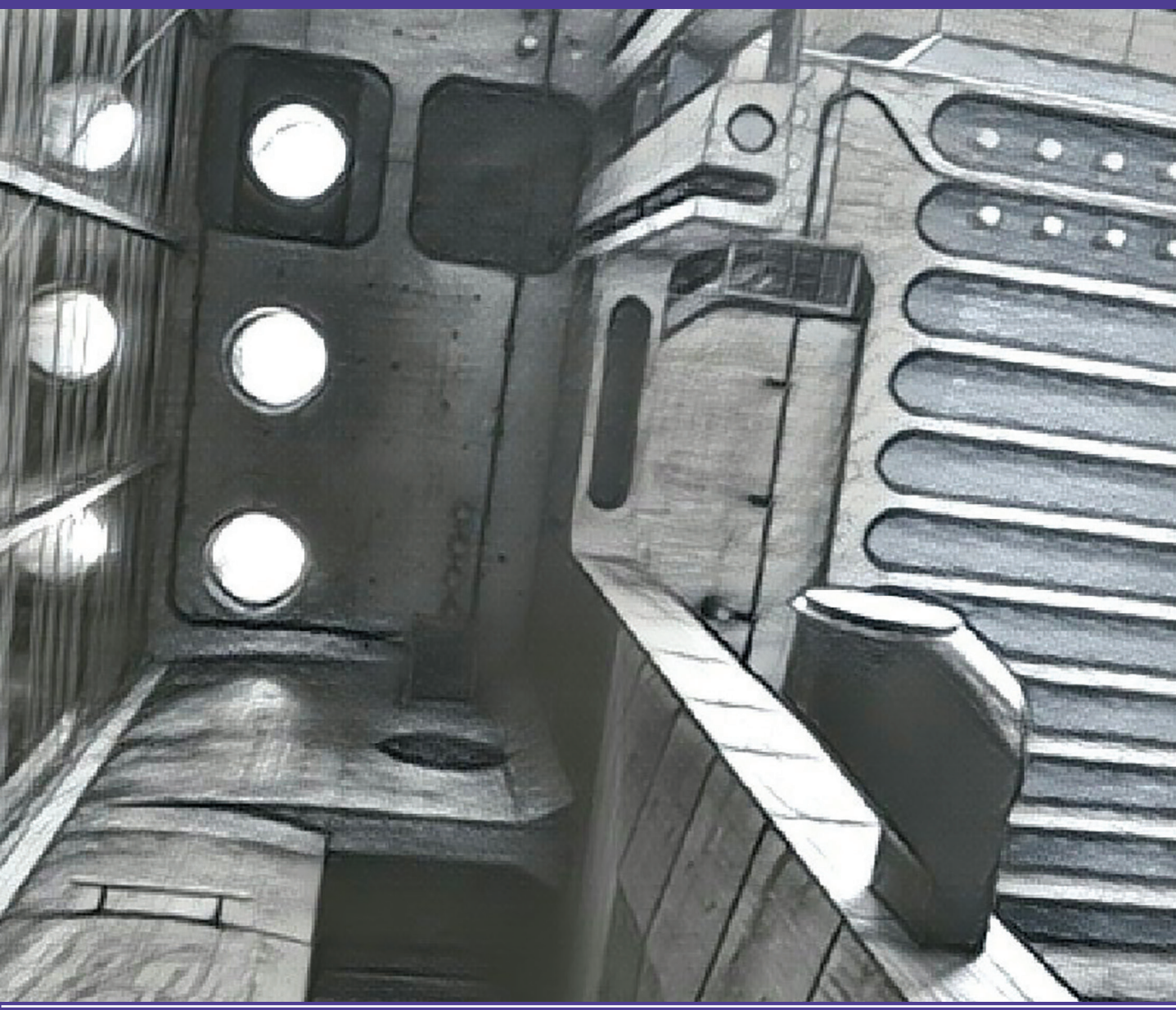
ISSN: 1390-4299
1390-3691

No. 20

URVIO

Revista Latinoamericana de Estudios de Seguridad



Ciberseguridad

Red Latinoamericana de Análisis de Seguridad y Delincuencia Organizada (RELASEDOR)
FLACSO Sede Ecuador • Junio 2017

URVIO

Revista Latinoamericana de Estudios de Seguridad

Red Latinoamericana de Análisis de Seguridad y Delincuencia Organizada (RELASEDOR)
y FLACSO Sede Ecuador
ISSN 1390-4299 (en línea) y 1390-3691 - Junio 2017 - No. 20

URVIO está incluida en los siguientes índices, bases de datos y catálogos:

- Emerging Sources Citation Index (ESCI). Índice del Master Journal List de Thomson Reuters.
- ERIH PLUS, European Reference Index for the Humanities and the Social Sciences. Índice de referencias.
- JournalTOCS. Base de datos.
- Directory of Research Journals Indexing (DRJI). Directorio.
- Actualidad Iberoamericana. Índice internacional de revistas.
- CLASE, Citas Latinoamericanas en Ciencias Sociales y Humanidades. Base de datos bibliográfica.
- Directorio LATINDEX, Sistema Regional de Información en Línea para Revistas Científicas de América Latina, el Caribe, España y Portugal.
- DIALNET, Universidad de La Rioja. Plataforma de recursos y servicios documentales.
- EBSCO. Base de datos de investigación.
- FLACSO-ANDES, Centro digital de vanguardia para la investigación en ciencias sociales - Región Andina y América Latina - FLACSO, Ecuador. Plataforma y repositorio.
- REDIB, Red Iberoamericana de Innovación y Conocimiento Científico. Plataforma.
- MIAR (Matriz de Información para el Análisis de Revistas). Base de datos.
- LatAm Studies. Estudios Latinoamericanos. Base de datos.
- Google académico. Buscador especializado en documentación académica y científica.

FLACSO ECUADOR

RELASEDOR
Red Latinoamericana de Análisis de Seguridad y Delincuencia Organizada

URVIO, **Revista Latinoamericana de Estudios de Seguridad**
Número 19, diciembre de 2016
Quito - Ecuador

ISSN 1390-4299 (en línea) y 1390-3691

URVIO, Revista Latinoamericana de Estudios de Seguridad, es una publicación electrónica semestral de FLACSO, sede Ecuador, fundada en el año 2007. La revista constituye un espacio para la reflexión crítica, el debate, la actualización de conocimientos, la investigación y la consulta sobre temas vinculados con la seguridad, el delito organizado, la inteligencia y las políticas públicas sobre seguridad en la región.

Disponible en:
http://revistas.flacsoandes.edu.ec/index.php/URVIO
http://www.flacsoandes.org/urvio/principal.php?idtipocontenido=13

El Comité Editorial de URVIO decidirá la publicación o no de los trabajos recibidos, sobre los cuales no se comprometerá a mantener correspondencia. Los artículos serán sometidos a la evaluación de expertos mediante el sistema de doble ciego. Las opiniones y comentarios expuestos en los trabajos son de responsabilidad estricta de sus autoras y autores, y no reflejan la línea de pensamiento de FLACSO, sede Ecuador. Los artículos publicados en URVIO son propiedad exclusiva de FLACSO, sede Ecuador. Se autoriza la reproducción total o parcial de los contenidos siempre que se cite como fuente a URVIO, Revista Latinoamericana de Estudios de Seguridad.

Envío de artículos
revistaurvio@flacso.org.ec

FLACSO, sede Ecuador
Casilla: 17-11-06362
Dirección: Calle Pradera E7-174 y Av. Diego de Almagro. Quito, Ecuador
www.flacso.edu.ec
Telf.: (593-2) 294 6800 Fax: (593-2) 294 6803

URVIO

Revista Latinoamericana de Estudios de Seguridad

Red Latinoamericana de Análisis de Seguridad y Delincuencia Organizada (RELASEDOR)
y FLACSO Sede Ecuador
ISSN 1390-4299 (en línea) y 1390-3691 - Junio 2017 - No. 20

Tema central

Ciberseguridad. Presentación del dossier. 8-15
Carolina Sancho Hirare

La política brasileña de ciberseguridad como estrategia
de liderazgo regional. 16-30
Luisa Cruz Lobato

Ciberdefensa y ciberseguridad, más allá del mundo virtual:
modelo ecuatoriano de gobernanza en ciberdefensa 31-45
Robert Vargas Borbúa, Luis Recalde Herrera, Rolando P. Reyes Ch.

La ciberdefensa y su regulación legal en Argentina (2006 - 2015). 46-62
Silvina Cornaglia y Ariel Vercelli

Actividades rutinarias y cibervictimización en Venezuela 63-79
Juan Antonio Rodríguez, Jesús Oduber y Endira Mora

Internet, la nueva era del delito: ciberdelito, ciberterrorismo,
legislación y ciberseguridad. 80-93
Vicente Pons Gamón

La nueva era de la información como poder y el campo
de la ciberinteligencia. 94-109
Camila Gomes de Assis

Misceláneo

La vinculación entre geopolítica y seguridad: algunas apreciaciones conceptuales y teóricas 111-125
Lester Cabrera Toledo

La construcción de confianza Estado-policías-comunidad, un problema de diseño institucional 126-144
Basilio Verduzco Chávez

Evaluación de las instituciones del sistema de justicia penal de la República de Panamá desde un enfoque de seguridad ciudadana (2004-2014) 145-165
Roberto Rodríguez-Rodríguez

Entrevista

Regionalismo de seguridad, la dinámica de la amenaza y el uso de la fuerza armada en América Latina
Entrevista a Jorge Battaglino 167-173
Marco Vinicio Méndez-Coto

Reseñas

Inteligencia estratégica contemporánea: perspectivas desde la región suramericana 175-177
Jyefferson Figueroa

Política editorial. 179-185

URVIO

Revista Latinoamericana de Estudios de Seguridad

Red Latinoamericana de Análisis de Seguridad y Delincuencia Organizada (RELASEDOR)
y FLACSO Sede Ecuador
ISSN 1390-4299 (en línea) y 1390-3691 - Junio 2017 - No. 20

Central topic

Cybersecurity. Introduction to Dossier 8-15
Carolina Sancho Hirare

The brazilian cybersecurity policy as a strategy
of regional leadership 16-30
Luisa Cruz Lobato

Cyber-defense and cybersecurity, beyond the virtual world: Ecuadorian model of
cyber-defense governance 31-45
Robert Vargas Borbúa, Luis Recalde Herrera, Rolando P. Reyes Ch.

The ciberdefense and its legal regulation in Argentina (2006 - 2015) 46-62
Silvina Cornaglia y Ariel Vercelli

Routine activities and cyber-victimization in Venezuela 63-79
Juan Antonio Rodríguez, Jesús Oduber y Endira Mora

Internet, the new age of crime: cibercrime, ciberterrorism,
legislation and cibersecurity 80-93
Vicente Pons Gamón

The new era of information as power and the field
of Cyber Intelligence 94-109
Camila Gomes de Assis

Miscellaneous

The link between geopolitics and security: a conceptual and theoretical assessment 111-125
Lester Cabrera Toledo

Constructing Trust on State-Police-Community relationships, a problem of Institutional Design 126-144
Basilio Verduzco Chávez

Evaluation of the Institutions of the Criminal Justice System of the Republic of Panama from the perspective of Citizen Security (2004-2014) 145-165
Roberto Rodríguez-Rodríguez

Interview

Regionalism of security, the dynamics of the threat and the use of armed force in Latin America
Interview to Jorge Battaglino 167-173
Marco Vinicio Méndez-Coto

Books reviews

Inteligencia estratégica contemporánea: perspectivas desde la región suramericana 175-177
Jyefferson Figueroa

Política editorial. 179-185

DOI: http://dx.doi.org/10.17141/urvio.20.2017.2601

Urvio, Revista Latinoamericana de Estudios de Seguridad, No. 20, Quito, junio 2017, pp. 46-62
RELASEDOR y FLACSO Sede Ecuador • ISSN 1390-4299 (en línea) y 1390-3691

La ciberdefensa y su regulación legal en Argentina (2006-2015)

The ciberdefense and its legal regulation in Argentina (2006-2015)[1]

Silvina Cornaglia[2] y Ariel Vercelli[3]

Fecha de recepción: 20 de febrero de 2017
Fecha de aceptación: 30 de abril de 2017

Resumen

En el artículo se analiza qué lugar ocupa y cómo se desarrolló la ciberdefensa dentro del sistema de defensa de la República Argentina. Para ello, se relevan y analizan las normas que se han producido sobre la temática durante el período 2006 – 2015. El estudio permite observar que dos instituciones han sido las más activas: por un lado, se destacan las regulaciones del Ministerio de Defensa y, por el otro, las regulaciones de la Jefatura de Gabinete de Ministros. La investigación tiene una doble finalidad. En primer lugar, favorecer un mayor nivel de sistematicidad legislativa en materia de ciberdefensa. En segundo lugar, producir información sustantiva para la elaboración de políticas públicas y actividades regionales de colaboración. El artículo es parte de una investigación mayor abocada al análisis de las diferentes formas de regular el ciberespacio.

Palabras clave: ciberdefensa; ciberespacio; leyes; República Argentina.

Abstract

The article analyzes the place and how cyberdefense was developed within the defense system of República Argentina. To this end, the norms that have been produced on the subject during 2006 - 2015 are relieved and analyzed. The study shows that two institutions have been the most active: on one hand, stand out the regulations of the Ministerio de Defensa, and, on the other, the regulations of the Jefatura de Gabinete de Ministros. The research has a double purpose. Firstly, to favor a greater level of legislative systemacy in cyberdefense. Second, to produce substantive information for the elaboration of public policies and regional collaboration activities. The article is part of a larger investigation focused on the analysis of the different ways of regulating cyberspace.

Keywords: ciberdefense; cyberspace; laws; Republic Argentina.

1 La obra intelectual se desarrolló gracias al apoyo de la Escuela del Cuerpo de Abogados del Estado (ECAE), el Consejo Nacional de Investigaciones Científicas y Técnicas (CONICET), el Instituto de Estudios Sociales de la Ciencia y la Tecnología (IESCT) de la Universidad Nacional de Quilmes (UNQ) y Bienes Comunes A. C.

2 Especialista en Asesoramiento Jurídico del Estado de la Escuela del Cuerpo de Abogados del Estado (ECAE), Abogada de la Universidad de Buenos Aires (UBA), Miembro del Observatorio de Defensa de la Universidad de la Defensa Nacional (UNDEF). Correo: silvina_cornaglia@hotmail.com

3 Doctor en Ciencias Sociales y Humanas de la Universidad Nacional de Quilmes (UNQ), Investigador de CONICET con lugar de trabajo en el Instituto de Estudios Sociales sobre la Ciencia y la Tecnología (IESCT) y Presidente de Bienes Comunes A. C. Correo: arielvercelli@arielvercelli.org

Introducción: nuevos enfoques sobre la ciberdefensa

La ciberdefensa ha adquirido gran relevancia mundial en las últimas décadas. Los ataques cibernéticos anónimos se han convertido en una fuente constante de amenazas, pues además de atacar las infraestructuras críticas de los países, afectan de forma directa y simultánea a millones de personas (Pastor Acosta *et. al*. 2009; Amaral 2014). El tema se ha transformado en un tema público a través de varios casos resonantes, entre otros, el ataque contra sitios *web* de Estonia en 2007 (diarios, bancos, ministerios), los ataques sufridos en 2010 por las centrifugadoras nucleares iraníes en Natanz mediante el *malware Stuxnet* (Gibney 2016), las filtraciones realizadas por *Wikileaks* (Assange, 2013), las filtraciones sobre ciberespionaje global que realizó Edward Snowden en 2013 (Poitras 2014) o el ataque realizado a través del *ransomware WannaCry* en 2017, que afectó más de 150 países (Rusia, EE.UU., Reino Unido, China, Italia, etc.). Ya es habitual que los medios de comunicación hablen y discutan sobre conceptos técnicos, tales como cibercrimen, ciberterrorismo, ciberespionaje, hacktivismo o ciberguerra (Adkins 2001; Gastaldi 2014).

La importancia de los ataques producidos, las consecuencias imprevisibles que pueden generar, la dificultad de identificar a los autores de los mismos y la carencia de definiciones legales precisas, han puesto a los diferentes gobiernos y a la comunidad internacional a trabajar tanto en sus jurisdicciones como en el ámbito regional y global. Rápidamente, la ciberdefensa comenzó a formar parte de un nuevo escenario de luchas, tensiones, intereses y negociaciones: entre otros, la protección de todo tipo de infraestructuras críticas (redes, recursos y servicios que -en caso de sufrir un ataque- podrían causar gran impacto en la seguridad de la población), el diseño de políticas públicas orientadas fortalecer la seguridad de la información, [4] la soberanía territorial y su particular relación con el ciberespacio (Eissa *et al*. 2014; Gastaldi 2014) o el normal y pacífico funcionamiento administrativo y jurídico-político de los Estados (Ferrero 2013; Illaro 2014).

La ciberdefensa no ha sido ni es materia simple. Se la puede caracterizar por su complejidad y cambio constante. Este es uno de los principales desafíos con que se enfrentan los Estados. Aún no existen convenciones o tratados internacionales que establezcan normas claras sobre la materia. Incluso, en el ciberespacio las tecnologías digitales y las regulaciones se van co-construyendo a través del tiempo y es posible observar que se diseñan tecnologías para producir los efectos de las regulaciones (Vercelli 2009; 2015). Por ello, las estrategias nacionales de defensa y la necesidad de generar nuevas capacidades comenzaron a ser considerados temas centrales y estratégicos dentro de los Ministerios de Defensa y otras agencias gubernamentales. Al respecto, en poco más de una década, es posible observar la aparición de todo tipo de iniciativas e instituciones a nivel mundial[5]: entre otras, el na-

4 En la actualidad, la mayor parte de la información que gestionan los organismos del Estado es procesada digitalmente. La seguridad de la información (o ciberseguridad) bien puede ser considerado un ítem complementario de la ciberdefensa de un país/región. Para Feliu Ortega (2012), la ciberdefensa comprende todas las acciones y medidas necesarias para garantizar la ciberseguridad de todos los sistemas tanto militares como civiles.

5 La Organización del Tratado del Atlántico Norte (OTAN) aprobó en 2008 su política de ciberdefensa. En 2011 realizó una revisión de dicha política y un Plan de Acción de Ciberdefensa. En la Cumbre de Gales, realizada en septiembre de 2014, reconoció la aplicabilidad al ciberespacio de la legislación internacional (incluyendo la legislación internacional humanitaria y la Carta de las Naciones Unidas). La Unión Europea (UE) adoptó una Estrategia de Seguridad Cibernética en febrero de 2013. Los estados miembros de

cimiento de comandos militares, autoridades nacionales/regionales, manuales y protocolos de acción (por ejemplo, el Manual de Tallin[6]) e, incluso, la aparición de grupos de emergencias cibernéticas tanto civiles como militares.[7]

La República Argentina y la Unión de Naciones Suramericanas (UNASUR) no se han mantenido ajenas a estas nuevas dinámicas de problemas. El Consejo de Defensa de la UNASUR ha considerado esta problemática en sus Planes de Acción 2012, 2013 y 2014.[8] A su vez, se incorporaron actividades específicas respecto de políticas, mecanismos y capacidades regionales para hacer frente a las amenazas cibernéticas e informáticas en el ámbito de la defensa. En el Plan de Acción 2015 se incorporó la temática como Grupo de Trabajo Extra Plan de Acción, cuyo objeto fue continuar con el Grupo de Trabajo de ciberdefensa y coordinar con el COSIPLAN[9] la realización de un seminario.[10] Incluso, el 13 de septiembre de 2013, los ministros de Defensa de Argentina y Brasil expresaron en el marco de un encuentro bilateral la importancia de trabajar en conjunto en la materia: incluyeron la ciberdefensa en la Declaración de Buenos Aires[11], acordaron la cooperación en defensa cibernética y la creación de un subgrupo de trabajo bilateral específico.

El sistema de defensa y la ciberdefensa en la República Argentina

En el contexto específico de la República Argentina, es posible identificar abundante normativa y múltiples acciones orientadas a mejorar las capacidades en ciberdefensa. Debido a su alta complejidad, la ciberdefensa no es fácilmente clasificable. Se encuentra aún en una etapa de expansión regulativa, de flexibilidad interpretativa y de amplio debate. Por ejemplo, entre otros puntos salientes, aún no está del todo claro qué significa la ciberdefensa y qué relaciones mantiene con el sistema de defensa nacional (Libro Blanco 2015). En igual sentido, es importante avanzar sobre los siguientes cuestionamientos: ¿Qué actividades representan un ciberataque a nivel nacional, regional o internacional?[12], ¿Cuáles son las instituciones públicas y las autoridades competentes para su gestión? y ¿Cuenta la República Argentina con una legislación sistemática en materia de ciberdefensa? Por ello, en este

la Organización de Estados Americanos (OEA) adoptaron por unanimidad la Estrategia Interamericana Integral de Seguridad Cibernética y aprobaron una declaración sobre Fortalecimiento de la Seguridad Cibernética (OEA 2014).

6 El Manual Tallin, es un documento no oficial, abocado a describir como pueden aplicarse reglas del derecho internacional a la guerra cibernética. Fue elaborado en el Centro de Excelencia para la Cooperación en Ciberdefensa de la OTAN. Define el ciberespacio como el entorno formado por componentes físicos y no físicos, caracterizados por el uso de computadoras y el espectro electromagnético para almacenar, modificar e intercambiar datos a través de redes informáticas (Schmitt 2013).

7 Por ejemplo, el Grupo de Respuesta a Emergencias Cibernéticas de Colombia –colCERT- y la Dirección de Ciencia, Tecnología e Innovación –Ctel (Gallardo 2014).

8 Dentro del contexto de integración política, económica, social y cultural materializada en la UNASUR, se ha constituido el Consejo de Defensa Suramericano (CDS), organismo para favorecer el diálogo y la cooperación política en temas de defensa.

9 Consejo Suramericano de Infraestructura y Planeamiento de UNASUR.

10 Plan de Acción 2015 del Consejo Defensa Suramericano.

11 Convenio N° 62 del Ministerio de Defensa, Declaración de Buenos Aires de los Ministros de Defensa del Brasil y Argentina, Buenos Aires, 13 de septiembre de 2013.

12 Sobre el uso de la fuerza el Manual Tallin considera que los artículos 2 y 51 de la Carta de las Naciones Unidas, relativos a la prohibición del uso de la fuerza y la legítima defensa, respectivamente, resultan aplicables en materia cibernética: ver reglas 10 y 11 (uso de la fuerza y evaluación). No son criterios legales formales.

apartado se ofrece un marco interpretativo y sistémico sobre qué relación existe entre el sistema de defensa y las incipientes regulaciones sobre ciberdefensa.

El concepto de ciberdefensa en la República Argentina debe interpretarse dentro de la tradición institucional amplia de su sistema de defensa en caso de agresiones. Existe una profunda articulación entre los conceptos centrales de la defensa en agresiones tradicionales y las posibles interpretaciones que puedan hacerse sobre el concepto de ciberdefensa como un ámbito específico de protección a cargo del Estado. La concepción argentina en materia de defensa, en general, se funda en el reconocimiento de la importancia que detenta la cooperación interestatal y la dimensión multilateral de la defensa y seguridad como instrumentos complementarios de la política de defensa propia. El sistema de defensa argentino tiene a su cargo la protección del Estado en relación a aquellos ataques que puedan afectar su soberanía, su independencia e integridad territorial. El sistema exige, por lo tanto, que la agresión pueda afectar alguno de estos elementos y que tenga origen externo. La reglamentación, además, requiere que el agresor sea un actor estatal.

La Ley de Defensa Nacional N° 23.554 (B.O. 5/05/1988) "establece las bases jurídicas, orgánicas y funcionales para la preparación, ejecución y control de la defensa nacional". La ley define la defensa nacional como la integración y la acción coordinada de todas las fuerzas de la Nación para la solución de aquellos conflictos que requieren el empleo de las Fuerzas Armadas, en forma disuasiva o efectiva, para enfrentar las agresiones de origen externo (Art. 2). Según el artículo nueve, "el sistema de defensa está integrado por el Presidente de la Nación; el Consejo de Defensa Nacional; el Congreso de la Nación; el Ministro de Defensa; el Estado Mayor Conjunto de las Fuerzas Armadas; el Ejército, la Armada y la Fuerza Aérea de la República Argentina; Gendarmería Nacional y Prefectura Naval Argentina; y el Pueblo de la Nación mediante su participación activa en los términos de la ley". El sistema de defensa está orientado a determinar la política de defensa nacional más adecuada a las necesidades del país (y su actualización). Dicha política debe surgir de la acción coordinada de los distintos miembros del sistema. La dirección de la defensa nacional y la conducción de las Fuerzas Armadas es competencia del Presidente de la Nación en su carácter de Jefe Supremo de la misma y Comandante en Jefe de las Fuerzas Armadas (Art. 10).

La reglamentación a la ley realizada mediante Decreto N° 727/2006 (B.O. 13/06/2006), establece en su artículo primero los requisitos para el empleo de las Fuerzas Armadas, los cuales consisten en la existencia de agresiones de origen externo perpetradas por fuerzas armadas pertenecientes a otro/s Estado/s. Asimismo, define la agresión de origen externo como "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". Uno de los puntos que queda expresamente establecido en la reglamentación es que el sistema de defensa argentino no podrá contemplar situaciones pertenecientes al ámbito de la seguridad interior, conforme la delimitación establecida en la Ley de Seguridad Interior N° 24.059 (B.O. 17/01/1992).[13]

13 Tanto la Ley N° 23.554 como la Ley N° 24.059 establecen una clara distinción jurisdiccional, orgánica y funcional entre la Defensa Nacional y la Seguridad Interior (diferencia

La Ley N° 24.948 (B.O. 8/04/1998) establece las bases políticas, orgánicas y funcionales fundamentales para la reestructuración de las Fuerzas Armadas, estableciendo en su artículo segundo que la política de defensa se sustenta en lograr consolidar e incrementar las capacidades espirituales y materiales que tornen eficaz una estrategia disuasiva, coadyuvando al mantenimiento de la paz y la seguridad internacionales. La Directiva de Política de Defensa Nacional, materializada en el Decreto N° 1714/ 2009 (B.O. 12/11/2009) y en su actualización conforme el Decreto N° 2645/2014 (B.O. 19/01/2015), inicia el planeamiento para la defensa nacional. De estos documentos derivan los principales lineamientos de la política de defensa y de la política militar de la República Argentina.

En este sentido, como pauta ordenadora del sistema,y como guía orientadora en materia de ciberdefensa, la Directiva destaca que el criterio esencial y ordenador sobre el cual se estructura nuestro sistema de defensa es el concepto de "legítima defensa", rechazando las políticas estratégicas de agresión en tanto se encuentran por fuera del marco jurídico internacional vigente. Al respecto establece que:

> La República Argentina sostiene una identidad estratégica de carácter 'defensivo', de rechazo y oposición a políticas, actitudes y capacidades ofensivas de proyección de poder hacia terceros Estados. Por lo tanto, la concepción y la disposición estratégica, la política de defensa y su consecuente política militar, así como el diseño de fuerzas y previsión de empleo y evolución del Instrumento Militar, se encuentran estructuradas según el principio de legítima defensa ante agresiones militares de terceros Estados (Decreto N° 2645/2014, Capítulo II, Política de Defensa Nacional).

En 2014, la actualización de la Directiva de Política de Defensa Nacional contempló de manera expresa la importancia del ciberespacio para el desarrollo de las operaciones militares y planteó la necesidad de adaptar los sistemas de defensa a estos nuevos componentes. La Directiva destaca que solo una parte de la amplia gama de operaciones cibernéticas, afectan el ámbito de la Defensa Nacional. Además, estableció que resulta sencillo desde el punto de vista fáctico determinar *a priori* y *ab initio* si la afectación se trata de una agresión militar estatal externa. Por tanto, es complejo determinar si una situación resulta competencia o no del sistema de defensa nacional. La inclusión de la ciberdefensa en la Directiva demuestra que las nuevas tecnologías de la información y las comunicaciones han adquirido un protagonismo estratégico en la defensa de la soberanía nacional.

El relevamiento normativo y su marco teórico-metodológico

En este apartado el trabajo de investigación se aboca al estudio exploratorio y al relevamiento de la normativa sobre ciberdefensa que se desarrolló en la República Argentina durante el período 2006 – julio de 2015. [14] Por un lado,

de naturaleza). La Ley N° 24.059 establece las bases jurídicas, orgánicas y funcionales del sistema de planificación, coordinación, control y apoyo del esfuerzo nacional de policía tendiente a garantizar la seguridad interior. Se define como seguridad interior a la situación de hecho basada en el derecho en la cual se encuentran resguardadas la libertad, la vida y el patrimonio de los habitantes, sus derechos y garantías y la plena vigencia de las instituciones del sistema representativo, republicano y federal que establece la Constitución Nacional.

14 El relevamiento realizado no alcanza las normativas posteriores al 10 de diciembre de 2015 (momento en el que se produce un cambio de gobierno en la República Argentina).

[1] se relevan las normativas sobre ciberdefensa que se han generado en la República Argentina durante el período 2006 – julio de 2015 y las actividades vinculadas. Por el otro, [2] se describen las normativas y el uso concreto del concepto de ciberdefensa que se presenta en las mismas. El relevamiento y descripción de las regulaciones comprendió tanto la normativa específica en materia de ciberdefensa como aquella vinculada a otros aspectos de la regulación del ciberespacio. Es decir, aquella que también resulta aplicable al objeto de estudio: por ejemplo, la normativa sobre seguridad de la información o la normativa sobre la regulación de Internet).

A continuación, se presenta el relevamiento de la normativa sobre ciberdefensa ordenada por organismos competentes. Del análisis realizado en el período, se destacan principalmente dos instituciones que han trabajado en la materia. Por un lado, [4] se describen las regulaciones públicas del Ministerio de Defensa: este Ministerio fortaleció sus políticas en ciberdefensa desde el año 2006 a partir de la constitución de su Comité de Seguridad de la Información. Por el otro, [5] se describe la normativa que vincula la ciberdefensa con las actividades de la Jefatura de Gabinete de Ministros (JGM): la Jefatura aportó abundante normativa vinculada al tratamiento seguro de la información. En la parte final, [6] se relevan otras normativas sobre la regulación de Internet que, por diferentes razones, también resultan relevantes en materia de ciberdefensa. En los siguientes apartados, con el objeto de facilitar la lectura, la normativa se presenta en orden cronológico.

Las normas vinculadas al Ministerio de Defensa

[a] Comité de Seguridad de la Información

Por Resolución del Ministerio de Defensa N° 364, del 12 de abril de 2006, se creó el Comité de Seguridad de la Información del Ministerio de Defensa.[15] El mismo se integró, entre otras, por las áreas con competencia en materia de política, planes y programas, presupuesto, tecnología, asuntos jurídicos, recursos humanos, administración y despacho (Art. 2). La coordinación del comité fue puesta a cargo del Subsecretario de Coordinación, de quien dependían las áreas de apoyo, conforme lo requerido en el artículo tercero de la Decisión Administrativa N° 669/2004. Este fue el primer antecedente normativo dentro del Ministerio de Defensa referido a uno de los aspectos de la ciberdefensa. Si bien solo se refiere a la seguridad de la información, puede considerarse el puntapié inicial. La norma ordena coadyuvar -desde las funciones propias del Ministerio- en el proceso de protección de infraestructuras críticas (proceso coordinado desde la Jefatura de Gabinete de Ministros).

[b] El ciberespacio para el sistema de defensa nacional

En el año 2010, la Secretaría de Estrategia y Asuntos Militares del Ministerio de Defensa constituyó un grupo de trabajo a los efectos de analizar, desde el punto de vista técnico y normativo, las implicancias del ciberespa-

15 La norma dio cumplimiento a lo establecido en la decisión administrativa N° 669/2004 (B.O. 22/12/2004) para los organismos del Sector Público Nacional comprendidos en los incisos a) y c) del artículo 8° de la Ley N° 24.156 (B.O. 29/10/1992).

cio para el sistema de defensa nacional. [16] La necesidad de contar con un análisis sobre la temática surgió de la permanente expansión de las redes informáticas en el mundo. El estudio comprendía los aspectos estratégicos, doctrinarios y normativos, vinculados con la normativa establecida en materia de defensa nacional. La constitución de un grupo de trabajo específico (conformado por miembros del Ministerio de Defensa, del Estado Mayor Conjunto y de las Fuerzas Armadas) representa uno de los primeros antecedentes sobre la necesidad de un trabajo coordinado en la materia de defensa. Sin embargo, aún no es posible encontrar un concepto *stricto sensu* sobre ciberdefensa. El concepto primario que se buscaba explorar desde todos los aspectos posibles era el ciberespacio, como un nuevo espacio de interés para la actuación de los organismos vinculados a la defensa.

[c] Unidad de Coordinación de Ciberdefensa

La resolución del Ministerio de Defensa N° 385, del 22 de octubre de 2013, creó la Unidad de Coordinación de Ciberdefensa en el ámbito de la Jefatura de Gabinete del Ministerio de Defensa. Su función específica consistió en coordinar las políticas y el desempeño de los actores vinculados a la ciberdefensa en la jurisdicción. El principal fundamento para la creación del área fue la existencia en las Fuerzas Armadas de un proceso de generación de capacidades y unidades especializadas para emergencias tele-informáticas. La constitución de la Unidad de Coordinación se enmarca en un concepto de ciberdefensa asociado a la protección del ciberespacio.

Se establece que la ciberdefensa requiere de la participación de todos los miembros del sistema de la defensa e innovación tecnológica del país. Entre sus funciones se destacan: a) realizar un relevamiento exhaustivo de infraestructuras, redes, recursos humanos, procesos y actividades relativas a ciberdefensa; b) entender en el diseño, planificación estratégica e implementación de políticas; c) impulsar el desarrollo doctrinario; d) analizar la evolución normativa; e) intervenir en la implementación de la Resolución de la Jefatura de Gabinete de Ministros N° 580/2011 (B.O. 2/08/2011). Una tarea especialmente asignada a esta Unidad fue la de elaborar una propuesta de estructura orgánica que asuma las competencias relativas al desarrollo e implementación de las políticas de ciberdefensa en la jurisdicción del Ministerio de Defensa. El proyecto se vio materializado mediante el dictado de la Resolución del Ministerio de Defensa N° 343 del 14 de mayo de 2014, que dispuso la creación de un Comando Conjunto de Ciberdefensa y la Decisión Administrativa N° 15/2015 (B.O. 11/03/2015) que estableció la incorporación de la Dirección General de Ciberdefensa. La estructura orgánica desarrollada tiende a favorecer la coordinación entre organismos y áreas con capacidad en la materia. Se vincula a un concepto de ciberdefensa integrado por múltiples facetas que comprenden desde el planeamiento, la doctrina, el aspecto normativo y la seguridad de la información hasta los aspectos operacionales militares específicos.

[d] Comando Conjunto de Ciberdefensa

La Resolución del Ministerio de Defensa N° 343, del 14 de mayo de 2014, dispuso la creación de un Comando Conjunto de Ciberdefensa dependiente orgánica, funcional y ope-

16 Resolución de la Secretaría de Estrategia y Asuntos Militares del Ministerio de Defensa N° 8 de fecha 14 de abril de 2010, artículo primero.

racionalmente del Estado Mayor Conjunto de las Fuerzas Armadas (Artículo primero de la Resolución MD N° 343/2014 del 14 de mayo de 2014). Su competencia específica es ejercer la conducción de las operaciones de ciberdefensa en forma permanente a los efectos de garantizar las operaciones militares del Instrumento Militar de la Defensa Nacional. [17] El Decreto N° 727/2006 (B.O. 13/06/2006) ha establecido que las operaciones militares son conducidas por el Estado Mayor Conjunto de las Fuerzas Armadas a través del Comando Operacional. Es por eso que la conducción de las operaciones en materia de ciberdefensa debe quedar a cargo de un órgano que se encuentre contenido en la estructura del Estado Mayor Conjunto y que mantenga vínculos permanentes de coordinación con las Fuerzas Armadas. La principal capacidad que debe desarrollar este nuevo comando es la de conjurar y repeler ciberataques contra infraestructuras críticas de la información y activos del Sistema de Defensa Nacional y de su Instrumento Militar.

Para definir su marco de actuación, se debe tener en cuenta que la misión principal del Instrumento Militar es conjurar y repeler toda agresión militar estatal externa contra los intereses vitales y estratégicos de la República Argentina. El país ha adoptado un modelo de defensa de carácter defensivo[18] que deberá guiar la generación de capacidades en la temática. La conducción del Comando se encuentra a cargo de un oficial superior en actividad del Ejército argentino que cuente con capacitación para la planificación y conducción de operaciones de ciberdefensa.

La conformación de este órgano específico dentro del Estado Mayor Conjunto responde a un concepto de ciberdefensa vinculado al ciberespacio no como un ámbito militar operacional específico, sino como una dimensión transversal a los ambientes operacionales tradicionales, por lo que se requiere un planeamiento militar conjunto, y una intervención también conjunta e integrada del Instrumento Militar. Queda también definida la principal función en materia de ciberdefensa, que es la conjurar y repeler ciberataques, función que en el caso específico del Instrumento Militar quedará limitada a aquellos que recaigan sobre infraestructuras críticas de la información y activos del Sistema de Defensa Nacional y de su Instrumento Militar. La norma aborda la ciberdefensa desde el punto de vista preventivo y defensivo, en concordancia con las políticas generales.

[e] Actualización de la Directiva de Política de Defensa Nacional

Mediante el Decreto N° 2645/2014 se aprobó una actualización contenida en el Decreto N° 1714/2009 (B.O. 12/11/2009). El documento reafirma los principios fundamentales del sistema de defensa y, en su Capítulo I, expresa:

> 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 di-

17 Este diseño institucional es acorde a lo establecido en el artículo quinto de la Ley N° 24.948 de Reestructuración de las Fuerzas Armadas, que establece que "tanto en las previsiones estratégicas como en la organización, el equipamiento, la doctrina y el adiestramiento, se dará prioridad al accionar conjunto y a la integración operativa de las fuerzas, así como con las fuerzas de seguridad en sus funciones de apoyo y con fuerzas del ámbito regional y las de los países que integren contingentes de paz por mandato de las Naciones Unidas".

18 Decreto PEN N° 1714 del 12 de noviembre de 2009 "Directiva de Política de Defensa Nacional", actualizada por Decreto PEN N° 2645 del 30 de diciembre de 2014.

> námica 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 el ciberespacial.

Se destaca que, si bien los ciberataques se originan en el mundo virtual conformado por redes de comunicación y sistemas informáticos, sus consecuencias impactan en el mundo físico y pueden afectar las más diversas infraestructuras críticas: agua potable, medios de comunicación o sistemas bancarios. La Directiva destaca las dificultades fácticas para determinar *a priori* y *ab initio* si la afectación califica como una agresión militar estatal externa objeto del sistema de defensa nacional. También plantea la necesidad de desarrollar capacidades operacionales en la dimensión ciberespacial tendientes a adquirir competencias en los ambientes terrestres, naval y aéreo; así como el de incrementar la ciberseguridad de redes pertenecientes al sistema de defensa nacional y de los objetivos de valor estratégico.

La Directiva contiene un aporte fundamental para el análisis, pues incorpora una definición de ciberdefensa en el marco del sistema de defensa nacional. Al respecto, en el Capítulo III, Apartado A.II, Punto 9, establece que "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". Esta definición se destaca por brindar el marco de actuación en la materia, no solo para el planeamiento y actividades futuras, sino que le da contenido a un conjunto de normas de diferente rango, previamente analizadas, que requerían de un concepto preciso para las funciones encomendadas. Este concepto se encuentra contenido en un decreto: es decir, tiene un rango normativo superior al resto de las regulaciones analizadas y sus criterios son obligatorios para todas aquellas normativas internas del Ministerio de Defensa.

[f] Dirección General de Ciberdefensa

El 4 de marzo de 2015 se aprobó la Decisión Administrativa N° 15/2015, por medio de la cual se crea dentro del Ministerio de Defensa la Dirección General de Ciberdefensa, dependiendo directamente de la Unidad Ministro. Esta nueva norma brinda una respuesta orgánica institucional a la necesidad de contar con un área responsable de la planificación, elaboración, supervisión y evaluación de políticas en materia de ciberdefensa para el Ministerio de Defensa y su Instrumento Militar dependiente. Tiene su fundamento en la tarea permanente de resguardar las redes, sistemas informáticos y activos.

La principal competencia de la Dirección General de Ciberdefensa consiste en intervenir en el planeamiento, formulación, dirección, supervisión y evaluación de las políticas específicas dentro del Ministerio de Defensa. Entre sus funciones destacan la coordinación con organismos y autoridades de los distintos poderes del Estado, la intervención en la orientación de las acciones de ciberdefensa ejecutadas por el Nivel Estratégico Militar, el control funcional sobre el Comando Conjunto de Ciberdefensa, la intervención en el diseño de políticas, normas y procedimientos de seguridad de la información y el fomento de políticas de formación de recursos humanos.

[g] Política de Seguridad

Por medio de la Resolución MD N° 781/2015 del 24 de julio de 2015 se aprobó la Política de Seguridad de implementación en la jurisdicción Ministerio de Defensa y organismos descentralizados en su órbita. Esta medida incorpora una 'Política de Seguridad de la Información' común e integrada que contempla las características propias de cada área u organismo. Tiene por objeto garantizar la continuidad de los sistemas de información, minimizar los riesgos de daño y asegurar el eficiente cumplimiento de los objetivos de la jurisdicción. La Resolución también crea un Comité de Seguimiento de Seguridad de la Información integrado por las áreas con competencia en la materia y que tiene por función realizar el seguimiento de la implementación y avances de la Política tanto en el Ministerio como en sus organismos.

Las normas vinculadas a la Jefatura de Gabinete de Ministros (JGM)

[a] Comités de Seguridad de la Información

La Decisión Administrativa N° 669/2004 de la JGM tuvo por objeto elevar los niveles de seguridad de los sistemas de información de los organismos públicos. La competencia recayó en la Subsecretaría de la Gestión Pública, pues se buscaba definir las estrategias vinculadas a tecnologías de la información, comunicaciones asociadas y sistemas electrónicos de tratamiento de la información dentro de la Administración Pública Nacional. Se estableció que los organismos del Sector Público Nacional debían adecuar su política de seguridad a la Política de Seguridad Modelo que sería aprobada por el Subsecretario de la Gestión Pública. El artículo 2° de la norma creó el Comité de Seguridad de la Información y obligó a cada organismo a conformar su propio Comité.

[b] Política de seguridad de la información modelo

La Oficina Nacional de Tecnologías de la Información aprobó mediante Disposición N° 1/2015 (B.O. 25/02/2015) la "Política de Seguridad de la Información Modelo" (que a su vez, reemplazó la que fuera aprobada por Disposición N° 3/2013). Este documento constituyó la base para la elaboración de las políticas específicas de cada uno de los organismos del Sector Público Nacional. Puede considerarse un compendio de buenas prácticas en materia de seguridad de la información. La JGM tenía a su cargo el establecimiento de las políticas de seguridad para la protección de los sistemas de información de la Administración Pública Nacional. Dentro de ese marco la Oficina Nacional de Tecnologías de la Información, organismo dependiente, tenía bajo su responsabilidad la formulación de políticas relativas a la seguridad de la información digitalizada y electrónica del Sector Público Nacional. El Decreto del Poder Ejecutivo Nacional N° 1067 del 10 de junio de 2015 modificó la estructura de la JGM y asignó la facultad de aprobar la Política de Seguridad Modelo a la Subsecretaría de Protección de Infraestructuras Críticas de Información y Ciberseguridad. Las políticas de seguridad de la información conforman procesos clave en materia de ciberdefensa.

[c] Programa Nacional de Infraestructuras Críticas de Información y Ciberseguridad

La JGM, por medio de la Resolución N° 580 del 28 de julio de 2011, creó, en el ámbito de la Oficina Nacional de Tecnologías de la Información el Programa Nacional de Infraestructuras Críticas de Información y Ciberseguridad. El principal fundamento para el establecimiento de esta política es la consideración de las infraestructuras digitales como infraestructuras críticas, imprescindibles para el funcionamiento de los sistemas de información y comunicaciones. En el artículo segundo se establece que:

> La elaboración de 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 24.156 y sus modificatorios, los organismos interjurisdiccionales, y las organizaciones civiles y del sector privado que así lo requieran, así como el fomento de 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 (Resolución N° 580 del 28 de julio de 2011).

La implementación de las políticas de seguridad se menciona de manera expresa en la normativa dictada por el Ministerio de Defensa, en especial la Resolución N° 385/2013, que manda a la Unidad de Coordinación de Ciberdefensa a intervenir en la implementación de la Resolución de la Jefatura de Gabinete de Ministros N° 580/2011.

[d] Aprobación de Estándares Tecnológicos

Por medio de la disposición de la Oficina Nacional de Tecnologías de la Información N° 3/2014 (B.O. 8/10/2014) se aprobaron los Estándares Tecnológicos para la Administración Pública Nacional Versión 2.0. Los mismos sustituyen los aprobados por la Disposición N° 1 del 24 de julio de 2013 y la Disposición N° 1 del 7 de julio de 2014 del mismo organismo. Los estándares son de aplicación en el Ministerio de Defensa y los organismos descentralizados en su órbita (la normativa comprende a toda la Administración Pública Nacional, centralizada y descentralizada, empresas de propiedad del Estado o en las que éste tenga mayoría accionaria, bancos oficiales y Fuerzas Armadas y de Seguridad, resultando exceptuados los organismos del sistema científico nacional).[19] La normativa fija estándares mínimos para compras y contrataciones de tecnologías de información y comunicaciones.[20] Desde el punto de vista de la ciberdefensa, la fijación de estándares mínimos de seguridad a toda la administración resulta una medida preventiva fundamental.

[e] Grupo de Trabajo ICIC – CERT (Computer Emergency Response Team)

En el marco de los objetivos establecidos en el Programa Nacional de Infraestructuras

19 Dentro del Ministerio de Defensa queda excluido de su aplicación obligatoria el Instituto de Investigaciones Científicas y Técnicas para la Defensa (CITEDEF) por integrar el Sistema Nacional de Ciencia, Tecnología e Innovación creado por la Ley N° 25.467.

20 Es así que todo organismo durante la tramitación de un expediente para la adquisición o arrendamiento de bienes y servicios de carácter informático debe remitir en forma previa toda la información relativa a sus proyectos a la Dirección Nacional de Estandarización y Asistencia Técnica de Jefatura de Gabinete, que produce su dictamen técnico al respecto: Art. 5 del Decreto N° 856/98 (B.O. 22/07/98).

Críticas de Información y Ciberseguridad, se dictó la Disposición de la Oficina Nacional de Tecnologías de la Información N° 2/2013 (B.O. 3/09/2013), que creó una serie de grupos de trabajo a fin de desarrollar proyectos y propuestas que promuevan la protección de infraestructuras críticas de información y ciberseguridad. Entre ellos, se encuentra el grupo de trabajo "ICIC – CERT" que administra y asesora sobre incidentes de seguridad a los organismos del Sector Público Nacional que hubieren adherido al Programa. La existencia de esta instancia de coordinación resulta necesaria para una política conjunta en materia de seguridad de la información. La norma también crea un Grupo de Acción Preventiva (ICIC – GAP), uno de Infraestructuras Críticas de Información (ICIC – GICI) y uno de Internet Sano (ICIC – INTERNET SANO).

[f] Subsecretaría de Protección de Infraestructuras Críticas de Información y Ciberseguridad

El Decreto N° 1067/2015 (B.O. 12/06/2015) modifica la estructura orgánica de la JGM mediante la creación de la Subsecretaría de Protección de Infraestructuras Críticas de Información y Ciberseguridad en el ámbito de la Secretaria de Gabinete. La misma, tiene como objetivo principal entender en la elaboración de la estrategia nacional de protección de infraestructuras críticas de información y ciberseguridad. La norma dispone la transferencia del "Programa Nacional de Infraestructuras Criticas de Información y Ciberseguridad", dependiente de la Oficina Nacional de Tecnologías de Información, a la órbita de la Dirección Nacional de Infraestructuras Críticas de Información y Ciberseguridad dependiente de la nueva Subsecretaría. El Subsecretario de Protección de Infraestructuras Críticas de Información y Ciberseguridad tendrá la facultad para aprobar la Política de Seguridad Modelo y dictar las normas aclaratorias y complementarias de la Decisión Administrativa N° 669/2004.

Otras normas vinculadas a la regulación de internet

[a] Comisión Argentina de Políticas de Internet

La Secretaría de Comunicaciones, con fundamento en la multiplicidad de áreas dentro del Sector Público Nacional con injerencia en temas vinculados a Internet, creó por Resolución N° 13/2014 (B.O. 23/04/2014) la Comisión Argentina de Políticas de Internet con el fin de articular la participación de los distintos actores en el diseño de una estrategia nacional sobre gobierno de Internet. Entre otras, la Resolución invitó a participar de la comisión a la Secretaría de Ciencia, Tecnología y Producción para la Defensa del Ministerio de Defensa. La medida se enmarcó en un escenario internacional lleno de expectativas ante la realización en Brasil de la Reunión Global de Múltiples Partes Interesadas sobre el Futuro de la Gobernanza de Internet – NETmundial (23 y 24 de abril de 2014 en San Pablo).

[b] Argentina Digital

La Ley N° 27.078 (B.O. 19/12/2014) declaró "de interés público el desarrollo de las tecnologías de la información y las comunicaciones, las telecomunicaciones, y sus recursos asociados", y estableció como finalidad de la misma garantizar el derecho humano a las comunicaciones y a las telecomunicaciones. La

ley creó su propia autoridad de aplicación, un organismo descentralizado y autárquico en el ámbito del Poder Ejecutivo Nacional, denominado Autoridad Federal de Tecnologías de la Información y las Comunicaciones (creados a su vez por el Decreto N° 677/2015, B.O. 29/04/2015). Esta normativa debe ser tenida en cuenta en materia de ciberdefensa puesto que se trata de una norma de orden público y que define, en el artículo 6, apartado b, los recursos asociados (es decir, infraestructuras físicas, los sistemas, los dispositivos, los servicios asociados con una red de telecomunicaciones o con un Servicio de Tecnologías de la Información y las Comunicaciones).

La ley no define el concepto de ciberespacio. Sin embargo, en su artículo 6 apartado g., se explica qué se entiende por tecnologías de información y comunicación: "conjunto de recursos, herramientas, equipos, programas informáticos, aplicaciones, redes y medios que permitan la compilación, procesamiento, almacenamiento y transmisión de información". En el artículo 62, inciso i, establece la obligación de atender los requerimientos en materia de defensa nacional y de seguridad pública formulados por las autoridades competentes.

Conclusiones: Hacia una mayor sistematización de la legislación en ciberdefensa

La ciberdefensa se ha transformado en un tema clave a nivel mundial. Desde hace varios años la red de redes puede ser considerada una fuente de amenazas para la defensa nacional/regional. Los avances científico-tecnológicos están cambiando -y adecuando- muchas de las tradicionales estrategias de defensa. El interés sobre ciberdefensa está expandiéndose rápidamente en Argentina y toda la región sur. En el período analizado es posible identificar que en Argentina se produjo un aumento significativo de la normativa específica. También se produjo un incremento de medidas de confianza mutua y cooperación tanto bilaterales como multilaterales en la región sur. Esto incluye el establecimiento de políticas comunes a través de órganos regionales: por ejemplo, el Consejo de Defensa Suramericano.

Específicamente, el estudio identifica que el concepto de ciberdefensa de la República Argentina, en el marco de la normativa que rige el sistema de defensa nacional, sigue un modelo de carácter defensivo y orientado al desarrollo de capacidades. Existe en la legislación Argentina una definición específica de ciberdefensa: la misma está contenida en la Actualización de la Directiva de Política de Defensa Nacional. El relevamiento también permite observar que, durante el período 2006 – julio 2015, se ha producido un aumento significativo en las regulaciones sobre la temática dentro del Estado Argentino. Éste se relaciona al crecimiento y desarrollo de nuevas amenazas provenientes del uso masivo de las tecnologías de información y comunicación. Como se ha resaltado durante el relevamiento, dicho crecimiento normativo no está exento de ambigüedades, interpretaciones y negociaciones: por ejemplo, qué significa el concepto de ciberdefensa, qué es y cómo se evalúa un ciberataque o, entre otros, qué criterios jurídico-políticos deben aplicarse.

La investigación también ha revisado cuáles fueron en el período las instituciones públicas argentinas competentes. Específicamente, la ciberdefensa ha sido regulada por el Ministerio de Defensa de la Nación a través de normativa de rango interno (resoluciones). También es posible destacar normativa del Poder Ejecutivo

Nacional (decretos). A esto se suman normativas vinculadas a seguridad de la información, infraestructuras críticas y regulaciones de Internet (por ejemplo, la Ley N° 27.078 de Argentina Digital). Sobre la temática también existen normas que otorgaron responsabilidades a la Jefatura de Gabinete de Ministros, y sus áreas dependientes, con el objeto de generar políticas comunes de aplicación a toda la Administración Pública Nacional.

Finalmente, la investigación permite concluir que el sistema legal argentino aún no dispone de una codificación general y sistemática sobre ciberdefensa. Una sistematización de los marcos jurídicos (y reglamentarios), así como una mayor definición de objetivos, competencias y funciones entre los diferentes organismos del Estado, podría ser de gran utilidad y ayudar a alcanzar múltiples objetivos estratégicos. Entre otros, [a] definir qué significa y cómo debe entenderse el concepto de ciberdefensa nacional / regional; [b] contribuir al diseño de tecnologías digitales orientadas a la defensa de los intereses nacionales / regionales; [c] favorecer procesos legislativos (del Congreso Nacional) que se orienten a regular tanto el sector público como las actividades críticas en manos del sector privado; [d] fortalecer la simetría y la correspondencia con las potenciales regulaciones regionales e internacionales sobre ciberdefensa; y [e] enriquecer los debates sobre ciberdefensa involucrando tanto actores de la política y las fuerzas armadas como de la academia, la sociedad civil y el sector privado nacional / regional.

Bibliografía

Adkins, Bonnie. 2001. "The spectrum of Cyberconflict. From hacking to information warfare. What is law enforcement´s role", http://handle.dtic.mil/100.2/ADA406949.

Amaral, Augusto César. 2014. "La amenaza cibernética para la seguridad y defensa de Brasil". *Revista Visión Conjunta* 10: 19-22. http://www.cefadigital.edu.ar/bitstream/123456789/32/3/VC%2010-2014%20AMARAL.pdf.

Assange, Julian. 2013. Criptopunks: La libertad y el futuro de Internet. Buenos Aires: Marea/Trilce.

Eissa, Sergio G, Gastaldi Sol; Iván Poczynok y Elina Zacarías Di Tullio. 2014. "El ciberespacio y sus implicancias para la defensa nacional. Aproximaciones al caso argentino". *Revista de Ciencias Sociales de la Universidad Nacional de Quilmes* 6 (25): 181–197. http://www.unq.edu.ar/catalogo/330-revista-de-ciencias-sociales-n-25.php.

Feliu Ortega, Luis. 2012. "La ciberseguridad y la ciberdefensa". España: Ministerio de Defensa de España.

Ferrero, Julio Alberto. 2013. "La Ciberguerra, génesis y evolución". *Revista General de Marina* 264: 81-97. http://publicaciones.defensa.gob.es/pprevistas/49e78d6b-fb63-65ab-9bdd-ff0000451707/index.html.

Gallardo, Sara. 2014. "Más allá de las TIC en Mindefensa". *Revista Sistemas, ACIS* 130 (7). http://52.0.140.184/revsistemas1/index .php/ediciones-revista-sistemas/edicion-130/item/156-m%C3%A1s-all%C3%A1-de-las-tic-en-mindefensa.

Gibney, Alex. 2016. *Zero Days*. EE.UU.: Jigsaw Productions y Participant Media (Documental).

Gastaldi, Sol y Justifró Candela. 2014. "La seguridad y la defensa en el ámbito ciberespacial. Informe de Investigación. Escuela de Defensa Nacional", http://www.edena.mindef.gob.ar/sol_gastaldi.html

Ministerio de Defensa, Presidencia de la Nación y República Argentina. 2015. *Libro Blanco de la Defensa*. Argentina: Ministerio de Defensa. http://www.mindef.gob.ar/institucional/pdfs/libro_blanco_2015.pdf.

Illaro, Eguskiñe Lejarza. 2014. "Ciberguerra, los escenarios de confrontación". *Revista del Instituto Español de Estudios Estratégicos* 18: 1-20. http://www.ieee.es/Galerias/fichero/docs_opinion/2014/DIEEEO18-2014_Ciberguerra_EscenariosConfrontacion_EguskineLejarza.pdf.

OEA (Organización de los Estados Americanos). 2014. *Tendencias en la seguridad cibernética en América Latina y el Caribe y respuestas de los gobiernos*. Washington: Secretaría de Seguridad Multidimensional. https://www.sites.oas.org/cyber/Documents/2014%20-%20Tendencias%20de%20Seguridad%20Cibern%C3%A9tica%20en%20Am%C3%A9rica%20Latina%20y%20el%20Caribe.pdf

Pastor Acosta, Oscar, José Antonio Pérez Rodríguez, Daniel Arnáiz de la Torre y Pedro Taboso Ballesteros. 2009. *Seguridad Nacional y Ciberdefensa*. Madrid: Cuadernos Cátedra ISDEFE. http://catedraisdefe.etsit.upm.es/wp-content/uploads/2010/07/CUADERNO-N%C2%BA-6.pdf.

Poitras, Laura. 2014. *Citizenfour*. Alemania, EE.UU, Reino Unido: Praxis Films/Participant Media/ HBO Films (Documental). https://citizenfourfilm.com/.

Schmitt, Michael, ed. 2013. Tallinn Manual on the International Law Applicable to Cyber Warfare gen. Nueva York: Cambridge University Press.

Vercelli, Ariel. 2009. Repensado los bienes intelectuales comunes: análisis socio-técnico sobre el proceso de co-construcción entre las regulaciones de derecho de autor y derecho de copia y las tecnologías digitales para su gestión. Edición en PDF. http://www.arielvercelli.org/rlbic.pdf

_____. 2015. "Repensando las regulaciones de Internet: análisis de las tensiones políticas entre no-regular y re-regular la red de redes". *Revista Latinoamericana de Comunicación Chasqui* 129: 95–112. http://revistachasqui.org/index.php/chasqui/issue/view/129_2015.

Documentos

Carta de las Naciones Unidas. 1945. "Conferencia de las Naciones Unidas sobre Organización Internacional", http://www.un.org/es/charter-united-nations/index.html.

Convenio del Ministerio de Defensa. 2013, de 13 de septiembre, Declaración de Buenos Aires de los Ministros de Defensa del Brasil y Argentina, http://www.ceedcds.org.ar/Espanol/09-Downloads/DECLARACION_ARG_BRASIL.pdf.

Decisión Administrativa 669/2004, de 20 de diciembre, Política de Seguridad de la Información (B.O. 22/12/2004), http://servicios.infoleg.gob.ar/infolegInternet/anexos/100000-104999/102188/texact.htm.

Decisión Administrativa 15/2015, de 4 de marzo, Estructura organizativa. Modificación (B.O. 11/03/2015), http://servi-

cios.infoleg.gob.ar/infolegInternet/anexos/240000-244999/244566/norma.htm.

Decreto 727/2006, de 12 de junio, de Reglamentación de la Ley Nº 23.554 (B.O. 13/06/2006), http://servicios.infoleg.gob.ar/infolegInternet/anexos/115000-119999/116997/norma.htm.

Decreto 1714/ 2009, de 10 de noviembre, Directiva de Política de Defensa Nacional (B.O. 12/11/2009), http://servicios.infoleg.gob.ar/infolegInternet/anexos/160000-164999/160013/norma.htm.

Decreto 2645/2014, de 30 de diciembre, Directiva de Política de Defensa Nacional. Apruébase actualización (B.O. 19/01/2015), http://servicios.infoleg.gob.ar/infolegInternet/anexos/240000-244999/240966/norma.htm.

Decreto 677/2015, de 28 de abril, de Argentina Digital. Autoridad Federal de Tecnologías de la Información y las Comunicaciones (B.O. 29/04/2015), http://servicios.infoleg.gob.ar/infolegInternet/anexos/245000-249999/246354/norma.htm.

Decreto 1067/2015, de 10 de junio, Decreto N° 357/2002. Modificación (B.O. 12/06/2015), http://servicios.infoleg.gob.ar/infolegInternet/anexos/245000-249999/247971/norma.htm.

Disposición de la Oficina Nacional de Tecnologías de la Información 2/2013, de 8 de agosto, Grupo de Trabajo "ICIC - CERT - Creación (B.O. 3/09/2013), http://servicios.infoleg.gob.ar/infolegInternet/anexos/215000-219999/219212/norma.htm.

Disposición de la Oficina Nacional de Tecnologías de la Información 3/2014, de 2 de octubre, Estándares Tecnológicos para la Administración Pública Nacional Versión 20.0 - Aprobación (B.O. 8/10/2014), http://servicios.infoleg.gob.ar/infolegInternet/anexos/235000-239999/236037/norma.htm.

Disposición de la Oficina Nacional de Tecnologías de la Información 1/2015, 18 de agosto, Requerimientos para la Conformación de las Autoridades de Registro (B.O. 25/02/2015), http://servicios.infoleg.gob.ar/infolegInternet/anexos/250000-254999/250974/norma.htm.

Ley 23554/1988, de 13 de abril, de Defensa Nacional (B.O. 5/05/1988), http://servicios.infoleg.gob.ar/infolegInternet/anexos/20000-24999/20988/texact.htm.

Ley 24.059/1991, de 18 de diciembre, de Seguridad Interior (B.O. 17/01/1992), http://servicios.infoleg.gob.ar/infolegInternet/anexos/0-4999/458/texact.htm.

Ley 24.156/1992, de 30 de septiembre, de Administración Financiera y de los Sistemas de Contabilidad del Sector Público Nacional (B.O. 29/10/1992), http://servicios.infoleg.gob.ar/infolegInternet/anexos/0-4999/554/texact.htm.

Ley 24.948/1998, de 18 de marzo, de Reestructuración de las Fuerzas Armadas (B.O. 8/04/1998), http://servicios.infoleg.gob.ar/infolegInternet/anexos/50000-54999/50229/norma.htm.

Ley 27.078/2014, de 16 de diciembre, de Argentina Digital (B.O. 19/12/2014), http://servicios.infoleg.gob.ar/infolegInternet/anexos/235000-239999/239771/texact.htm.

Resolución de la Jefatura de Gabinete de Ministros 580/2011, de 28 de julio, Créase el Programa Nacional de Infraestructuras Críticas de Información y Ciberseguridad (B.O. 2/08/2011), http://servicios.infoleg.gob.ar/infolegInternet/anexos/185000-189999/185055/norma.htm.

Resolución de la Secretaría de Comunicaciones 13/2014, de 22 de abril, Comisión Argentina de Políticas de Internet (B.O. 23/04/2014), http://servicios. infoleg. gob.ar/infolegInternet/anexos/225000-229999/229123/norma.htm.

Resolución del Ministerio de Defensa 364/ 2006, de 12 de abril.

Resolución del Ministerio de Defensa 385/ 2013, del 22 de octubre.

Resolución del Ministerio de Defensa 343/ 2014, del 14 de mayo.

Resolución del Ministerio de Defensa 781/ 2015, del 24 de julio.

Resolución de la Secretaría de Estrategia y Asuntos Militares del Ministerio de Defensa 8/2010, de 14 de abril.