Centro de Estudios Grl Mosconi
Prospectiva Tecnológica Militar

Esp. López Lio Rodrigo 22 Agosto 2017

Argentina y la difusión de poder en el ciberespacio

Abstract: *En este escenario, el ciberespacio, los actores con capacidades de influir en el escenario político se multiplican. El ciberespacio actúa como un difusor de poder a fin de contrarrestar las condiciones de asimetría. La transnacionalización del conflicto y las no-fronteras del escenario cibernético encuentran problemas en la definición actual de los campos de actuación de las Fuerzas de Seguridad y de Defensa en la Argentina, a través de este trabajo se busca describir estos procesos de transnacionalización de amenazas, donde el soft power y la capacidad manifiesta de estas sub unidades, pone a prueba las teorías concebidas para analizar a los agentes y el plano internacional para identificar si a través de ellas es posible analizar el impacto del ciberespacio en la supervivencia del Estado.*

Desarrollo Tecnológico, Relaciones Internacionales y Asimetría

El continuo desarrollo de las nuevas tecnologías de información (TI), los avances de las comunicaciones y su correspondiente implementación en todos los sectores, tanto públicos como privados y la sociedad en general, expone un "ecosistema" cada vez más complejo, dinámico e interrelacionado, en donde se vislumbra en primer lugar la dependencia de las TIC (Tecnologías de Información y Comunicación) y en segundo término el aspecto facilitador a las potenciales amenazas de traspasar fronteras nacionales, continentales y la capacidad de actuar a veces de forma anónima.

Esto repercute especialmente en el Estado nacional, principal componente del sistema internacional. Según Buzán, la globalización implica el incremento en los elementos de interacción entre Estados, lo cual en parte, se explica por las innovaciones tecnológicas que apareja el siglo XXI.

En 1977 durante la administración de Carter, EEUU inicia un proceso de reacción ante la pérdida de credibilidad internacional por sus intervenciones en Vietnam y Chile, Desde entonces, Washington enfatizó el desarrollo tecnológico, la USIA (Agencia de Información de los Estados Unidos), agencia dedicada a la diplomacia comienza un proceso de expansión de medios y redes de comunicación (a fin de aumentar la proyección exterior del país), recordemos que en los 60 se comenzaba a diseñar e implementar ARPANET[1] y años más tarde su apertura al mundo en lo que hoy conocemos como el ciberespacio. Observamos de este modo como para mantener su poder, las unidades políticas deben replantearse continuamente sus estrategias de influencia y proyección a fin de adecuarse a los nuevos escenarios.

La transnacionalidad inherente a las Tecnologías de la Información puestas en un contexto de nuevas amenazas, representa un desafío para la defensa de componentes esenciales de los Estados, como lo son las Infraestructuras Criticas[2]. Por este motivo, resulta imperativo que los Estados tomen su presencia en el ciberespacio dentro de sus consideraciones político-estratégicas.

Hasta hace unos años los riesgos y retos de seguridad cibernéticos sólo se trataban dentro de pequeños grupos de expertos, posteriormente se evidenció que el ciberespacio introduce graves vulnerabilidades en unas sociedades cada vez más interdependientes. Los "ciberataques" eran considerados un riesgo real, pero de ámbito y consecuencias limitados, y que sólo requería respuestas técnicas de determinados sectores y profesionales.
En su artículo Understanding Fourth Generation War, Lind[3] establece un marco de entendimiento para clasificar/diferenciar los conflictos, en lo que él define Las Cuatro Generaciones de la Guerra Moderna.

[1] ARPANET: La Advanced Research Projects Agency Network fue una red de computadoras del Departamento de Defensa de los Estados Unidos cuyo fin era la utilización como medio de comunicación entre unidades militares y académicas.
[2] Infraestructura Crítica son aquellas instalaciones, redes, servicios, equipos físicos y tecnología de información, cuya interrupción, alteración, o destrucción comprometa los intereses vitales de la Nación. Es decir afectando en la salud, seguridad, o el bienestar económico de los ciudadanos o en el sostenimiento del Estado. LOPEZ LIO, R. *Ciberdefensa e Infraestructuras Críticas.* Instituto de Inteligencia de las Fuerzas Armadas. 2016.
[3] Lind, W. *Understanding Fourth Generation War*. Military Review, 2004.

A las características predominantes de las Guerras de Tercera Generación (descentralización e iniciativa), las Guerras de Cuarta Generación agregan la pérdida del monopolio de la guerra por parte del Estado. Esto se debe a la aparición de nuevos actores no estatales en los conflictos, quienes utilizan diferentes herramientas para entablar la guerra, la cual no se circunscribe al mero empleo de fuerzas militares.
En este sentido se manifiesta Sepúlveda Muñoz, quien afirma que "al mundo globalizado le corresponden amenazas globales y los distintos sistemas de defensa deben readaptarse para hacer frente a éstas con garantías de éxito"[4.] Donde es necesario analizar las amenazas y desafíos a los que se debe hacer frente en el escenario nacional, regional e internacional; evaluando los medios con los que se cuenta para hacer frente a esas amenazas".

En concordancia con Nye, con la difusión de poder que se da en el ciberespacio, a raíz de la diversidad de actores que interactúan en el mismo, uno de los cambios sustanciales en el escenario Político Internacional es el rol de los actores no estatales, los cuales están incrementando su poder de actuación, jugando un papel cada vez más destacado que los Estados ya no pueden ignorar. Más adelante se evidenciará como la transnacionalización de las amenazas, lo difuso del concepto frontera y la supervivencia del Estado, tienen lugar en el ciberespacio.
Este trabajo apunta en parte, a describir cómo los procesos de transnacionalización de amenazas de todo tipo y de erosión de fronteras que amenazan la supervivencia del Estado encuentran su correlato en el ciberespacio, donde la asimetría entre actores no resulta un límite.

Las nuevas amenazas y los conflictos asimétricos

Si tomamos la definición de amenaza como el "conjunto de circunstancias que integradas constituyen un factor potencial de daño cierto y que bajo ciertas circunstancias puede producirse" (Laiño, 1991) y entendiendo que la misma adquiere significados dispares en función de los tiempos históricos. La guerra no sigue modelos de desarrollo unidireccionales sino que adapta sus características a una situación dada (Clausewitz,

[4] Sepúlveda, M. *La Seguridad Internacional ante las nuevas amenazas*. En Defensa nacional: dimensiones internacionales y regionales. 2007; p63

1832), y que está sujeta a la interacción de factores mucho más complejos. La defensa nacional o la seguridad internacional pueden verse atacadas por elementos muy variados que cuentan con medios aún más dispares, conformando un escenario de amenazas convencionales y no convencionales diverso.

La Guerra Asimétrica se da entre fuerzas disimilares que utilizan determinados factores o estrategias para alterar el escenario del enfrentamiento y así obtener una ventaja sobre el oponente. La asimetría puede darse en el campo político-estratégico, en plano militar-estratégico, ser operacional o bien una combinación de los mismos.[5]

Ciberguerras como conflictos asimétricos

También puede ser entendido como Guerra Asimétrica el uso de nueva tecnología con que una fuerza militar derrota a otra fuerza. Lo asimétrico abarcaría todo aquello que altera el campo de batalla de manera tal que se niega la ventaja del oponente: estrategias, tácticas, armas, personal[6]… (Benedicto Salmerón)

En los noventa la publicación del artículo Cyberwar is Comming! (Arquilla & Ronfeldt, 1993) pronosticaba un nuevo tipo de conflicto, las ciberguerras, definiéndolas como guerras que giran en torno a la información y las comunicaciones, son guerras sobre conocimiento.

Situamos a las Ciberguerras, las cuales son conflictos eminentemente Asimétricos, dentro de las Nuevas Amenazas. Richard Clarke (2010) define la ciberguerra como: cualquier penetración no autorizada por parte de, en nombre de, o en apoyo a, un gobierno en los ordenadores o las redes de otra nación, en la que el propósito es añadir, alterar o falsificar información o causar daños a, o perturbar el adecuado funcionamiento de, un ordenador, un dispositivo de red o los objetos controlados por el sistema informático[7.] Algunos analistas han considerado que, junto al mar, la tierra, el aire y el espacio, el ciberespacio constituye el quinto dominio en el cual se puede librar la guerra (Lynn, 2010).

[5] Una situación de asimetría se produce cuando una (o más) de las partes en conflicto actúa, piensa y se organiza en forma diferente a lo que su oponente espera, buscando maximizar sus puntos fuertes e intentando explotar las debilidades de su adversario con el objetivo de lograr libertad de acción, autonomía y tiempo. METZ, Steven: "Strategic Asymmetry", 2001.

[6] Benedicto Salmerón, R. *Teorías y conceptos para entender formas actuales de hacer la guerra.* Universitat Autónoma de Barcelona. p 28

[7] Clarke, R y Knake, R. *Cyber War. The next Threat to National Security and what to do about it.* Harper Collins, 2010.

Los procesos de convergencia de conectividad y accesibilidad involucró también a las redes y sistemas industriales, posicionando a las Infraestructuras Criticas como objetivos de ciberataques debido a la posibilidad de acceso, impacto productivo, imagen internacional, daños asociados, etc. poniendo de manifiesto las nuevas amenazas y vulnerabilidades que los Estados deben atender.

A su vez, la atribución del conflicto se complejiza dada las dificultades de la identificación del atacante y no existe una disuasión eficaz para un ataque cibernético, haciendo aún más interesante este tipo de objetivos en estos conflictos asimétricos.

Ciberguerras - Tiempo, Fronteras y Atribución

Una de las particularidades más interesantes del ciberespacio es que el factor tiempo deja de ser una limitación en las comunicaciones entre los diferentes actores, por lo que las distancias geográficas se vuelven irrelevantes. Esta particularidad permite el incremento del número de participantes en la ciberguerra, puesto que da acceso a nuevos actores. La muerte de la distancia supone que los conflictos armados incluso los de pequeña escala, sean difíciles de aislar geográficamente. El ciberespacio facilita que los episodios bélicos desborden su ámbito regional y puedan alcanzar un impacto global, dado que los espacios virtuales empleados en una ciberguerra pueden ser los pertenecientes a personas, instituciones, empresas o naciones que no participan del conflicto y que no tienen interés o conocimiento de que sus espacios cibernéticos están siendo empleados para atacar otros espacios.

Una característica de la ciberguerra reside en los problemas de atribución de responsabilidades. Los países atacados se ven en la necesidad de gestionar las consecuencias del ataque, pero también de articular de manera inmediata una respuesta frente a una agresión que procede de diferentes puntos del planeta, sin que pueda conocerse la responsabilidad real de cada uno de los equipos atacantes.

Como se ha mencionado anteriormente, las TIC se han convertido en un conjunto de herramientas utilizadas por todos los sectores, tanto públicos como privados, de un Estado. La interrupción de las mismas podría provocar la pérdida de vidas humanas y de bienes materiales, un colapso en la economía y por esta razón, se debe trazar una estrategia que

permita la correcta defensa del "*ciberespacio local"* y las Infraestructuras Criticas de un Estado.

Identificación de Amenazas

Es posible clasificar las amenazas en el ciberespacio en Amenazas Naturales (Desastres Naturales, Inundaciones, Incendios, Terremotos) Amenazas Físicas (Daño en los sistemas, intrusiones físicas, sabotajes, espionaje) Amenazas Humanas (Hackers, insiders, ingeniería social, conocimiento). Como agentes o actores de los ataques: Estados, Crimen Organizado, Hacktivismo, Terrorismo, Actores Internos, Profesionales de Seg. Inf., Organizaciones Privadas, Cibervandalismo.

Detrás de un ataque existe una combinación entre motivación, método y vulnerabilidad. La motivación para efectuar un ataque puede deberse a una motivación externa, interna basada en el disfrute o interna basada principios u obligaciones morales.

El o los objetivos de un ataque pueden ser diversos, desde un acceso no autorizado a un sitio web hasta una disrupción de un servicio como la energía eléctrica. En este sentido los objetivos de una ciberguerra y el cibercrimen suelen ser similares, es entonces donde la motivación de los actores es uno de los factores determinantes en la diferenciación entre los actos de ciberguerra y cibercrimen.

El ciberespacio, desafíos para los paradigmas de las Relaciones Internacionales

Como mencionamos anteriormente la diferenciación de los distintos tipos de actos "maliciosos" en el ciberespacio es la motivación del actor y en este sentido el Ciberespacio pone a prueba el criterio tradicional de las fronteras nacionales, y con ello la figura del Estado como poseedor del uso de la fuerza legítima. Cuando mencionábamos anteriormente que en el plano del ciberespacio, en cierta medida, "todos compiten por igual" diferentes actores se encuentran expuestos y con capacidad de realizar un ciberataque, debemos preguntarnos qué sucede con el contrato social y la protección que el Estado brinda a su comunidad, de las demás unidades políticas y de aquellos actores no estatales que, gracias

al efecto difusor de poder del ciberespacio, cuentan con capacidad de influir en el escenario político.

En este sentido es interesante preguntarnos si ante las características del ciberespacio, su nivel de interconexión, amenazas y vulnerabilidades, las teorías de las Relaciones Internacionales pueden analizar el impacto del ciberespacio en la seguridad y supervivencia del Estado.

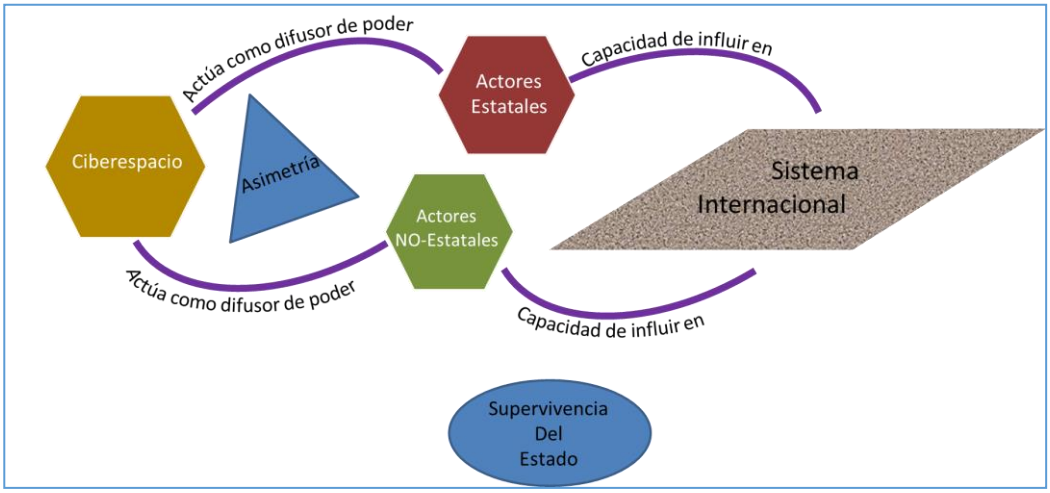

Fig. 1 Ciberespacio y la influencia en el Sistema Internacional.

Realismo

En esta corriente encontramos a los autores Niebuhr, Morgenthau, Aron, Carr, Kissinger o Kennan, en el caso del neorrealismo a los autores Keohane, Waltz o Gilpin.

Podemos identificar las siguientes premisas o lineamientos del realismo:

- Los agentes claves en el sistema son las naciones-estado.
- Entre las naciones-estado pueden clasificarse en grandes potencias y estados menores.
- La política interna con sus intereses de estado son separados de la política exterior.
- Los principios morales no pueden aplicarse a acciones políticas.
- Ausencia de instituciones políticas con autoridad en el entorno internacional. "El gobierno es un agente, no un patrón. Su obligación primordial es respecto de los

intereses de la sociedad nacional que representa, no respecto de los impulsos morales que los elementos individuales de dicha sociedad puedan experimentar"[8]

- El poder como determinante del comportamiento internacional. "La política internacional, como toda política, es una lucha por el poder. Cualesquiera que sean los fines últimos de la política internacional, el poder es siempre el fin inmediato"[9]
- El poder abarca las capacidades militares, económicas y tecnológicas de los estados mientras que el prestigio consiste en las percepciones de otros estados respecto de las capacidades de un Estado y su capacidad y disposición de expresar su poder[10].

Para los teóricos del realismo las Relaciones Internacionales son conflictivas y los intereses de los Estados pueden contraponerse, las RI son anárquicas, aquí (exceptuando determinadas características técnicas y de administración de Internet), podemos decir que el ciberespacio es un plano anárquico. No obstante cuando para los realistas el Estado es el único actor que se reconoce y donde estos (los Estados) actúan como entidades monolíticas, observamos que las élites políticas o los actores no estatales usan el ciberespacio a fin de buscar la alteración de las relaciones de poder dentro de la estructura. O lo que es peor, el efecto de las operaciones cibernéticas o un ataque, más allá del agente o motivación del mismo genera la misma alteración.

Como así también que dentro del ciberespacio suceden transacciones que van más allá de las fronteras nacionales, y que no son iniciadas ni controladas en su totalidad por autoridades estatales. Y que estos actores no estatales ejercen fuerte influencia en el comportamiento de los estados como en el de otras unidades del ámbito mundial.

Respecto a la interdependencia entre dos o más unidades, para Waltz[11] no existe la interdependencia entre Estados, en contraposición a lo que sucede en el ciberespacio. Mientras que cuando indica que la anarquía es un estado de guerra, y que es justamente ese

[8] KENNAN, *Morality and Foreign Policy*, Foreign Affairs 1985
[9] MORGENTHAU, *Politics among Nations: The Struggle for Power and Peace*.1960
[10] GILPIN, *War and Change in World Politics. 1981*
[11] Waltz, Teoría de la Política Internacional, Grupo Editor Latinoamericano, 1988.

riesgo de guerra lo que limita las demandas de los actores estableciéndolos dentro de parámetros previsibles, por contrapartida en el ciberespacio no existe tal previsibilidad dada la constante aparición de vulnerabilidades y amenazas.

Los realistas abordarían la problemática del ciberespacio de la misma forma que han abordado la transnacionalización, la interdependencia o la globalización, es decir como epifenómenos que pueden afectar las estructuras domesticas pero que no alteran la anarquía del Sistema Internacional. En este sentido debemos mencionar que el impacto del ciberespacio ha tenido consecuencias económicas, sociales y culturales que han llegado a alterar el poder. Keohane y Nye[12], destacan que las tecnologías de información y comunicación aumentaron el peso relativo del conocimiento como fuente del *soft power*, convirtiéndolo en el recurso de poder más importante en las relaciones internacionales. Pero para el realismo el Estado todavía es visto como el actor principal negando que los actores no-estatales puedan ejercer poder (semejante al militar).

Liberalismo

Las contribuciones más importantes de la teoría liberal pueden resumirse en: pluralidad de los actores internacionales, importancia de los factores políticos internos en la determinación del comportamiento internacional de los actores, el rol de las instituciones en el establecimiento de las normas para los actores estatales.

Si bien se aprecia cierta coincidencia con el realismo al centrarse en el papel del actor estatal en el plano político, en el liberalismo se sostiene que los Estados no son los únicos importantes en las Relaciones Internacionales, sino que pone en juego el rol de los actores no estatales como empresas trasnacionales, grupos de presión, partidos políticos, etc. En este sentido el liberalismo permite mostrar los grupos emergentes en el ciberespacio.

Sin embargo para el liberalismo, que tiende a enfatizar los aspectos positivos de las relaciones como la interdependencia e interconexión, en el ciberespacio estos aspectos son vulnerabilidades e inseguridad para el Estado.

El liberalismo, en el campo del ciberespacio, presta debida atención a la creciente pluralidad y a los actores no estatales emergentes. En este aspecto dos enclaves de la teoría

[12] Keohane y Nye, *Power and Interdependence in the information Age*, Foreign Affairs, 1998.

liberal a considerar son: la colaboración del sector público y privado y la fusión de las esferas civil y militar. El desarrollo de las TIC es considerado como una continuación y ampliación de la nacionalización de la sociedad y economía, que comenzó con el comercio. El sesgo liberal hacia el modernismo tiende a destacar los aspectos positivos y no los negativos de esta interdependencia e interconexión. Las amenazas en el ciberespacio y demás desafíos del avance tecnológico son claros en el debilitamiento de la soberanía y la seguridad del Estado.

Situación en la Argentina

Es posible observar que la Argentina cuenta con determinadas estructuras con sus niveles de injerencia en el ciberespacio y que existe un marco normativo compuesto por leyes, disposiciones, doctrinas y decretos específicos relacionados con la Ciberdefensa, Ciberseguridad. No obstante no existen protocolos de actuación coordinada, y este tipo de segmentación resulta una complejización en la resolución y mitigación de ataques o incidentes.

Como se ha mencionado anteriormente el ciberespacio es un escenario donde diversos actores interactúan entre sí, en base a una arquitectura compleja de interconexión mundial, desde lo estrictamente técnico resulta complejo a priori la identificación del origen de un ataque, si el mismo corresponde a un actor estatal, una fuerza armada o una persona aislada. En este sentido las leyes actuales limitan considerablemente el accionar de los distintos actores internos respecto del nuevo escenario y sus amenazas.

A continuación se detallan cuáles son los actores internos con injerencia en el ámbito ciber[13].

Institución	Dirección General de Ciberdefensa (Ministerio de Defensa)
Línea de Tiempo	2013 Se crea la Unidad de Coordinación de Ciberdefensa. 2014 Se crea el comando Conjunto de Ciberdefensa.

[13] Desarrollado en *Ciberdefensa e Infraestructuras Críticas*, LOPEZ LIO, R. Instituto de Inteligencia de las Fuerzas Armadas. 2016

	2016 Se firma el convenio marco entre el Ministerio de Defensa y el Ministerio de Modernización.
Acontecimientos	Res. MD N385/13 - Unidad de Coordinación de Ciberdefensa Res. MD N343/14 - Creación del Comando de Ciberdefensa
Acontecimientos especiales	2010 Libro Blanco para la Defensa, incluye apartado de Ciberespacio 2014 Edificio de Ciberdefensa
Detalles	Estructura: Ministerio de Defensa Dirección General de Ciberdefensa Comando Conjunto de Ciberdefensa Centro de Ciberdefensa Ejercito – Centro de Ciberdefensa F.A – Centro de Ciberdefensa A.R.A
Injerencia	Conjurar y repeler ciberataques contra las infraestructuras críticas de la información y los activos del Sistema de Defensa Nacional y de su Instrumento Militar dependiente.

Institución	**Dirección Nacional de Infraestructuras Críticas y Ciberseguridad (Ministerio de Modernización)**
Línea de Tiempo	1999 Conformación del ArCERT. 2011 Creación del Programa Nacional de Infraestructuras Críticas y Ciberseguridad. 2015 Creación de Subsecretaria de Protección de Infraestructuras Críticas y Ciberseguridad. 2015 Nueva Estructura de la Dirección Nacional de Infraestructuras Críticas y Ciberseguridad.
Acontecimientos	Res. 81/99 SFP - Creación del ArCERT Res. 580/2011 – Programa Nacional de Infraestructuras Críticas de Información y Ciberseguridad
Acontecimientos especiales	Decisión administrativa 232/2016 Aprobación estructura Organizativa (La Dirección Nacional de Infraestructuras Críticas de Información y Ciberseguridad pasa de Jefatura de Gabinete al Ministerio de Modernización) Responsable de la Seguridad de los Centro de Datos Nacionales
Detalles	Estructura: Ministerio de Modernización Subsecretaria de Tecnología y Ciberseguridad Dirección Nacional de Infraestructuras Críticas de Información y Ciberseguridad
Injerencia	• Sector Público Nacional (estipulado en el art. 8 de la Ley 24.156 y aquellos asociados que adhieren al Programa Nacional. • Asistir al Ministro en la formulación de un marco regulatorio específico que propicie la identificación y protección de las infraestructuras críticas del Sector Público Nacional, y a las organizaciones civiles, del sector privado y del ámbito académico que así lo requieran, fomentando la cooperación y colaboración de los mencionados sectores.

	• Entender en los procesos relativos al accionar del equipo de respuesta a emergencias informáticas a nivel nacional (CERT NACIONAL). • Desarrollar programas de asistencia a los organismos del Sector Público Nacional y a las provincias y municipios que así lo requieran en el ámbito de su competencia y en coordinación con los organismos competentes. • Difundir las mejores prácticas y elaborar políticas de capacitación para el Sector Público Nacional y contribuir a la capacitación de las organizaciones civiles, del sector privado y del ámbito académico en temas de seguridad de la información y protección de información crítica, que así lo requieran. • Seguridad de los Centro de Datos Nacionales

Institución	**Dirección Operacional de Inteligencia sobre la Ciberseguridad (Agencia Federal de Inteligencia)**
Línea de Tiempo	2001 Ley de Inteligencia Nacional 2015 Creación de la Agencia Federal de Inteligencia
Acontecimientos	27/11/2001 – Ley 25.520 Ley de Inteligencia Nacional 5/6/2002 – Dec. 950/2002 Reglamentación de la Ley de Inteligencia 25/2/2015 – Ley 27.126 modificación de la Ley 25.520 contempla Creación de la AFI
Acontecimientos especiales	6/7/2015 Dec. 1311/15 Doctrina de Inteligencia
Detalles	Estructura: Dirección Operacional de Inteligencia sobre la Ciberseguridad Dirección de Inteligencia Informática – Dirección de Inteligencia sobre Delitos Informáticos
Injerencia	• Producción de Inteligencia orientada al conocimiento de actividades relativas a riesgos y conflictos vinculados o derivados del uso de la tecnologías de información y la comunicación, que afecten a la defensa nacional o a la seguridad interior y de los grupos nacionales o extranjeros responsables de llevar a cabo estas actividades. • Producción de Inteligencia orientada al conocimiento de las actividades que pudieran configurar delitos informáticos en cualquiera de sus formas y modalidades, y de los grupos nacionales o extranjeros responsables de llevar a cabo estas actividades.

Institución	**Ministerio de Justicia**
Línea de Tiempo	2000 Ley de Protección de Datos Personales

	2008 Ley Delitos Informáticos
Acontecimientos	4/10/2000 - Ley 25.326 - Protección de Datos Personales 4/6/2008 - Ley 26.388 - Delitos Informáticos 5/10/2011 Res. 866/2011 y 1500/2011 - Creación Comisión Técnica Asesora de Cibercrimen - Convenio de Budapest 11/10/2011 Resolución 69/2016 Creación de Programa Nacional
Acontecimientos especiales	11/03/2016 Res 69/2016 Creación Programa Nacional contra la criminalidad informática
Detalles	Estructura Ministerio de Justicia y Derechos Humanos Programa Nacional contra la criminalidad informática
Injerencia	• Promover las acciones necesarias para mejorar las respuestas del sistema penal frente al desafío que plantean los delitos informáticos y los delitos cometidos valiéndose de herramientas de tecnología informática. • Propiciar la eficiencia en la investigación de las causas penales mediante la utilización de medios modernos de obtención de pruebas basados en tecnología informática y de las telecomunicaciones, garantizando que su utilización se rija por normas respetuosas de los derechos fundamentales de los ciudadanos. • Reformas que resulten necesarias en la legislación penal y procesal penal. • Proyectos normativos de cooperación judicial entre la nación y las provincias a fin de mejorar la eficiencia en la persecución de los delitos informáticos como en todo lo atinente a la cooperación interjurisdiccional en la obtención de evidencia digital. • Capacitación de los operadores del sistema penal tanto federal como provincial sobre la materia. • Coordinación de acciones con organismos nacionales e internacionales. • Promover la cooperación entre sector público - sector privado para el mejoramiento de las investigaciones que involucren la necesidad de obtener evidencia digital en la que sea necesaria la colaboración de los proveedores de servicios de internet u otros entes con acceso a datos informáticos que puedan resultar de interés para las investigaciones. • Propiciar la participación de la República Argentina en los foros internacionales y en las Convenciones y mecanismos internacionales de Cooperación sobre la materia que resulten convenientes para nuestro país.

Institución	**Ministerio de Seguridad**
Línea de Tiempo	2008 Ley de Delitos Informáticos.

	2013 Ley Grooming.
Acontecimientos	Ley 26.388 Ley 26.904 Resolución 234/2016 Protocolo General de Actuación.
Acontecimientos especiales	Protocolo General de Actuación para las Fuerzas Policiales y de Seguridad en la Investigación y Procesos de Recolección de Pruebas en Ciberdelitos. (Resolución 234/2016)
Detalles	Estructura: Ministerio de Seguridad Fuerzas de Seguridad (Gendarmería Nacional Argentina – Prefectura Naval Argentina) – Fuerzas Policiales (Policía Federal Argentina – Policía de Seguridad Aeroportuaria)
Injerencia	• A los fines de la investigación de los ciberdelitos alcanzados por el presente protocolo las Fuerzas Policiales y de Seguridad podrán hacer y solicitar el uso de las técnicas de investigación establecidas en los Códigos de Fondo, Procedimentales y leyes especiales de la jurisdicción correspondiente. • Las denuncias en materia de ciberdelitos, deben cumplir con lo establecido en el Código Procesal Penal de la Nación, los Códigos Procesales de cada provincia y de la CIUDAD AUTÓNOMA DE BUENOS AIRES, en cuanto a su recepción, forma, contenido. • Recibida la denuncia por cualquiera de los canales existentes, los miembros de las Fuerzas Policiales y de Seguridad deberán comunicar de inmediato al Ministerio Público Fiscal quienes a su vez, pondrán en conocimiento la denuncia en caso de tratarse del delito de grooming o pornografía infantil a la "Red 24/7". Al momento de la recepción de la denuncia los miembros de las Fuerzas Policiales y de Seguridad deben procurar el aseguramiento de la prueba.

Institución	**Unidad Fiscal Ciberdelincuencia (Procuración General de la Nación)**
Línea de Tiempo	2012 Prueba Piloto Equipo Fiscal "A" de la Unidad Fiscal Este. 2013 Asignación exclusiva Equipo Fiscal "A". 2015 Unidad Fiscal Ciberdelincuencia.
Acontecimientos	Resolución 444/13 Asignación Equipo Fiscal "A" Resolución 3743/15 Unidad Fiscal Ciberdelincuencia.
Acontecimientos especiales	Designación Punto Focal Ciberdelitos Resolución 756/16 Guía de obtención, preservación y tratamiento de evidencia digital.
Detalles	Estructura: Procuración General de la Nación Unidad Fiscal Especializada en Ciberdelincuencia (UFEG)
Injerencia	• La Unidad Fiscal podrá entender en casos de ilícitos constituidos por ataques a sistemas informáticos, o cuando el medio comisivo principal o accesorio de una conducta delictiva incluya la utilización de sistemas informáticos, con

	especial atención en el ámbito de la criminalidad organizada, trata de personas, tráfico de estupefacientes, lavado de dinero y terrorismo, etc. • Habilitada a intervenir en todo proceso en el que sea necesario realizar investigaciones en entornos digitales, localización de imputados a través de Internet.

Tabla 1. Tabla de injerencia de Actores internos en la Argentina.

Abordaje como Política Pública

Entendiendo que la problemática del ciberespacio debe abordarse como una cuestión estratégica a nivel Estado y que una Política Pública es el "conjunto de acciones u omisiones que manifiestan una determinada modalidad de intervención del Estado en relación con una cuestión que concita la atención, interés o movilización de otros actores de la sociedad civil".[14]

Las políticas públicas pueden clasificarse según su alcance, interés al que responden, consenso, ámbito de acción, el territorio que cubren y el tema que abordan. Para la problemática del Ciberespacio, esta política pública resulta estratégica, siendo así su planeamiento, considerándola de largo plazo. Son denominadas políticas de Estado debido a que trascienden el periodo legalmente establecido de mandato electoral.

Como se mencionó anteriormente, el ciberespacio se ha ido convirtiendo en un nuevo lugar de conflicto, disputa y competencia de intereses, de forma tal que no es posible por parte de los Estados ignorar la importancia política del mismo. Por lo que el tema debe estar en la *Agenda Política*, considerándose como factor clave la articulación técnico-política.

Definición de Infraestructura Crítica

Como parte de una estrategia de Ciberseguridad se debe contemplar la definición de que son las Infraestructuras Críticas, y la elaboración de estándares de seguridad para su aseguramiento.

[14] Oscar Oszlak y Guillermo O´Donnell, *Estado y políticas estatales en América Latina: hacia una estrategia de investigación*. 1976

Desarrollar una definición basada en los intereses vitales nacionales[15], hace a esta definición lo suficientemente amplia y objetiva en el sentido de que no se define sobre bases que puedan cambiar en el corto plazo o dependiendo de los objetivos políticos, sino con la intención de que permanezca en el tiempo y con un sustento sólido como son los intereses nacionales. Así mismo la utilización de la segmentación por sectores facilitaría su identificación y agrupamiento.

Estructura interagencial

La implementación de una estructura de tipo interagencial conformada por los actores internos con injerencia permitiría a la Argentina una oportunidad para dar respuesta a la problemática del ciberespacio. De esta manera se utiliza la autoridad legítima de cada entidad según las necesidades que se planteen a fin de agilizar la resolución de incidentes, mejorar los canales de información y los procedimientos actuales. El desarrollo de un sistema integral que permita conocer cabalmente el estado de situación de cada una de las Infraestructuras Críticas de la Argentina y la seguridad de sus ciudadanos. Permite establecer niveles de madurez de forma coordinada. Disminuyendo de esta forma los esfuerzos aislados.

La creación del Comité de Ciberseguridad puede ser un primer paso en esta dirección, para luego conformar una unidad operativa de tipo interagencial.

Si bien la integración cívico-militar y de diferentes actores *con peso* puede imaginarse como compleja, puede ser la oportunidad no solo para cubrir los desafíos en el ciberespacio sino también para posicionar a la Argentina como un actor líder en la región en materia de ciberdefensa.

Estrategias Sectoriales

Como parte de una política pública el Estado deberá considerar el planeamiento de capacidades a desarrollar. Estas capacidades le permitirían a la Argentina alcanzar niveles de madurez propicios para efectuar el aseguramiento de sus Infraestructuras Críticas y de su

[15] Desarrollado en *Ciberdefensa e Infraestructuras Críticas*, LOPEZ LIO, R. Instituto de Inteligencia de las Fuerzas Armadas. 2016

ciberespacio local. A su vez, la materialización de una Interagencia y un Plan Nacional de Ciberdefensa a través de la concreción de estrategias sectoriales que impulsan diferentes proyectos en materia de ciberseguridad y defensa permitirían a la Argentina alcanzar la resiliencia suficiente en este plano. Estas estrategias permitirían a la Argentina su posicionamiento como actor relevante e influyente en la región y el sistema internacional.

Apuntes finales

El ciberespacio ha contribuido a que el mundo se encuentre integrado, gracias al desarrollo económico-tecnológico, vinculando todas las partes del sistema global. Si bien esta integración no se ha logrado desde el punto de vista político-cultural. Las características más fuertes del ciberespacio (velocidad en las comunicaciones, interconexión de redes desde diversos puntos del globo, nuevas concepciones de negocios, manejo de infraestructura) nos muestran que la capacidad de estas redes, con sus carencias de diseño, está disponibles y accesibles para todos los actores. Algunas naciones y grupos sub-nacionales intentan resistir dichos procesos integrativos a fin de afirmar su propia identidad e independencia, las fuerzas transnacionales que confluyen en el ciberespacio emergen en la escena internacional. Las naciones-estado se vuelven cada vez más sensibles y vulnerables a los cambios, la transnacionalidad de los ataques informáticos y la imperfección de los sistemas de seguridad para evitarlos y deben ajustar sus políticas en consecuencia para regular y controlar la actividad internacional.

En el ciberespacio cada uno de los sectores críticos para el funcionamiento de un Estado se encuentra vinculado y expuesto a través de las tecnologías de información. De esta manera, se vislumbran necesidades de coordinación política entre actores tradicionales y no tradicionales para atender a la problemática del ciberespacio, entendido como un todo anárquico y carente de fronteras.

El énfasis liberal en una pluralidad de actores mundiales es quizás un punto de partida como contribución a la construcción de una teoría con respecto a la seguridad en el ciberespacio. No obstante las visiones realistas del Estado como agente clave del sistema y que debe ocuparse de su preservación resultan imprescindibles para que, en nuestro caso

Argentina, se tomen las definiciones pertinentes a fin de trazar una estrategia en lo relativo al ciberespacio y la ciberdefensa.

La integración de los actores, con injerencia en el ciberespacio, en una estructura adecuada podría salvar los inconvenientes legales, dinamizar procedimientos y obtener una visión integral del ciberespacio, las amenazas y la resolución de incidentes.

Bibliografía

- Arquilla, J., & Ronfeldt, D. (1993). Ciberwar is coming! Comparative Strategy.
- Bartolomé, M. (2006). La Seguridad Internacional post 11S: situación, debates, tendencias. Buenos Aires: Instituto de Publicaciones Navales.
- Bejarano, (2013). Poder Blando frente a Poder Duro en el ciberespacio. Instituto Español de Estudios Estratégicos.
- Benedicto Salmerón, R. Teorías y conceptos para entender formas actuales de hacer la guerra. Universitat Autónoma de Barcelona.
- Clarke, R., & Knake, R. (2010). Cyber War. The Next Threat to National Security and what to do about it. Nueva York: Harper Collins.
- Clausewitz, K. V. (2009). De la Guerra. Buenos Aires: Ediciones Libertador
- Gilpin, (1981). War and Change in World Politics.
- Huntington, (1993). The Clash of Civilizations. Foreign Affairs.
- KENNAN, (1985). Morality and Foreign Policy, Foreign Affairs.
- Keohane y Nye, (1998). Power and Interdependence in the information Age, Foreign Affairs.
- Laiño, A. (1991). Una aproximación teórica al concepto de Defensa. Buenos Aires: Centro de Estudios Internacionales.
- Lind, W. (2004). Understanding Fourth Generation War. Military Review.
- LOPEZ LIO, R. (2016). Ciberdefensa e Infraestructuras Críticas. Instituto de Inteligencia de las Fuerzas Armadas.
- METZ, Steven (2001). Strategic Asymmetry.
- MORGENTHAU. (1960). Politics among Nations: The Struggle for Power and Peace.
- Sepúlveda, M. (2007). La Seguridad Internacional ante las nuevas amenazas. En Defensa nacional: dimensiones internacionales y regionales.
- Waltz, (1988) Teoría de la Política Internacional, Grupo Editor Latinoamericano.