias Políticas en la Universidad de San Martín (UNSAM). Profesor adjunto en la Universidad de Buenos Aires, en la Universidad Nacional de San Martín y en el Instituto Universitario de la Gendarmería Nacional. Investigador de UBACyT.

Sol Gastaldi es licenciada en Ciencias Políticas de la Universidad de Buenos Aires (UBA) y Magíster en Defensa Nacional (Escuela de Defensa Nacional-EDENA). Investigadora invitada en la Universidad Nacional de Quilmes.

María Elina Zacarías Di Tullio es licenciada en Ciencias Políticas de la Universidad de Buenos Aires (UBA) y candidata a Magíster en Defensa Nacional (Escuela de Defensa Nacional-EDENA). Investigadora

invitada en la Universidad Nacional de Quilmes. Directora de Coordinación y Planificación Estratégica de la Policía de Seguridad Aeroportuaria.

Iván Poczynok es licenciado en Sociología de la Universidad de Buenos Aires (UBA). Maestrando en Defensa Nacional (Escuela de Defensa Nacional-EDENA). Profesor e investigador en formación en la Universidad de Buenos Aires, e investigador invitado en la Universidad Nacional de Quilmes. Es director de Gestión del Conocimiento en la Policía de Seguridad Aeroportuaria.

Cómo citar este artículo

Eissa, Sergio Gabriel *et al.*, "El ciberespacio y sus implicancias para la defensa nacional. Aproximaciones al caso argentino", *Revista de Ciencias Sociales, segunda época*, año 6, Nº 25, Bernal, Editorial de la Universidad Nacional de Quilmes, otoño de 2014, pp. 181-197, edición digital, <http://www.unq.edu.ar/catalogo/330-revista-de-ciencias-sociales-n-25.php>.