La Ciberdefensa en su laberinto. Cambio de rumbo en la concepción de ciberdefensa durante la gestión de Mauricio Macri (2015-2019)

Cyberdefense in its labyrinth. Change of course in the concept of cyber defense during the Mauricio Macri administration (2015-2019)

SERGIO G. EISSA, ANA ALBARRACÍN KETICOGLU

Facultad de Defensa Nacional, Universidad de la Defensa Nacional, Argentina
seissa@yahoo.com

La ciberdefensa, en tanto problema público, se convirtió en un nuevo espacio de disputa entre los actores políticos que, en el escenario burocrático, pujaron por su definición entre principios del Siglo XXI y el año 2014. En un artículo previo (Eissa, et al, 2019) sosteníamos que la definición de ciberdefensa no es inocua por al menos tres (3) motivos. En primer lugar, el ciberespacio ponía en "jaque" la separación orgánica y funcional entre la defensa y la seguridad interior. En segundo lugar, la decisión sobre cómo se resolvía esa separación frente a la problemática que el ciberespacio representaba para la seguridad nacional de Argentina. Por último, las Fuerzas Armadas pujaron junto al Estado Mayor Conjunto por que la definición de ciberdefensa evadiera el límite que definían las leyes de seguridad interior y defensa nacional.

El objetivo del presente artículo es analizar los cambios que

pudieron haberse efectuado a partir de la presidencia de Mauricio Macri (2015-2019), a la luz de la modificación del Decreto Nº 727/2006 y la aprobación de la Directiva de Política de Defensa (DPDN) 2018 que dejaron abierta la posibilidad de que el sistema de defensa pueda intervenir frente a amenazas de origen transnacional.

Introducción

La ciberdefensa, en tanto problema público, se convirtió en un nuevo espacio de disputa entre los actores políticos que, en el escenario burocrático, pujaron por su definición entre principios del Siglo XXI y el año 2014. En un artículo previo (Eissa, et al, 2019) sosteníamos que la definición de ciberdefensa no era inocua por al menos tres (3) motivos. En primer lugar, el ciberespacio ponía en "jaque" la separación orgánica y funcional entre la defensa y la seguridad interior. En segundo lugar, la decisión sobre cómo se resolvía esa separación frente a la problemática que el ciberespacio representaba para la seguridad nacional de Argentina. Por último, las Fuerzas Armadas pujaron con el Estado Mayor Conjunto ya no por la definición, sino sobre a quién le correspondía operar en el ciberespacio y cómo. Este proceso culminó el año 2014 con la creación del Comando Conjunto de Ciberdefensa y con una definición de ciberdefensa que se amoldaba al límite poroso que definían las leyes de seguridad interior y defensa nacional.

El objetivo del presente artículo es analizar los cambios que pudieron haberse efectuado a partir de la presidencia de Mauricio Macri (2015-2019) y sus Ministros de Defensa, Julio Martínez (2015-2017) y Oscar Aguad (2017-2019), a la luz de la modificación del Decreto Nº 727/2006 que definía que la misión principal de las Fuerzas Armadas es la de conjurar y repeler toda agresión estatal militar externa (AEME) y la aprobación de la Directiva de Política de Defensa

(DPDN) 2018, que se concentraron en analizar las amenazas transnacionales, dejando abierta la posibilidad de que el sistema de defensa pueda intervenir frente a estas temáticas.

El marco teórico lo provee el modelo analítico Glass Onion (Eissa, 2015), que a partir del instrumental de las teorías públicas y de la Escuela de Copenhague, sostiene que la definición de una cuestión (ciberespacio) cuando es problematizada –esto es debatida en la agenda pública y la agenda gubernamental– tiene implícita una solución. Por tal motivo, los actores políticos y sociales, domésticos y externos, pujan por imponer una definición que sea funcional a sus intereses y sistemas de creencias. Obviamente, no todos los actores tienen la misma capacidad de poder y saben que el decisor elige una alternativa de política pública con escasez de tiempo y en un contexto de ambigüedad: no sabe. La hipótesis que subyace al trabajo es que durante el gobierno de Mauricio Macri las definiciones adoptadas en materia de ciberdefensa entre 2010 y 2015 fueron modificadas, pasando de una concepción de ciberespacio como ambiente transversal al resto de los dominios operacionales tradicionales donde hacer la guerra (tierra, mar, aires y espacio exterior), para empezar a ser entendido como un nuevo dominio y que abarca también la problemática de las amenazas transnacionales a través del ciberespacio.

Para ello, el artículo se organiza en tres partes. En la primera se repasa brevemente la definición adoptada en materia de ciberdefensa entre el 2010 y el 2015. Seguidamente se analizan los cambios normativos y las implementaciones realizadas durante el gobierno de Mauricio Macri, bajo las gestiones de Julio Martínez (2015-2017) y Oscar Agüad (2017-2019). Finalmente se presentan algunas reflexiones.

Antecedentes de la Ciberdefensa en Argentina

Una de las primeras iniciativas vinculadas a la temática del ciberespacio fue el decreto Nº 624/2003. Éste 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 sea 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 1028 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, estableciendo normas para el control técnico y administración.
- 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, interviniendo junto con el Ministerio de Relaciones Exteriores, Comercio Internacional y Culto en el otorgamiento de los mismos.

El 3 de agosto de 2005, el Director Nacional de la Oficina Nacional de Tecnologías de Información dictó la disposición Nº 6, por la cual se aprobó la "Política de Seguridad de la Información Modelo" que cada organismo de la Administración Pública debía tomar como base para elaborar sus propias políticas, de acuerdo a lo establecido en la decisión administrativa Nº 669/2004 de la Jefatura de Gabinete de Ministros.

En relación a estas atribuciones, la resolución de la Jefatura de Gabinete de Ministros Nº 580/11 instituyó, en el ámbito de la ONTI, el "Programa Nacional de Infraestructuras Críticas de Información y Ciberseguridad".

Esta última atribución es de gran importancia para analizar la contribución que el Sistema de Defensa Nacional puede hacer a la estrategia de ciberseguridad de la Nación en su conjunto. Al respecto, cabe destacar que por medio del artículo 5º esta resolución invita a todas las entidades y jurisdicciones (incluyendo al Ministerio de Defensa y a sus Fuerzas Armadas) a adherir a este Programa. Por otro lado, en el artículo 6º se afirma que la implementación del Programa no supondrá la interceptación ni la intervención en conexiones o redes de acceso privado de acuerdo a lo "estatuido por la Ley Nº 25.326 de Protección de Datos Personales y su Decreto Reglamentario Nº 1558 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 Externa.

Los problemas que se presentaron rápidamente al Ministerio de Defensa fueron dos. En primer lugar, ¿cómo trasladar la separación entre defensa y seguridad interior al ciberespacio? En segundo lugar, las Fuerzas Armadas ya habían creado estructuras orgánicas responsables de la cuestión ciberespacial, sin conducción ni lineamientos políticos, ¿quién sería entonces el responsable de conducir las operaciones militares en materia de ciberdefensa?

En efecto, el Ejército Argentino, la Armada Argentina y la Fuerza Aérea Argentina habían avanzado –por distintas motivaciones– en la creación de sus elementos de ciberdefensa.

En primer lugar, la Armada Argentina implementó la primera segregación entre la naciente internet y sus redes internas al crear el Departamento de Seguridad Informática en el ámbito del Servicio de Informática de la Armada, el cual fue el responsable de poner en vigencia normas y procedimientos de protección de los activos de información elaborados por distintos actores de esa Fuerzas –como los Servicios de Informática, Comunicaciones e Inteligencia–. Posteriormente, y como resultado de los dispuesto en la Resolución Nº 48/2005 SIGEN "Normas Generales de Control Interno para Tecnologías de Información", la Armada Argentina puso en marcha el Grupo de Trabajo "Comité de la Seguridad de la Información" para implementar lo dispuesto por la ONTI. A fines del año 2006 esa propuesta fue elevada al Jefe del Estado Mayor General de la Armada, siendo aprobada a inicios del año 2007. El siguiente paso fue crear dentro de la estructura orgánica de la Fuerza el "Servicio de la Seguridad de la Información" en el año 2008 que fue reemplazado en el 2010 por el actualmente vigente "Servicio de Ciberdefensa y Seguridad de la Información de la Armada Argentina". En el ámbito del actual Servicio de Ciberdefensa se realizaron las primeras pruebas de concepto tecnológicas a efectos de

definir las funcionalidades de la Capacidad de Ciberdefensa de la Armada Argentina y, de las mismas, surgió el modelo tecnológico que le permitió dotar a esta Fuerza de un Centro de Ciberdefensa, siendo este el primero operativo en la jurisdicción del Ministerio de Defensa y las Fuerzas Armadas.

En cuanto al Ejército, existía una Dirección de Seguridad Informática antes de la creación de la ONTI. Paralelamente, y hacia el 2011, el CITEDEF contaba con una Gerencia de Seguridad Informática donde pusieron en marcha un grupo de investigación ciberdefensa en el cual participaban, entre otros el coronel Hugo Ballesteros y el Ing. Carlos Benítez. A partir de la llegada de General César Milani –compañero de Ballesteros–, el tema ciberdefensa recibió mucho impulso y se creó el Centro de Ciberdefensa el 14 de noviembre de 2014 con los citados entre otros: el coronel Juan José Benítez, el coronel Marcelo Ozan, el Ing. Pablo Lazaro, el Ing. Juan Manuel Mosso, el Ing. José Luis López; dependiente de la Jefatura II Inteligencia del Ejército. Este equipo de especialistas multidisciplinarios logró diseñar, desarrollar e implementar todo el ciclo de respuestas de incidentes en el ciberespacio. Se pudo disponer de los tres componentes principales: a) la documentación pertinente como ser: políticas, manuales, guías y procedimientos para el manejo de incidentes; b) la tecnología necesaria para el manejo de incidentes; y c) el recurso humano capacitado a la altura de poder cumplir la exigencia impuesta. Esto se logró gracias a la selección de personal, capacitaciones específicas para entrenarlo en el manejo de incidentes en centros de capacitación reconocidos como Base4, ITCollege, NeoSecure, Escuela Superior Técnica del Ejército, etc., reforzando con la ejecución de ejercicios militares de ciberdefensa.

Mientras el General César Milani estuvo al frente de inteligencia y de la Fuerza, el tema ciberdefensa recibió mucho apoyo en recursos humanos, equipamiento y, por supuesto, en presupuesto. Esa Dirección General logró generar los procedimientos, equipamiento y personal sobre

ciberdefensa directa y empezaron a realizar desarrollos a partir de software libre principalmente y solo en la herramienta SIEM combinado con software comercial. Además, se desarrollaron aplicaciones específicas como analizador de malware estático y dinámico, analizador de código fuente de software para detectar vulnerabilidades antes de su implementación, herramienta para la gestión de incidentes, analizador de vulnerabilidades, etc. Todas estas aplicaciones y el conocimiento desarrollado fueron ofrecidos a la ONTI y a los componentes de ciberdefensa de las otras FFAA y del CCCD (Comando Conjunto de Ciberdefensa). Esto, aunque continuó, se desaceleró con el relevo del Jefe del Ejército General César Milani. Más recientemente, ciberdefensa pasó a depender Dirección General de Comunicaciones e Informática, lo cual aún genera muchos problemas para que se prioricen sus requerimientos presupuestarios. Asimismo, el otro inconveniente que se presenta en la actualidad es que ciberdefensa continúa separada de Seguridad de la Información, cuando sería más conveniente que estén bajo una misma conducción o al menos con una profunda integración.

Por su parte, la Fuerza Aérea Argentina empezó a preocuparse por la seguridad de las redes cuando incorporó a los aviones A4-AR a fines de la década de 1990 –particularmente en relación con la carga de datos de las missions planning a las mission computer–. A partir del antecedente del año 1995 en investigación y desarrollo (I+D), como parte de temas de guerra electrónica (EW), contactaron a un grupo de la Universidad de Buenos Aires (UBA), que estudiaba virus informáticos, pero la iniciativa fue desactivada poco tiempo después. Más tarde, la Dirección de Informática empezó a trabajar con la cuestión de seguridad de la información hasta que fue creada la Dirección de Ciberdefensa, que surge tras la concreción de estudios de doctrina específicos y conjuntos realizados con las otras fuerzas en el Estado Mayor Conjunto de las Fuerzas Armadas.

En el año 2008 se produce una reunión entre el Comodoro Jorge Salvador Ierache, el Capitán de Navío Pablo Sorrentino, el Coronel Juan José Benítez y un asesor de la Subsecretaría de Planeamiento Estratégico y Política Militar en el ámbito del Estado Mayor Conjunto de las Fuerzas Armadas (EMCO). En dicho encuentro surge el tema de ciberdefensa y la preocupación de que ni el EMCO ni el Ministerio de Defensa estuvieran haciendo algo al respecto.

Paralelamente, el Secretario de Planeamiento, Gustavo Sibilla, le solicitó a la Armada Argentina que contribuya con información al "Tablero de Comando" sobre el estado de los sistemas de armas. La Armada se negó a brindar esa información porque sostuvo que las comunicaciones no eran seguras. Frente a esta situación se conformó un equipo de trabajo para desarrollar la "Red de Comunicaciones Estratégicas Seguras". Este trabajo fue conducido por el Director de Inteligencia Estratégica Militar, Carlos Aguilar (2007-2010).

Desconociendo esta última situación, y a instancias del asesor de la Subsecretaría de Planeamiento Estratégico y Política Militar, el Subsecretario José Luis Sersale (2007-2009) propuso la creación de un Grupo de Trabajo de Ciberdefensa en el ámbito de la Secretaría de Estrategia y Asuntos Militares, conducida por Germán Montenegro (2007-2009).

Luego de los cambios producidos en la Secretaría de Estrategia y Asuntos Militares (SEAM), cuando en febrero de 2009 se hizo cargo de ésta Gustavo Sibilla (2009-2010), dicha instancia ministerial constituyó finalmente en su ámbito de dependencia un Grupo de Trabajo destinado a analizar las implicancias estratégicas, doctrinarias y normativas del ciberespacio en el Sistema de Defensa Nacional de la República Argentina (resolución SEAM Nº 08/2010) en abril del 2010.

En el marco de la antedicha resolución, la Subsecretaría

de Planeamiento Estratégico y Política Militar convocó a la primera reunión de trabajo el 28 de abril de 2010 que se realizó en las oficinas de dicha Subsecretaría. Debido a la alta convocatoria que suscitó el tema entre las Fuerzas Armadas, hubo que cambiar el lugar de la reunión. Es en esa instancia donde el Ministerio de Defensa toma conocimiento de los avances realizados por cada una de las Fuerzas Armadas en materia de ciberdefensa.

A lo largo de ese año, el grupo se reunió en varias oportunidades produciendo diversos informes, pero sin que llegara ni a elaborar una norma de carácter ministerial ni a confeccionar una doctrina en el Nivel Estratégico Nacional.

Un año más tarde, el PLANCAMIL 2011 incorporó la ciberdefensa en el Área de Capacidad 3 (AC3) "Vigilancia, Reconocimiento e Inteligencia", proponiendo la creación de la Agencia de Ciberdefensa. Sin embargo, si bien el PLANCAMIL estableció los lineamientos generales para el desarrollo de esta Área de Capacidad –en el marco de las disposiciones doctrinarias y normativas de la Política de Defensa Nacional–, no precisó los criterios específicos necesarios para desarrollar la estructura de la Agencia.

Por tal motivo, la Dirección General de Planeamiento y Estrategia elevó a la Subsecretaría de Planeamiento Estratégico y Política Militar, en marzo de 2012, un proyecto de resolución que tenía por objetivo precisar las responsabilidades orgánicas y funcionales del Sistema de Defensa Nacional en materia de ciberdefensa. Dicha propuesta quedó estancada en la Secretaría de Estrategia y Asuntos Militares (SEAM), a cargo de Oscar Cuatromo (2011-2013), porque el nuevo funcionario entendía que la ciberdefensa era una temática de inteligencia militar.

Es por esto que, durante la gestión de Oscar Cuattromo se produjeron dos procesos de debate paralelos en torno a la definición de ciberdefensa. El primero se realizó en el ámbito

de la Dirección Nacional de Inteligencia Estratégica Militar, dirigida por María Lourdes Puente Olivera, y a quien el SEAM asignó la tarea de retomar el debate iniciado por la resolución SEAM Nº 8/2010, y en el marco de la elaboración de la segunda Directiva de Política de Defensa Nacional (DPDN). En efecto, la Resolución Nº 580/2011 estableció la necesidad de proponerle al Ministro de Defensa un proyecto de resolución para determinar el rol de la jurisdicción en este tema.

A tal efecto, la Dirección de Inteligencia Estratégica Militar (DNIEM) realizó varias reuniones a lo largo del año 2012 con participación mayoritaria de las Fuerzas Armadas. Dicho proceso culminó con la elaboración de un documento contribuyente a la elaboración de la segunda DPDN y con un proyecto de resolución sobre ciberdefensa que fue elevado al Ministerio de Defensa en octubre de 2012. Ese proyecto también fue girado por el SEAM a la DGPLA para que ésta se expidiera, la cual objetó el proyecto porque no se ajustaba al marco legal vigente.

El segundo proceso tuvo lugar principalmente en el Estado Mayor Conjunto de las Fuerzas Armadas (EMCO). Éste dispuso en mayo de 2012, en base a la resolución SEAM Nº 8/2010, la creación de un equipo técnico dirigido a redactar una propuesta de la arquitectura de la Agencia de Ciberdefensa, que había sido ordenada por el PLANCAMIL 2011 (Resolución EMCO Nº 59/12). Como resultado de la labor de dicho equipo, el EMCO elevó al Ministerio de Defensa un conjunto de aportes y contribuciones doctrinarios orientados a identificar estrictamente el ámbito de aplicación de la ciberdefensa.

La Dirección General de Planeamiento y Estrategia (DGPLA) analizó los aportes del EMCO y se inició un intercambio de documentos, en donde la primera sugirió cambios y precisiones al documento.

Más allá de las observaciones, la Dirección General de Planeamiento y Estrategia asesoró al Secretario de Estrategia

y Asuntos Militares que la "capacidad de ciberdefensa" debía ser encuadrada como una capacidad –valga la redundancia– operacional y no de inteligencia y que, para ello, el Instrumento Militar debía estar en capacidad exclusivamente de:

a. Garantizar la protección de las redes informáticas y activos de la Jurisdicción Ministerio de Defensa y de su Instrumento Militar dependiente;

b. Garantizar la defensa contra aquellos ciberataques que pretendan obstaculizar las operaciones militares del Instrumento Militar en cumplimiento de su misión principal; y

c. Desarrollar capacidades para realizar operaciones cibernéticas de defensa indirecta en el ciberespacio, en el marco estricto de la misión principal asignada al Instrumento Militar.

Asimismo, esa dependencia sugirió que, en la órbita del Sistema de Defensa Nacional, se emplee el término "ciberataque" y/o "agresión cibernética" para referirse exclusivamente a:

a. Las operaciones ciberespaciales que pretendan afectar las redes informáticas y activos del Ministerio de Defensa y las capacidades de su dependiente Instrumento Militar.

b. Las operaciones ciberespaciales conducidas por actores estatales militares externos que pretendan obstaculizar las operaciones militares del Instrumento Militar en cumplimiento de su Misión Principal.

Recién durante la gestión del Ministro Agustín Rossi se alcanzó una definición de ciberdefensa, luego de los intercambios entre Jefatura de Gabinete del Ministerio, la

Subsecretaría de Planeamiento Estratégico y Política Militar, con el asesoramiento de la Dirección General de Planeamiento y Estrategia. La coordinación entre ambas áreas culminó en la redacción de tres documentos.

La Directiva de Política de Defensa 2014 estableció que:

> *La dimensión ciberespacial, sin locación física específica propia, genera replanteos sobre las tradicionales categorías con las que se aborda la "guerra real" y exige, por la dinámica propia de la innovación tecnológica, una rápida adaptación para los Sistemas de Defensa respecto de sus componentes. En las últimas décadas, muchos países vienen reorientando esfuerzos y recursos para resguardar no sólo los espacios tradicionales (terrestre, marítimo y aeroespacial), sino también al ciberespacial. Éste no constituye un "espacio en sí mismo", sino una dimensión que atraviesa a dichos espacios físicos, con medios y reglas propias. Si bien las acciones de ciberguerra poseen su origen en el ámbito virtual de las redes de comunicación y sistemas informáticos, sus efectos impactan sobre el mundo físico, pudiendo afectar, por ejemplo, el tráfico aéreo y terrestre, el control de las infraestructuras críticas, el abastecimiento energético y de agua potable, entre otros. Dentro de la amplia gama de operaciones cibernéticas, sólo una porción de éstas afectan específicamente el ámbito de la Defensa Nacional. En efecto, en materia de ciberdefensa existen dificultades fácticas manifiestas para determinar a priori y ab initio si la afectación se trata de una agresión militar estatal externa. Por tal motivo, resulta necesario establecer dicha calificación a posteriori actuando como respuesta inmediata el Sistema de Defensa únicamente en aquellos casos que se persiguieron objetivos bajo protección de dicho sistema, es decir que poseen la intención de alterar e impedir el funcionamiento de sus capacidades.*

En este sentido, la DPDN 2014 ordenaba que:

> *El MINISTERIO DE DEFENSA elaborará las normas para la creación de una instancia de naturaleza operacional en materia de Ciberdefensa, de acuerdo a lo previsto en el Plan de Capacidades*

> *Militares (PLANCAMIL 2011). Asimismo, se procederá a la adhesión del MINISTERIO DE DEFENSA al "Programa Nacional de Infraestructuras Críticas de la Información y Ciberseguridad" de la OFICINA NACIONAL DE TECNOLOGÍAS DE LA INFORMACIÓN (ONTI) de la JEFATURA DE GABINETE DE MINISTROS. Por último, ordenará al ESTADO MAYOR CONJUNTO DE LAS FUERZAS ARMADAS la elaboración de un Plan de Desarrollo de Ciberdefensa para el período 2014-2018.*
>
> *En función del marco normativo y doctrinario del Sistema de Defensa Nacional de la REPÚBLICA ARGENTINA, se entenderá por "Ciberdefensa" a las acciones y capacidades desarrolladas por el INSTRUMENTO MILITAR en la dimensión ciberespacial de carácter transversal a los ambientes operacionales terrestre, naval y aéreo.*

Mientras que al Estado Mayor Conjunto de las Fuerzas Armadas se le instruía que:

> *Respecto de la dimensión ciberespacial de los ambientes operacionales terrestre, naval y aéreo, según surge de la presente Directiva, el ESTADO MAYOR CONJUNTO DE LAS FUERZAS ARMADAS deberá elaborar, por instrucción del MINISTERIO DE DEFENSA, un Plan de Desarrollo de la Ciberdefensa para el período 2014-2017.*

En función de lo expuesto, se decidió crear una instancia ministerial para que supervisara las acciones del EMCO y las Fuerzas en materia de ciberdefensa. En efecto, la Jefatura de Gabinete del Ministerio de Defensa propuso que se creara la Dirección General de Ciberdefensa (Decisión Administrativa Nº 15 del 4 de marzo de 2015).

En segundo lugar, y dado que la DGPLA planteaba que debía evitarse que en el marco del debate de la ciberdefensa se colara la intervención de las Fuerzas Armadas en la seguridad interior, el principal escollo era cómo "separar" en el ciberespacio las agresiones externas militares estatales de

aquellas que fueran de naturaleza criminal. En este punto se asesoró al Ministro de Defensa que:si bien era cierto que por las características del ciberespacio no se podía determinar

a. el origen de la amenaza, en cambio se podía circunscribir la ciberdefensa a aquellas amenazas que afectaran la libertad de maniobra de las Fuerzas Armadas; afectaran los objetivos de valor estratégico; y

b. que era una capacidad del nivel operacional —no de inteligencia—, y que debía desarrollar capacidades para realizar operaciones de ciberdefensa indirecta (ataques) en el ciberespacio.

La Resolución MD Nº 343 del 14 de mayo de 2014 creó el Comando Conjunto de Ciberdefensa bajo dependencia del Estado Mayor Conjunto de las Fuerzas Armadas, asignándole la misión de "conducir las operaciones de ciberdefensa". En segundo lugar, la Resolución MD Nº 344 del 14 de mayo de 2014, de carácter secreto —y aún vigente—, definió cual era el alcance de las operaciones de ciberdefensa; ordenó la elaboración de la doctrina básica conjunta, derivada y de procedimientos, que debía ser aprobada por el Ministerio de Defensa.

La ciberdefensa durante el gobierno de Mauricio Macri (2015-2019)

Durante el gobierno de Mauricio Macri comienza un período de transición para el sector de ciberdefensa, marcado por un cambio en la concepción del ciberespacio que impulsa a la cúpula del gobierno a dotar con nuevos instrumentos y funciones a la Defensa Nacional para la protección de la soberanía nacional en el ciberespacio. Este período de transición es el resultado de la continuación de ciertos

lineamientos establecidos por el gobierno anterior y algunos matices propios que proponen una ruptura (aunque no tajante) con la concepción anterior.

Este proceso comienza junto con la toma de posesión del cargo de Presidente de la Nación, cuando a través del Decreto Nº 13/2015 se consideraba:

> *Que para impulsar las políticas de jerarquización del empleo público y su vínculo con las nuevas formas de gestión que requiere un Estado moderno, como así también el desarrollo de tecnologías aplicadas a la administración pública central y descentralizada, que acerquen al ciudadano a la gestión del Gobierno Nacional, así como la implementación de proyectos para las provincias y municipios de políticas de tecnologías de la información, se hace necesaria la creación del MINISTERIO DE MODERNIZACIÓN.*

La creación del Ministerio de Modernización estimuló las políticas de digitalización del Estado Nacional y concientización en materia de ciberseguridad. A la vez, la nueva cartera ministerial se hizo con el control del Programa de Infraestructuras Críticas de la Información y de la Comunicación creado en 2011 bajo la órbita de Jefatura de Gabinete de Ministros.

En consonancia con este programa, se hizo efectiva la Política de Seguridad de la Información a través de Resolución Nº 59/2016. Esta política se sustenta en los lineamientos fijados por la Política de Seguridad de la Información (política modelo) establecida en 2011 en la órbita de la Oficina Nacional de Tecnologías de la Información y tiene por objeto la protección de la información de un rango amplio de amenazas para poder continuar con el normal funcionamiento del organismo.

En enero de 2016, el Poder Ejecutivo Nacional modificó estructuralmente la cartera ministerial de defensa a través del Decreto Nº 42/2016, suprimiendo la Dirección General de

Ciberdefensa y elevándola al rango de Subsecretaría bajo el paraguas de la Secretaría de Ciencia, Tecnología y Producción para la Defensa, y brindándole a ésta las mismas funciones que poseía su antecesora.

El Subsecretario de Ciberdefensa se planteó la necesidad de incorporar tecnología. A tal efecto, consultó con las Fuerzas cuáles deberían ser los requerimientos técnicos con los que debía contar el oferente. Dichos requerimientos fueron elevados por la Armada Argentina que, luego de una reunión con el EMCO, la Fuerza Aérea Argentina y el Ejército, quedaron plasmados en el documento "Requisitos funcionales para la ciberdefensa".

A partir de ello, se contactaron a empresas rusas, israelíes, francesas y suizas, y se terminaron las remodelaciones del sitio para instalar el Comando Conjunto de Ciberdefensa en Puerto Madero. Particularmente con los franceses y suizos se empezaron a realizar reuniones de trabajo y capacitación. Sin embargo, sus propuestas se cayeron por falta de presupuesto. Se evaluó vender el edificio que había sido acondicionado en Puerto Madero, Ciudad Autónoma de Buenos Aires, y mudarse a Villa Martelli o al CITEDEF para financiar la adquisición de equipamiento.

En julio de 2017, Oscar Aguad fue designado Ministro de Defensa. Días después (el 28 de julio de 2017), se hizo público el decreto Nº 577 en el cual se ratificó la necesidad de crear una Estrategia Nacional de Ciberseguridad que contemplara: propósitos y objetivos, la creación de un sistema normativo acorde, medidas técnicas, organizacionales y políticas que permitan proteger al ciberespacio; la definición de Infraestructuras Críticas y el desarrollo de una cultura de ciberseguridad.

Con ese objeto, la mencionada normativa resolvió dotar al país de un Comité de Ciberseguridad en el que participen los Ministerios de Modernización, Defensa y Seguridad, y

que tenga por finalidad desarrollar la Estrategia Nacional de Ciberseguridad. Este decreto puso al mando del Comité al Ministerio de Modernización y lo estimuló a convocar a otros organismos para participar de sus actividades. En consonancia con lo establecido, los ministerios de Relaciones Exteriores y Culto, Justicia y Derechos Humanos y Jefatura de Gabinete de Ministros participan activamente de las reuniones del Comité. La definición de la Estrategia divide las funciones en materia de ciberseguridad y ciberdefensa entre las distintas carteras ministeriales. De tal forma, el Ministerio de Defensa, siguiendo con los lineamientos establecidos en la resolución Nº 343/2014, asumió la responsabilidad de resguardar las Infraestructuras Críticas del país. En virtud de ello, el Comité cuenta con una subcomisión destinada a definir y delimitar cuáles deberían ser dichas Infraestructuras Críticas que deberán ser aprobadas por el Poder Ejecutivo Nacional y no únicamente por el Ministerio de Defensa. Por su parte, el Ministerio de Seguridad apoyó ese rol para el Ministerio de Defensa y ellos optaron por ocuparse de problemáticas de cibercrimen. Las Fuerzas no fueron consultadas para la elaboración de esta estrategia.

El 22 de febrero de 2018 asumió un nuevo Subsecretario de Ciberdefensa, el cual impulsó las negociaciones gobierno a gobierno para la adquisición de equipamiento.

En el marco de la Cumbre del G-20, el decreto N° 125 de febrero de 2018 declaraba secreta la adquisición de materiales bélicos requeridos por el Estado Mayor Conjunto. Tras la promulgación del decreto, Edgardo Aguilera informaba sobre la puja entre Rusia e Israel por hacerse con el mercado argentino de adquisición de materiales de ciberseguridad y ciberdefensa. En virtud de ello, la visita oficial del Primer Ministro israelí y empresarios del sector de ciberdefensa (representantes de las empresas Verint, Elbit y Mey Cyber), en septiembre de 2017, buscaron fortalecer los lazos comerciales en respuesta a la necesidad argentina de adquirir material

destinado a la protección del ciberespacio. La visita oficial culminó con la firma de un Memorándum de entendimiento entre la Agencia Argentina de Inversiones y Comercio Internacional y su homóloga israelí, el Instituto Israelí de Exportación y Cooperación Internacional, para la promoción de las inversiones y comercio entre ambos Estados.

Por su parte, Rusia, a través de su Embajada en Buenos Aires, organizó un encuentro entre Softline International (empresa rusa de ciberseguridad); el Subsecretario de Ciberdefensa, Ing. Parodi; y el jefe del Estado Mayor del Comando Conjunto de Ciberdefensa, el comodoro Horacio Ghiosi. Dado que el gobierno argentino optó por el esquema G2G (negociaciones gobierno a gobierno) para la adquisición de equipamiento, en enero de 2018 entró en vigor un acuerdo de protección mutua de la información secreta en el ámbito de la cooperación técnica militar que complementa el Convenio de Cooperación Técnica Militar suscrito en 2004 y posibilita que empresas rusas puedan presentarse a los llamados de licitación argentina para adquisición de materiales bélicos.

La puja por abastecer de material cibernético tiene sus orígenes en la creación del proyecto núcleo ISOC & CSIRT/CERT para la ciberdefensa. Dicho proyecto concentra todos los esfuerzos del Ministerio de Defensa para la adquisición de cibercapacidades, porque a través de este programa se proyecta crear un CERT/CSIRT en el seno de la Subsecretaría de Ciberdefensa que tenga como misión principal la protección de las Infraestructuras Críticas (IC) de la Defensa Nacional, esto es, toda infraestructura necesaria para el buen funcionamiento de la vida del Estado y sus habitantes. El proyecto se completó con la creación de un Centro de Seguridad de la Información e Inteligencia Artificial (ISOC) bajo la conducción del Comando Conjunto de Ciberdefensa, que se encargará de proteger las Infraestructuras Críticas propias del Instrumento Militar, es decir, aquellas que dependan directamente de las Fuerzas Armadas. Finalmente, del llamado a licitación participaron las empresas israelíes Rafael Systems, Verint, Israel Aerospace

Industries y Elbit.

Tras algunos vaivenes e irregularidades en la puja por proveer a la Argentina de tecnología, y luego de realizar consultas al Comando Sur, la Subsecretaría de Ciberdefensa, a través de la Decisión Administrativa N° 1658/2018, aprobó un gasto por U$S 5.245.000 derivado del acuerdo de implementación del Proyecto Núcleo de CSIRT y CERT de Ciberdefensa, suscripto el 21 de septiembre de 2018 entre los Ministerios de Defensa de Argentina e Israel, haciendo oficial la compra a Rafael Systems.

La instalación y puesta en funcionamiento del CSIRT y CERT finalizó el 2 de noviembre de 2018 y ello incluyó:

- Construcción y adecuación de las salas del ISOC & CSIRT/CERT y Centro de Datos en el Edificio Cóndor;
- Instalación eléctrica y fibra óptica desde el Centro de Cómputos a ISOC & CSIRT & CERT y red de distribución de puestos de trabajo;
- Instalación de fibra óptica en puestos de trabajo SOC del Ejército Argentino en el Edificio Libertador;
- Instalación de fibra óptica desde el Centro de Cómputos a puestos de trabajo SOC de la Armada Argentina en el Edificio Libertad; y
- Distribución de equipamiento informático a los sitios de información.

Tal como había sido proyectado, la finalización de la instalación del hardware y software y puesta en marcha del sistema núcleo ISOC & CSIRT/CERT se realizó el 14 de noviembre de 2018, días antes del inicio de la cumbre del G20 en Buenos Aires en diciembre de 2018.

Los Juegos Olímpicos de la Juventud realizados en Buenos

Aires en el año 2018, así como la Cumbre del G20 efectuada en la misma ciudad en noviembre de ese año, permitieron efectuar un monitoreo desde el CSIRT de la defensa, y se trabajó coordinadamente con el Ministerio de Seguridad y Modernización. Al respecto, el Subsecretario de Ciberdefensa, Alfredo Parodi, sostuvo que "el G20 nos hizo enfrentar el problema real de cómo defender el ciberespacio (...). Fuimos a proteger en profundidad cada uno de los elementos que estaban contenidos en nuestras redes".

El Ministro de Defensa, Oscar Aguad, puso especial énfasis en la reconversión de las Fuerzas Armadas. En este sentido, los principales puntos de reforma se refieren a "achicar estructuras, fusionar secretarías, cuidar los espacios fronterizos de la Argentina y definir un programa de ciberdefensa coordinado con todo el gobierno nacional."

La reforma de las funciones de las Fuerzas Armadas tuvo su punto culmine en julio de 2018 con la presentación de los decretos Nº 683 y 703.

Por un lado, el decreto Nº 683/2018, promulgado el 23 de julio de 2018, modifica el núcleo sustancial del decreto Nº 727/2006 que establecía que el Instrumento Militar de la Nación sería empleado de forma disuasiva o efectiva ante agresiones estatales militares de origen externo. El actual decreto reemplazó este concepto por el de agresiones de origen externo, lo cual permite hacer una lectura amplia en cuanto a la magnitud y origen de las amenazas, dejando abierta la posibilidad de interpretar la nueva doctrina de tal manera que se habilite el accionar de las Fuerzas Armadas en cuestiones de seguridad interior.

A la vez, esto supuso, para cuestiones de ciberdefensa, dejar de lado la limitación impuesta por la definición de agresiones estatales de origen externo, dado que algunos interpretaban que restringía la posibilidad de actuación de las Fuerzas Armadas ante agresiones en el ciberespacio puesto

que resulta difícil atribuir con exactitud la autoría de las agresiones cibernéticas. Así, el decreto Nº 683/2018 posibilita el accionar del Instrumento Militar en el ciberespacio para repeler y contrarrestar ciberataques sin importar el origen del ataque.

Por otra parte, la nueva DPDN 2018 (Decreto Nº 703), promulgada el 30 de julio de 2018, en su diagnóstico global de la Apreciación del Escenario Global y Regional concentra sus esfuerzos en el fenómeno ciberespacial, haciendo hincapié en que las Fuerzas Armadas de todo el globo han incorporado al ciberespacio como ámbito de interés gracias a la interdependencia tecnológica y los riesgos asociados a la militarización del ciberespacio.

Dentro de sus enunciados destaca:

> *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.*

A partir de este enunciado, se llama a la Defensa Nacional a adoptar medidas y acciones que permitan resguardar la seguridad cibernética de las Infraestructuras Críticas de la Defensa Nacional, haciendo extensible las funciones del sistema de Defensa Nacional sobre aquellas infraestructuras que sean consideradas vitales para garantizar la soberanía e independencia del Estado, su integridad territorial y la protección de la vida y la libertad de sus integrantes.

Ante el riesgo de la utilización del ciberespacio con fines militares, la DPDN 2018 convoca a adecuar la organización militar al impacto de este riesgo, la orientación de la política de ciberdefensa a la reducción de vulnerabilidades de los activos estratégicos de interés y a la cooperación con otras áreas del Estado responsables en la política de ciberseguridad nacional. Además, incita a fortalecer las capacidades "de anticipación, disuasión, vigilancia y control de la seguridad cibernética de las infraestructuras críticas del Sistema de Defensa Nacional" y privilegia los desarrollos tecnológicos multiplicadores en áreas como la ciberdefensa, alerta estratégica y sistemas de C4ISV.

Aunque no lo expresa textualmente, se puede apreciar un cambio en la concepción de la DPDN de 2014 a la actual respecto a la definición del ciberespacio. La primera de ellas presentaba al ciberespacio como un ámbito transversal a los dominios tradicionales (tierra, mar, aire y espacio exterior), mientras que la actual, se refiere a la militarización del ciberespacio y a la extensión de la disuasión al ámbito cibernético, lo que supone, en definitiva, que el ciberespacio es considerado un dominio en sí mismo.

Sin lugar a dudas, la DPDN de 2018 advierte sobre el rumbo de las políticas que estaban siendo desarrolladas por el actual gobierno en materia de Defensa Nacional y jerarquiza las cuestiones de ciberdefensa en la agenda del Ministerio, lo cual puede verse reflejado principalmente a partir de la llegada de Aguad al Ministerio de Defensa.

Finalmente, el 25 de octubre de 2019 se hizo oficial la Resolución MD N° 1380 con cuatro anexos bajo secreto militar y uno de carácter público. El anexo 4 público define como ciberdefensa:

> *a las acciones y capacidades desarrolladas por el MINISTERIO DE DEFENSA, EL ESTADO MAYOR CONJUNTO y las FUERZAS ARMADAS para anticipar y prevenir ciberataques y ciberexplotación de las redes nacionales que puedan afectar*

> *al Ministerio de Defensa y al Instrumento Militar de la Defensa Nacional, como así también a las infraestructuras Críticas operacionales soporte de los Servicios Esenciales de interés para la Defensa o Infraestructuras operacionales soporte de procesos industriales de fabricación de bienes sensibles para la Defensa o que posibiliten el acceso a los activos digitales estratégicos adjudicados a su custodia.*

Con respecto a este punto, cabe señalar la incompatibilidad de esta definición con lo dispuesto en la Resolución MD Nº 344 del 14 de mayo de 2014, de carácter secreto, que seguía vigente y que —como señalamos ut supra— definió cual era el alcance de las operaciones de ciberdefensa; ordenó la elaboración de la doctrina básica conjunta, derivada y de procedimientos, las cuales debían ser aprobadas por el Ministerio de Defensa.

El artículo segundo de dicha resolución crea el Centro Nacional de Ciberdefensa en el ámbito de la Subsecretaría de Ciberdefensa, donde funcionan el CSIRT de Defensa, el iSOC del EMCO y el CyberLab (Laboratorio de Análisis Cibernético). Y crea, mediante el artículo cuarto, un Comité Consultivo de Ciberdefensa en la órbita de la Secretaría de Estrategia y Asuntos Militares a fin de realizar estudios para definir el plan de adecuación de Organizaciones Militares y la preparación de una propuesta de la DEPEM (Directiva para la Elaboración del Planeamiento Estratégico Militar).

El Centro Nacional de Ciberdefensa fue finalmente emplazado en las oficinas del Instituto de Investigaciones Científicas y Técnicas para la Defensa (CITEDEF) en Villa Martelli, Provincia de Buenos Aires, siendo este inaugurado el día 5 de noviembre de 2019, 5 días antes de hacerse efectivo el cambio de gobierno. Por su parte, las unidades orgánicas de cada una de las Fuerzas continuarían alojadas en sus respectivos lugares de emplazamiento. Una de las problemáticas que sigue sin resolverse es que dichas unidades tienen diferentes estructuras y dependencias. La Armada cuenta con un Servicio de Ciberdefensa y Seguridad de la

Información que depende del Subjefe; el Ejército Ciberdefensa dependía de la Jefatura de II de inteligencia y pasó a depender de Comunicaciones e Informática, pero manteniéndose separada de Seguridad de la Información; y la Fuerza Aérea Argentina tiene ciberdefensa y seguridad de la información unificados dependiendo también del Subjefe.

Asimismo, la norma citada aprobó "La política de ciberdefensa" que, al conceptualizar al ciberespacio como un espacio soberano, llama a disponer acciones para fortalecer las capacidades de vigilancia y control. Para ello, enumera los siguientes objetivos:

- Anticipar y prevenir ataques en el ciberespacio;
- Disminuir vulnerabilidades y aumentar la resiliencia de los sistemas de redes TICs de las FFAA, EMCO y MINDEF;
- Detectar amenazas y gestionar riesgos de ciberatauqes y recuperación de los sistemas e infraestructura crítica de interés para la Defensa Nacional;
- Adoptar las acciones contra potenciales adversarios o agentes hostiles que afecten la integridad y disponibilidad de las redes y sistemas de la Defensa;
- Contribuir a potenciar la base tecnológica e industrial nacional de ciberseguridad en trabajo conjunto con el Ministerio de Relaciones Exteriores y del Ministerio de Producción;
- Impulsar programas de capacitación, para superar brecha entre los recursos humanos disponibles y los demandados.

Asimismo, esta resolución establece cuatro líneas de acción:

- Crear el Centro Nacional de Ciberseguridad que funcionará en CITEDEF a fin de desarrollar capacidades

en el ciberespacio, asegurar la libertad de acción en el quinto dominio y proteger la información transportada por redes y sistemas de las FFAA, EMCO y MINDEF y proteger las IC de la Defensa Nacional;

- Proteger al ciberespacio como espacio soberano a través de herramientas de inteligencia artificial y machine learning con el objeto de registrar los ataques en el CSIRT de Defensa a fin de elaborar estadísticas y cooperar con otros organismos;
- Realizar trabajos de reingeniería de las redes dependientes de las FFAA, EMCO y MINDEF; y
- Lograr la convergencia de las capacidades de las FFAA.

Estas cuatro líneas de acción serían gestionadas a través de políticas regulatorias, de desarrollo de capacidades y de concientización y capacitación.

Además, la Resolución desarrolla un "Plan Nacional de Protección de Infraestructuras criticas Cibernéticas de la Defensa Nacional" que tiene como objetivo principal "fortalecer la seguridad y la capacidad de recuperación de la infraestructura crítica de la Defensa". La norma define como Infraestructuras Críticas (IC) de la Defensa Nacional a: 1) aquellas de interés para la Defensa Nacional: a) infraestructuras TO de soporte de servicios esenciales (industria energética y nuclear) y b) infraestructuras TO de soporte de procesos industriales de fabricación de bienes sensibles (explosivos, moderadores de fisión de reactores nucleares y aquellos con capacidad de dañar masivamente el medioambiente); y c) las infraestructuras del sistema de Defensa Nacional que son aquellas TO y TI pertenecientes al Instrumento Militar y al MINDEF.

De esta forma, la política de ciberdefensa complementa la Estrategia Nacional de Ciberseguridad al delimitar el accionar del sistema de Defensa en el ciberespacio.

Reflexión final

El cambio de gobierno en 2015 supuso el regreso de la Unión Cívica Radical al Ministerio de Defensa. Durante la administración de Julio Martínez, las Fuerzas Armadas y el Comando Conjunto de Ciberdefensa, y a diferencia de lo que sucedió en otros ámbitos del Sistema de Defensa Nacional, efectuaron una leve modificación a la Resoluciones Nº 344/2014, incorporando a la infraestructura crítica, pero sin derogarla. Asimismo, pese a la modificación del Decreto Nº 727/2007 y de la aprobación de la DPDN 2014, la posibilidad de diseñar el Instrumento Militar tomando como hipótesis cualquier agresión externa no significó un cambio en materia de ciberdefensa porque el Ministerio de Seguridad retuvo de facto la responsabilidad de diseñar sus políticas, estratégicas y orgánicas para hacer frente a problemas emanados del ciberdelito, mientras que el Ministerio de Modernización o Jefatura de Gabinete, dependiendo del año del que hablemos, retuvieron la responsabilidad emanada del paraguas de la ciberseguridad.

Durante la llegada de Oscar Aguad al Misterio de Defensa se intentó presentar el tema como una novedad, cuando en realidad el Ministerio ya trabaja en el tema desde el año 2008 y las Fuerzas desde mediados de los años ´90. Es más, hubo más de continuidad que de cambio en relación a los Ministros de Defensa de Cristina Fernández de Kirchner ya que en general se continuó con las actividades destinadas a la ciberdefensa.

No obstante, se produjeron dos cambios significativos en línea con la orientación de política de ciberdefensa. Por un lado, se impulsó un cambio de concepción del ciberespacio: se consideró al ciberespacio como un quinto dominio. En consonancia con esto, la Directiva Política de Defensa Nacional de 2018 y el Decreto Nº 683/2018, modificatorio del 727/2006, adoptaron al ciberespacio como un quinto dominio e incluyeron a la infraestructura crítica nacional dentro de

los objetivos a proteger por parte de la ciberdefensa; esto sin cambiar las normas vigentes.

Por último, se adoptó incorporar tecnología vinculada al Estado de Israel, y de este con el Reino Unido de Gran Bretaña, abandonando la política de buscar un desarrollo autónomo. Esto no es nuevo en la política de defensa argentina ya que el país siempre recurrió a material bélico inglés y/o occidental pese a que persiste una problemática territorial con Gran Bretaña.

La ciberdefensa se ha convertido en la panacea del Sistema de Defensa argentino porque es sin duda más barata que recuperar la capacidad de combate de la Fuerza Aérea. Al adoptar la visión de la ciberdefensa como quinto dominio se piensa a esta como un escenario en el cual se pueden producir efectos políticos y estratégicos: en términos de Clausewitz, ganar la guerra. Finalmente, las maniobras de Rusia y la Organización del Tratado del Atlántico Norte, realizadas durante el tercer trimestre de 2018, desmienten esa apreciación estratégica.

Referencias bibliográficas

Bibliografía

EISSA, S.; GASTALDI, S.; POCZYNOK, IVÁN & ZACARÍAS DI TULLIO, E. (2014). "El ciberespacio y sus implicancias para la defensa nacional. Aproximaciones al caso argentino" *Revista de Ciencias Sociales. Segunda Época* 6 (25): pags. 181-197.

EISSA, S. (2015), *¿La irrelevancia de los Estados Unidos? La política de defensa argentina (1983-2010)*. BUENOS AIRES: ARTE Y PARTE.

EISSA, S. & ABARRACÍN KETICOGLU, A. (2019), "¿QUO VADIS CIBERDEFENSA? EL CASO ARGENTINO" *Apuntes Estratégicos* 1: págs. 114-132.

SAÍN, G. (2015), "Cibercrimen: el delito en la sociedad de la información", en EISSA, S. (Coord.). *Políticas públicas y seguridad ciudadana*. Buenos Aires: Eudeba.

Fuentes periodísticas

AGUILERA, E. (13 de febrero de 2018). Rusia e Israel pujan por vender ciberseguridad para el G-20. Disponible en http://www.ambito.com/912214-rusia-e-israel-pujan-por-vender-ciberseguridad-para-el-g-20. Consulta: 10 de marzo de 2019.

AGUILERA, E. (7 de septiembre de 2018). Polémica en el concurso de empresas para ciberdefensa del G-20". Disponible en http://www.ambito.com/933043-polemica-en-el-concurso-de-empresas-para-ciberdefensa-del-g-20. Consulta: 15 de marzo de 2019.

DINATALE, M. (23 de abril de 2018). El gobierno reunió a la cúpula de las Fuerzas Armadas para analizar los cambios en el rol de los militares. Disponible en https://www.infobae.com/politica/2018/04/23/el-gobierno-reunio-a-la-cupula-de-las-fuerzas-armadas-para-analizar-cambios-en-el-rol-de-los-militares/. Consulta: 20 de abril de 2019.

ESTADO MAYOR CONJUNTO DE LAS FUERZAS ARMADAS (2019, 10 de junio), Se realizó el primer seminario sobre la Ciberdefensa en la República Argentina. Disponible en http://www.fuerzas-armadas.mil.ar/Noticia-2019-06-10-seminario-ciberdefensa.aspx. Consulta 29 de agosto de 2019.

LARRE, A. (5 de diciembre de 2019). Argentina ya tiene listo su Centro Nacional de Ciberdefensa. Disponible en https://www.infodefensa.com/latam/2019/12/05/noticia-argentina-tiene-listo-centro-nacional-ciberdefensa.html. Consulta: 28 de septiembre de 2019.

MINISTERIO DE DEFENSA (2019, 24 de junio). El comandante conjunto de Ciberdefensa expuso en el seminario Ciberdefensa: un imperativo estratégico de la República Argentina. Disponible en https://www.argentina.gob.ar/noticias/el-comandante-conjunto-de-ciberdefensa-expuso-en-el-seminario-ciberdefensa-un-imperativo). Consulta: 29 de agosto de 2019.

ROCA, M. (2019, 31 de agosto) Así se preparan las FF.AA. argentinas para hacer frente a la guerra electrónica. Disponible en https://www.infobae.com/def/defensa-y-seguridad/2019/08/28/asi-se-preparan-las-ff-aa-argentinas-para-hacer-frente-a-la-guerra-electronica/. Consulta: 13 de septiembre de 2019.

Informes gubernamentales

AGENCIA ARGENTINA DE INVERSIONES Y COMERCIO INTERNACIONAL Y EL INSTITUTO ISRAELÍ DE EXPORTACIÓN Y COOPERACIÓN INTERNACIONAL (2017). Memorándum de Entendimiento sobre Promoción de las Inversiones y el Comercio entre la República Argentina y el Estado de Israel.

REPÚBLICA ARGENTINA Y FEDERACIÓN RUSA (2018). Acuerdo sobre la Protección Mutua de la Información Secreta en el ámbito de la Cooperación Técnica Militar.

PODER EJECUTIVO NACIONAL (2019). Respuesta a la solicitud de Información Pública. IF-2019-2115065-APN-DNAIP#AAIP

Normativa

DECISIÓN ADMINISTRATIVA 669 (2004). Jefatura de Gabinete de Ministros, República Argentina.

DECRETO 1028 (2003). República Argentina. Disponible en http://servicios.infoleg.gob.ar/infolegInternet/anexos/90000-94999/90082/norma.htm. Consulta: 30 de septiembre de 2020.

DECRETO 125 (2018). República Argentina. Disponible en https://www.argentina.gob.ar/normativa/nacional/decreto-125-2018-306822. Consulta: 30 de septiembre de 2020.

DECRETO 13 (2015). República Argentina. Disponible en http://servicios.infoleg.gob.ar/infolegInternet/anexos/255000-259999/256606/norma.htm. Consulta: 30 de septiembre de 2020.

DECRETO 2645 (2014). Directiva de Política de Defensa Nacional. República Argentina. Disponible en http://servicios.infoleg.gob.ar/infolegInternet/verNorma.do?id=240966. Consulta: 30 de septiembre de 2020.

DECRETO 42 (2016). República Argentina. Disponible en http://servicios.infoleg.gob.ar/infolegInternet/anexos/255000-259999/257609/norma.htm. Consulta: 30 de septiembre de 2020.

DECRETO 577 (2017). República Argentina. Disponible en http://servicios.infoleg.gob.ar/infolegInternet/anexos/275000-279999/277518/norma.htm. Consulta: 30 de septiembre de 2020.

DECRETO 624 (2003). República Argentina. Disponible en http://servicios.infoleg.gob.ar/infolegInternet/anexos/85000-89999/87826/norma.htm. Consulta: 30 de septiembre de 2020.

DECRETO 683 (2018). República Argentina. Disponible en https://www.argentina.gob.ar/normativa/nacional/decreto-683-2018-312581. Consulta: 30 de septiembre de 2020.

DECRETO 703 (2018). Directiva de Política de Defensa Nacional, República Argentina. Disponible en https://www.boletinoficial.gob.ar/detalleAviso/primera/189076/20180731. Consulta: 30 de septiembre de 2020.

DECRETO 727 (2006). República Argentina. Disponible en http://servicios.infoleg.gob.ar/infolegInternet/anexos/115000-119999/116997/norma.htm. Consulta: 30 de septiembre de 2020.

DISPOSICIÓN ADMINISTRATIVA 6 (2005). ONTI, República Argentina. Disponible en https://www.argentina.gob.ar/normativa/nacional/disposici%C3%B3n-6-2005-108672.

Consulta: 30 de septiembre de 2020.

DISPOSICIÓN ADMINISTRATIVA 1 (2015). Ministerio de Defensa, República Argentina. Disponible en http://servicios.infoleg.gob.ar/infolegInternet/anexos/240000-244999/242859/norma.htm. Consulta: 30 de septiembre de 2020.

Ministerio de Defensa. (2016). Resolución 59.

RESOLUCIÓN 1380 (2019). Ministerio de Defensa, República Argentina.

RESOLUCIÓN 343 (2014). Ministerio de Defensa, República Argentina.

RESOLUCIÓN 344 (2014). Ministerio de Defensa, República Argentina.

RESOLUCIÓN 48 (2005). SIGEN. República Argentina

RESOLUCIÓN 580 (2011). Jefatura de Gabinete de Ministros, República Argentina.

RESOLUCIÓN 59 (2012). Estado Mayor Conjunto de las Fuerzas Armadas, República Argentina.

RESOLUCIÓN 8 (2010). Ministerio de Defensa, República Argentina

RESOLUCIÓN SEAM 8 (2010). Ministerio de Defensa. República Argentina.

Fuentes

Entrevista reservada con Fuente A (civil), 17 de agosto de 2018, Buenos Aires, Argentina.

Entrevista reservada con Fuente B (civil), 3 de septiembre de 2018, Buenos Aires, Argentina.

Entrevista reservada con Fuente D (militar), 26 de septiembre de 2018, Buenos Aires, Argentina.

Entrevista reservada con Fuente E (militar), 28 de septiembre de 2018, Buenos Aires, Argentina.

Entrevista reservada con Fuente H (militar), 27 de septiembre de 2018 y 30 de octubre de 2018, Buenos Aires, Argentina.

Entrevista reservada con Fuente X (civil), 17 de agosto de 2018, Buenos Aires.

Entrevista con el Brigadier (RE) Alejandro Moresi, 27 de septiembre de 2018, Buenos Aires, Argentina.

Palabras clave: Argentina – Defensa – Seguridad Interior – Fuerzas Armadas – Ciberdefensa

Keywords: Argentina – Defense – Law Enforcement – Armed Forces – Cyber defense

Abstract

Cyber defense, as a public problem, became a new space of dispute between political actors who, in the bureaucratic scenario, pushed for its definition between the beginning of the 21st century and 2014. In a previous article (Eissa, et al., 2019) it was argued that the definition of cyber defense is not innocuous for at least three (3) reasons. In the first place, cyberspace puts in "check" the organic and functional separation between defense and internal security. Secondly, the decision on how that separation was to be resolved when facing the problem that cyberspace represented for the national security of Argentina. Lastly, the Armed Forces, together with the Joint Chiefs of Staff, pushed for the definition of cyber defense to evade the limits defined by the laws of internal security and national defense.

This article aims to analyze the changes that may have been made since the presidency of Mauricio Macri (2015-2019), in the light of the modification of Decree No. 727/2006 and the approval of the Defense Policy Directive (DPDN) 2018 which allowed the defense system to intervene against threats of transnational origin.