UNIVERSIDAD NACIONAL DE LA PLATA

FACULTAD DE CIENCIAS JURÍDICAS Y SOCIALES

MAESTRÍA EN INTELIGENCIA ESTRATÉGICA NACIONAL

TESIS

Inteligencia Nacional y Estrategia de Ciberseguridad Nacional

MAESTRANDO: Ana Alicia Albarracín Keticoglu

DIRECTOR DE TESIS: Rodrigo Cárdenas Holik

2019

Índice

AGRADECIMEINTOS

A mi familia, por el apoyo incondicional;

A los entrevistados y en especial a aquellos que leyeron esta tesis de forma parcial o total para guiarme en el proceso;

Al grupo de investigación de "soberanía nacional y ciberespacio" de la UNDEF porque mi participación en el grupo se ve reflejada en la elaboración de esta tesis;

A mi director, Mg. Rodrigo Cárdenas Holik, por servir de guía en el desarrollo de esta investigación.

ABREVIACIONES

AC3: Área de Capacidad 3 (Vigilancia, Reconocimiento e Inteligencia)

AFI: Agencia Federal de Inteligencia

APN: Administración Pública Nacional

ARSAT: Empresa Argentina de Soluciones Satelitales S.A.

CCCD: Comando Conjunto de Ciberdefensa

CCDCOE: Centro de Excelencia de Cooperación en Ciberdefensa de la OTAN

CERT: Equipo de Respuesta ante Emergencias Informáticas.

CIC: Centro de Ingeniería de Ciberdefensa

CICTE: Comité Interamericano contra el Terrorismo

COC: Centro de Operaciones de Ciberdefensa

CRIDEF: Criptografía para la Defensa

CSIRT: Computer Security Incident Response Team

DGCD: Dirección General de Ciberdefensa

DGPLA: Dirección General de Planeamiento y Estrategia

DINICRI: Dirección Nacional de Inteligencia Criminal

DINIEM: Dirección Nacional de Inteligencia Estratégica Militar

DOC: Dirección Operacional de Inteligencia sobre Ciberseguridad

DPDN: Directiva Política de Defensa Nacional

EMCO: Estado Mayor Conjunto de las Fuerzas Armadas

ENCS: Estrategia Nacional de Ciberseguridad

ENI: Escuela Nacional de Inteligencia

ENISA: Agencia de Seguridad de las Redes y de la Información

FFAA: Fuerzas Armadas

FFSS: Fuerzas de Seguridad

ICIC: Infraestructuras Críticas de la Información y de la Comunicación

IM: Instrumento Militar

INVAP: Investigaciones Aplicadas.

IVR: inteligencia, vigilancia y reconocimiento

MINDEF: Ministerio de Defensa

MINMOD: Ministerio de Modernización

MINSEG: Ministerio de Seguridad

PLANCAMIL: Plan de Capacidades Militares

PROCAMIL: Proyecto de Capacidades Militares

TDA: Televisión Digital Abierta

TICs: Tecnologías de la Investigación y la Comunicación

OEA: Organización de Estados Americanos

ONG: Organización No Gubernamental

ONTI: Oficina Nacional de Tecnologías de la Información

OTAN: Organización del Tratado del Atlántico Norte

UIT: Unión Internacional de Telecomunicaciones

UNDEF: Universidad de la Defensa Nacional

INTRODUCCIÓN

La Inteligencia Nacional[1] tiene la capacidad, a través del ciclo y de la producción de inteligencia, de definir los riesgos, las amenazas y las oportunidades que se le presentan a un Estado ante una determinada situación. Resulta clave la determinación de estos factores para que un Estado tenga la capacidad de aplicar políticas adecuadas ante un determinado problema.

Uno de los factores más importantes de la globalización del siglo XXI resulta ser la difusión de Tecnologías de la Información y de la Comunicación (TICs) que viene de la mano de los avances tecnológicos, la innovación y el desarrollo de ciencia y tecnología y la propagación de lo que se conoce como *Internet of Everything*[2] (Internet de todo).

La interconexión generada a partir de la proliferación de los fenómenos y servicios antes mencionados encierra dos efectos principales. En el marco de esta tesis nos centraremos en los efectos negativos, tomando como base que la proliferación tecnológica no sólo supone mayor potencia de procesamiento de información y su interconexión, sino que también el incremento de los riesgos que trae aparejado el ambiente informático (riesgo inherente) y cómo esto brinda mayores oportunidades para que actores externos intenten explotar tales vulnerabilidades.

Hoy, el ambiente cibernético es definido como un nuevo ecosistema, que sirve como herramienta para actores de diversos tipos, sean estos estatales o no estatales (militares, civiles y paraestatales). De esta forma, el ambiente informático termina siendo escenario de criminalidad organizada y compleja de los cuales antes solamente nos preocupábamos dentro de nuestras fronteras nacionales y que hoy terminan sumergiéndose en las posibilidades que ofrece el ciberespacio para su propagación, financiamiento, reclutamiento, propaganda y solidificación. Permite además, librar la guerra en tiempos de paz, evolucionando la forma de hacer la guerra a través de una ventaja que podríamos denominar como semi-absoluta al suponer que una ventaja en el ciberespacio es capaz de dejar desconectado por completo a los tomadores de decisiones del adversario respecto a sus recursos humanos, tecnológicos e incluso con su población

[1] Según el artículo 2 de la ley 27.126, se entiende por Inteligencia Nacional a la actividad consistente en la obtención, reunión, sistematización y análisis de la información específica referida a los hechos, riesgos y conflictos que afecten la Defensa Nacional y la seguridad interior de la Nación.

[2] Según Cisco, Internet of Everything es la conexión inteligente entre personas, procesos, información y las cosas. Su importancia radica en que vuelve más relevante esa conexión. Concepto extraído de: http://ioeassessment.cisco.com/learn/ioe-faq

civil. La inteligencia en el ciberespacio sirve hoy de herramienta para desarrollar tareas de inteligencia y contrainteligencia, entendida esta última como el conjunto de actividades que apuntan a evitar acciones de espionaje, sabotaje, infiltración y propaganda, dejando en manos de los organismos de inteligencia a la guerra de la información, haciendo de la obtención y denegación de información el objetivo principal en este nuevo tipo de conflicto.

Estas problemáticas no escapan de la realidad regional y nacional. Nuestro país es uno de los países de la región que cuentan con mayor actividad cibernética criminal, por lo que me resulta clave entender los esfuerzos (plasmados a través de políticas públicas en cuestiones de ciberseguridad, ciberdefensa y ciberinteligencia) llevados a cabo por nuestro país para contrarrestar estas amenazas y obtener de la inteligencia estratégica el valor de la información oportuna para la toma de decisiones en este contexto.

Este análisis resulta fundamental para entender e iluminar sobre la evolución y los matices que ha adquirido el fenómeno cibernético en nuestro país logrando visualizar los riesgos, amenazas y oportunidades a los que se enfrenta, a la vez que dilucidamos sobre las causas que hicieron que aún hoy no exista una Estrategia Nacional de Ciberseguridad (ENCS) que defina los lineamientos claves para la obtención de un ciberespacio con menos riesgos.

Ante este interrogante principal, la *hipótesis preliminar* propuesta para servir de guía a esta investigación será la siguiente: la falta de una Estrategia Nacional de Ciberseguridad en Argentina se debe a la incapacidad de definir los lineamientos conceptuales y la eficaz vinculación entre las normas y las políticas desarrolladas.

Siguiendo esta premisa, el *objetivo general* de investigación será el de iluminar sobre los factores que diluyen la definición de una ENCS. A tal efecto, el desarrollo de esta tesis se centrará en responder tres *objetivos específicos* que, en su conjunto, resultan vitales para responder la premisa principal.

Estos tres objetivos son:

- Rastrear información respecto a la influencia del contexto internacional en la definición del Sistema de Ciberseguridad Nacional.
- Iluminar sobre las falencias de las políticas relacionadas a la ciberseguridad[3] y la ciberdefensa[4] puestas en marcha en nuestro país.

[3] Como parte del sistema de seguridad interior.
[4] Como parte del sistema de defensa nacional.

- Indagar sobre el rol de la inteligencia en el trazado de políticas públicas destinadas a los ámbitos de la ciberseguridad y ciberdefensa.

Uno de los principales motivos para desarrollar este tema de tesis es que el fenómeno cibernético afecta cada vez más la vida cotidiana, por lo que ha dejado de ser una amenaza a futuro para convertirse en una amenaza presente que tiene el agravante de mutar sus características de ataque en ataque. De esta forma, la academia tiene la difícil tarea de actuar como enlace y generador de puentes entre quienes son los encargados de tomar las decisiones y la sociedad en general para ayudar a comprender y actuar de la mejor manera posible ante los desafíos que presenta el ambiente cibernético.

Es por lo expuesto que considero importante entender los efectos del fenómeno a partir de la producción de inteligencia, para que la información obtenida sea adecuada, oportuna y ponga de manifiesto las necesidades de nuestro sistema a partir del conocimiento de los riesgos, amenazas y oportunidades a los que se enfrenta nuestro país. Una vez obtenido el conocimiento de la situación, será posible que el nivel político desarrolle un planeamiento estratégico más eficaz y una Estrategia Nacional acorde a la situación particular y a las necesidades a las que nos enfrentamos. En este contexto será importante analizar la vinculación entre el plan de inteligencia nacional y la elaboración de esa estrategia nacional, la cual será de vital importancia para la consecución de los intereses vitales de la Nación y retroalimentará las políticas destinadas a reducir los niveles de incertidumbre que plantea el ciberespacio.

La importancia misma de la investigación radica en conocer el problema, ya que, caso contrario resultará difícil proponer soluciones eficaces. Así, la importancia es de conocimiento: conocer para comprender, conocer para actuar, conocer para prepararnos ante los desafíos que depara el ambiente cibernético y su dinámica evolución.

Dado que el fenómeno cibernético es un área de estudio relativamente nueva para los analistas vinculados a la seguridad internacional, la presente tesis tiene por objeto realizar un aporte a los campos de estudio de inteligencia nutrido de la contribución teórica que hacen reconocidos analistas internacionales sobre cuestiones específicas vinculadas a la ciberseguridad, ciberdefensa y ciberinteligencia. La originalidad de este análisis radicará en visualizar estos tres componentes en un mismo análisis para el caso específico de Argentina, con mayor interés en analizar el rol del Sistema de Inteligencia en el ambiente cibernético, lo cual, hasta la actualidad, se encuentra poco o nada desarrollada.

Dado que se trata de una realidad subjetiva y que se pretende un análisis en profundidad y detalle en relación al tema de estudio, para esta investigación en particular se hizo uso de metodología cualitativa. De ello resulta el análisis del caso argentino a través de diversas técnicas de producción de datos, entre las que encontramos: análisis de documentos, observación no participante y entrevistas a especialistas vinculados a las tres dinámicas de estudio que tuvieron por objeto obtener y registrar sus experiencias en el proceso de evolución de las políticas de ciberseguridad, ciberdefensa y ciberinteligencia en Argentina entre los años 2007 y 2017. Además, la investigación se nutrió de la participación de quien escribe en el proyecto de investigación denominado "Ciberdefensa y soberanía nacional" en el marco de investigación de la Universidad de la Defensa Nacional.

Este documento cuenta con dos partes bien definidas. En primer lugar, un título dedicado a hacer un repaso sobre el estado del arte, en el que se hará una revisión de las investigaciones desarrolladas por la academia anglosajona para luego dar paso a los estudios realizados por académicos argentinos sobre la temática que nos compete. Esta primera parte será complementada con el marco teórico específico utilizado para el análisis de la cuestión.

Respecto al desarrollo de la investigación, esta cuenta con tres capítulos que responden a los objetivos específicos arriba mencionados y que tienen por objeto confrontar la hipótesis preliminar propuesta.

El primer capítulo, rastreará información respecto a la influencia del contexto internacional en la definición del sistema de ciberseguridad nacional, para lo cual, se expondrá sobre las distintas dinámicas que adquiere el fenómeno cibernético como fenómeno de la seguridad internacional para luego analizar sus efectos en el ámbito local y definir si la cuestión cibernética es una amenaza real que asecha a nuestro país.

En un segundo capítulo, se plasmarán las políticas de ciberseguridad y ciberdefensa puestas en marca en nuestro país, haciendo una breve mención a los esfuerzos por digitalizar el país y la Administración Pública Nacional (APN) y la creación de normativas acorde a los problemas vinculados al ambiente cibernético. Este capítulo tiene por objeto vislumbrar la eficiencia de las políticas desarrolladas a lo largo de nuestro período de estudio.

El tercer capítulo, tiene el objetivo de indagar sobre el rol de la inteligencia en el trazado de políticas públicas destinadas a los ámbitos de ciberseguridad y ciberdefensa,

para lo cual se trabajará exhaustivamente la normativa vigente para luego analizar el proceso de intervención de los distintos organismos del Sistema de Inteligencia Nacional en el ciberespacio, sus capacidades y funciones como organismos destinados al análisis de información que tiene por misión nutrir a la toma de decisiones para lograr ciertos estándares de seguridad nacional.

Al finalizar y a modo de cierre de la investigación se confrontará la hipótesis propuesta a partir de las conclusiones preliminares obtenidas de cada capítulo.

PRIMERA PARTE

ESTADO DEL ARTE

En el transcurso del siglo XXI, y especialmente a partir del año 2010, encontramos diversos estudios que toman como unidad de análisis al ciberespacio desde distintas perspectivas.

En cuanto a la percepción de la difusión de las TICs como uno de los aspectos más importantes de la globalización del siglo XXI, algunos autores hablan de una nueva revolución industrial (la cuarta), otros la denominan la revolución de la información, e incluso se refieren a ella como la segunda revolución de las máquinas.

En este sentido se pronuncian Keohane y Nye (1998) en la actualización de sus escritos *poder e interdependencia*, donde profundizan sobre la variable tecnológica que hace a la interdependencia en política internacional. Los autores ven al ciberespacio como un lugar *en todas partes y en ninguna parte*. Establecen que las normas deben regir en el ciberespacio al igual que en el mundo real.

Manifiestan que la revolución de la información no es nueva, sino que lo es el ámbito virtual que nos permite acortar aún más las distancias y obtener información en el instante. Revelan que la política afecta a la revolución de la información tanto como la revolución de la información afecta a la política. Esta revolución altera la interdependencia compleja por la multiplicidad de canales de comunicación que se crean en la política internacional.

Los autores vuelven a recordarnos que la información es poder. Tras esta afirmación, el poder –como recurso– es afectado por esta nueva revolución.

Para Klaus Schwab (2017), el mundo transita hoy la cuarta revolución industrial. Esta revolución se manifiesta a través de la invención de tecnologías cada vez más sofisticadas e integradas que están transformando las sociedades y la economía mundial y menciona que es la fusión de tecnologías y su interacción a través de los dominios físicos, digitales y biológicos lo que hace que la cuarta revolución sea fundamentalmente diferente. Estas transformaciones significan que las empresas necesitan invertir en sistemas de seguridad contra ciberdelitos con el objeto de prevenir ataques por parte de delincuentes o activistas o fallos involuntarios en la infraestructura digital. En este contexto, los gobiernos deben adaptarse al desplazamiento del poder que cada vez más se encuentra del lado de actores no estatales. En definitiva, para el autor, *"es la capacidad de los gobiernos de adaptarse la que determinará su supervivencia."* (p. 93).

En cuanto al estudio propio del ciberespacio, dentro de la academia norteamericana, Singer y Friedman (2014) manifiestan la importancia de analizar las vulnerabilidades del ciberespacio para poder adelantarse a las intrusiones que puedan afectar a los sistemas. Para esto plantean la necesidad de contar con red teams[5], penetration testing[6], contratar expertos en seguridad (no provenientes de la empresa o entidad en la que van a evaluar los riesgos) y/o realizar juegos de simulación de crisis que permite, además de evaluar los riesgos, entrenar a los operarios en manejo de crisis. Estas herramientas resultan de gran utilidad para la producción de inteligencia oportuna que permita tomar las decisiones necesarias para fortalecer la seguridad en el ciberespacio. Algunas de estas actividades se realizan mediante la implementación de metodologías de análisis de riesgo y de modelado de amenazas.

Para Joseph Nye (teórico idealista/liberalista de las relaciones internacionales), los Estados tienen la necesidad de generar un "ciberpoder" o "poder cibernético", el cual es definido como la capacidad de utilizar el ciberespacio para generar ventajas e influenciar eventos que se desarrollen en otro ambiente operacional y a través de los instrumentos de poder. En su rol de asesor, presenta al ciberespacio como un nuevo dominio de gran importancia, ya que sin importar las dimensiones de *hard* y *softpower* que ostente el país en cuestión, actualmente los Estados se ven obligados a compartir escenarios con nuevos y diversos actores, presentándoles mayores dificultades a la hora de controlar las fronteras cibernéticas. (2010).

Por su parte, los analistas de RAND Corporation, John Arquilla y David Ronfeld (1993) introducen los conceptos *Netwar* y *Cyberwar*. Ambos se relacionen con la obtención de información y la forma de comunicación, con la búsqueda de conocimiento que responda las preguntas: ¿Quién sabe qué?, ¿cuándo?, ¿dónde?, ¿por qué?, ¿cuán segura es una sociedad y el instrumento militar del adversario? Lo cual supone la producción de inteligencia, ya que responde a los elementos esenciales de información

Mientras que el primer concepto (*netwar*) se refiere a la obtención de información referente a conflictos de carácter político y social, y su objetivo es tratar de modificar el

[5] Los equipos rojos ayudan a anticipar y explicar las acciones de los adversarios y a explotar las oportunidades de la propia empresa. Tienen por objeto: identificar vulnerabilidades significativas, descubrir nuevos usos de las innovaciones, desafiar suposiciones, brindar un reporte respecto a una nueva idea o concepto propuesto y revelar las consecuencias de las diferentes perspectivas (en particular: riesgos). (IBM, 2005).

[6] Los test de penetración en el sistema tienen por objeto reconocer que tipo de información puede ser obtenida por un atacante, analizar si existen vulnerabilidades en los servidores, intentar explotar vulnerabilidades y realizar informes de inteligencia sobre los resultados obtenidos. (Gómez Vieites, 2007).

conocimiento que posee una determinada sociedad, haciendo hincapié en la opinión pública y las elites a través de diversas herramientas (excepto el instrumento militar); el segundo concepto (*cyberwar*) se refiere a la conducción y su preparación, con el objeto de llevar adelante operaciones militares relativas a la información para así, modificar y eliminar información y sistemas de comunicaciones, prohibir el acceso a la información al adversario y obtener información sobre sus planes de acción.

Estos autores nos permiten apreciar las acepciones que posee la guerra de la información en el poder militar y el rol que cumple la inteligencia dentro de las operaciones que tienen por objeto atacar el ambiente informático.

Hebert Lin (2016) nos habla de la gobernanza de las TICs. Muestra a las ciberarmas como una nueva preocupación y menciona la complejidad de sus estructuras. Diferencia entre ciberataques y ciberexploración, donde entra en juego el ciberespionaje realizado por los Estados que se lleva a cabo en el marco de la inteligencia y que, por ende, resulta enmarcada en las competencias legales que poseen los Estados. Concluye que la gobernanza en el ciberespacio resulta difícil por la naturaleza misma del ecosistema, entre estas características destaca: la facilidad de acceso a material útil para desarrollar ciberarmas, no requieren de infraestructura compleja, la diversidad y difusión de actores, su capacidad de generar consecuencias graves y la gran difusión que posee como instrumento civil.

Respecto a las vulnerabilidades que presenta el ciberespacio, desde el ambiente de la seguridad informática, Kevin Mitnick y William L. Simón[7] (2007) nos muestran que, al ser el hombre imperfecto y la tecnología una creación del hombre, esta supone falencias, errores o vulnerabilidades que pueden ser explotadas por aquellos que conocen sobre su funcionamiento, sean o no especialistas en cuestiones informáticas o simplemente aficionados con interés en estas herramientas. A tal fin, la creatividad y el ingenio no tienen límites a la hora de aprender a identificar y explotar esas vulnerabilidades para beneficio propio, sea que el mismo suponga un rédito económico, satisfacción de necesidades o incluso generar la capacidad de limitar la libertad de acción de otro actor.

Respecto al tema específico de esta tesis (aunque con un estudio de caso diferente al argentino), Miguel Rego[8](2012) nos presenta las consideraciones del Instituto Español

[7] Kevin Mitnick es un ex hacker que actualmente se desarrolla como consultor en temas de seguridad cibernética, mientras que William L. Simón se desarrolla como escritor y guionista.
[8] Director del Instituto Español de Ciberseguridad de ISMS Forum Spain y director ERS-IT de Deloitte

de Ciberseguridad ante la necesidad de establecer una Estrategia de Ciberseguridad Nacional por parte de España (el documento fue realizado antes que España escribiera su estrategia). El autor concluye que la elaboración de inteligencia oportuna y actualizada sobre los problemas que afectan el ciberespacio y un incremento en la cooperación internacional y la articulación entre las diversas agencias del Estado para tratar la problemática, harán que el gobierno pueda asumir la responsabilidad, el liderazgo y la protección efectiva del ciberespacio.

Adentrándonos en la academia argentina, específicamente al área de la Defensa Nacional encontramos autores (civiles y militares), que buscan iluminar las cuestiones de ciberdefensa y ciberseguridad.

Uno de los principales temas de debate de los autores argentinos ronda en la necesidad de incorporar a la ciberdefensa en el marco legal de consenso básico respecto de la división que existe entre la Seguridad Interior y la Defensa Nacional desde la década de 1980.

A tal efecto, Candela Justribó, Sol Gastaldi y Jorge Fernández (2014) esquematizan las políticas llevadas a cabo por nuestro país en materia de ciberseguridad y ciberdefensa y plantean la importancia de la cooperación regional para la defensa nacional argentina ejemplificando los acercamientos con Brasil para llevar a cabo acciones cooperativas en el ambiente cibernético. Los autores concluyen que "se observa de relevancia que la futura Estrategia Nacional de Ciberseguridad vincule pluralmente las demandas de los sectores gubernamentales, los poderes legislativo y judicial, con las demandas del sector privado y de las universidades, así como también de organizaciones no gubernamentales." (p 14).

Las autoras sugieren:

> "Reflexionar sobre la necesidad de llegar a un consenso político y académico sobre los conceptos que envuelve la ciberdefensa para así, aplicarlos al marco legal, y poder llevar a cabo acciones que posibiliten la protección de nuestra infraestructura crítica, brindada por las agencias estatales indicadas para ello. La globalidad que caracteriza al ciberespacio no debe eclipsar el hecho de que las operaciones en el ciberespacio tienen consecuencias sobre el ámbito físico, y por lo tanto, no es ajeno a los límites geográficos que configuran los Estados-Nación." (Gastaldi, Justibró, 2014, p 13).

Además, diferencian entre las acciones cibernéticas que son llevadas a cabo por delincuentes y por las Fuerzas Armadas, siendo estas últimas participes de ciberespionaje

y ciberguerra, mientras que los delincuentes son autores de cibercrimen, ciberterrorismo y hacktivismo.

La importancia de este trabajo radica en la compilación de conceptos elaborados por la academia nacional e internacional referentes al ambiente cibernético y, por ende, las distintas visualizaciones que se hacen sobre la temática desde ambos puntos de vista.

En un tercer documento, las autoras, a partir de la diferenciación entre Defensa Nacional y Seguridad Interior, dividen en tres categorías esenciales al ambiente cibernético para estudiar el fenómeno. Así, proponen diferenciar entre ciberdefensa, ciberseguridad y ciberinteligencia. (Justibró, Gastaldi, 2014).

Esto nos permite distinguir tres categorías de análisis que presentan características propias pero se encuentra interrelacionadas. Así, se pretende redefinir la vinculación de estos tres conceptos a "Ciberseguridad Nacional", extrapolando los componentes de la Seguridad Nacional al sistema de Seguridad Cibernética Nacional.

Eissa, Gastaldi, Poczynok y Zacarías Di Tullio (2014) hacen un reconto de las diversas definiciones de ciberguerra e incursionan en dar respuesta al ¿cuándo las vulneraciones y afecciones del ciberespacio se vuelven competencia del instrumento militar? y, por ende, la respuesta a tales incidentes son considerados parte del paraguas de la Defensa Nacional. Los autores manifiestan que los ciberataques que tienen por objeto afectar a la defensa nacional son aquellos que pretenden perjudicar las infraestructuras críticas del enemigo, dañar el sistema de C4IVR[9], crear oportunidades de ataques a infraestructuras del enemigo y negar sus capacidades. Ante estas amenazas y a partir del marco legal de nuestro país, los autores analizan cuales son las funciones de la defensa nacional argentina en el marco del ciberespacio.

El Cnel. Héctor Flores (2015) considera la necesidad de ser conscientes para poder brindar soluciones eficaces a los nuevos problemas. Define a las cuestiones del ciberespacio dentro del ámbito de la seguridad y la defensa por ser, aún hoy, el Estado el actor central de las Relaciones Internacionales. (Flores: 2015).

Gastaldi y Justibró (2016) desarrollan la política de ciberdefensa implementada por Argentina. Las autoras mencionan que las Fueras Armadas (argentinas y brasileras) identifican como áreas estratégicas: la tecnología nuclear, lo cibernético y lo aeroespacial. Además mencionan la distinción tajante entre defensa y seguridad en Argentina que se traduce directamente al ciberespacio. Introducen aportes sobre el planeamiento

[9] C4IVR = Comando, control, comunicaciones, computación, inteligencia, vigilancia y reconocimiento.

estratégico en esta área y definen como principal desafío el de adquirir capacidades en ciberdefensa.

Eduardo Alfredo Leiva (2015) realiza un estudio comparativo de Estrategias Nacionales de Ciberseguridad (ENCS) y brinda un panorama de la situación general en Argentina. El autor toma la definición de Estrategia Nacional de Ciberseguridad brindada por Luiijf: *"un plan de acción nacional sobre la base de una visión nacional para lograr un conjunto de objetivos que contribuyan a la seguridad del ciberespacio*" [Luiijf et al.,2013] (p.163) estableciendo que la misma,

> "Se encuentra a un alto nivel en la pirámide organizacional de una nación, y establece una serie de objetivos nacionales y prioridades que deben alcanzarse en un plazo determinado. Como tal, proporciona un marco estratégico para la implementación de un Sistema de Ciberseguridad Nacional, que se entiende como un conjunto de órganos, organismos y procedimientos que permiten la dirección, control y gestión de la Ciberseguridad." (Leiva, 2015, p 163).

De esta forma, el especialista en informática nos da un panorama de la importancia estratégica de definir una ENCS para nuestro país.

En cuanto a la ciberdefensa en el ámbito de la UNASUR, Candela Justibró (2014) y Gilberto Aranda Bustamante y otros (2015), hacen un recorrido por la creación del CDS y la implementación de la temática (defensa cibernética) entre sus planes de acción. Ambos documentos reconocen que la inserción de la temática en la agenda regional fue impulsada por Argentina y Brasil. El segundo trabajo plantea la necesidad de construir la ciberpaz para así afianzar a la región como zona de paz, aunque no explica el término utilizado que puede llegar a ser considerado de fácil deducción.

En cuanto al sector de Organizaciones Regionales, el informe sobre Ciberseguridad de 2016 realizado por el BID nos muestra, en primera instancia, un panorama general de la situación actual de la región en temas de cooperación, tendencias de la seguridad cibernética, el estado normativo y como afectan las cuestiones cibernéticas al desarrollo económico y sostenible, mientras que, en una segunda parte realiza un breve análisis de las tendencias cibernéticas de cada país de la región.

Con esta muestra significativa de estudios realizados por la academia nacional e internacional sobre el ciberespacio, resulta interesante desarrollar una investigación que contemple no sólo cuestiones de ciberdefensa y su impacto en la defensa nacional (lo cual fue más desarrollado por los académicos argentinos), sino abarcar un amplio espectro de

estudio que contemple las cuestiones de ciberseguridad, ciberinteligencia y ciberdefensa y su manifestación en Argentina.

MARCO TEÓRICO

Aunque los escritos referidos al ciberespacio no contemplan una visión teórica en particular o no existe alguna que se adapte por completo al estudio de este espacio, el desarrollo de esta tesis tendrá como guía para el análisis los postulados realistas de las Relaciones Internacionales. Estos aportes se centran en los conceptos básicos de la teoría clásica, para dar lugar a los aportes del neorrealismo.

En primera instancia, el modelo planteado por el padre del realismo, Hans Morgenthau, nos permite analizar las relaciones internacionales a través de una concepción estatocéntrica, donde el Estado se presenta como el único actor digno de consideración en el sistema internacional gracias a su carácter político. Aunque este punto supone una debilidad para el análisis del ciberespacio dada la diversidad de actores que entran en juego en este nuevo dominio, cabe resaltar, que este análisis se centrará en el accionar del Estado Argentino ante el fenómeno cibernético, lo cual nos abre la posibilidad de analizar la problemática desde esta postura del realismo.

El autor presenta dos nociones de análisis. La primera de ellas se refiere al interés nacional, el cual es presentado como la esencia de la política y es ajeno a circunstancias de tiempo y lugar. El autor plantea que el tipo de interés depende del contexto político y cultural dentro del cual se formula la política exterior. Para él, el interés nacional de cualquier Estado siempre será preservar su existencia y supervivencia, volviendo a la política exterior racional. La segunda noción se refiere al equilibrio de poder, el cual resulta de la acción política de los Estados.

Para Hans Morgenthau, solamente una política exterior racional es capaz de minimizar los riesgos y maximizar los beneficios, cumpliendo con el precepto moral de la prudencia y el requerimiento del éxito.

Por otra parte, el autor se refiere a la sociedad internacional en términos hobbesianos, estableciendo que sin un poder centralizado, el sistema internacional es por naturaleza conflictivo, dado que coexisten múltiples unidades que son antagónicas entre ellas.

Para él, el Estado, al tener el poder supremo dentro del territorio, tiene el deber de guardar la paz y el orden (política interna). En este sentido, se analizará el rol del Estado argentino como proveedor de la seguridad con el objeto de contrarrestar los efectos del fenómeno cibernético.

Raymond Aron destaca:

> "Debido a la existencia de múltiples unidades políticas autónomas, el objetivo principal de cada unidad es asegurar su seguridad y, en última instancia, su supervivencia. […] En las relaciones internacionales, los diplomáticos-estrategas enfrentan el riesgo de la guerra desde que se enfrentan con oponentes en una situación de <<incesante rivalidad en la cual cada lado se reserva el derecho a recurrir a la razón última, es decir, a la violencia>> En la conceptualización de Aron, las relaciones entre las naciones a menudo están marcadas por el conflicto, si bien la esencia de la política no descansa, en su opinión, exclusivamente en una lucha por el poder. Esencialmente, las relaciones entre unidades políticas consisten en las alternativas de la guerra y la paz, dado que toda colectividad existe entre partes amigas y enemigas, neutrales o indiferentes. El estatus de las unidades políticas está determinado por los recursos materiales o humanos que puedan atribuirle a la acción diplomática-estratégica." (Dougherty y Pfaltzgraff, 1990, p 126 - 127).

Siguiendo los postulados planteados por Raymond Aron es posible analizar el fenómeno cibernético como una alternativa tanto a la guerra como a la paz, proyectando que las capacidades cibernéticas no sólo son una nueva forma de hacer la guerra sino que también implica una forma de hacer la guerra en tiempos de paz, tal como se analizará al tratar los temas de ciberdefensa.

Partiendo de la base de los supuestos planteados por ambos autores, la protección de los intereses vitales de una Nación y, especialmente, su supervivencia son los objetivos últimos e indiscutibles de los Estados. La articulación del Estado hoy en día se encuentra condicionada por el funcionamiento del ciberespacio, lo que vuelve a este un dominio de gran importancia para la Seguridad Nacional. Así, en términos realistas, los gobiernos deberían prestarle especial atención a la seguridad ciberespacial dada la magnitud que posee este ecosistema en la vida del hombre y en los intereses de las naciones. De esta manera, nos centraremos en el análisis de un fenómeno que asecha la seguridad nacional e internacional y, por ende, desde la óptica del realismo, merece especial atención.

Siguiendo esta misma línea de pensamiento, Kenneth N. Waltz (1988), autor por antonomasia del realismo estructural, propone analizar la política (tanto doméstica como internacional) como una estructura, es decir, como unidades yuxtapuestas de diferentes maneras que se comportan también de formas diferentes y que, por lo tanto, producen resultados distintos.

Para el autor, debe examinarse la estructura de la política doméstica a fin de señalar una distinción entre expectativas acerca de la conducta y los resultados que obtienen las naciones en el plano interno y externo, para así poder comprender la política internacional.

Define a la estructura política doméstica según a) el principio que ordena: es decir, sus partes se encuentran en relaciones de supra/sub/ordinación: algunas están autorizadas a ordenar mientras que otras tienen el deber de obedecer; b) el carácter de las unidades: se refiere a la especificidad de las funciones de las unidades diferenciadas y c) por la distribución de capacidades que poseen dichas unidades, es decir, la atribución de mayores o menores capacidades para desempeñar tareas similares.

Kenneth Waltz establece que los problemas se presentan a nivel global, pero las soluciones que se dan, dependen de la política nacional, ya que cada Estado es el único responsable de resguardar su supervivencia. De esta forma, la posibilidad de desarrollar una acción efectiva depende en gran medida de obtener los medios necesarios, pero depende más aún de la existencia de condiciones que permitan a las naciones y otras organizaciones a seguir las políticas y estrategias apropiadas para contrarrestar las amenazas.

Tomando este aspecto como clave se analizará la política doméstica desarrollada por Argentina a fin de dar respuesta al fenómeno cibernético, haciendo hincapié en el rol de las estructuras que toman parte en la lucha contra dicho fenómeno, los medios de los que disponen y la falta de una estrategia a nivel nacional y de las respectivas estrategias sectoriales (dependiente de cada ministerio interviniente).

Cuando nos referimos a amenazas, Steven Lobell (2009), se refiere al Estado como nexo entre la política doméstica e internacional.

El autor se refiere a los preceptos de los realistas defensivos, que establecen que en el nivel sistémico (global) el sistema internacional empuja a los Estados a perseguir su supervivencia y seguridad, por lo que la maximización de poder relativo conlleva comportamientos de contra-balance (de poder), haciendo que el Estado expanda sus capacidades según se vea forzado por el entorno o Estados agresores. En cambio, para el realismo ofensivo, el sistema internacional empuja a los Estados a maximizar su cuota relativa de poder mundial para asegurarse, en síntesis, a mayor poder y fuerza del Estado, menor es la amenaza.

En el segundo nivel (sub-sistémico o regional), la competencia ocurre entre los actores regionales más relevantes. Estos tienen por objetivo ejercer el liderazgo o hegemonía en la región. En cambio, en el tercer nivel (doméstico) la competencia se da entre actores internos, así el Estado es el representante de grupos de poder que tienen la capacidad de ejercer influencia. El Estado, en definitiva, se ocupa de la distribución de los efectos de la política exterior en el balance interno de poder político y económico.

En conclusión, el rol del Estado en el primer y segundo nivel es la búsqueda y obtención de poder e influencia, mientras que en el tercer nivel, se centra en la redistribución de los efectos de la política exterior en la vida doméstica propia.

De esta forma, el Estado tiene la capacidad de evaluar los riesgos en todos los niveles, amenazas que emanan de otros actores (grandes potencias, actores regionales y locales), amenazas según la distribución de poder, de manipular el poder político y económico y de manipular actores domésticos y grupos de interés de otros Estados.

En su afán por vislumbrar cómo identifican las amenazas los Estados desde una óptica neorrealista, menciona que los Estados deben detectar cuáles son las amenazas a las que se enfrentan y que esta identificación de amenazas no siempre resulta oportuna, dado que si los Estados se enfocan en una sola amenaza o en una equivocada, entonces resulta difícil entender las motivaciones e intenciones detrás de la política exterior de los Estados.

Para el autor la definición de amenazas está basada en los componentes específicos de poder. Así, la percepción de las amenazas depende de qué componente de poder se vea amenazado o en riesgo. Entre los componentes de poder, el autor incluye los siguientes factores: territorio, población, ideología, industria y poder militar. Así, diferente componente de poder significa también diferente amenaza. De esta forma, la identificación errónea del componente de poder que se ve amenazado significa que los Estados apliquen políticas que tomen como eje el componente de poder equivocado respecto de sus intereses, y por ende, las políticas aplicadas resultan nada eficientes.

Además, para el autor, el Estado es el encargado de desarrollar y formular la gran estrategia con el objeto de maximizar la seguridad nacional. Esta gran estrategia debe incorporar los componentes de poder adecuado y no centrarse únicamente en el poder militar, implica un planeamiento a largo plazo y su ejecución en tiempos de guerra y de paz.

Siguiendo lo planteado por Lobbell, cabe analizar si nuestro país está haciendo una apreciación de amenazas adecuada, si el fenómeno cibernético es o no una amenaza para la Argentina y cuáles son los componentes de poder que utiliza para contrarrestarla partiendo de su percepción de amenazas.

Ahora bien, resulta imprescindible analizar el fenómeno cibernético desde una teoría específica. De esta forma, encontramos una teoría preliminar propuesta por Stuart Starr (2009). Con el objeto de ser de utilidad para los tomadores de decisiones, el autor plantea la problemática a través de diversas variables.

Realiza una pirámide como marco holístico que tiene de base toda infraestructura relacionada al ciberespacio, es decir: componentes, sistemas y sistemas de sistemas que se encuentran interconectadas con los niveles de poder (P/DIME: político/diplomático, informático, militar y económico) que sientan las bases para el empoderamiento de entidades que se encuentran en la parte superior de la pirámide (pueden ser desde individuos hasta terroristas, criminales transnacionales, Estados-Nación, Organizaciones Internacionales, corporaciones y más). Estos tres componentes se encuentran afectados en todo momento por reglas institucionales, como ser: gobierno, consideraciones legales, regulaciones, información compartida y consideración de libertades civiles.

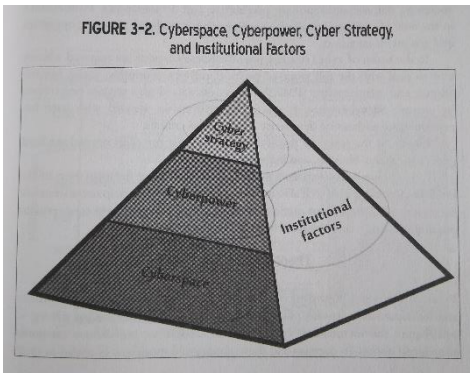
El autor toma el concepto de ciberespacio propuesto en la National Military Strategy for Cyberspace Operations de 2006 que lo define como: *"an operational domain whose distinctive and unique character is framed by the use of electronics and the electromagnetic spectrum to create, store, modify, exchange, and exploit information via interconnected and internetted information systems and their associated infrastructures."* (Starr, 2009, p 47 – 48). Es decir, un dominio operacional cuyo carácter distintivo y único se encuentra enmarcado por el uso de la electrónica y el espectro electromagnético para crear, almacenar, modificar, intercambiar y explotar información a través de sistemas de información interconectados e internet y sus infraestructuras asociadas.

A la vez, define ciberpoder como *"the ability to use cyberspace to create advantages and influence events in the other operational environments and across the instruments of power (P/DIME paradigm). The emphasis is placed on the military and informational levers of power."* (Starr, 2009, p 48). Es decir, la habilidad de usar el ciberespacio para crear ventajas e influenciar en eventos en otros entornos operativos y en todos los instrumentos de poder (con énfasis en lo militar y palancas informativas de poder)

Se refiere a ciberestrategia de la siguiente manera: *"development and employment of capability to operate in cyberspace, integrated and coordinated with the other operational domains, to achieve or support the achievement of objectives across the elements of national power."*(Starr, 2009, p 48). Es decir, el desarrollo y empleo de capacidades para operar en el ciberespacio de forma integrada y coordinada con los otros dominios operacionales (tierra, mar, aire, espacio exterior) a fin de lograr o apoyar el logro de los objetivos a partir de todos los elementos de poder nacional.

Con estos conceptos, el autor recrea la imagen de la pirámide y, esta vez, pone en la cúspide a la ciberestrategia, en la base el ciberespacio y en el medio el ciberpoder. Todos estos, vuelven a estar afectados por factores institucionales.

Gráfico 1 (Starr: 2009)



La imagen de esta nueva pirámide nos muestra la importancia de la estrategia en el ambiente cibernético. Sin el planeamiento oportuno realizado desde el más alto nivel resulta casi imposible establecer la correcta relación entre las capacidades (ciberpoder) y el objeto a proteger (ciberespacio).

Este marco, sirve a los efectos de la investigación porque nos permite analizar el rol de la ciberestrategia, analizar las falencias institucionales que dan aviso e iluminan la problemática de no definir una Estrategia Nacional destinada al área de la Ciberseguridad.

Estudiar la ciberestrategia en los términos propuestos por Starr nos permite adentrarnos en cuestiones tales como: actores, normas, potenciales adversarios que pretendan explotar las vulnerabilidades, las diversas actividades (perjudiciales) que se realizan en el ciberespacio, sin dejar de lado aquellos factores institucionales que afectan (según la pirámide propuesta por el autor) a la ciberestrategia (y demás componentes).

En este marco, Daniel T. Kuebl (2009) habla del ciberpoder como medio para desarrollar y ejecutar la política. Mencionando que en cuestiones domésticas, el ciberpoder, sirve para conectar al gobierno con el pueblo y brindar nuevos servicios, mientras que en cuestiones de política internacional cada vez es más usado el *smartpower* para perseguir objetivos estratégicos. Para el autor:

> "Cyber strategy is the development and employment of strategic capabilities to operate in cyberspace, integrated and coordinated with the other operational

domains, to achieve or support the achievement of objectives across the elements of national power in support of national security strategy."[10] (Kuebl, 2009, p 40).

Según el autor, para desarrollar una ciberestrategia es necesario crear cibercapacidades que ayuden al logro y consecución de los objetivos propuestos en esta estrategia, ya que gran parte de la misma debe estar destinada a describir de qué forma serán utilizadas estas capacidades.

Stuart Starr (2011) nos muestra que es necesario que el tomador de decisiones se adelante a los hechos y conozca las vulnerabilidades para así poder adelantarse a los ataques cibernéticos. Para el autor:

> "In the area of cyberspace, it is important to perform technology projections to identify potential key breakthroughs (e.g., cloud computing); explore options to enhance attribution in cyberspace; develop techniques to protect essential data from exfiltration or corruption; and formulate an objective network architecture that is more secure and identify options to transition to it."[11] (Starr, 2011, p 23)

De esta forma, el autor nos permite recordar la importancia de desarrollar tareas de inteligencia que nos sea oportuna con el objeto de adelantarnos a los hechos y prevenir ataques. En este sentido, la idea principal de esta tesis manifiesta la importancia de la información y el conocimiento oportuno. Es por ello que, además de guiarnos por los preceptos que rigen las relaciones internacionales desde la óptica de la teoría del realismo clásico y el neorrealismo, se trabajará con aquellas ideas emanadas de distintos autores que resaltan la importancia de la obtención de información para la toma de decisiones, lo cual pone énfasis en la importancia de esta tesis como parte de una Maestría en Inteligencia Estratégica que busca, en última instancia, la prevención de escenarios disruptivos en el ciberespacio.

En este sentido, Sun Tzu en el "Arte de la Guerra" ([1958] 2007) describe la importancia del conocimiento al mencionar que es imposible ganar una batalla sin conocer las capacidades propias y las del enemigo, mientras que es menos riesgoso entrar

[10] Ciberestrategia es el desarrollo y empleo de capacidades estratégicas para operar en el ciberespacio, de forma integrada y coordinada con otros dominios operacionales, para dar soporte a los objetivos a través de los elementos de poder nacional en soporte de la estrategia de seguridad nacional. (Traducción propia).

[11] En el área del ciberespacio, es importante realizar proyecciones tecnológicas para identificar potenciales avances, explorar opciones para mejorar atribuciones en el ciberespacio, desarrollar técnicas para proteger información esencial de infliltración o corrupción, y formular una arquitectura de red objetiva que sea más segura y permita identificar opciones para hacer la transición. (Traducción propia)

en combate cuando se conoce la situación de uno mismo y es casi imposible perder cuando además se cuenta con conocimiento del adversario, es decir, un completo conocimiento del contexto y de la situación estratégica.

Para el autor:

> Solamente un gobernante brillante o un general sabio, que pueda utilizar a los más inteligentes para el espionaje, puede estar seguro de la victoria. El espionaje es esencial para las operaciones militares, y los ejércitos dependen de él para llevar a cabo sus acciones. No será ventajoso para el ejército actuar sin conocer la situación del enemigo, y conocer la situación del enemigo no es posible sin el espionaje. (SunTzu, [1958] 2007, p 93-94).

El autor, si bien escribe sobre el uso de las fuerzas armadas, consigue demostrar la incapacidad de llevar adelante cualquier acción si no se cuenta con la información adecuada, entendiendo a ésta como oportuna (tiempo) y pertinente (objeto).

Es en este punto en el que radica la importancia del autor para la investigación. La necesidad de realizar análisis de inteligencia se da por la importancia del conocimiento, que por sí mismo supone una ventaja a la hora de enfrentarnos a nuestros oponentes y de ser conscientes de los puntos débiles propios y del adversario que pueden ser explotados. Al tener conocimiento de estos hechos, los encargados de tomar decisiones tienen la posibilidad de palear las fallas a las que se enfrentan.

Otro autor de gran peso para la investigación propuesta es Nassim Nicholas Taleb ([2007] 2016). La teoría del Cisne Negro nos hace reflexionar sobre aquellos sucesos considerados improbables que cuando suceden, tienen grandes efectos. Al ser considerados improbables no nos preparamos para enfrentarlos, motivo por el cual las consecuencias del suceso resultan catastróficas.

El autor sostiene que "*en el mundo moderno dominan los sucesos raros…hoy día las fuentes de los Cisnes Negros se han multiplicado más de lo que se puede medir*." (Taleb, [2007] 2016, p 113).

El concepto puede ser aplicado para las cuestiones de ciberseguridad y ciberdefensa en Argentina, donde las políticas implementadas resultan insuficientes para la complejidad de las amenazas que acechan al ciberespacio dado que se considera altamente improbable que algunas de esas amenazas surtan efectos en nuestro país o bien, que la relación costo-beneficio de invertir lo necesario en estas cuestiones resulta muy

costoso teniendo en cuenta las probabilidades de que ocurran hechos que tengan consecuencias graves.

Así, el escepticismo sobre la posibilidad de que ocurra un hecho trascendente en el ciberespacio potencia las vulnerabilidades y, por ende, la probabilidad de que tenga lugar un hecho de tal envergadura. La teoría del cisne negro nos sirve, entonces, para justificar el por qué debemos mantenernos preparados.

SEGUNDA PARTE

CAPÍTULO 1
ANÁLISIS DE LA SITUACIÓN ESTRATÉGICA

Introducción

Uno de los factores más importantes de la globalización del siglo XXI es la difusión de TICs. La inmensidad de lo virtual y sus posibilidades, generan que el ambiente informático sea escenario de crimen organizado, tareas de inteligencia e incluso de la guerra. Siendo la cuestión cibernética un fenómeno global que afecta la seguridad internacional, el presente capítulo persigue el objetivo de rastrear información respecto a la influencia del contexto internacional en la definición del sistema de Ciberseguridad Nacional de nuestro país.

En los términos planteados por Kenneth Waltz, los problemas a la seguridad internacional se presentan a nivel global, pero las soluciones son de carácter nacional ya que dependen de la política doméstica de los Estados, por ser éste el único responsable de resguardar su supervivencia.

Siguiendo a Steven Lobell (2009), vemos que el Estado tiene la tarea de detectar cuáles son las amenazas a las que se enfrenta e identificar cuáles son los componentes de poder (territorio, población, ideología, industria y poder militar) en riesgo a partir de la percepción de amenazas. En este sentido, se analizará al ciberespacio como un fenómeno multifacético capaz de poner en riesgo diversos factores de poder desde la óptica arriba mencionada.

Entonces, cabe preguntarnos: ¿la cuestión ciber es una problemática que afecta directamente al Estado argentino o es simplemente una interpretación errónea de las amenazas globales que se identifican como propias de la República Argentina? Aunque esta tesis parte de la base de que el fenómeno cibernético es una amenaza real para nuestro país, en este capítulo se pondrá en duda dicha premisa con el objeto de verificar su veracidad.

Con el fin de responder al objetivo planteado, este capítulo estará dividido en tres instancias que intentarán responder cómo influye el contexto internacional en la definición del sistema de ciberseguridad nacional y si la cuestión cibernética es en realidad una amenaza real para la Argentina.

Para esto, una primera instancia, y a modo ilustrativo, nos brinda un panorama general de cómo el fenómeno cibernético cobra forma en cuestiones de seguridad, defensa e inteligencia en el ambiente global, utilizando datos que revelan la importancia de este

fenómeno para el mundo. Entre ellos, los más importantes son los ciberataques que nos permiten ejemplificar las vulnerabilidades de los Estados ante ataques perpetuados por cibercriminales, operaciones de inteligencia, e incluso por las fuerzas armadas.

Una segunda instancia se refiere a cuál es el grado de exposición de nuestro país ante incidentes cibernéticos. Para esto, se trabajó con una pequeña muestra de los ciberataques más significativos que tuvieron lugar en la Argentina durante los últimos diez años y que lograron evidenciar el grado de vulnerabilidad de nuestro país ante el fenómeno. Estudios de empresas de seguridad informática y mapas de ciberataques en tiempo real complementan este panorama.

En última instancia, se expondrá sobre los distintos tipos de respuesta que dio la comunidad internacional ante el fenómeno en cuestión. Este apartado se hace eco de las distintas iniciativas, tanto individuales como colectivas que instrumentó la comunidad internacional ante la necesidad de dar respuesta a incidentes cibernéticos. Partiendo de la base del Índice Global de Ciberseguridad, se hará referencia solamente a algunos de los instrumentos que componen las cinco categorías de análisis de la Unión Internacional de Telecomunicaciones (de ahora en más UIT). Es en éste apartado donde se hará mención a las buenas prácticas internacionales que surtieron efectos en nuestro país y que lograron nutrir el sistema de Ciberseguridad Nacional en Argentina.

A. La cuestión cibernética como fenómeno de la seguridad internacional

Uno de los factores más importantes de la globalización del siglo XXI resulta ser la difusión de Tecnologías de la Información y de la Comunicación (TIC's) que viene de la mano de los avances tecnológicos, la innovación, el desarrollo de ciencia y tecnología y la propagación de lo que se conoce como *Internet of Everything*[12] (Internet de todo).

Hoy, el ambiente cibernético es definido como un nuevo ecosistema, que sirve como herramienta de militares (teatro de operaciones), civiles (cibercriminales, hacktivistas, hackers, crackers, phreakers y otras alimañas) y paraestatales (ciberterroristas).

[12] Según Cisco, Internet of Everything es la conexión inteligente entre personas, procesos, información y las cosas. Su importancia radica en que vuelve más relevante esa conexión. Concepto extraído de: CISCO. Internet of Everything FAQ. (Consultado el 7 de septiembre de 2017). Recuperado de: http://ioeassessment.cisco.com/learn/ioe-faq

La diversidad de actores y objetivos nos lleva a analizar la problemática desde tres puntos de vista diferentes, la seguridad, la defensa y la inteligencia. Esto nos permite vislumbrar el espectro del fenómeno cibernético en todas sus dimensiones.

En palabras de Klaus Schwab (2017), la cuarta revolución industrial, los avances tecnológicos y la brecha cada vez más marcada de desigualdad social que esta genera, conlleva un cambio en el carácter de las amenazas a la seguridad internacional, ya que, entre otras cosas, ofrece a los individuos cada vez más maneras de dañar al otro en gran escala, produciendo así una mayor sensación de vulnerabilidad.

a. Seguridad

Los espacios tradicionales donde se desarrollaron históricamente los fenómenos que acechan a la seguridad internacional hoy se han visto complementados por un nuevo espacio en el que es imposible hablar de soberanía territorial[13] en términos clásicos. La inmensidad de lo virtual y sus posibilidades generan que el ambiente informático sea escenario de criminalidad organizada y compleja. Delitos de los cuales antes sólo nos preocupábamos dentro de nuestras fronteras nacionales, hoy terminan sumergiéndose en las posibilidades que ofrece el ciberespacio para su propagación, financiamiento, reclutamiento, propaganda y solidificación.

Para Juan Salom Clotet (2010), casi no podemos imaginar la realización de cualquier delito sin que los medios tecnológicos aparezcan ya que prácticamente todo cabe en estos medios, lo que hace a la idea de ciberdelitos cada vez más amplia y global.

Tal como lo expresa la Estrategia Internacional para el Ciberespacio (norteamericana), *"las amenazas de seguridad cibernética pueden poner en peligro la paz y la seguridad internacionales en general, a medida que las formas tradicionales de conflicto se extienden al ciberespacio."* (White House: 2011, p 4).

De esta manera, encontramos que delitos tales como el robo de información, usurpación de identidades, los secuestros extorsivos, el grooming, el tráfico ilícito de estupefacientes, de armas, de pornografía infantil; la producción y comercialización de material apócrifo (piratería); la promoción de ideales que tienen la capacidad de crear lobos solitarios o coyotes[14], grupos subversivos y hasta de desestabilizar a un Estado;

[13] Según Von Heinegg (2013), cuando hablamos de soberanía territorial, estamos hablando de independencia. Independencia de un territorio para ejercer funciones de forma exclusiva ante cualquier otro Estado.

[14] Término utilizado en España, ya que se considera que un lobo por naturaleza siempre actúa en conjunto con la manada, mientras que el coyote si actúa de forma separada al resto de su especie.

delitos financieros; ataques contra la infraestructura crítica (IC) de una nación; entre otros; son algunos de los delitos que hoy adquieren forma en el ciberespacio.

Con el objeto de vislumbrar la magnitud del fenómeno, cabe resaltar algunos de los datos aportados por organismos internacionales que han estudiado la cuestión cibernética.

En primera instancia, Naciones Unidas nos muestra las formas que adquiere el cibercrimen y cómo afectan, con distintas dinámicas, a las regiones de todo el globo. En general, el fraude o falsificación informática fue el delito más común en todas las regiones durante 2013, mientras que acciones que involucran la xenofobia y el racismo dentro del entorno digital fueron las menos extendidas. La producción, distribución o posesión informática de pornografía infantil es la modalidad de cibercrimen que más acecha a Europa y América, seguido por actos informáticos que causan daños personales que se dirigen, principalmente, contra los usuarios residentes en África y América. (UNDOC: 2013).

Según datos aportados por *The Global Risk Report 2018* del Foro Económico Mundial (WEF por sus siglas en inglés), los riesgos cibernéticos se han incrementado en el año 2017 al igual que en los últimos cinco años, por lo que se espera que sigan en aumento en 2018 y los años venideros. Por una parte, el comercio a través de la dark web[15] ha intensificado sus ventas en el año 2016 gracias a la accesibilidad que ofrece para los ciberatacantes ya que, solamente en el año 2016, 357 millones de nuevas variantes de código malicioso (malware) fueros relanzadas, mientras troyanos destinados a corromper la seguridad del sector bancario fueron cotizados en alrededor de los 500 dólares, resultando altamente atractivo para aquellos interesados en la comisión de estos delitos. (WEF: 2018).

Según muestra este mismo informe, de los cinco principales riesgos probables, los ciberataques ocupan la tercera posición, siendo el robo de datos el cuarto en la lista, mientras que el resto de los riesgos se encuentran relacionados a cuestiones ambientales. En cuestión de impacto de los principales riesgos, la tabla de posicionamientos cambia de manera radical desplazando la cuestión cibernética para dar lugar a cuestiones sociales y de geopolítica. Esto, puede deberse a diversas cuestiones, ejemplo de ello es que muchas

[15] El término “se refiere a sitios con fines delictivos o contenido ilegal, y a sitios "comerciales" donde los usuarios pueden adquirir bienes o servicios ilícitos.” En contraposición, el término Deep web “se refiere a todas las páginas web que los motores de búsqueda no pueden identificar.” Término extraído de Kaspersky Lab (consultado el 3 de abril de 2019 en https://www.kaspersky.es/resource-center/threats/deep-web)

veces las ciberamenazas solamente cobran notoriedad cuando afecta a millones de usuarios al mismo tiempo, o divulga documentos confidenciales de los Estados, o afecta gravemente el funcionamiento empresarial o la vida de los particulares.

Cientos de ejemplos ponen al descubierto la relevancia de la cuestión cibernética en el sistema internacional, entre los más notorios encontramos: 1) WannaCry: en el año 2017 el *ransomware* afectó alrededor de 300.000 computadoras a nivel mundial, dispersando sus efectos en cerca de 150 países en cuestión de horas, logrando poner en jaque la seguridad de entidades dedicadas a las finanzas, la salud, las telecomunicaciones, el gobierno y otras instituciones; 2) el escándalo de la filtración de datos de Facebook a Cambridge Analytica a través de la aplicación "This is Your Digital Life" que logró reunir datos de miles de usuarios, la cual pasó a manos de Cambridge Analytica con el objeto de influir en las decisiones de esos usuarios (especialmente en época electoral).

El ejemplo clásico de ciberataque que desestabilizó a un país es el ocurrido en Estonia en el año 2007 (Lewis: 2016), cuando una serie de ciberataques sin precedentes se dio en medio de la pugna (entre Rusia y Estonia) por la reubicación de un monumento de la era soviética. La dependencia a fuentes de tecnologías de la información por parte de Estonia fue explotada a través de diversos ataques cibernéticos que tuvieron lugar en el transcurso de un mes, resultando de ello la necesidad de las autoridades de desconectar el país por completo en el plazo de 48 horas. De esta forma, sus sistemas informáticos quedaron bloqueados y se interrumpió todo tipo de servicio para detener los ataques realizados contra las IC del país. A posteriori, y de manera preventiva, la OTAN junto con Estonia crearon el Centro de Excelencia de Cooperación en Ciberdefensa[16] en el año 2008, a partir del cual reconocieron al ciberespacio como el quinto dominio en el cual se expande la responsabilidad de los aliados por cooperar en materia de defensa (principalmente) y seguridad.

Estos datos muestran que la capacidad de los ciberataques destinados al ámbito de la seguridad de las empresas, las naciones y los particulares, son cada vez más amplias y efectivas. Millones de dólares son robados mensualmente a través de herramientas digitales, por lo que el costo financiero de mantener seguro los sistemas es cada vez mayor, ya que existe diversidad de atacantes y modalidades utilizadas por los actores cibernéticos para la consecución de sus alimañas.

[16] CCDCOE. "About us" (consultado el 12 de mayo de 2018 en https://ccdcoe.org/about-us/)

Jurídicamente, resulta sencillo alegar que se trata de delitos tradicionales que cobran forma a través de la herramienta digital, que incluso encajan en las definiciones penales tradicionales y, por ende, sería oportuno hablar del ciberespacio como medio de comisión de delitos y no como un fenómeno en sí mismo. Hay quienes defienden la necesidad de definir como nuevos delitos a aquellos que adquieren forma en el ciberespacio.

La segunda postura es la asumida por los líderes mundiales, quienes han intentado, por diversos medios, tipificar las cuestiones referentes a la ciberseguridad y la ciberdefensa de los Estados. Un instrumento internacional que hace a la tipificación de estos delitos es el Convenio sobre la Ciberdelincuencia, más conocido como Convención de Budapest que, en el año 2001 se hizo eco de la problemática y llamó a los Estados parte del Consejo de Europa y otros a aplicar una política penal común con el objeto de proteger a la sociedad de la ciberdelincuencia. La convención insta a los Estados a tipificar delitos tales como el acceso ilícito, la interceptación ilegal de datos informáticos, los ataques contra la integridad de los datos, aquellos relacionados con la pornografía infantil, el fraude y la falsificación informática y otros. Además, esta iniciativa refuerza la cooperación internacional en procedimientos relativos a delitos relacionados con sistemas y datos informáticos y para la obtención de pruebas. (Consejo de Europa: 2001).

Lo cierto es que, si bien los ciberdelitos representan la manifestación de los delitos tradicionales en el ciberespacio, las TICs se han convertido en medio y facilitador de la comisión de delitos de diversa envergadura, pero también en la finalidad de estos. Esto se debe a las características particulares que presenta este nuevo escenario. El ciberespacio logra desdibujar las líneas definidas por la soberanía territorial de los Estados, para convertir a los delitos tradicionales en delitos globales, con mayor alcance y magnitud (lo cual promueve la cooperación internacional para hacer frente a este fenómeno), a la vez que logra ocultar la identidad de los atacantes. Esto es, en definitiva, lo que resulta alarmante cuando hablamos de la cuestión cibernética como fenómeno de la seguridad internacional.

b. Defensa

Cuando hablamos del fenómeno en términos netamente militares, encontramos que este ambiente nos brinda la posibilidad de librar guerras en un nuevo espacio transversal a todos los teatros de operaciones, de realizar apoyo logístico en una guerra

tradicional, de operar tecnología desde una base de comando y control que se encuentre a miles de kilómetros del lugar al cual se desea atacar y, por ende, permite salvaguardar al instrumento militar. Así, la ciberdefensa implica una nueva forma de hacer la guerra, una forma que nos permite librar la guerra en tiempos de paz, o tal como lo plantea Schwab, las distinciones entre tiempos de guerra y paz se están desdibujando.

Vemos entonces, cómo el ambiente cibernético y la irrupción del avance tecnológico repercute en la defensa de las naciones de forma tal que incentiva profundas transformaciones en el instrumento militar. En definitiva, el aparato militar tiene el deber de aggiornarse a las realidades del contexto, para así prepararse para posibles eventualidades. El ciberespacio, propone una nueva forma de hacer la guerra y, por ende, una nueva forma en que el aparato militar debe adoctrinarse.[17]

Tal como demostraron las teorías del poder aéreo, marítimo y terrestre, los avances tecnológicos de cada época producen un gran impacto en lo político y lo militar. Esta premisa es aplicada también al ciberespacio, ya que la conectividad digital posee implicancias en las interacciones económicas, políticas y militares. (Rattray, G. J.: 2016). En definitiva, la evolución de este espacio implica nuevas formas de hacer la guerra. Esta nueva forma de hacer la guerra surte efectos en el mundo físico traspasando el ambiente virtual. En palabras de Schwab, los conflictos futuros posiblemente tengan una ciberdimensión, dado que es poco factible que un oponente no se sienta tentado por la idea de "*alterar, confundir o destruir los sensores, las comunicaciones y la capacidad de toma de decisiones de su enemigo"* (2017: p. 111).

Esta guerra está relacionada con la obtención de información y los medios de comunicación. Para algunos especialistas, la ciberguerra supone todo ataque dirigido a través de las herramientas digitales (sin importar el blanco de ataque), mientras que para otros se refiere a la utilización del ciberespacio para el apoyo logístico en los espacios tradicionales de conflicto. Los autores Arquilla y Ronfeld (1993) definen a la ciberguerra como la conducción y preparación del aparato militar con el fin de llevar adelante operaciones militares relativas a la información que tengan por objeto modificar y eliminar información y sistemas de comunicaciones, prohibir el acceso del adversario a la información propia y obtener información sobre sus planes de acción.

[17] Adoctrinarse en el buen sentido de la palabra, es decir, en cuestiones referidas al conjunto de medidas y prácticas que tienen por objeto inculcar ciertos valores, formas de pensar y actuar.

En definitiva, se trata de operaciones militares de inteligencia, ya que los usos de la ciberguerra suponen, la injerencia por parte de uno de los actores en el sistema de comunicación del enemigo, o incluso, el control de los sistemas de armas a través del sabotaje, el robo de información, entre otras.

Ejemplo de acciones de ciberguerra es el conflicto entre Georgia y Osetia del Sur en el año 2008, donde Rusia, en oposición al primero, intervino no sólo a través de sus fuerzas armadas sino también a través de ciberataques dirigidos contra los sitios webs de Presidencia de la República, el Parlamento, los Ministerios de Asuntos Exteriores, Defensa y Ciencia y Educación; instituciones educativas; agencias de comunicaciones; el Banco Central y otras instituciones financieras. A través de esto se logró el cometido de bloquear la capacidad de toma de decisiones del gobierno al interrumpir las comunicaciones entre los mismos funcionarios y del gobierno con la sociedad. Una segunda dimensión tuvo lugar como guerra psicológica con fines de reclutamiento, ya que se utilizaron las redes sociales para conseguir adeptos a la causa rusa. La respuesta de Georgia ante esta situación fue el pedido de cooperación ante la comunidad internacional para bloquear los efectos de los ciberbombardeos debido a que no contaba con un desarrollo tecnológico capaz de mantener la seguridad de sus IC. (Ganuza Artiles, N.: 2010).

Torres Soriano (2018) explica que la introducción de ciberarmas en operaciones militares contribuye a aumentar la "niebla de la guerra" y, por ende, dificulta el proceso de toma de decisiones del adversario. Para el autor, la militarización de este espacio incide en el equilibrio nuclear, ya que brinda la posibilidad de que un Estado poseedor de armas nucleares pierda la capacidad de comunicarse y transmitir órdenes respecto a su arsenal.

Siguiendo esta línea, el objeto de la ciberguerra es cegar al enemigo, mantenerlo incomunicado y sin capacidad de tomar decisiones. En definitiva, la combinación de capacidades militares con capacidades cibernéticas brinda la posibilidad de destruir por completo al enemigo privándolo del control de sus sistemas de armas para contrarrestar los ataques, a la vez de que le permite reducir los efectos políticos que poseen las acciones ofensivas, ya que faculta a los gobiernos para resguardar la vida de su instrumento militar.

Las formas que adquiere esta nueva guerra y la importancia de la dimensión cibernética en el mundo se encuentran expuestas en la Directiva de Política de Defensa Nacional del año 2014 de la República Argentina, cuando en ella se menciona que:

> "Los usos militares de las novedosas tecnologías asociadas a la robótica, cibernética, sensores remotos, entre otros desarrollos en materia de ciencia y tecnología, han impulsado nuevas formas de librar la guerra que exhiben un salto cualitativo hacia un nuevo paradigma tecnológico. El empleo de aviones no tripulados en los teatros de operaciones es el ejemplo más cabal de esta tendencia. De igual modo, estos cambios traen aparejados también modificaciones sustanciales sobre la profesión militar, en el sentido de representar no sólo novedosas técnicas en el empleo de los sistemas de armas, sino también al modificar la tradicional configuración del campo de batalla, el rol del soldado y de las operaciones.
>
> Otro aspecto asociado [..] es la importancia que está adquiriendo el ciberespacio para el desarrollo de las operaciones militares. La dimensión ciberespacial, sin locación física específica propia, genera replanteos sobre las tradicionales categorías con las que se aborda la "guerra real" y exige, por la dinámica propia de la innovación tecnológica, una rápida adaptación para los Sistemas de Defensa respecto de sus componentes. En las últimas décadas, muchos países vienen reorientando esfuerzos y recursos para resguardar no sólo los espacios tradicionales (terrestre, marítimo y aeroespacial), sino también al ciberespacial." (DPDN: 2014, 5).

La cuestión ciber posee gran relevancia gracias a que muchas veces representa una guerra a ciegas por parte de los Estados. En cuestiones de ciberguerra, el suprimir sentidos tales como vista, oídos y habla de quienes toman de decisiones genera grandes ventajas para el atacante otorgándole el factor sorpresa en beneficio propio, a la vez que permite aumentar (incluso al máximo) los niveles de incertidumbre del oponente. De ocurrir esto, existen mayores posibilidades de que ocurra un cisne negro para aquel actor que tiene fuera de juego sus sentidos.

c. Inteligencia

Así como las cuestiones de defensa y seguridad se presentan de forma manifiesta en el ciberespacio, las cuestiones de inteligencia se acomodan a las herramientas digitales para llevar a cabo tareas de inteligencia y contrainteligencia, entendida esta última como el conjunto de actividades que apuntan a evitar acciones de espionaje, sabotaje, infiltración y propaganda. La ciberinteligencia hoy en día es utilizada para combatir, contrarrestar y mitigar la gran variedad de crímenes que se presentan en el ciberespacio, pero también es utilizada para robar información sensible vinculada a innovaciones tecnológicas, propiedad intelectual, o incluso influir en el pensamiento de las personas a través de la denominada ingeniería social.

El choque de intereses entre gobiernos, empresas y entidades dedicadas a la investigación y el desarrollo de nuevos productos pone de manifiesto la importancia del uso del ciberespacio como medio facilitador para obtener y denegar información.

En definitiva, esta nueva forma de hacer la guerra revitalizó el rol de la información como activo estratégico a obtener, destruir y proteger. Siguiendo esta línea de pensamiento, podríamos decir que la guerra de la información hoy es librada por la inteligencia.

Tal como explica Torres Soriano (2018) la ciberinteligencia tiene por objeto la infiltración para obtener acceso a redes y sistemas y realizar ataques para activar la defensa del oponente para poder determinar sus capacidades en el ciberespacio.

Esto permite no solamente determinar cuáles son las vulnerabilidades del oponente sino también reducir la incertidumbre. Extrapolando el pensamiento de Sun Tzu, es imposible ganar una batalla sin conocer las capacidades propias y las del enemigo, por lo que las tareas de espionaje resultan esenciales en el desarrollo de los conflictos cibernéticos y tradicionales.

Las acciones de ciberinteligencia y ciberespionaje se encuentran en manos de todo tipo de actores (no solamente Estados) que realizan estas tareas para la consecución de sus objetivos. Al igual que en el mundo físico, resulta de vital importancia ocultar la verdad si se pretende obtener los resultados esperados, por lo que los actores hacen todo lo posible para ocultar su identidad y las cibercapacidades creadas y utilizadas para espiar y dañar al enemigo.

Existen diversos ejemplos de ciberespionaje de los cuales se atribuye su autoría a Estados. Uno de los más relevantes es el caso de la operación denominada Careto o The Mask. Este malware espió sectores estratégicos alrededor de 31 Estados, haciéndose con información confidencial de las propias instituciones de gobierno, hasta los aparatos diplomáticos, el sector energético, empresas privadas, entidades avocadas a la investigación, activistas y otros. Desde el año 2007 hasta su descubrimiento en 2013, se dedicó a la recolección de información confidencial pasando inadvertido para los sistemas de seguridad informáticos. Dicho ataque se lo atribuye a España dado que los países afectados por Careto se encontraban vinculados con la política exterior española. (Kaspersky: 2014).

Otro antecedente importante de ciberinteligencia es el caso de Red October o Rocra que entre los años 2007 y 2013 recolectó información sensible de gobiernos

alrededor del mundo, aunque con un período mucho más activo entre 2010 y 2012. Con especial interés por los países de la ex Unión Soviética y Asia Central, el troyano se dedicó a recolectar información sensible de instituciones de gobierno (principalmente del sector diplomático y militar), industrias estratégicas (aeroespacial, nuclear y energética) e instituciones dedicadas a la investigación científica. Dado los blancos elegidos y el lenguaje utilizado en la programación esta operación de inteligencia es atribuida a Rusia.[18]

Algunas veces, este tipo de operaciones se convierten en ataques. Es el caso del emblemático gusano Stuxnet que atacó a las centrífugas nucleares de Irán. Recordemos que en el año 2010 el malware se propagó contra la infraestructura de la central nuclear iraní en Natanz. El resultado de este ataque fue efectivo, y logró realizar su cometido que era retrasar el programa iraní, afectando el funcionamiento de cientos de centrífugas al entrar en contacto con los sistemas SCADA de control y monitoreo de procesos. Si bien no hubo un reconocimiento formal por parte de los responsables, se cree que el ataque fue de autoría norteamericana e israelí dado que se produce en medio de las negociaciones sobre el plan nuclear iraní. Aunque esto no fuese cierto, los expertos entienden que el diseño tan sofisticado de este código requirió de un presupuesto sumamente elevado, por lo que se deduce que estuvo en manos de por lo menos un Estado.

Luego de ser conocido Stuxnet, los códigos fueron reprogramados en nuevos elementos de ciberataques, transformándose en malwares conocidos como: Duqu (diseñado para robar información sobre los sistemas de control industrial), Flame (diseñado para ciberespionaje) y Gauss (para robo de información personal).

La dificultad a la hora de precisar al responsable del acto (es decir, atribuir el ataque), la falta de conocimiento y/o de consciencia por parte de los usuarios, la falta de leyes, de fronteras, de soberanía y del control efectivo de este espacio por parte de los Estados, sumado al bajo costo de desarrollar ciberarmas y su impacto global; la incapacidad de establecer límites de forma tradicional; la difícil detección de agresiones en el ambiente cibernético y la necesidad de desarrollar la creatividad para contrarrestar todas las amenazas que se hacen presentes en este espacio propicia y motiva a los distintos actores para llevar a cabo tareas de inteligencia que le permitan conseguir con éxito la realización de sus hazañas.

[18] SecureList. (January 14, 2013). "Red October" Diplomatic Cyber Attacks Investigation. (consultado el 15/05/2018) Recuperado de: https://securelist.com/red-october-diplomatic-cyber-attacks-investigation/36740/#1

Vemos entonces, que al ser el fenómeno cibernético una amenaza que cobra forma en materia de seguridad, defensa e inteligencia, puede ser entendido como un fenómeno multifacético que pone en riesgo a todos los elementos de poder enumerados por Steven Lobbell, ya que es susceptible de ser utilizado para influir las ideologías de las personas (lo cual puede ser entendido como guerra psicológica), sirve de medio e instrumento para desarrollar operaciones militares, es capaz de vulnerar la seguridad y privacidad de las personas, es un fenómeno idóneo de afectar la industria de cualquier Estado y a la vez, dependiendo del tipo de ataque, puede vulnerar el mundo físico comprometiendo el componente territorial de una Nación.

B. El fenómeno cibernético en Argentina

Los postulados de Steven Lobell nos invitan a replantearnos la posibilidad de pensar si el fenómeno cibernético es en realidad una amenaza real para nuestro país y cuáles son los factores de poder que se ven afectados por dicha amenaza a la seguridad.

Cuando pensamos en el fenómeno cibernético, es casi imposible no ligarlo a países como Corea del Norte, China, Rusia y Estados Unidos. Incluso si analizamos el ranking de los países más afectados por ciberataques, vemos que países como Alemania, Japón, Canadá, Nueva Zelanda y Australia se encuentran entre los países más afectados, al igual que Brasil e India que, dependiendo las mediciones, se encuentran entre los primeros diez blanco de ciberataques. Ahora bien, resulta necesario interrogarnos respecto a ¿cuál es el lugar que ocupa Argentina en este contexto? Si analizamos los mapas de ciberataques en tiempo real[19] vemos que Argentina posee un lugar preponderante entre los primeros 40 blancos de ciberataques a nivel mundial, por lo cual, podemos comprender que Argentina posee gran actividad cibernética criminal.

Existen datos que pueden reflejar esta realidad. En el año 2014, por ejemplo, Argentina (13%), Brasil (49%) y Chile (19%) eran foco del 80% de los ataques de phishing[20] en Latinoamérica. Junto con México (6%) y Colombia (7%), cooptaban el 95% de estos ciberataques, a pesar de representar menos de un tercio de los países de la región. Sin dudas, Brasil era, por lejos, el blanco más atacado de la región (aún hoy se mantiene así).[21]

---

[19] Los días 5, 7 y 10 de mayo de 2018 se consultó los mapas de KasperskyLab, Norse y TeamCymru.

[20] Se entiende por phishing al robo de información altamente sensible a través del engaño. Concepto extraído de www.ba-csirt.gob.ar , consultado el 4 de abril de 2019.

[21] Gutiérrez Amaya, C. (10/10/2014). Brasil, Chile y Argentina sufren el 80% del phishing en Latinoamérica. *WeLiveSecurityEset*. (Consultado el 23 de mayo de 2018) Recuperado de:

Ya en 2015, Argentina era considerada por los expertos como "uno de los países con la actividad criminal cibernética más alta del mundo." (Trend Micro/OEA: 2015, p 18). Los costos de este tipo de delitos pueden verse reflejados en las cifras expuestas en el informe de ciberseguridad de América Latina y el Caribe:

> "Según algunos cálculos, el cibercrimen le cuesta al mundo hasta US$575.000 millones al año, lo que representa 0,5% del PIB global. Eso es casi cuatro veces más que el monto anual de las donaciones para el desarrollo internacional. En América Latina y el Caribe, este tipo de delitos nos cuestan alrededor de US$90.000 millones al año." (Observatorio de la Ciberseguridad: 2016, IX).

Según datos aportados por el mismo observatorio, la penetración de internet en la sociedad argentina en el año 2016 era ya del 65%. Esto, sumado a las distintas iniciativas implementadas por los gobiernos de Cristina Fernández de Kirchner y Mauricio Macri,[22] que tuvieron y tienen como objeto la digitalización y la extensión de los usos de las TICs en la sociedad argentina, supone una tendencia hacia el incremento de las vulnerabilidades que se reflejan en el ciberespacio.

Según Kaspersky Lab[23], en el año 2016 nuestro país se encontraba entre los 10 principales blancos de ataques al sector bancario, en ese año, los troyanos dirigidos a las instituciones financieras eran una de las prácticas más elegidas por los criminales cibernéticos.

Según el boletín de estadísticas de Kaspersky Lab de 2017[24], Argentina forma parte del grupo de países que se encuentran inmediatamente después de los 20 Estados más afectados por esta problemática, lo cual arroja luz sobre el grado de exposición que

---

https://www.welivesecurity.com/la-es/2014/10/10/brasil-chile-y-argentina-sufren-el-80-del-phishing-en-latinoamerica/

[22] Esto puede verse reflejado en iniciativas de gobierno como lo son los programas "Conectar Igualdad" que, desde el año 2010, buscaba garantizar el acceso de los estudiantes a recursos tecnológicos. Durante los ocho años de su implementación, 6 millones de computadoras fueron entregadas a alumnos de todo el país. Este proyecto, actualmente está mutando a "aprender conectados", dado que según los datos del gobierno, el problema dejó de ser el acceso a las TICs gracias al proyecto anterior, por lo que ahora es necesario enfocarse en desarrollar competencias que harán foco en la robótica y la programación. Davidovsky, S. (9/5/2018). Cuál es el objetivo de Aprender Conectados, el plan educativo que reemplaza a Conectar Igualdad, en La Nación. (consultado el 6 de septiembre de 2018 en https://www.lanacion.com.ar/tecnologia/cual-es-el-objetivo-de-aprender-conectados-el-plan-educativo-que-reemplaza-a-conectar-igualdad-nid2132718)

[23] Kaspersky Lab. (17/8/2016). Ataques financieros aumentaron un 16% en el segundo trimestre. (Consultado el 5 de marzo de 2018 en https://latam.kaspersky.com/blog/kaspersky-lab-ataques-financieros-aumentan-un-16-en-el-segundo-trimestre/7511/)

[24] KasperskyLab. (28/11/2017). Estadisticas generales 2017, (consultado el 5 de junio de 2018 en https://kasperskycontenthub.com/securelist/files/2017/12/KSB_statistics_2017_SP_final.pdf)

posee nuestro país ante las ciberamenazas. Además, el mismo organismo asegura que durante el año 2018, América Latina estará más expuesta a operaciones cibernéticas militares secretas realizadas por la inteligencia de los Estados a partir del uso de plataformas digitales abocadas exclusivamente al espionaje. Práctica que viene incrementándose desde el año 2014.

Actualmente, Brasil es el país con mayor ciber actividad de la región, por lo que no parecería raro que, más allá de las relaciones de cooperación que se llevan a cabo bilateralmente, nuestro país sea blanco de cibercriminalidad y tareas de ciberespionaje propiciadas por la potencia emergente.

Durante los últimos diez años, Argentina ha sido foco de diversos ciberataques (todos con distintos grados de repercusión sobre la seguridad nacional). Algunos de ellos tuvieron a las instituciones de gobierno argentinas como único objetivo estratégico, otros atacaron países de todo el globo. A continuación, se hará mención, a modo de ejemplo, de algunos ataques a los que se expuso nuestro país a lo largo del siglo XXI con el objeto de visualizar la exposición de nuestro país respecto al fenómeno cibernético.

- En el año 2005, el sitio web de Presidencia de la Nación sufrió una intromisión mediante la cual se modificaron frases de uno de los discursos del entonces Presidente de la Nación, Néstor Kirchner. (Borghello, C. y Temperini, M.: 2013).
- Entre 2007 y 2013, 31 Estados fueron víctimas del caso de ciberespionaje denominado Careto o The Mask. Esta operación de inteligencia alcanzó, aunque en menor medida que en el resto del mundo, a los sectores estratégicos de Argentina. (Kaspersky Lab: 2014).
- En 2009, el sitio web del padrón electoral fue atacado. Aunque no tuvo grandes efectos, los intrusos agregaron leyendas ofensivas durante las elecciones legislativas. (Leiva: 2015).
- En el año 2010, la AFIP fue víctima del robo de información de sus bases de datos. (Leiva: 2015).
- En 2012, Anonymous lanzó la llamada Operación Quirófano, tuvo por objeto interrumpir el normal funcionamiento de los sitios web (incluido el de Presidencia) para protestar contra el gobierno por las retenciones a las importaciones de la industria médica que no permitían que ingresara al país

medicamentos e insumos necesarios para que los centros médicos realizaran sus tareas.[25]

- A fines de 2012, el grupo hacktivista denominado Lulz Sec Perú llevó adelante un ataque al Ministerio de Defensa argentino que terminó en la filtración de información sensible de cuestiones estratégicas del Ministerio.[26]
- En el año 2013, Anonymous puso en funcionamiento la Operación Fuck Gobierno, a través de la cual, en el lapso de 24 horas realizó ataques de DDoS (denegación distribuida de servicio) a más de cien sitios oficiales del gobierno argentino. (Borghello, C. y Temperini, M.: 2013). Este mismo año, el grupo de hackers saboteó el sitio web del INDEC, a modo de protesta por las mentiras que arrojaban los datos de dicho organismo.[27]
- El 20 de noviembre de 2016, el Municipio de 25 de Mayo (provincia de Buenos Aires) fue objeto de un ataque de phishing mediante el cual los cibercriminales robaron 3,5 millones de pesos a la tesorería municipal. El hecho ocurrió a partir de una copia de la página web de Banca Internet Provincia, a partir del cual los estafadores robaron las credenciales del contador municipal y realizaron 24 transferencias fraudulentas a supuestos proveedores.[28]
- En el año 2016, Anonymous lanzó la Operación Oplcarus con el objeto de derribar las páginas webs de instituciones financieras consideradas corruptas alrededor del mundo. Entre la lista de estas instituciones se encontraba el Banco Central de la República Argentina junto al Banco Mundial, FMI, la Reserva Federal norteamericana, la Bolsa de New York y Bancos Centrales de distintos países.[29]
- En 2017, más de 30 correos electrónicos del Ministerio de Seguridad de la Nación fueron víctimas de un ataque a través de phishing que terminó en el robo de

[25] Infobae. (9/7/2012). "Anonymous inició la Operación Quirófano y hackea páginas en Argentina", en *perfil,* Buenos Aires (consultado el 8 de enero de 2018 en https://www.infobae.com/2012/07/09/658114-anonymous-inicio-la-operacion-quirofano-y-hackea-paginas-argentina/)

[26] Sobre este ataque en particular se volverá en el capítulo 3. Para más información ver Lee Johnstone. (31/12/2012). "Argentina Ministry of DefenseHacked, DocumentsleakedSiteDefaced", en *Cyberwar news* (consultado el 12 de enero de 2018 en https://www.cyberwarnews.info/2012/12/31/argentina-ministry-of-defense-hacked-documents-leaked-site-defaced/)

[27] Goujon, A.(7/1/2013). "Anonymous dio de baja el sitio del INDEC en Argentina", en *WeLiveSecurityEset.* (consultado el 8 de enero de 2018 en https://www.welivesecurity.com/la-es/2013/01/17/anonymous-dio-baja-sitio-indec-argentina/)

[28] Pagnotta, S. (7/8/2017). "Confirman que fue phishing lo que permitió el robo de 3,5 millones en Argentina", en *WeLiveSecurityEset* (consultado el 17 de enero de 2018 en https://www.welivesecurity.com/la-es/2017/08/07/confirman-phishing-robo-argentina/)

[29] Security radware. (6/8/2017). "Oplcarus 2017", en *securityradware* (consultado el 16 de enero de 2018 en https://security.radware.com/ddos-threats-attacks/threat-advisories-attack-reports/opicarus2017/)

información sensible. Entre estos correos se encontraba el de la titular de dicho organismo.[30]

- En 2017, Argentina fue víctima de WannaCry, el ransomware que afectó instituciones de 150 países alrededor del mundo.

Cabe resaltar que los ciberataques dirigidos hacia nuestro país son indudablemente más numerosos, por lo que podemos pensar que la falta de acceso a tal información es resultado de que muchas veces los actores atacados no denuncian públicamente lo ocurrido, o bien, debido a que si existe registro de ciberataques, su carácter confidencial bloquea el acceso de la academia y la sociedad civil a este tipo de información. En definitiva, los ciberataques dirigidos a nuestro país expuestos en este apartado sirven de muestra representativa a modo de iluminar sobre la existencia de la vulnerabilidad del ciberespacio en la Argentina.

Si entendemos que la tarea principal de la contrainteligencia es evitar que el enemigo/adversario obtenga información sensible de nosotros, los casos de los ataques al Ministerio de Seguridad y el de Defensa muestran una clara falencia en la consecución de esas funciones.

Es claro que los ciberataques criminales son los que priman en la Argentina. Tal como podemos descifrar de los ciberataques arriba mencionados, factores de poder tales como ideológico, poblacional y militar ya han sido vulnerados, siendo, las instituciones de gobierno, uno de los principales blancos de ataque cibernético.

C. Respuestas locales y globales ante el fenómeno cibernético

Vemos cómo este fenómeno es capaz de afectar a distintas naciones, empresas, personas e instituciones simultáneamente utilizando un único código malicioso, es por ello que los gobiernos deben adaptarse. Siguiendo lo expuesto por Kenneth Waltz, es el Estado quien tiene el monopolio del uso de la fuerza y, por ende, el actor que por antonomasia que debe proveer la seguridad de sus ciudadanos, por lo que resulta necesario preguntarnos ¿cuáles son las medidas que fueron tomando los distintos gobiernos para proteger a sus ciudadanos, empresas e instituciones para lograr así que la articulación de sus funciones no se vea afectada?

[30] La Nación. (1/2/2017). "También hackearon 30 correos del Ministerio de Seguridad", en *La Nación*, Buenos Aires (consultado el 15 de enero de 2018 en https://www.lanacion.com.ar/1980702-tambien-hackearon-30-correos-del-ministerio-de-seguridad)

La Unión Internacional de Telecomunicaciones (UIT), en su afán por analizar (de forma comparada) cuál es el nivel de ciberseguridad que poseen países, esquematizó en cinco categorías las distintas medidas, a saber: aspectos legales, medidas técnicas, medidas organizacionales, construcción de capacidades y cooperación.

Según el ranking aportado por el índice de ciberseguridad mundial, los países que han tomado medidas más eficientes para hacer frente al fenómeno de la ciberseguridad son: Singapur (0.925), Estados Unidos (0.919), Malasia (0.893), Omán (0.871), Estonia (0.846), República de Mauricio (0.830), Australia (0.824), Georgia y Francia (0.819), Canadá (0.818) y Rusia (0.788)[31]. En este ranking, Argentina ocupa la posición número 62[32] con una calificación de 0.482, muy por debajo de los países que se encuentran en la cima, lo que pone de manifiesto que las políticas, buenas prácticas, mecanismos de respuesta a incidentes e iniciativas de diversa índole adoptadas por Argentina resultan insuficientes.[33] (ITU: 2017).

A continuación utilizaremos las categorías propuestas por el UIT para hacer mención de los instrumentos que fueron creando los Estados para hacer frente al fenómeno cibernético tanto desde lo individual en su política doméstica, como desde lo colectivo a través de la cooperación internacional ya que por la naturaleza misma del ciberespacio resulta casi imposible hacer frente a este problema de manera aislada.

a. Aspectos legales

Uno de los aspectos legales a los que se refiere la UIT es la legislación sobre cibercrimen. En este sentido, nos recuerda que Colombia[34] fue uno de los primeros países en establecer este tipo de normas modificando el Código Penal a través de la ley 1273 (2009) que creó un bien jurídico tutelado denominado "protección de la información y de los datos", en el cual se concibió la figura legal de delitos relacionados al acceso ilegal y la obstaculación de un sistema informático, el daño informático, la interceptación de datos informáticos, la violación de datos personales y otros que, a partir de esa ley empezaron a ser concebidos como delitos con penas punitorias reales.

En materia legal internacional, el Consejo de Europa, junto con la participación de potencias extra regionales, elaboró en el año 2001 el Convenio sobre

[31] Los números que se encuentran más próximos al 0 son los menos eficientes, mientras que los que se acercan al 1 son los que demuestran mayor eficiencia.
[32] De un total de 192 países calificados.
[33] Respecto a las iniciativas desarrolladas por Argentina se volverá en el Capítulo segundo de esta tesis.
[34] Argentina, tal como se verá en el capítulo 2, lo hizo un año antes, en 2008.

Cibercriminalidad[35] también conocido como Convenio de Budapest sobre ciberdelincuencia, entrando en vigor en julio de 2004. Dicho tratado tiene por objeto aplicar una política penal común en los Estados Parte para proteger a la sociedad de la ciberdelincuencia. A tal objeto, reconoce la necesidad de cooperar entre los sectores público y privado y reforzar la cooperación internacional. El tratado propone terminología común, la tipificación penal de delitos relacionados a la cibercriminalidad y un derecho procesal colaborativo (asistencia mutua) basado en la cooperación internacional.

b. Medidas organizacionales

Dentro de estas medidas encontramos la necesidad de definir estrategias holísticas de ciberseguridad como factor que permite a los Estados aggiornarse al cambio constante que se produce en el ambiente informático gracias al continuo y acelerado avance tecnológico que pone en jaque la seguridad de las naciones.

Ahora bien, ¿a qué nos referimos cuando hablamos de Estrategia Nacional de Ciberseguridad? Según Stuart Starr (2016, p 48), se define como "*the development and employment of capabilities to operate cyberspace, integrated and coordinated with the other operational domains, to achieve or support the achievement of objectives across the elements of national power.*"[36]

En definitiva, una estrategia de ciberseguridad a nivel nacional plantea los objetivos a cumplir permitiendo establecer las bases políticas para conseguir un ciberespacio seguro. Una estrategia nos brindará respuestas a preguntas tales como ¿cuál es el diagnóstico del problema?, ¿cuál es el objetivo central y cuáles son los objetivos específicos?, ¿cuál es el plan de acción a seguir?, ¿cuáles son los elementos a proteger?, ¿cuáles son los organismos involucrados?, ¿cuál será el ámbito de acción de cada organismo?, ¿cuáles son las cibercapacidades que pretende desarrollar el Estado y para qué?

Una estrategia de este tipo supone una actualización por parte de los Estados, donde se intenten contrarrestar los desafíos que traen aparejado los desarrollos tecnológicos y la creciente dependencia tecnológica. De no conseguirlo, el riesgo inherente asociado a las TICs se potencia, incrementando así sus efectos sobre la vida de

[35] Argentina, como se verá en el capítulo segundo, es parte del Convenio de Budapest aunque guarda ciertas reservas.

[36] El desarrollo y empleo de capacidades para operar en el ciberespacio, de forma integrada y coordinada con los otros dominios operacionales, en soporte de la consecución de sus objetivos a través de los elementos de poder nacional. (Traducción propia).

las personas, las empresas y los Estados hasta el punto de volvernos incapaces de contrarrestar sus efectos, ya que los problemas derivados de la interconexión mundial han dejado de ser un problema futuro para convertirse en un problema presente que requiere de un análisis estratégico y un proyecto eficaz para socavar sus resultados.

Respecto a esta medida, podemos apreciar que potencias preocupadas por el desarrollo de cibercapacidades y el logro de un ciberespacio seguro han enfocado sus esfuerzos en la adopción de estrategias nacionales.

El caso más emblemático, definitivamente es el de Estonia, quien adoptó su primera estrategia de ciberseguridad en el año 2008 como respuesta a los ataques recibidos en 2007. Esto, llevó al país a convertirse en uno de los primeros Estados en desarrollar una estrategia de ciberseguridad complementaria a su estrategia de seguridad nacional. (Lewis, J.: 2016)

Los hechos ocurridos en Estonia (2007), Georgia (2008) e Irán (2011), demostraron que el mundo requería medidas preventivas, por lo que la adopción de la estrategia de Estonia provocó un efecto dominó en el ámbito internacional. A partir de allí, diversos Estados comenzaron a definir sus estrategias destinadas al ambiente cibernético. Tal es el caso de Canadá en el año 2010; Alemania, Francia y Estados Unidos en 2011; España y Japón en 2013. (Leiva: 2015).[37]

A nivel regional, en América Latina, solamente seis países[38] han logrado definir sus estrategias. Colombia, fue el primero en adoptar este tipo de instrumento en el año 2011 y logró realizar una revisión de esta en 2016 que fue denominada "Política Nacional de Seguridad Digital." Panamá siguió sus pasos en el año 2013, mientras que países como Paraguay, Chile, Costa Rica y México[39] hicieron lo mismo en 2017. (Hernández, J. C.: 27/2/2018).

En contraposición, gran parte de los países de todo el globo (y en especial de América Latina) ha desarrollado una serie de buenas prácticas y políticas de ciberseguridad sin lograr definir una estrategia holística de estas características, lo cual no resulta del todo ventajoso dado que estas políticas no necesariamente persiguen un hilo conductor y un objetivo claramente definido.[40]

[37] Para ampliar información, consultar Leiva: 2015.
[38] Los países que han elaborado sus estrategias en base a recomendaciones de la OEA, tal como se está planteando en Argentina, fueron Chile, Colombia y Paraguay. Entrevista reservada con Fuente E (civil), 13 de septiembre de 2018, Buenos Aires.
[39] México fue el último país latinoamericano en presentar su estrategia en ciberseguridad.
[40] Este es el caso de Argentina, que preveía hacer oficial su Estrategia Nacional de Ciberseguridad en noviembre del año 2018 pero que todavía en febrero de 2019 no surtió efectos.

Otra práctica común es la creación de una agencia que se encargue de coordinar la ciberseguridad a nivel nacional. Esta práctica es aún más extendida que la anterior, ya que podemos apreciarla incluso en países que no cuentan con una estrategia como la denominada anteriormente.

Ejemplo de esto, sin dudas excepcional, es el de Reino Unido. Su *National Cyber Security Center* tiene por objeto proteger los servicios críticos de los posibles ciberataques, la gestión de incidentes y mejorar la seguridad de las TICs. Este centro nuclea al gobierno, las industrias y la academia. Este organismo realiza dos eventos sobre ciberseguridad en el Reino Unido, uno de ellos a nivel nacional (CyberUK) donde nuclea expertos provenientes del gobierno; las IC; la academia y el tercer sector, y el otro, a nivel regional (CyberThreat) que nuclea a profesionales de la comunidad europea que tiene por objeto analizar respuestas a incidentes por parte de la comunidad.[41] Vemos entonces, que el NCSC no se limita únicamente al ámbito de la defensa cibernética y al control de incidentes cibernéticos, sino que es capaz de crear cibercapacidades a la vez que propicia la capacitación y el trabajo conjunto de los sectores público, privado y la academia.

c. Medidas técnicas

Una de las prácticas más extendida entre los Estados es la adopción de Equipos de Respuesta ante Incidentes de Seguridad Informática (CERT).

Los objetivos de estos centros son: evitar que se produzcan incidentes, mitigar y dar respuesta a incidentes, controlar y minimizar los daños para que el impacto de los ciberataques sea el menor posible, lograr una rápida recuperación y analizar los hechos ocurridos para prevenir ataques a futuro y (en el peor de los casos), saber cómo mitigarlo.

Mapa 1: CSIRTs en el mundo

Esta es una de las prácticas más extendidas en todo el globo, dado que, sin ella la exposición a ciberataques resulta mayor y el grado de respuesta a ciberataques parecería ínfimo. Por su parte, la UIT ha venido colaborando con diversos Estados para lograr el desarrollo de CERTs nacionales, tal es así que se están desarrollando evaluaciones en 71 Estados para establecer centros de este tipo y así poder avanzar en la protección del ciberespacio a nivel global.

[41] NCSC. (11/5/2018). The National Cyber Security Centre. UK. Recuperado de: https://www.ncsc.gov.uk/

Según datos aportados por el organismo, a nivel global existen 103 CERTs nacionales, tal como puede verse en el mapa N°1[42]. En el caso de los países de América Latina y el Caribe, al año 2016, gran parte de la región contaba con centros de estas características, entre ellos Argentina.[43]

Una forma en que se instrumentan las buenas prácticas arriba mencionadas, son las comunicaciones constantes entre CERTs/CSIRTs nacionales con el objeto de compartir información. Ejemplo de esto es la red de seguridad hemisférica de los CSIRTs creada bajo la estructura del CICTE de la OEA, en la cual participa Argentina.

d. Construcción de capacidades

Actualmente, los países invierten cada vez más en Comandos Cibernéticos que le permitan desarrollar las capacidades necesarias para protegerse de esta nueva guerra. Es el caso de Estados Unidos, Irán, Israel, la península de Corea, Rusia y China, para dar un ejemplo.

El caso por antonomasia es el de los Estados Unidos. Las autoras Li, J. y Daugherty, L. (2015) nos dan a conocer ciertos datos sobre la cuestión. Dado que la ciberseguridad es de vital importancia para la seguridad norteamericana, en el año 2009 el Departamento de Defensa (DoD) creó el CyberCom, el cual representa el 5% de las fuerzas armadas norteamericanas y tiene por misión supervisar las operaciones cibernéticas y liderar las cuestiones de ciberdefensa. Bajo el paraguas de inteligencia, el CyberCom se ha ido expandiendo desde su creación. Ya en 2014 su presupuesto era de 4,7 mil millones de dólares (superaba el presupuesto en defensa). Ya en ese entonces, se vieron en la necesidad de incorporar mil ciberguerreros nuevos por no parecer suficientes para las necesidades del mañana. Según datos aportados por el DoD, el 78% de esta fuerza está compuesta por personal civil, y solamente el 22% por personal militar, siendo las operaciones cibernéticas ofensivas ejecutadas no sólo por militares sino también civiles.

En el caso de nuestro país, el Ministerio de Defensa ha desarrollado un Comando Conjunto de Ciberdefensa que tiene por misión proteger las IC vinculadas al Instrumento Militar y servir de apoyo a las operaciones militares.

---

[42] ITU. (1/5/2018). CIRT Programme. Recuperado de: https://www.itu.int/en/ITU-D/Cybersecurity/Pages/Organizational-Structures.aspx

[43] Confrontar en *Ciberseguridad ¿estamos preparados en América Latina y el Caribe?* Informe de Ciberseguridad 2016.

Para Craig y Valeriano (2016), el desarrollo de comandos cibernéticos y la adopción de ciberarmas se encuentran íntimamente relacionadas al dilema de seguridad.[44] Los autores ejemplifican esta relación a través de las rivalidades existentes entre Estados Unidos e Irán (por un lado), y entre ambas Coreas (por el otro). Para los autores, los mapas de ciberataques, los presupuestos destinados al Cibercomando y la cantidad de personal dedicado al sector cibernético, prueban el interés de los Estados por desarrollar ciberarmas. De esta forma, la construcción de capacidades se vincula a la necesidad de los países a hacer frente a su percepción de amenazas.

e. Mecanismos de cooperación

Existen diversos instrumentos a través de los cuales se manifiesta la cooperación. Uno de ellos es la celebración de acuerdos internacionales que pueden desarrollarse bilateral o multilateralmente. El caso por antonomasia de la celebración de acuerdos multilaterales es, sin lugar a dudas, la creación del Convenio de Budapest del año 2001 (anteriormente detallado), del que forman parte no solamente Estados europeos sino también potencias extra regionales como Estados Unidos, Canadá, Japón y diversos países latinoamericanos. Este convenio sirve de marco para la cooperación en investigaciones destinadas a cuestiones específicas de cibercrimen.

Otra forma de llevar adelante cooperación en el ámbito internacional es la generación de espacios de diálogos dentro de foros y organismos internacionales de diversa índole. Naciones Unidas, desde la UIT, se encarga de desarrollar buenas prácticas en cuestiones de ciberseguridad y el análisis e investigación de las capacidades desarrolladas por cada Estado para determinar un índice global de ciberseguridad que ayuda a visualizar las fortalezas y debilidades de cada Estado en las cinco cuestiones planteadas anteriormente. En el caso de la OEA encontramos iniciativas de cooperación hemisféricas ante delitos cibernéticos y el fortalecimiento de capacidades de respuesta ante incidentes cibernéticos. Ejemplo de esto es la Declaración "Fortalecimiento de la Seguridad Cibernética en las Américas"[45] elaborada por el CICTE[46] en el año 2012 y los efectos que tuvo en la región.

Por su parte, en el marco de la Unión Europea, la Agencia de Seguridad de las Redes y de la Información (ENISA) se encarga de asesorar al sector público y privado de

[44] Dilema de seguridad: para los realistas ofensivos los Estados invierten en armas generando una carrera armamentista o un rearme cuando existe una percepción de amenaza gracias al consumo de armas de un país enemigo.
[45] De ella se hará referencia en el capítulo 2.
[46] CICTE: Comité Interamericano contra el Terrorismo de la Organización de Estados Americanos.

la comunidad para fomentar la adopción de Estrategias Nacionales de Ciberseguridad, fomentar la cooperación regional para crear capacidades y dar respuesta a incidentes cibernéticos y desarrollar la capacitación en manejo de crisis.

En el caso de la OTAN, el Centro de Excelencia de cooperación en ciberdefensa tiene entre sus funciones cooperar en cuestiones vinculadas a la educación, la investigación, el intercambio de información, el desarrollo de capacidades y el trabajo conjunto en materia de ciberdefensa. Sin lugar a dudas, los ejemplos más significativos de estos instrumentos son: a) el Global Forum on Cyber Expertise y b) el Forum of Incident Response and Security Teams. El primero de ellos cuenta con la participación de 38 Estados, diversas ONG y entidades privadas. Este organismo, tiene por objeto extender las buenas prácticas, la experiencia de sus miembros y la construcción de capacidades entre los participantes[47]. El segundo, cuenta con equipos de respuestas a incidentes cibernéticos de 88 países alrededor del mundo. Este organismo tiene por objeto compartir información sobre buenas prácticas, cuestiones técnicas, herramientas, información sensible, experiencias y la promoción del desarrollo de herramientas y CERT's alrededor del mundo.[48]

Otra forma que adquiere la cooperación internacional es la generación de capacidades a través de la capacitación mediante ejercicios combinados (práctica común en el ámbito de la seguridad internacional). El objetivo de estas prácticas es desarrollar capacidades, compartir información, realizar trabajos conjuntos en el marco de la gestión de incidentes y el manejo de crisis para así contribuir a profundizar los conocimientos las fuerzas de acuerdos a las buenas prácticas de aquellos países que se encuentran más preparados y establecer parámetros de acciones de prevención y respuesta para mitigar incidentes.

Ejemplos de estas prácticas son los ejercicios de ciberdefensa organizados por la OTAN anualmente desde 2010. En los *Locked Shields* (o escudos bloqueados) participan los Estados miembros de la OTAN y colaboran distintas fuerzas armadas y algunas empresas como Siemens, Cyber Test Systems, Iptron, Guard Time y otras. (CCD COE: 24-28 april 2017). En el caso de la Unión Europea, ENISA organiza cada dos años el CyberEurope simulando escenarios de crisis donde participan el sector público y privado

[47] GFCE. "The GFCE Organization". (consultado el 5 de marzo de 2018 en https://www.thegfce.com/organization)
[48] FIRST. "Mission." (consultado el 5 de marzo de 2018 en https://www.first.org/about/mission)

de todos los Estados Miembros.[49] En el marco de la OEA se realiza el International CyberEx en colaboración con el Instituto Nacional de Ciberseguridad de España (INCIBE) dirigido a los países miembros de la OEA y algunos invitados, se basa en un modelo de competencia que sirve de entrenamiento y capacitación para los participantes provenientes del sector público, privados y la academia.[50]

Estas simulaciones, en definitiva, intentan entrenar a los participantes, brindando la posibilidad de trabajar en conjunto y así poder potenciar las capacidades de cooperación entre los distintos países.

En definitiva, estos espacios de diálogo y los ejercicios combinados son manifestaciones de la inserción y/o participación de los países en el ámbito internacional. Cabe resaltar que todas las actividades vinculadas a la OEA arriba mencionadas cuentan con la participación de Argentina como país parte de dicho organismo.

Todos los instrumentos hasta aquí mencionados (provenientes de las cinco categorías desarrolladas por la UIT), no se adaptan a una única categoría ya que vinculan la política doméstica con la política exterior de los Estados.

Es posible vislumbrar que a pesar de que la cuestión cibernética es la más nueva de las amenazas transnacionales, los Estados han sabido comprender los efectos de esta para tomar medidas que ayuden a prevenir sus consecuencias.

Conclusiones parciales

El siglo XXI, caracterizado por el avance de las TICs como factor preponderante de la globalización, nos hace dar cuenta de que la tan pensada como *amenaza del mañana* o *amenaza del futuro* no es otra cosa que una de las principales amenazas actuales y que reviste gran importancia para la seguridad internacional.

A lo largo de este capítulo se puede apreciar que la cuestión cibernética como fenómeno de la seguridad internacional cobra distintas dinámicas, entre ellas las referidas a cuestiones de seguridad, inteligencia (estratégica, operacional y táctica) y defensa. Estas dinámicas aparecen a través de diversas manifestaciones con características propias que mutan de ataque en ataque según los intereses de sus actores y, por ende, es capaz de afectar a cualquier componente de poder de los Estados.

---

[49] ENISA. (2018). Cyber Europe. Recuperado de: https://www.enisa.europa.eu/topics/cyber-exercises/cyber-europe-programme

[50] CyberEx. "Description". (Consultado el 9 de marzo de 2018 en https://www.incibe-cert.es/en/international-cyberex)

Tal como lo plantea Kenneth Waltz, si bien los problemas a la seguridad internacional se plantean en el ámbito global, son los Estados, a partir de sus políticas domésticas, quienes proponen soluciones en el ámbito local que terminan afectando al ámbito global. En este sentido, en respuesta a dicho fenómeno, la comunidad internacional ha desarrollado diversos mecanismos que se manifiestan de forma individual y colectiva. La peligrosidad del fenómeno ha convocado a los distintos Estados a adoptar las medidas delineadas por terceros según los resultados logrados.

Ahora bien, el interrogante principal de este capítulo fue el de averiguar si el fenómeno cibernético es una amenaza real para la Argentina y cuáles son los factores de poder que pone en riesgo la percepción de dicha amenaza. Lo cierto es que Argentina, en este corto siglo XXI, se ha visto afectada con enormes cuotas de actividad cibernética criminal (no a los niveles de las principales potencias mundiales como Estados Unidos, Rusia y China, pero sí a nivel regional), siendo uno de los países de la región que se encuentran más expuestos a incidentes de seguridad de la información. Partiendo del hecho de que los ataques cibernéticos mencionados en el desarrollo de este capítulo solamente representan una muestra (tal vez poco significativa en relación a su número pero lo suficientemente significativa en cuanto al golpe que significó para nuestro país ser víctimas de estos ciberataques) de los que en verdad hubo en nuestro país, resulta inequívoco inferir que el fenómeno cibernético representa una amenaza real y latente para el país foco de estudio y que por ende, no tiene otra opción que la de tomar medidas para contrarrestar y prevenir los efectos del fenómeno cibernético. En cuanto a los componentes de poder en riesgo, vemos que, al ser un fenómeno multifacético es capaz de afectar todos los componentes de poder. Si bien estos componentes en Argentina no han sido afectados a gran escala es necesario estar preparados para prevenir y preservar su buen funcionamiento y seguridad.

Ahora bien, es menester suponer que el sistema internacional no sólo nos afecta a partir de la imposición de amenazas, sino también brindando soluciones estándares ante este flagelo a través de la experiencia de los grandes afectados, y es que la experiencia ajena ha contribuido innumerables veces a cuestiones estratégicas, tanto en tiempos de paz como de guerra, por lo que es posible que esta contribuya a mantener estable el ecosistema del ciberespacio. En esta línea, las cuestiones de ciberseguridad han sido contrarrestadas a través de herramientas creadas de forma individual y colectiva para responder, prevenir y contener los distintos ciberataques. Así, encontramos la adopción

de estrategias nacionales de ciberseguridad, la creación de CERTs nacionales, la celebración de acuerdos internacionales (bilaterales y multilaterales), la inserción y participación en organizaciones y foros en la arena internacional, la adopción de buenas prácticas y tantos otros elementos sirven hoy de herramientas concretas para la mitigación de los efectos de los ataques cibernéticos. De gran parte de estas medidas se ha hecho eco nuestro país.

De esta manera, es posible suponer que el contexto internacional influye en la definición del sistema de ciberseguridad a nivel nacional, siendo el escenario internacional y las políticas domésticas de los estados factores que se retroalimentan mutuamente. Por un lado, el contexto internacional permite cotejar las cartas que se barajan internacionalmente para aplicarlas de la mejor manera a la situación actual y futura de cada actor del sistema internacional, mientras que las políticas nacionales destinadas a dar solución a determinadas problemáticas repercuten en el ámbito global, tal como lo plantea Kenneth Waltz.

En este marco, nuestro país se ha visto tentado a adoptar algunas de las herramientas aportadas por otros países a fin de paliar la situación, pudiendo interpretar que existe cierto grado de influencia del contexto internacional en la definición del sistema de ciberseguridad nacional. Esto no implica un involucramiento de un país extranjero en la definición de las políticas locales, sino más bien la utilización de experiencias ajenas para dar respuesta a las particularidades con las que se presenta el fenómeno cibernético en Argentina.

En el siguiente capítulo analizaremos en profundidad cuáles fueron esas medidas adoptadas por Argentina a lo largo del siglo XXI para contrarrestar el fenómeno cibernético desde las esferas de la defensa nacional y la seguridad interior.

CAPÍTULO 2
ANÁLISIS DE LA POLÍTICA DOMÉSTICA: CIBERSEGURIDAD Y CIBERDEFENSA

Introducción

El objetivo que guiará el presente capítulo es el de iluminar sobre las falencias de las políticas relacionadas a la ciberseguridad y la ciberdefensa puestas en marcha en nuestro país. Los postulados que guiarán dicho análisis serán los planteados por Kenneth Waltz al visualizar la política de forma estructural que obliga a analizar la estructura de la política doméstica a fin de vislumbrar los resultados obtenidos.

A tal efecto, se analizará, en una primera instancia, algunas de las medidas aplicadas por los gobiernos de Cristina Fernández de Kirchner y Mauricio Macri tendientes a incrementar la digitalización del país, intensificando los usos de tecnología por parte de la Administración Pública Nacional y reduciendo la brecha digital en la población en general.

Acto seguido, se desarrollará lo referido a la definición de la cuestión cibernética en materia legal, teniendo presente las divisiones entre ciberseguridad y ciberdefensa que surgen del análisis normativo, pero también aquellas normas referidas exclusivamente a la protección de datos personales y cuestiones vinculadas al cibercrimen.

En una tercera instancia, se hará foco en el desarrollo de la cuestión analizando las partes involucradas en el proceso, sus funciones y capacidades. De esta manera, en materia de seguridad interior, se esquematizarán las distintas medidas que fueron nutriendo la ciberseguridad en Argentina para luego dar lugar al análisis en materia de defensa nacional, a través de la evolución de la ciberdefensa en nuestro país. A partir de allí, y como subapartado especial, se hará mención a los indicios de elaboración de una Estrategia Nacional de Ciberseguridad que fueron impulsados por el gobierno de Mauricio Macri desde julio de 2017. Todas estas medidas serán desarrolladas según la creación de estructuras en los distintos ámbitos de la Administración Pública Nacional vinculada con la ciberseguridad, ciberdefensa y el cibercrimen, partiendo de los postulados expuestos por Calam, Chinn, Fantini Porter y Noble (2018) quienes evidencian que los Estados que han desarrollado una única organización con la responsabilidad general en cuestiones de ciberseguridad obtienen resultados más eficaces y ponen de manifiesto la necesidad de entrelazar los límites institucionales de los distintos

departamentos, agencias y funciones para tratar de forma eficaz la ciberseguridad nacional.

A. Avance de las TICs en Argentina

Según el Observatorio de Ciberseguridad de América Latina y el Caribe (2016), Argentina -con una población de 42.980.026- registraba, en el año 2016, 66.356.509 abonos de celulares y 27.937.016 personas contaban con acceso a internet, configurando una penetración real de internet en ese año del 65%.

Ahora bien, si en el año 2016 encontramos estos datos cabe preguntarnos ¿cómo fue evolucionando el acceso a internet de la sociedad argentina y cuáles fueron las principales medidas tomadas por el gobierno para difundir el acceso a nuevas tecnologías y a internet? En este sentido, según datos arrojados por la Unión Internacional de Telecomunicaciones, en el año 2010 Argentina contaba con 19 millones de usuarios de internet, lo cual representa el 45% de su población para ese año. Para el año 2016, esta cifra se incrementa a 31 millones de usuarios, cubriendo el 71% del total de la población total[51], logrando que el acceso a internet crezca de forma más que proporcional al aumento poblacional, aumentando, el primer ítem en 12 millones de usuarios, mientras que el segundo sólo lo hizo en casi 3,5 millones de personas.

Por su parte, el gobierno nacional se ha enfocado desde hace ya varios años en la digitalización de la sociedad argentina a través de diversos proyectos que permitieron contraer la brecha tecnológica entre los distintos sectores sociales y dentro de la APN.

En el año 2006, a través de la ley 26.092, el Estado Nacional creó la Empresa Argentina de Soluciones Satelitales S.A., más conocida como ARSAT, con el propósito de mantener la posición orbital 81° Longitud Oeste brindada por la UIT a nuestro país. Desde ARSAT, el gobierno ha elaborado una serie de proyectos que tienen por objetivo brindar servicios telecomunicacionales a través de distintos medios. Con este propósito, desde 2010, el Estado Nacional le dio la responsabilidad a ARSAT del diseño, fabricación, puesta en órbita y operación de satélites propios con el objeto de incrementar las capacidades nacionales en materia de telecomunicaciones. A tal efecto, INVAP, empresa contratista encargada de la producción de ARSAT 1 y 2, puso en órbita al primero de ellos el 16 de octubre de 2014, lanzando al espacio el segundo en septiembre

[51] ITU. *Statistics. New data visualizationon Internet usersby región and country, 2010 – 2016* (consultado el 6 de noviembre de 2018 en https://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx)

de 2015 (ambos desde las Guayanas Francesas)[52]. De esta forma, y tal como lo describe Rodolfo Leonel Del Negro (2016), Argentina se hacía con el control efectivo de la posición orbital 81° LO, reclamada también por Gran Bretaña, y accedía a todo el mercado sudamericano, América Central y el Caribe y el sur de Estados Unidos en materia de telecomunicaciones, lo cual permite difundir el contenido multimedia desarrollado en Argentina y todo lo que eso conlleva (ejemplo: exportar la propia cultura). A partir de los proyectos de ARSAT el gobierno nacional cuenta con la capacidad de brindar servicios tele comunicacionales en todo el continente, a través de programas como Televisión Digital Abierta (TDA), el Plan de conectividad de escuelas rurales y el Plan Federal de Internet que tienen como objetivo expandir el acceso a internet en el territorio argentino.

Paralelamente a los proyectos realizados por ARSAT que promueven el acceso a internet, el Decreto 459/2010, promulgado por la entonces Presidente de la Nación, Cristina Fernández de Kirchner, ponía en funcionamiento el Programa Conectar Igualdad con el objeto de promover la inclusión digital haciendo disminuir la brecha tecnológica. A tal efecto, el gobierno nacional proporcionaba computadoras a alumnos y docentes de educación secundaria de escuelas públicas, educación especial e institutos de educación docente con el objetivo claro de garantizar el acceso de los jóvenes a las nuevas tecnologías. El programa entregó, entre 2010 y mediados de 2016, un aproximado de cinco millones y medio (5.421.596) de notebooks en escuelas secundarias, especiales, técnicas y de formación docente de todo el país.[53]

En diciembre de 2016, este programa fue transferido a la órbita del Ministerio de Educación de la Nación. Las evaluaciones "Aprender" de ese año (2016), iluminaron sobre el porcentaje de acceso tecnológico de docentes y alumnos. Del primer grupo, el 94% contaba con computadoras en su hogar, 4 de cada 10 habían sido destinatarios de computadoras portátiles provistas por el Estado bajo el programa Conectar Igualdad, el 83% de esos destinatarios eran poseedores de otra computadora en el hogar, mientras que casi un 89% tenía acceso a internet. Respecto al segundo grupo, los resultados arrojaron que el 87% de estudiantes de secundaria y el 67% de estudiantes de primaria eran

[52] INVAP. Satélites ARSAT. (consultado el 5 de noviembre de 2018 en http://www.invap.com.ar/es/espacial-y-gobierno/proyectos-espaciales/satelite-arsat.html)

[53] ANSES. (13/07/2016), "Conectar Igualdad ya superó las 100.000 notebooks entregadas en 2016", en ANSES noticias (consultado el 29 de octubre de 2018 en http://noticias.anses.gob.ar/noticia/conectar-igualdad-ya-supero-las-netbooks-entregadas-en-1736).

poseedores de computadoras en el hogar y que dos tercios de los estudiantes tienen acceso a internet en el hogar. (Ministerio de Educación: 2018).

Estos datos iluminaron sobre la necesidad de modificar el núcleo del programa, lo que trajo como respuesta su modificación. En abril de 2018, el Decreto 386 consideraba:

> Que el "PROGRAMA CONECTAR IGUALDAD.COM.AR" se creó oportunamente para abordar la brecha digital existente en el país, pero a OCHO (8) años de su lanzamiento, debe concluirse que este concepto mutó dando lugar al de alfabetización digital dónde la mera entrega de equipamiento dejó de ser suficiente si no se abordan contenidos específicos con una orientación pedagógica clara e integral en los establecimientos educativos, como núcleos determinantes responsables de los procesos de enseñanza y de aprendizaje.

Así, el PEN hacía oficial la creación del Plan Aprender Conectados bajo la órbita del Ministerio de Educación. Dicho plan tiene como ejes principales, no sólo el equipamiento tecnológico, sino también el desarrollo de contenidos, la conectividad y la formación docente, con el objeto de desarrollar capacidades, saberes fundamentales y educación digital. De esta manera, el Plan Conectar Igualdad pasó a formar parte de Aprender Conectados, siendo el encargado de dotar a los centros educativos (más no a docentes y alumnos) de tecnología adecuada para la puesta en funcionamiento del nuevo plan de alfabetización digital.

Desde el cambio de gestión, el gobierno de Mauricio Macri ha intensificado su deseo de llevar adelante la digitalización del Estado. Para ello, creó el Ministerio de Modernización (en diciembre de 2015) con el objeto de desarrollar planes de trabajo que permitan lograr agilidad y transparencia en la gestión a través de una Argentina más conectada. A tales efectos, el Decreto 434/2016 del Ejecutivo Nacional aprobaba el Plan de Modernización del Estado incluyendo cinco ejes principales, a saber:

- *Plan de Tecnología y Gobierno Digital: incorpora tecnología y redes con el fin de facilitar la interacción entre la sociedad y los organismos del Estado, a la vez que busca evolucionar a una administración sin papeles, automatizando la interacción entre los diferentes organismos gubernamentales;*
- *Gestión integral de recursos humanos: cambio organizacional que incorpore nuevas tecnologías en los procesos con el objeto de lograr mayor profesionalización de los trabajadores de la Administración Pública Nacional (APN);*

- *Gestión por resultados y compromisos públicos: la institucionalización de procesos que permitan la evolución de procesos y la definición de prioridades para la toma de decisiones, logrando implementar las decisiones y reasignar los recursos con el objeto de lograr un Estado más eficiente. A la vez, promover un modelo de gestión por resultados y calidad de servicios, basado en la transparencia de la gestión;*
- *Gobierno abierto e innovación pública: promover la participación social en la evaluación y el control de programas de los organismos públicos para lograr mayor confianza por parte del ciudadano con el gobierno;*
- *Estrategia país digital: estrategia transversal a las cuatro anteriores que tiene por objeto crear un marco de intercambio y colaboración mutua entre las administraciones públicas provinciales, municipales y de la Ciudad Autónoma de Buenos Aires.*

A través de dicho plan, el gobierno ha venido interviniendo en los organismos públicos con el objeto de digitalizar sus archivos, unificar las plataformas web en un único dominio que logre integrar toda la información del Estado nacional e implementar innovaciones tecnológicas a lo largo de todo el país para facilitar y agilizar los trámites y servicios brindados por la APN.

De esta manera, encontramos una voluntad manifiesta por parte del Estado de incorporar tecnologías en toda la APN y contraer, cada vez más, la brecha digital a nivel social.

B. Normativa vigente

Antes de introducirnos de lleno en la evolución de las políticas de ciberseguridad y ciberdefensa es menester ahondar en la normativa vigente que nos permite definir el alcance de la cuestión y analizar cuáles fueron los avances legales que logró nuestro país en materia cibernética.

Por una parte, la ley N° 23.554 de Defensa Nacional establece, en su artículo segundo, que la defensa nacional es

> La integración y la acción coordinada de todas las fuerzas de la Nación para la solución de aquellos conflictos que requieran el empleo de las Fuerzas Armadas, en forma disuasiva o efectiva, para enfrentar las agresiones de origen externo. Tiene por finalidad garantizar la soberanía e independencia de la Nación

> Argentina, su integridad territorial y capacidad de autodeterminación; proteger la vida y libertad de sus habitantes.

A dicho concepto, el Decreto 727/2006 agregaba que las Fuerzas Armadas (FFAA) serían utilizadas únicamente ante agresiones de origen externo perpetradas por las FFAA pertenecientes a otro Estado, limitando así el accionar del Instrumento Militar (IM). Esta limitación puede generar inconvenientes a la hora de hablar del ambiente cibernético, dado que la agresión puede o no ser estrictamente militar. El Decreto 683/2018 suprime lo expuesto por el Decreto 727/2006 dejando abierta la posibilidad de actuación por parte del IM ante cualquier agresión externa que sea incompatible con la Carta de Naciones Unidas, suprimiendo (aunque no necesariamente de forma consciente) la dificultad de actuar en el ambiente cibernético.

A pesar de ello, la Directiva Política de Defensa Nacional (DPDN por sus siglas) del año 2014 definía al ciberespacio como una dimensión transversal a los espacios tradicionales y advertía que solamente cuando operaciones cibernéticas tengan por fin impedir o afectar el funcionamiento del sistema de defensa nacional se habilitaba a las FFAA a actuar.

En la siguiente directiva (2018), el ciberespacio y su militarización cobraron mayor preponderancia reconociendo que el desarrollo de medios cibernéticos sirve para explotar las vulnerabilidades de los sistemas de comunicación, comando, control, computación, vigilancia y reconocimiento y destacando que las amenazas cibernéticas sofisticadas provienen de agencias militares y de inteligencia de otros Estados. Ante esto, brinda mayores capacidades al IM con el objeto de que logre reducir las vulnerabilidades del sistema de defensa nacional y pueda cooperar con otras agencias del gobierno respecto a cuestiones de ciberseguridad nacional.

En materia de seguridad pública, la ley N° 24.059 de Seguridad Interior establece en su artículo segundo que la seguridad interior es:

> La situación de hecho basada en el derecho en el cual se encuentran resguardadas la libertad, la vida y el patrimonio de sus habitantes, sus derechos y garantías y la plena vigencia de las instituciones del sistema representativo, republicano y federal que establece la Constitución Nacional.

Más adelante, la ley agrega que esta implica el empleo de elementos humanos y materiales de todas las fuerzas de seguridad (incluidas todas las fuerzas policiales provinciales) de la Nación.

De esta forma, se pone de manifiesto un sistema de defensa nacional y seguridad interior fragmentada que es posible extrapolar a cuestiones de ciberseguridad y ciberdefensa. Siguiendo esta lógica y así como la ley 24.059 en sus títulos V y VI habilita a las FFAA a actuar en cuestiones de seguridad interior de forma complementaria/subsidiaria al accionar de las FFSS, más adelante veremos cómo en la actualidad los elementos vinculados a la ciberseguridad y la ciberdefensa trabajan (solamente en algunos casos) de forma coordinada aunque manteniendo la división de sus funciones.

Por otro lado, en materia de seguridad de la información, Argentina ha desarrollado diversas leyes que pretenden regular y proteger a los usuarios, entre ellas: 1) ley N° 25.326 (2000) de Protección de Datos Personales: se refiere a la protección integral de datos personales asentados en archivos, registros, bancos de datos u otros medios técnicos de tratamiento de datos (tanto públicos como privados) destinados a dar informes para garantizar el derecho al honor y la intimidad de las personas. Dicha ley establece que la recolección de datos debe darse de acuerdo con su finalidad y ámbito de aplicación y sólo de conformidad explicita del titular de dichos datos, caso contrario el tratamiento de datos se considera ilícito. Por su parte, el responsable de archivar los datos debe garantizar la seguridad de los mismos y el secreto profesional; 2) la ley N° 25.506 de Firma Digital, vigente desde el año 2001, reconoce los efectos jurídicos del empleo y uso de la firma digital y electrónica y, pone de manifiesto los derechos y obligaciones del titular de la firma digital y la autoridad de aplicación, además de exponer conceptos como criptografía; 3) la ley N° 26.388 (2008), modificatoria del Código Penal, introdujo conceptos vinculados a delitos informáticos, incorporando sanciones penales a delitos como la producción, financiación, publicación, divulgación, posesión (y otras) de pornografía infantil; el acceso indebido a comunicaciones no dirigidas a su persona; el acceso ilícito a un sistema o dato informático de acceso restringido; el acceso ilegal a un banco de datos personales; la difusión, por parte de un funcionario público o aquel que adquiriera dicha información de forma ilegal, de información clasificada; la alteración de sistemas informáticos o transmisión de datos; entre otros; y 4) la ley 26.904, introdujo en el Código Penal, la figura del grooming, definiendo a este delito como el contactar a una

persona menor de edad por medio de comunicaciones electrónicas, telecomunicaciones o cualquier otra tecnología de transmisión de datos, con el propósito de cometer cualquier delito contra la integridad sexual.

Haciéndose eco del derecho internacional público, el 15 de diciembre de 2017 el gobierno adoptó la ley 27.411 con el objeto de aprobar la adhesión al Convenio sobre Ciberdelito (o Convención de Budapest). Dicha adhesión fue realizada con las siguientes reservas: a) el artículo 6.1.b[54] no regirá dado que prevé el supuesto de anticipación de la pena mediante la tipificación de actos preparatorios, lo cual resulta ajeno a la tradición legislativa del país; b) los artículos 9.1.d / 9.2.b / 9.2.c[55] no regirán por entenderlos incompatible al Código Penal argentino; c) hace una reserva parcial del artículo 9.1.e[56] haciéndolo aplicable de acuerdo a la legislación vigente, cuando la posesión fuera cometida con inequívocos fines de distribución y comercialización; d) el artículo 22.1.d[57] no regirá dado que difiere de las reglas que rigen la definición de la competencia penal nacional; y e) hace reserva de aplicación del artículo 29.4[58] alegando que el requisito de doble incriminación es una de las bases fundamentales de la ley de cooperación internacional en materia penal.

C. Políticas de ciberseguridad y ciberdefensa

Calam, Chinn, FantiniPorter y Noble (september 2018) aseguran que los Estados que han desarrollado una única organización con la responsabilidad general en cuestiones de ciberseguridad poseen resultados más eficaces, dado que de esta forma, quien se encarga de tomar las decisiones, los recursos asignados (presupuesto, recursos humanos y tecnología) y quien conoce el ambiente cibernético poseen un diálogo directo. De lo

[54] A saber, art. 6.1.b: posesión de dispositivos, programas informáticos, contraseñas, código de acceso o datos informáticos con la intención de utilizarlos para cometer alguna infracción a la ley.
[55] A saber, art. 9.1.d: "procurarse o procurar a otro pornografía infantil a través de un sistema informático." | art. 9.2.b: "una persona que aparece como un menor adoptando un comportamiento sexualmente explícito" (se considera pornografía infantil) | art. 9.2.c: "imágenes realistas que representen un menor adoptando un comportamiento sexualmente explícito" se considera pornografía infantil. (p. 12 y 13).
[56] A saber, art. 9.1.e: posesión de pornografía infantil en un sistema informático o en un medio de almacenamiento de datos informáticos. (p. 12).
[57] A saber, art. 22.1.d: las partes adoptarán medidas legislativas cuando la infracción se haya cometido por "uno de sus súbditos, si la infracción es punible penalmente en el lugar donde se ha cometido o si la infracción no pertenece a la competencia territorial de ningún Estado." (p. 21)
[58] A saber, art. 29.4 sobre conservación inmediata de datos informáticos almacenados: "si un Estado exige la doble incriminación como condición para atender a una demanda de asistencia para registrar o acceder de otro modo, decomisar u obtener por otro medio, o lograr la comunicación de dichos datos, por infracciones diversas a las establecidas en los art. 2 a 11 […] podrá negarse a la demanda de conservación […] si tiene fundadas sospechas de que, en el momento de la comunicación de los datos, el otro Estado no cumplirá la exigencia de la doble incriminación." (p. 27).

contrario se reduce la eficiencia, lo cual puede traducirse en malas políticas, normativas débiles y falta de inversión.

Un claro ejemplo de eficiencia, según los autores, es el *National Cyber Security Center* creado en el año 2016 por Reino Unido. Esta superestructura nuclea todos los esfuerzos del Estado para velar por un ciberespacio seguro, proteger las Infraestructuras Críticas, el buen funcionamiento de las empresas y a los usuarios en general.

a. Políticas de ciberseguridad

En el caso de Argentina, los esfuerzos por tratar la cuestión cibernética (desde la óptica de la seguridad) de forma estructural se potencian en el año 2011, cuando Jefatura de Gabinete de Ministros creó, a través de la Resolución 580, el Programa Nacional de Infraestructuras Críticas de la Información y de la Comunicación en el ámbito de la Oficina Nacional de Tecnologías de la Información (ONTI), dependiente de la Subsecretaría de Tecnologías de Gestión de la Secretaría de Gabinete. El objeto de dicho programa era adoptar un marco jurídico regulatorio que permita la identificación y protección de las infraestructuras estratégicas y críticas del Sector Público Nacional.

Así, la resolución dotaba al Programa ICIC de los siguientes objetivos:[59]

a) Elaborar normas pertinentes para los usos de las TICs en el sector público;
b) Colaborar con el sector privado y fortalecer los lazos público-privados;
c) Administrar la información de reportes de incidentes;
d) Establecer prioridades y planos estratégicos de ciberseguridad e implementar avances tecnológicos para la protección de IC;
e) Investigar sobre nuevas tecnologías y herramientas de seguridad informática que puedan ser aplicadas en la Administración Pública;
f) Asesorar y alertar a los organismos adheridos sobre los riesgos del ciberespacio;
g) Coordinar la implementación de ejercicios de respuesta;
h) Promover la coordinación entre las redes de información del sector público;
i) Elaborar un informe anual de la situación de la ciberseguridad;
j) Monitorear los servicios brindados por la Administración Pública a través de internet;

[59] Estos objetivos más adelante se verán reflejados en la creación de estructura organizacional del Programa ICIC.

k) Promover la concientización de los riesgos del uso de medios digitales en el sector público y los usuarios en general y la necesidad de coordinar los esfuerzos público-privados para proteger las IC;
l) Difundir información útil para incrementar la seguridad de las redes;
m) Interactuar con equipos de similar naturaleza.

Por su parte, la ONTI sería la responsable de coordinar las actividades desarrolladas por el Programa con otras agencias del gobierno, organizaciones civiles y el sector privado.

En septiembre de ese año, la ONTI aprobaba el formulario de adhesión al programa y un convenio de confidencialidad con el objeto de que los organismos del sector público y organizaciones civiles y privadas puedan sumarse a las actividades y políticas fijadas por el nuevo programa de ciberseguridad.

De esa manera, Jefatura de Gabinete de Ministros se hacía responsable del desarrollo de las políticas de ciberseguridad en Argentina.

A partir de entonces, el Programa ICIC estaría encargado de desarrollar alertas, recomendaciones y capacitaciones para el personal de la APN, tomar denuncias de incidentes en el ciberespacio y adoptar normas y estándares vinculados a la seguridad de la información.

Aún hoy[60] dicho programa es el encargado de difundir una serie de recomendaciones que tienen por objeto concientizar a los usuarios provenientes de todos los ámbitos (aunque en especial a los agentes de la APN) respecto a la seguridad de la información. En este sentido, si analizamos el sitio web del programa encontraremos una serie de recomendaciones de distinta índole, entre las que se destacan: contraseñas seguras, resguardo de información (impresa, escrita y hablada), protección de recursos móviles (computadoras, celulares), protección de pendrives, utilización de redes de organismos públicos (Ministerios), usos de internet, de aplicaciones, de mail corporativo, privacidad e incluso se advierte sobre medidas contra el ciberbullying y el grooming.[61]

[60] Noviembre de 2018.
[61] Jefatura Gabinete de Ministros. Recomendaciones de Ciberseguridad, en Argentina.gob.ar . (consultado el 1 de noviembre de 2018 en https://www.argentina.gob.ar/modernizacion/infraestructuras-criticas-de-informacion-y-ciberseguridad/recomendaciones)

Las alertas emitidas por el programa responden, en primera instancia, a la divulgación de información sobre vulnerabilidades del sistema que vienen acompañadas de actualizaciones seguras.

Por otra parte, en materia de capacitación, el Programa ICIC ha venido desarrollando una serie de cursos a nivel federal. En la actualidad, los cursos destinados a agentes de la APN han cobrado mayor protagonismo en el INAP (portal de capacitación del Estado), donde se puede encontrar variedad de recursos educativos a fin de concientizar al personal en materia de seguridad de la información. Esto complementa los Ejercicios Nacionales de Respuesta a Incidentes Cibernéticos que se han realizado bajo la coordinación del Programa ICIC y que fueron desarrollados con el objeto de capacitar personal en diversas materias que hacen a la seguridad de la información desde la perspectiva legal e incluso la detección de vulnerabilidades y protección informática. En consonancia con esto, *"el ejercicio consiste en un entrenamiento concreto de ciberseguridad"* y convoca a los especialistas de seguridad informática de los distintos organismos del Estado para que *"analicen, detecten y resistan distintos ataques generados con la intención de impactar en sus infraestructuras y sustraer, modificar o eliminar la información."*[62]

En otro orden de ideas, el 7 de marzo de 2012, el Comité Interamericano Contra el Terrorismo (de ahora en más será denominado CICTE) aprobó la Declaración "Fortalecimiento de la Seguridad Cibernética en las Américas" a través de la cual, los Estados Parte de la OEA (entre ellos Argentina), se comprometieron a:

a) Que todos los Estados establezcan y fortalezcan sus *Computer Security Incident Response Team* (de ahora en más, CSIRT);
b) Participar en la Red de Seguridad Hemisférica de los CSIRT y de Autoridades en Seguridad Cibernética, aumentando el intercambio de información, la cooperación para proteger las IC y prevenir y responder incidentes en el ambiente cibernético;
c) Reforzar la seguridad y la resistencia de las TICs ante ciberamenazas, incluyendo aquellas contra las IC (a saber: denomina IC a los sistemas de energía, financieros, transporte y telecomunicaciones);

[62] InfoSecurity News. (octubre 2015). "Entrevista. Argentina – Ejercicio Nacional de Respuesta a Incidentes Cibernéticos", en *infosecuritynews* (consultado el 28 de febrero de 2019 en http://www.infosecurityvip.com/newsletter/entrevista_oct15.html)

d) Desarrollar una estrategia nacional de seguridad cibernética integral en la cual se involucre a todos los actores pertinentes en el proceso de desarrollo e implementación;
e) Promover la cooperación público-privada.

En ese marco, la ONTI, a través de la Disposición 2/2013 del 8 de agosto de ese año, dispuso de la creación de cuatro grupos de trabajo, a saber: ICIC - CERT, ICIC - GAP (Grupo de Acción Preventiva), ICIC - GICI (Grupo de Infraestructuras Críticas de la Información) e ICIC - INTERNET SANO.

El primero de ellos con las funciones de administrar información de reportes de incidentes en el sector público adherido, asesorar en cuestiones técnicas, centralizar los reportes de incidentes ocurridos en redes teleinformáticas, coordinar a las unidades de administración de dichas redes y difundir información útil.

El segundo grupo de trabajo fue creado con el objeto de investigar nuevas tecnologías y herramientas de seguridad informáticas, incorporar dichas tecnologías para minimizar las posibles vulnerabilidades, brindar asesoramiento sobre dichas herramientas y técnicas y monitorear los servicios del sector público en internet.

Por su parte, el Grupo de Infraestructuras Criticas de la Información se hizo con la responsabilidad de: adoptar normas para incrementar los niveles de seguridad, colaborar con el sector privado, establecer prioridades y planes estratégicos, alertar a organismos adheridos y coordinar los ejercicios de respuesta a incidentes.

Mientras que, el último de estos grupos de trabajo tenía por objeto elaborar planes de concientización sobre el uso de medios digitales en el sector público y a los usuarios en general, pero también reparar sobre el rol compartido entre el sector público y privado en la protección de IC.

Todos estos grupos debían, a la vez, interactuar con equipos similares.[63]

En septiembre de 2013, la ONTI aprobaba la actualización de la Política de Seguridad de la Información Modelo[64], que había sido implementada en el año 2005, tras considerar un incremento en la cantidad y variedad de amenazas y vulnerabilidades que poseen los activos de información. Esta política debía ser interpretada como un modelo de mejores prácticas en materia de seguridad de la información para que organismos de

[63] Actualmente estos grupos no están en actividad.
[64] Con el fin de mantener su vigencia y nivel de eficacia, la ONTI actualizó nuevamente este documento en febrero de 2015.

la Administración Pública puedan replicarla y ajustarla a sus necesidades y funciones para lograr óptimos estándares de seguridad. Su objetivo es el de velar por la protección de la información de un gran espectro de amenazas y vulnerabilidades a fin de asegurar su confidencialidad, integridad, disponibilidad y legalidad.

En junio de 2015, el gobierno nacional, a través del Decreto N° 1067, creó la Subsecretaría de Protección de Infraestructuras Críticas de Información y Seguridad en el ámbito de la Secretaría de Gabinete de Jefatura de Gabinete de Ministros, transfiriendo el Programa ICIC a la órbita de la Dirección Nacional de Infraestructuras Críticas de la Información y la Ciberseguridad, dependiente de la recién creada Subsecretaría. Dicha Subsecretaría, tenía entre sus objetivos: a) elaborar normas y estándares de seguridad de la información, por lo que se incitaba a aprobar la Política de Seguridad Modelo; b) identificar y proteger las IC; c) elaborar la estrategia nacional de protección de IC; d) supervisar, monitorear, analizar y detectar los activos críticos de la información; e) entender en los procesos del CERT nacional; f) elaborar políticas de capacitación para la APN, organizaciones civiles, el sector privado y la academia; y g) elaborar programas de asistencia a la APN. De esta forma, la responsabilidad de protección de IC y de seguridad de la información conferida a la ONTI desde 2011 fue trasladada a la nueva Subsecretaría.

A pesar de que uno de los objetivos de esta dependencia era el elaborar una Estrategia Nacional referida a la protección de IC, y por ende a la ciberseguridad, no se logró llevarlo a cabo. A pesar de ello, este objetivo impulsó la creación de una mesa de trabajo de ciberseguridad que logró establecer cuatro reuniones entre la Dirección de Nic Ar (dependeinte del Ministerio de Relaciones Exteriores y Culto), la Dirección Nacional de Protección de Datos Personales (dependiente del Ministerio de Justicia), la Dirección General de Ciberdefensa (del Ministerio de Defensa), el Ministerio Público Fiscal, Jefatura de Gabinete de Ministros (a través de la Subsecretaría arriba mencionada) y la Agencia Federal de Inteligencia. (ICIC: 2015)

Dichas reuniones tuvieron el objetivo de entablar diálogos tendientes a coordinar acciones y proyectos de ciberseguridad y protección de Infraestructuras Críticas de la Información y la Ciberseguridad que tengan por misión elaborar una Estrategia Nacional de Protección de ICIC que contemple la aplicación de políticas conjuntas en este sentido. (ICIC: 2015).

Ahora bien, el proceso de creación de una superestructura capaz de centralizar el control de las políticas destinadas a la ciberseguridad se hace manifiesto a partir del

cambio de administración a nivel nacional, bajo la presidencia de Mauricio Macri. En diciembre de 2015, a través del Decreto N° 13, el nuevo gobierno consideraba:

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

Entre las funciones con las que se dotaba a la nueva cartera ministerial, encontramos:

a) Intervenir en la definición de estrategias y estándares sobre tecnologías de información, comunicaciones asociadas y otros sistemas electrónicos de tratamiento de información de la Administración Nacional;
b) Diseñar, coordinar e implementar la incorporación y mejoramiento de los procesos, tecnologías, infraestructura informática y sistemas y tecnologías de gestión de la Administración Pública Nacional;
c) Proponer diseños en los procedimientos administrativos que propicien sus simplificación, transparencia y control social y elaborar los desarrollos informáticos correspondientes;
d) Actuar como autoridad de aplicación del régimen normativo que establece la infraestructura de firma digital para el sector público nacional;
e) Intervenir en el desarrollo de sistemas tecnológicos con alcance transversal o común a los organismos y entes de la APN;
f) Entender en lo relativo a las políticas, normas y sistemas de compras del sector público nacional.

Dentro del nuevo ministerio, la Subsecretaría de Tecnología y Ciberseguridad, a través del Decreto 898/2016, adquirió las funciones de: elaborar una estrategia para la protección de Infraestructuras Críticas de la Información y de la Ciberseguridad; supervisar el funcionamiento de los servicios de infraestructura de los centros de datos; garantizar la confiabilidad y disponibilidad de los sistemas informáticos de la APN; asistir a usuarios de tecnología del sector público; entender en materia de dictado de normas, políticas, estándares y procedimientos de tecnología y seguridad informática; asistir en la

definición de IC y fomentar la cooperación con otros sectores; difundir las mejores prácticas y capacitaciones; supervisar el accionar de la ONTI; entre otras.

De esta manera, el Ministerio de Modernización se hacía con la responsabilidad general en materia de ciberseguridad a nivel nacional, lo cual no quiere decir que sea esta la única agencia de gobierno en Argentina con la capacidad de tomar decisiones para la adopción de medidas de respuesta ante incidentes cibernéticos. Así, desde diciembre de 2015 hasta mediados del año 2018, la responsabilidad sobre la seguridad de la información en Argentina recayó en el nuevo Ministerio de Modernización, que, tras su disolución pasó a depender nuevamente de Jefatura de Gabinete de Ministros.

En marzo de 2016, el Ministerio de Justicia y Derechos Humanos creó el Programa Nacional contra la Criminalidad Informática a través de la Resolución N° 69. Este programa tuvo dos objetivos: 1) promover las acciones necesarias para mejorar las respuestas del sistema penal frente a los delitos informáticos; y 2) propiciar la eficiencia en las investigaciones penales mediante herramientas tecnológicas garantizando el buen uso de las mismas.

En consonancia con esto, el Ministerio de Justicia promueve nueva legislación penal y procesar para enfrentar los ciberdelitos, realiza capacitaciones en materia de delitos informáticos, evidencia digital, proceso penal y cooperación internacional; y forma a los operadores del sistema penal en cuestiones relacionadas a la investigación de crímenes infromáticos.[65]

Tras cumplir el primer año de gestión, en diciembre de 2016, Mauricio Macri presentó los 100 objetivos de gobierno que fueron agrupados en ocho áreas diferentes, entre las que figura la ciberseguridad como objetivo número 74, bajo el área de "combate al narcotráfico y mejora de la inseguridad".[66]

La importancia que sugieren las cuestiones cibernéticas se vieron reflejadas en el ámbito internacional. La cooperación en el marco de la OEA llevó a un CERT de Argentina (CERT UNLP) a participar del primer CyberEx organizado en conjunto con INCIBE España con el objeto de desarrollar un ciberejercicio en el que participen 45 equipos técnicos provenientes de distintos Estados que permita fortalecer las capacidades

[65] PEN. Nueva capacitación en ciberdelito para fiscales especializados, (consultado el 4 de marzo de 2019 en https://www.argentina.gob.ar/noticias/nueva-capacitacion-en-ciberdelito-para-fiscales-especializados)

[66] Para nuestro entrevistado denominado Fuente D, esto puede ser leído *"como que hay 73 prioridades antes o que compone los proyectos estratégicos del actual gobierno sin ocupar necesariamente el lugar número 74 porque todos los objetivos son igualmente importantes"*. Entrevista reservada con Fuente D (civil), 11 de septiembre de 2018, Buenos Aires, Argentina.

de respuesta a incidentes cibernéticos, mejorar la colaboración y la cooperación internacional en esta materia. En el año 2016 Argentina obtuvo el segundo puesto de este ciberejercicio, solamente por detrás de Colombia, mientras que para los años 2017 y 2018 se hizo del quinto puesto.[67]

Una de las principales formas de distribuir responsabilidades en el ámbito de la ciberseguridad e impulsar el objetivo de gobierno N° 74 fue la creación de estructuras referidas al cibercrimen dentro del Ministerio de Seguridad de la Nación. Para ello, el día 12 de octubre de 2017, a través de la Resolución ministerial N° 1107-E, se conformaba el Comité de Respuesta de Incidentes de Seguridad Informática del Ministerio de Seguridad con el objeto de:

- Coordinar acciones ante usos nocivos y/o ilícitos de infraestructuras tecnológicas, redes, y sistemas de información y comunicación del Ministerio y órganos dependientes;
- Colaborar en la protección de las IC del Ministerio y sus órganos dependientes;
- Fomentar la confianza y seguridad de las redes y la información que por ellas circula;
- Divulgar el valor de la seguridad de la información;
- Difundir mejores prácticas para la prevención y respuesta a incidentes;
- Cooperar con organizaciones nacionales e internacionales de seguridad con el fin de compartir información para hacer frente de forma eficaz a las amenazas cibernéticas;

Este Comité fue integrado por un equipo de ocho agentes federales (dos agentes por cada fuerza: Gendarmería Nacional, Policía Federal Argentina, Policía de Seguridad Aeroportuaria y Prefectura Naval) con la misión de funcionar los 365 días del año 24/7.

Más tarde, a través de la Decisión Administrativa N° 299 de marzo de 2018, se aprobó la nueva estructura organizativa del Ministerio de Seguridad. En ella se hizo oficial la creación de la Dirección Nacional de Investigaciones que tendrá por objetivo el conducir las investigaciones sobre crimen organizado y delitos complejos, para lo cual deberá:

[67] International CyberEx (consultado el 28 de febrero de 2019 en https://www.cyberex.es/international/es/resultado_2016)

> "coordinar la aplicación de políticas, estrategias y acciones en las investigaciones sobre criminalidad organizada y en particular en la atención de los delitos del terrorismo, tráfico de armas, trata de personas, tráfico de vehículos y autopartes, ciberdelitos, lavado de dinero, delitos económicos y secuestros." (Anexo 2, p. 20)

En el anexo cuarto de dicha normativa, se detalla el accionar de la Dirección de Investigaciones del Ciberdelito, entre las que figuran:

- *Asistir al Director Nacional en la elaboración de objetivos, políticas y estrategias nacionales para combatir la delincuencia virtual, las diferentes modalidades de estafa que se dan en Internet y otros delitos a través de las redes sociales, en particular los dirigidos contra la infancia, la integridad sexual y de terrorismo.*
- *Investigar la ocurrencia de los delitos descriptos anteriormente articulando y coordinando con las áreas específicas de las Fuerzas Policiales y de Seguridad así como con otros organismos o instituciones estatales o privadas, que resulten adecuados para el caso.*
- *Participar, en la medida de las instrucciones que reciba, en la elaboración de proyectos de denuncias criminales y demás denuncias judiciales relacionadas con los delitos mencionados.*
- *Asistir al Representante del Gobierno Nacional como parte querellante, en las investigaciones criminales que se realicen en denuncias sobre los delitos de su competencia.*
- *Estudiar técnicamente las cambiantes particularidades de las modalidades delictivas enunciadas, diseñando y proponiendo medidas para evitar su realización y propagación.*
- *Diseñar y proponer un "Plan Federal de Prevención de Delitos Tecnológicos y ciberdelitos" y coordinar su implementación.*
- *Elaborar y ejecutar el proyecto de creación del Registro de Peritos Oficiales en Ciberdelitos en colaboración con el Poder Judicial, basado en un área propia, articulada con las Fuerzas Policiales y de Seguridad, capaz de realizar los estudios e investigaciones técnico-científicas necesarias para apoyar los casos judiciales.*

Así, a partir del año 2018 las cuestiones relacionadas al cibercrimen serían coordinadas directamente por ésta nueva dirección, en el marco del Ministerio de Seguridad, con competencia directa para requerir la colaboración de las Fuerzas de Seguridad a nivel federal. En palabras de la Ministra de Seguridad, Patricia Bullrich, desde dicha dirección se coordina la creación de las direcciones de ciberdelito de todas las policías.[68]

Hasta el momento, la Dirección ha venido trabajando en el fomento de campañas de concientización y detección de vulnerabilidades lanzando ciberataques de distinto tipo (phishing por ejemplo) para detectar el grado de vulnerabilidad de los usuarios en general y luego contactarse con ellos para generar mayor conciencia en el uso del ciberespacio[69]. En este sentido, Patricia Bullrich detallaba:

> "en cada una de las 34 reuniones del G20, previas a la cumbre, Pablo Lázaro (Director de Investigaciones de Ciberdelito del Ministerio de Seguridad de la Nación), realiza ataques para ver si estamos protegidos, generamos pruebas constantemente para ver la capacidad de protección."[70]

b. Políticas de ciberdefensa

En el caso de la Defensa nacional, el descubrimiento de las cuestiones vinculadas al ciberespacio surge años antes por impulso de las FFAA que crearon sus propios elementos de ciberdefensa. Durante todo el siglo XXI, cada fuerza desarrolló estructuras vinculadas a la seguridad de la información que, ya en 2014, se habían convertido en Centros de Ciberdefensa con capacidades operativas (o SOC)[71].

Desde el Ministerio de Defensa, los primeros esfuerzos se remontan a 2006, cuando se crea el Comité de Seguridad de la Información a través de la Resolución Ministerial N° 364, con el objeto de contribuir, en coordinación con Jefatura de Gabinete de Ministros, a la protección de Infraestructuras Críticas. (MINDEF: 2018).

---

[68] Schulkin, J. (3 de agosto de 2018). "Realizan simulaciones de respuesta a ataques cibernéticos en la Argentina antes del G20", en *infobae* (consultado el 17/9/2018 en https://www.infobae.com/tecno/2018/08/03/simulaciones-de-respuesta-a-ataques-ciberneticos-en-la-argentina-antes-del-g20/)

[69] Entrevista reservada con Fuente D (civil), 11 de septiembre de 2018, Buenos Aires, Argentina.

[70] Schulkin, J. (3 de agosto de 2018). "Realizan simulaciones de respuesta a ataques cibernéticos en la Argentina antes del G20", en *infobae* (consultado el 17/9/2018 en https://www.infobae.com/tecno/2018/08/03/simulaciones-de-respuesta-a-ataques-ciberneticos-en-la-argentina-antes-del-g20/)

[71] Para ampliar sobre el desarrollo de las FFAA en materia cibernética (el cuál no hace al tema central de esta tesis) consultar Albarracín Keticoglu, Ana y Segio Eissa. (2019). "Ciberdefensa en Argentina. Pujas en torno a su definición", mimeo, Buenos Aires, Argentina.

Años más tarde, la Resolución MD N° 8/2010 del Secretario de Estrategia y Asuntos Militares ordenó la creación de un grupo de trabajo con el objeto de analizar, desde el punto de vista estratégico y normativo, la relevancia e implicancia del ciberespacio para el Sistema de Defensa Nacional. (Justibró, Gastaldi y Fernandez: 2014).

Durante el año 2010, el grupo de trabajo realizó varias reuniones que produjeron diversos informes sin llegar a elaborar ningún documento de carácter estratégico o normativa ministerial. Por su parte, el Proyecto de Capacidades Militares de 2010 definía a la ciberdefensa como un área de capacidades de inteligencia, lo que se vio replicado en el Plan de Capacidades Militares de 2011. Esto impulsó la participación de la DINIEM en el proceso de debate de la definición de ciberdefensa.[72] El debate[73] dentro del Estado Mayor Conjunto de las Fuerzas Armadas (EMCO) culminó con la propuesta de creación de una Agencia de Ciberdefensa. (Albarracín y Eissa: 2019).

En 2013, tras considerarse que el desarrollo y expansión de las TICs exponen la importancia del ciberespacio como ámbito de interés para la Defensa Nacional, se creó la Unidad de Coordinación de Ciberdefensa a través de la Resolución MD N° 385. La cual tenía por función:

- *Coordinar las políticas y desempeño de los actores involucrados a la ciberdefensa;*
- *Efectuar un relevamiento de las IC, recursos humanos, actividades y procesos vinculados a la ciberdefensa;*
- *Diseñar, planificar estratégicamente e implementar las políticas de ciberdefensa;*
- *Impulsar el desarrollo doctrinario;*
- *Analizar la evolución normativa de la ciberdefensa;*
- *Intervenir en la implementación del Programa ICIC y coordinar el trabajo interagencial;*
- *Cooperar con el ámbito académico y científico;*
- *Fomentar la formación de recursos humanos;*
- *Promover la adopción de procedimientos y protocolos comunes.*

[72] El proceso referido a la DINIEM se expondrá en el capítulo siguiente.
[73] Para ampliar información sobre el proceso de debate consultar Albarracín Keticoglu, Ana y Sergio Eissa. (2019). "Ciberdefensa en Argentina. Pujas en torno a su definición", mimeo, Buenos Aires, Argentina.

En este sentido, se consideró necesario tramitar la adhesión del Ministerio de Defensa al Programa ICIC y elaborar una norma que delimite el alcance de la ciberdefensa. (Albarracín y Eissa: 2019).

En materia internacional, durante noviembre de 2013 se desarrollaron reuniones bilaterales entre los Ministerios de Defensa de Argentina y Brasil en las que se acordaron realizar actividades de cooperación e intercambio entre ambos países en áreas referidas a la capacitación, métodos y sistemas tecnológicos, desarrollo doctrinario e investigación científica. (Ministerio de Defensa de Brasil: 2013). En el marco de dichas reuniones, los Ministros de Defensa de Argentina y Brasil firmaron una declaración conjunta en la que se destaca la importancia de la cooperación entre ambas naciones en materia de defensa y sostiene la necesidad de impulsar la cooperación en defensa cibernética. (Ministerios de Defensa de Argentina y Brasil: 2013).

El punto culmine en la evolución de la ciberdefensa llega cuando el Ministerio de Defensa crea las últimas dos estructuras. La primera de ellas se oficializó a través de la Resolución 343 de mayo de 2014, tratándose de la creación del Comando Conjunto de Ciberdefensa bajo la órbita del Estado Mayor Conjunto de las Fuerzas Armadas, con el objeto de garantizar la defensa contra ciberataques que pretendan obstaculizar las operaciones del Instrumento Militar y garantizar la defensa contra aquellos ciberataques dirigidos a objetivos de valor estratégico para el sistema de Defensa Nacional. Este Comando, a su vez, fue dotado de un Centro de Operaciones de Ciberdefensa que realizará tareas de detección de anomalías en redes informáticas del IM, examinar falsos positivos, analizar el nivel de riesgo de los eventos y alertar al IM sobre incidentes cibernéticos; y un Centro de Ingeniería de Ciberdefensa que cuenta con tareas de análisis técnico, forensia y resiliencia, es decir, recuperar las capacidades de la tecnología afectada.[74]

Desde su creación, el CCCD ha venido desarrollando vínculos con países alrededor del mundo. Desde el año 2015 hasta la actualidad ha participado de reuniones bilaterales con sus homólogos de Alemania, Brasil, Chile, Colombia, España, Estados Unidos, Israel, Italia, Japón, Perú y Uruguay, con el objeto de conocer de qué forma afrontan estos países las cuestiones de defensa cibernética, generar vínculos e intercambios en la materia[75]. Con este propósito, por iniciativa española en el año 2016

[74] Entrevista reservada con Fuente I (militar), 4 de octubre de 2018, Buenos Aires, Argentina.
[75] Entrevista reservada con Fuente I (militar), 4 de octubre de 2018, Buenos Aires, Argentina.

surgió el Foro Iberoamericano de Ciberdefensa. En su primer encuentro, dicho Foro contó con la participación de Argentina, Brasil, Chile, Colombia, España, México, Perú y Portugal esclareciendo la necesidad de cooperar en la materia en áreas vinculadas a la formación, ejecución de ejercicios conjuntos, intercambio de información, investigación en innovación en ciberdefensa.[76]

En la actualidad, Argentina concentra sus esfuerzos para estimular los lazos internacionales a través de dicho Foro. En este sentido, el CCCD participó con sus pares de Brasil, Colombia, España, México y Portugal, del ejercicio de ciberdefensa desarrollado en 2017 en Brasilia, el cual contó con tres (3) fases: reconocimiento del Simulador Nacional de Operaciones Cibernéticas; identificación de vulnerabilidades; y mitigación en base a la cooperación.[77]

En marzo de 2018, Buenos Aires fue sede del II Foro Iberoamericano de Ciberdefensa, en el cual, los países parte decidieron desarrollar dos actividades anuales, a saber: una reunión anual durante el mes de marzo y un ejercicio combinado anual entre las Fuerzas Armadas durante el mes de octubre.[78] Cabe resaltar que el ciberejercicio de 2018 tuvo sede en Madrid durante el mes de octubre y contó con la participación de equipos provenientes de Argentina, Brasil, Chile, Colombia, España, Portugal y México. La empresa española Indra fue quien proporcionó la ingeniería y soporte técnico necesarios para el desarrollo del ejercicio, desarrollando escenarios donde las delegaciones debían defender infraestructuras críticas de distintos tipos de incidentes cibernéticos como denegación de servicios, *botnet*, cifrado de información y otros.[79] Por otra parte, al finalizar la reunión del Foro en Buenos Aires, Portugal se comprometió a elaborar un esquema de los procedimientos para llevar adelante las actividades del Foro.

[76] Infodefensa (2016, 3 de junio), "España y seis países latinoamericanos acuerdan un programa común de ciberdefensa", en *Infodefensa*, Madrid (consultado el 7 de septiembre de 2018 en http://www.infodefensa.com/es/2016/06/03/noticia-espana-latinoamerica-acuerdan-colaborar-ciberdefensa.html).

[77] Szklarz, E. (21 de diciembre de 2017), "Brasil promueve primer Ejercicio Iberoamericano de Defensa Cibernética", en *Diálogo-Américas* (consultado el 17 de septiembre de 2018 en https://dialogo-americas.com/es/articles/brazil-organizes-first-ibero-american-cyber-defense-exercise).

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

[79] Estado Mayor de la Defensa de España (2018, 26 de octubre), "Equipos de siete naciones participan en el II Ejercicio del Foro Iberoamericano de Ciberdefensa", en *Estado Mayor de la Defensa de España,* Madrid (consultado el 29 de octubre de 2018 en http://www.emad.mde.es/EMAD/novemad/noticias/2018/10/Listado/181029-ni-foro-iberomaricano-ciberdefensa.html).

Dicho esquema contemplará las necesidades de los países parte. Además, se aprobó el ingreso de Uruguay como miembro activo del Foro.[80]

Cabe resaltar que hasta marzo de 2019 (fecha de la próxima reunión[81]), Argentina ejerce la presidencia pro témpore del Foro[82]. De esta manera, el CCCD es el encargado de establecer contactos y comunicaciones paralelas con todos los miembros del Foro para determinar las sedes y la coordinación de los próximos eventos que fueron fijados en Brasil y Colombia respectivamente para el ciclo 2019.[83]

Ejercicios similares fueron desarrollados también bajo la coordinación de Colombia y Estados Unidos en octubre de 2016. En ellos, las Fuerzas Armadas argentinas participaron de las primeras Ciber Olimpíadas Militares de las Américas. En dicha competencia participaron trece equipos provenientes de países de la región, aunque fueron Brasil, Colombia y Argentina (en ese orden) quienes lograron imponerse ante el resto.[84] En el año 2018, el equipo argentino del CCCD -cuyo núcleo principal estaba integrado por efectivos de la Armada Argentina- logró resaltar entre los trece (13) participantes regionales, clasificando en la instancia preliminar (online) para competir en el ejercicio de modalidad presencial.[85]

Respecto a la segunda estructura creada por el ministerio, la Dirección General de Ciberdefensa (DGCD), creada a través de la Decisión Administrativa N° 15/2015 le otorgó las funciones de *"intervenir en el planeamiento, formulación, dirección, supervisión y evaluación de las políticas de ciberdefensa."* (DGCD: 2015, p. 13). Desde su creación, la DGCD ha desarrollado diversas actividades, entre ellas, diversas jornadas conjuntas de ciberdefensa en las que participaron no solamente miembros de la Dirección sino también personal del CCCD, las fuerzas armadas e incluso la DINIEM con el objeto de realizar una puesta en común sobre los avances logrados por cada área pero también

[80] Cabe resaltar que el interés por el Foro se encuentra en aumento. Tal es así que Italia pidió su adhesión a pesar de no ser un país Iberoamericano. Entrevista reservada con Fuente F (militar), 3 de octubre de 2018, Buenos Aires, Argentina.
[81] Hasta el 4 de abril de 2019 no se encontró menciones sobre la celebración de dicha reunión.
[82] Se refiere al ejercicio de la responsabilidad administrativa sobre todo documento y comunicación que se genere hasta la siguiente reunión.
[83] Entrevista reservada con Fuente F (militar), 3 de octubre de 2018, Buenos Aires, Argentina.
[84] Fuerzasmilitares.org (2016, 25 de octubre), "Colombia ocupa segundo puesto de las Primeras Ciber Olimpiadas Militares de las Américas", en *fuerzasmilitares.org*, Colombia (consultado el 13 de septiembre de 2018 en http://www.fuerzasmilitares.org/notas/colombia/fuerzas-militares/7153-cberolimpiadas-2016.html).
[85] Fuerzas-armadas.mil (2018, 13 de septiembre), "Equipo del Comando Conjunto de Ciberdefensa logró clasificarse para las Ciberolimpiadas Militares 2018", en *fuerzas-armadas.mil.ar*, Buenos Aires (consultado el 13 de septiembre de 2018 en http://www.fuerzas-armadas.mil.ar/Noticia-2018-09-13-ciberdefensa-competencia.aspx).

el tratamiento de temas específicos de formación, capacitación, requerimientos y el alcance de los niveles de ciberdefensa directa y su vinculación entre las dependencias de la ciberdefensa. Estas reuniones tuvieron como resultado el determinar que cada fuerza será responsable de proteger su propia IC, mientras que el CCCD tiene la misión de proteger las IC del Estado Mayor Conjunto de las Fuerzas Armadas (EMCO). (DGCD: 2015).

En materia de formación, la DGCD presentó ante la CONEAU un proyecto de Maestría de Ciberdefensa para la UNDEF que contenía también dos especializaciones relacionadas a la seguridad de la información y la criptografía y seguridad teleinformática. Por otra parte, para el Instituto Universitario del Ejército se habilitaron cursos de capacitación dirigidos a personal civil y militar en los que predominaba el conocimiento en materia de seguridad de la información, manejo de nuevas TICs pero también forensia informática y seguridad teleinformática. Por su parte, dentro del Instituto Universitario Aeronáutico se pretendió realizar transferencia de conocimiento a través del desarrollo de un laboratorio con sensores que tengan por objeto analizar la exposición de la red a internet. (DGCD: 2015).

La DGCD incitó los proyectos de desarrollo, innovación e investigación. Respecto al desarrollo e innovación, el MINDEF realizó un acuerdo con la Universidad Nacional de Rosario con el objeto de desarrollar la distribución de un sistema operativo basado en Linux caracterizado por sus elevados estándares de seguridad. Por otra parte, desarrolló un proyecto de sistema de Gestión de Riesgos IT que tiene por objeto evaluar los riesgos generando una matriz con ellos. Además, se creó el sitio web www.ciberdef.mindef.gob.ar que tiene por objeto publicar y difundir las actividades vinculadas a la ciberdefensa en Argentina. Por último, con el objeto de proteger las comunicaciones de datos se creó el Proyecto CRIDEF (Criptografía para la Defensa). En materia de investigación, la DGCD creó una red de sistemas señuelos (denominada honeypot) con el objeto de exponer la red señuelo y así obtener información de ataques para generar estadísticas y analizar tendencias. (DGCD: 2015).

El cambio de gobierno y administración del Ministerio de Defensa, el Poder Ejecutivo Nacional modificaría estructuralmente (a través del Decreto N°42/2016) la cartera ministerial, convirtiendo la DGCD en Subsecretaría de Ciberdefensa bajo la esfera de la Secretaría de Ciencia, Tecnología y Producción para la Defensa congelando así parte de las actividades desarrolladas por la Dirección. En marzo de 2018, a través de la DA

N° 310, el Ministerio dotó a la Subsecretaría de Ciberdefensa de una Dirección de Asuntos Regulatorios de Ciberdefensa y una Dirección de Diseño de Políticas para la Ciberdefensa. La primera de ellas con la responsabilidad primaria de intervenir en los aspectos regulatorios del sistema de ciberdefensa, de las TICs y las IC a través de propuestas normativas, protocolo y procedimientos de actuación, y asistiendo en la cooperación con organismos nacionales y extranjeros. La segunda, por su parte, con la misión de asistir en el armado y supervisión de investigaciones, el desarrollo y transferencia tecnológica del todo lo dependiente del Ministerio de Defensa.

c. Estrategia Nacional de Ciberseguridad (ENCS)

Para Daniel T. Kuebl (2009) el ciberpoder es un medio para desarrollar y ejecutar la política y sirve para conectar al gobierno con el pueblo y brindar nuevos servicios (política doméstica) y como elemento de smartpower para perseguir objetivos estratégicos en la arena internacional. Según el autor, para desarrollar una ciberestrategia es necesario crear cibercapacidades que ayuden al logro y consecución de los objetivos propuestos en esta estrategia, ya que gran parte de la misma debe estar destinada a describir de qué forma serán utilizadas estas capacidades.

Para Stuart Starr (2016), una ciberestrategia supone la correcta relación entre las capacidades (el ciberpoder) y el objetivo a proteger (es decir, el ciberespacio).

La idea de elaborar una ENCS empieza a resonar en Argentina en el año 2012, a partir de la Declaración del CICTE denominada "Fortalecimiento de la Seguridad Cibernética de las Américas", que tenía entre sus líneas que los países parte adopten y desarrollen una estrategia nacional de seguridad cibernética integral.

En junio de 2015, el elaborar una estrategia nacional de protección de IC se convirtió en un objetivo real, aunque sin resultado alguno. A pesar de las cuatro reuniones que surgieron de la mesa de trabajo de ciberseguridad en la que participaron miembros del Ministerio de Defensa, la Agencia Federal de Inteligencia, el Ministerio de Relaciones Exteriores y Culto, el Ministerio de Justicia, el Ministerio Público Fiscal y Jefatura de Gabinete de Ministros (tal como se comentó con anterioridad), esta mesa de trabajo no logró su cometido.

A pesar de ello, el objetivo, logró traspasar las gestiones nacionales y ser impulsado a través de la creación del Ministerio de Modernización de la Nación. En consonancia con esto, el 28 de julio de 2017 el PEN aprobaba el Decreto N° 577 a través

del cual se creaba el Comité de Ciberseguridad, integrado por los Ministerios de Modernización, Defensa y Seguridad, el cual tenía a su cargo la elaboración de una Estrategia de Ciberseguridad Nacional.

Dicha normativa, ponía a la cabeza del Comité y de la elaboración de la estrategia, al Ministerio de Modernización, impulsando al Comité a adoptar normas de seguridad cibernética, convocar a otros organismos a participar, fijar los lineamientos para definir las IC y participar de todas las actividades que se desarrollen en el marco de la ciberseguridad.

Esta directiva se encuentra en consonancia con lo expuesto por Calam, et al (september 2018), quienes mencionan que para tratar de forma eficaz la ciberseguridad nacional de cualquier país, es necesario entrelazar los límites institucionales, articulando el desempeño de los distintos departamentos, agencias y funciones (civiles y militares).

A fin de cumplir con su cometido, la Agencia Federal de Inteligencia (a través de la Dirección Operacional de Ciberinteligencia) y los Ministerios de Relaciones Exteriores y Culto (a través de nic.ar[86]), Justicia y Derechos Humanos (a través de la Dirección Nacional de Protección de Datos Personales) y Jefatura de Gabinete de Ministros, tomaron un rol protagónico en las reuniones del Comité.[87]

La definición de las funciones de cada ministerio en este ámbito, delineado por los primeros esbozos de la Estrategia Nacional de Ciberseguridad, transfiere los conceptos legales de seguridad interior y defensa nacional al ámbito cibernético. Así, cuestiones de ciberseguridad y ciberdefensa son divididas entre las distintas carteras ministeriales, haciendo responsable de la ciberdefensa al Ministerio de Defensa, de las cuestiones de cibercrimen al Ministerio de Seguridad y de la ciberseguridad a Modernización/Jefatura de Gabinete de Ministros.

A tal fin, el Comité de Ciberseguridad cuenta con cinco grupos de trabajo encargados de elaborar planes específicos referidos a políticas, protocolos, Infraestructuras Criticas, capacitación y cooperación internacional. En este sentido, estos grupos de trabajo deben a) definir e implementar los procesos, procedimientos, roles e intercambio de información sobre alertas de ciberseguridad[88]; b) definir cuáles serán las IC que el Ministerio de Defensa, desde su sistema de ciberdefensa, deberá proteger para

[86] Nicar es el organismo que administra el dominio ".ar"
[87] Niss, O. (2017). "Ciberseguridad y ciberdefensa en el Estado", mimeo, Rosario, Argentina.
[88] Niss, O. (2017). Op cit., Rosario, Argentina.

asegurar el buen funcionamiento del ciberespacio a nivel nacional[89]; c) elaborar un plan de lucha contra el ciberdelito (el primero será planificado para el período 2018-2020) con el objeto de establecer una política de ciberpatrullaje que permita obtener información de fuentes abiertas y foros públicos[90], d) desarrollar un plan de concientización y capacitación que, a través de una encuesta para medir la necesidad de capacitación, logró realizar charlas de concientización en la APN[91] y e) fomentar, de forma coordinada, la cooperación internacional.

Complementariamente, cada órgano de gobierno con responsabilidad en el ciberespacio deberá definir su propia estrategia para el ambiente cibernético a fin de concluir los lineamientos establecidos por la ENCS.

Con reuniones frecuentes por parte del Comité, se estimaba que la ENCS se haría oficial en noviembre de 2018, antes de la Cumbre de Presidentes del G-20[92], lo cual, no sucedió. En sus líneas, el borrador de la estrategia establece que la protección de IC de la Defensa Nacional serán responsabilidad del Ministerio de Defensa, abriendo los parámetros anteriores mediante los cuales las Fuerzas Armadas y el sistema de Defensa nacional se hacían con la tarea de proteger única e íntegramente las IC pertenecientes al instrumento militar (IM). Así, las FFAA y el Comando Conjunto de Ciberdefensa seguirán haciéndose cargo de las IC del IM, mientras que el Ministerio de Defensa, a través de la Subsecretaría de Ciberdefensa, será el encargado de proteger los activos críticos a nivel nacional.[93]

En miras a los esfuerzos por desarrollar la ENCS, y en el marco de la Declaración "Fortalecimiento de la Seguridad Cibernéticas en las Américas" del CICTE, el Comité Tripartito trabaja en conjunto con la OEA, quien proporciona recomendaciones y capacitaciones al personal vinculado con la elaboración de la Estrategia.

En este marco, los primeros días de agosto de 2018 se desarrolló un curso de "liderazgo y Estrategia de Ciberseguridad" brindado por la Florida International University en Buenos Aires, en el que se trataron los siguientes temas: amenazas cibernéticas, Estrategia organizacional de seguridad cibernética, desarrollo de marcos

[89] Entrevista reservada con Fuente A (civil). 17 de agosto de 2018, Buenos Aires, Argentina.
[90] Entrevista reservada con Fuente D (civil). 11 de septiembre de 2018, Buenos Aires, Argentina. Según esta fuente la idea de la comisión que se encuentra elaborando el plan de lucha contra el ciberdelito es la de desarrollar investigaciones sin desarrollar, necesariamente, acciones de inteligencia, dado el nivel de rechazo de esta actividad por gran parte de la población civil.
[91] Entrevista reservada con Fuente J (civil), 14 de noviembre de 2018, Buenos Aires, Argentina.
[92] Entrevista reservada con Fuente E (civil), 13 de septiembre de 2018, Buenos Aires, Argentina.
[93] Entrevista reservada con Fuente A (civil). 17 de agosto de 2018, Buenos Aires, Argentina.

nacionales, implementación efectiva y simulación de amenazas. En esta oportunidad, si bien la actividad estuvo a cargo de la FIU, también participaron los otros partners de la OEA (US National Defense University, Microsoft, Trend Micro y United Data Technologies).[94]

A modo de cierre de este apartado podemos ver que el desarrollo y evolución de la ciberdefensa y la ciberseguridad en nuestro país ha ido variando en intensidad según cada agencia de gobierno y las distintas administraciones nacionales, quedando relegada hasta hace poco la necesidad de crear una Estrategia Nacional de Ciberseguridad.

Conclusiones parciales

El objetivo de este capítulo fue el de iluminar sobre las falencias de las políticas relacionadas a la ciberseguridad y la ciberdefensa puestas en marcha en nuestro país. Para ello, en una primera instancia pudimos apreciar que las administraciones de Cristina Fernández de Kirchner y Mauricio Macri han concentrado sus esfuerzos en expandir y difundir Tecnologías de la Información y de la Comunicación no sólo a la APN sino también en la sociedad en general. Ahora bien, la difusión tecnológica trae aparejado también la exposición a nuevas vulnerabilidades relacionadas a la seguridad de la información. Algunas de estas vulnerabilidades son aquellas reflejadas en el primer capítulo de esta tesis, cuando se hizo mención de una muestra (poco significativa en número pero no en magnitud) de los ciberataques que fueron realizados contra nuestro país. Estos, y otros, fueron algunas de las causas que hicieron que la elite política preste mayor atención a la necesidad de establecer medidas de ciberseguridad y ciberdefensa que tengan por misión el mitigar y proteger al país de las vulnerabilidades que plantea el ciberespacio.

Una forma de intentar prepararse y prevenir delitos cibernéticos fue el establecimiento de leyes que sancionan el accionar delictivo en el ciberespacio. A tal efecto, la tipificación de delitos informáticos, la adhesión al régimen establecido por la Convención de Budapest (a pesar de sus reservas) y la creación de las leyes de protección de datos personales y firma digital crean un sistema abocado a la penalización de dichas acciones. Mientras que leyes como las de defensa nacional (y sus decretos reglamentarios)

[94] Schulkin, J. (24 de julio de 2018). "Expertos de la Universidad Internacional de Florida capacitarán a profesionales argentinos sobre ciberdelincuencia." *Infobae*. (consultado el 21 de octubre de 2018). Recuperado de: https://www.infobae.com/tecno/2018/07/24/expertos-de-la-universidad-internacional-de-florida-capacitaran-a-profesionales-argentinos-sobre-ciberdelincuencia/

y seguridad interior permiten definir y delimitar el accionar de las Fuerzas Armadas y de Seguridad en el ciberespacio.

Respecto a la creación de políticas de ciberdefensa y ciberseguridad, para Calam et al, una única organización con responsabilidad general en materia de ciberseguridad resulta más eficiente. A pesar de esto, vemos que en el caso de Argentina las funciones de ciberseguridad nacional se encuentran separadas entre los distintos organismos del Estado, de modo tal que la toma de decisiones se encuentra en manos de cada dependencia, resaltando el trabajo individual de cada una de ellas.

De esta forma, la creación de estructuras referidas a la ciberseguridad y ciberdefensa ha ido variando en tiempo e intensidad. Por un lado, el Programa ICIC ha ido mutando de dependencia, mientras que en el ámbito del Ministerio de Defensa las estructuras han tenido una evolución constante, dejando de lado los incipientes organismos para dar paso a otros más avanzados. En manos del Ministerio de Seguridad, la responsabilidad en materia de cibercrimen es todavía una práctica novedosa, dado que, a pesar de que las Fuerzas de Seguridad venían trabajando en cuestiones relacionadas a los delitos informáticos, es recién a partir del establecimiento de la seguridad cibernética como uno de los cien objetivos de gobierno en el año 2016 que comienza el proceso de creación de estructuras vinculadas al cibercrimen dentro de dicho ministerio. De esta manera, podemos apreciar que cada organismo tuvo su propia dinámica en lo referido a funciones, debates y creación de capacidades en materia cibernética.

Si tomamos en consideración los ciberataques mencionados en el capítulo anterior, podemos deducir que gran parte del impulso de las políticas de ciberdefensa y ciberseguridad se encuentran íntimamente relacionadas con ciberataques anteriores. Es decir, fue luego de un ataque a la seguridad de la información vinculada a los Ministerios de Defensa y Seguridad que se incrementa la necesidad de producir lineamientos que sirvan de respuesta a la problemática. Esto convierte a las políticas de ciberseguridad y ciberdefensa en políticas sectoriales que surgieron de forma reactiva y no preventiva.

La forma que ha encontrado el gobierno para lograr un trabajo integral en materia de ciberseguridad nacional que promueva la actividad interagencial ha sido a través de la creación de una mesa de trabajo conjunto en 2015 que luego daría paso a la creación del Comité de Ciberseguridad, del cual se nutren, no solamente los Ministerios de Defensa, Seguridad y Jefatura de Gabinete de Ministros (a través de Modernización), sino que se nutre también de la participación de los Ministerios de Relaciones Exteriores y Culto,

Justicia y Derechos Humanos y la Agencia Federal de Inteligencia, siendo proclive a incorporar representantes de los organismos de gobierno que sean necesarios para lograr la eficiente funcionalidad de los programas de ciberseguridad nacional.

En este panorama, la ENCS viene a encargarse de la limitación de funciones de cada organismo aunque las acciones que pueda desarrollar cada uno seguirá dependiendo de la voluntad y el interés político que le asigne a la cuestión cibernética cada gobierno y ministro de turno de cada cartera.

En conclusión, las políticas desarrolladas para paliar la cuestión cibernética en nuestro país han fallado, en un primer momento, en no dimensionar los efectos y la gravedad que conlleva el fenómeno. Esto se está revirtiendo desde el año 2015, aunque en 2017 logró mayor impulso gracias a la definición de funciones que establecen la realización del proceso de creación de una Estrategia Nacional de Ciberseguridad que permita ordenar las acciones de los organismos involucrados, a la vez que pone a la cabeza del asunto a un órgano coordinador (Ministerio/Secretaría de Modernización) que intervenga en la integración sistemática de los organismos vinculados a la ciberseguridad, el cibercrimen y la ciberdefensa, generando así un diálogo constante entre las agencias participantes con responsabilidad en la cuestión.

El siguiente capítulo tratará, de forma específica, el rol del Sistema de Inteligencia Nacional en el ciberespacio, analizando de qué forma nutre a la definición de políticas vinculadas a la seguridad cibernética.

CAPITULO 3
INTELIGENCIA ESTRATÉGICA EN EL CIBERESPACIO

Introducción

El último objetivo específico a tratar en el desarrollo de esta tesis tiene la misión de "indagar sobre el rol de la inteligencia en el trazado de políticas públicas destinadas a los ámbitos de la ciberseguridad y la ciberdefensa", por lo cual, este tercer capítulo tendrá como columna vertebral el investigar cómo llegó la cuestión cibernética al seno de los distintos organismos del Sistema de Inteligencia Nacional y cuáles son los roles operativos de las principales dependencias. Para esto, se hará foco en la Dirección Nacional de Inteligencia Criminal y la Dirección Nacional de Estrategia Militar, ya que ambas direcciones tienen a su cargo la tarea de dar aviso, de manera oportuna, sobre los riesgos y oportunidades que implica alcanzar los objetivos fijados por las políticas de defensa y seguridad, y dentro de las mismas, las que se ejecutan en el ciberespacio.

Para ello, en una primera instancia se expondrán los lineamientos teóricos que reconocidos especialistas hacen sobre el rol de los organismos de inteligencia en el ciberespacio, para luego dar lugar a la respuesta de dos interrogantes principales, a saber: ¿cuál es el rol del sistema de inteligencia argentino en cuestiones cibernéticas tomando como base el marco legal? y ¿cómo funcionan operativamente los distintos instrumentos de este sistema y a que forma de realizar inteligencia responden sus operaciones? Seguidamente y para finalizar, se hará mención de cuestiones referidas a la formación de agentes de inteligencia en materia cibernética.

A. La inteligencia en el ciberespacio

Antes de analizar la inteligencia en el ciberespacio es preciso hacer una diferenciación preliminar entre los distintos tipos de inteligencia que tienen relación con componentes tecnológicos para luego analizar cuál de ella es la más específica a la hora de analizar el accionar de los organismos del sistema de inteligencia nacional en el ciberespacio.

a) Definiendo inteligencia estratégica, inteligencia científico tecnológica e inteligencia digital.

Tal como sintetiza Marcelo de los Reyes (2018), la actividad de inteligencia debe desarrollarse para la adecuada toma de decisiones que sirve para prevenir y resolver conflictos que pueden derivar en crisis.

De esta forma, los conocimientos proporcionados por la inteligencia tienen por objeto servir de insumo para la toma de decisiones, al hacerlo, la inteligencia adquiere valor en sí misma.

En este sentido, cuando hablamos de inteligencia estratégica nos referimos a una actividad proactiva, producida en el marco de una visión de futuro, de lo posible y deseable que produce conocimiento vital para la supervivencia nacional. Esta inteligencia se orienta a objetivos nacionales, ayudando a definir objetivos factibles, generando una base para el planeamiento y el logro de dichos objetivos. (Anónimo: 2009).

En otro orden de ideas, cuando nos referimos a inteligencia científico tecnológica hablamos del producto resultante de la recolección, procesamiento, evaluación, análisis e interpretación de la información científica y técnica referida a cuestiones de ingeniería, investigación y desarrollo, sistemas, armas, sistemas de armas, y otros. Su objetivo es proporcionar un panorama de las áreas de interés en ciberseguridad, tecnología e ingeniería a otras áreas de inteligencia y servir de base para los proyectos de investigación y desarrollo. (Trentadue: 2016).

En cambio, la inteligencia digital se refiere al conjunto de técnicas de reunión de información que utilizan medios digitales para la obtención y procesamiento de la información. Esta incluye técnicas de OSINT, GEOINT, IMINT, CIBINT y WEBINT.

Mientras que la inteligencia digital se refiere a los medios por los cuáles se obtiene la información, la inteligencia científico tecnológica centra sus estudios en el análisis de un objeto de estudio específico, como lo es la tecnología en todos sus aspectos.

En definitiva, aunque los tres tipos de inteligencia denotan ciertas diferencias entre sí, son complementarias, dado que la inteligencia científico tecnológica y la inteligencia digital pueden servir de instrumento para la inteligencia estratégica.

b) Inteligencia y ciberespacio

Sherman Kent (2016, p. 4) presenta a la inteligencia como conocimiento y advierte que *"the intelligence activity consists basically of two operations. […] Surveillance operation […] and research operation"*[95]. La primera se refiere a *"many ways by which*

[95] La actividad de inteligencia consiste básicamente en 2 operaciones: operaciones de vigilancia y operaciones de investigación. (Traducción propia).

the contemporary world is put under close and systematic observation"[96], mientras que la última equivale al *"attempts to establish meaningpatterns out of what appears to be going on now"*[97]. De esta forma, el conocimiento equivale entonces a una ventaja relativa por sobre la otra parte.

En este sentido, el conocimiento representa una ventaja a la hora de tomar decisiones sólo si este conocimiento es completo, seguro, entregado a tiempo y capaz de servir como base para la acción (Kent: 2016). Un conocimiento que cumpla con estos lineamientos sirve a la toma de decisiones de forma eficaz, obstaculizando y previniendo un cisne negro.[98]

Estas operaciones descriptas por Kent se traducen al ciberespacio. De esta forma, la ciberinteligencia es la realización de operaciones de investigación y vigilancia en el ambiente cibernético.

En esta misma línea, diversos autores intentan definir el rol del sistema de inteligencia en el ciberespacio. Uno de ellos es el coronel Matthew M. Hurley (2014) que en su afán por conceptualizar las tareas de inteligencia, vigilancia y reconocimiento (IVR) cibernético para contribuir a la doctrina de la Fuerza Aérea (por lo que trata la temática desde la inteligencia operacional), establece que a estas tareas lo componen dos actividades: una desde y otra para el ciberespacio. Hurley describe a la primera como la explotación de redes para emplear la información obtenida en apoyo de operaciones, es decir, la extracción de datos de las redes del adversario en busca de información con valor de inteligencia que se pueda recopilar en el ámbito cibernético a través de medios de comunicación, chats privados, videos, etc. La segunda, en cambio, es descripta como IVR para apoyar la superioridad ciberespacial, es decir, garantizar la capacidad de trabajo coordinado, garantizar la producción de inteligencia y diseminación de la información obtenida que permita desarrollar las operaciones cibernéticas.

Por su parte, Lourdes Puente Olivera se refiere a dos formas o tipo de inteligencia. Una de ella referida a la utilización del ciberespacio como medio para obtener información (es decir, operación de vigilancia), mientras que la otra se vincula al ciberespacio en sí mismo, enfocado en el cómo operar dentro del dominio. Para la autora la inteligencia debe definir que tengo y que hay que saber para conocer este espacio, dado

[96] Formas a través de las cuales el mundo actual es puesto bajo observación. (Traducción propia).
[97] Intenta establecer patrones de significado de lo que arecer estar bien. (Traducción propia).
[98] Un cisne negro es un suceso considerado improbable, que cuando sucede tiene efectos devastadores. Para ampliar, ver Taleb, N. N. (2016). *El Cisne Negro. El impacto de lo altamente improbable.* Buenos Aires, España: Paidós.

que de esta manera se conocerán las vulnerabilidades y oportunidades propias para tomar las decisiones de cómo actuar.[99]

Al respecto, Hugo Miguel nos propone como definición de ciberinteligencia la siguiente:

> "Proceso de búsqueda, localización, registro, análisis y diseminación de la información inherente al ciberespacio y tiene por objeto parametrizar las amenazas en ese ambiente, para lo cual debe ante todo generar las preguntas que nos permitan elaborar el índice básico de información y determinar los factores fijos propios (reales o virtuales) que identifican nuestro teatro de operaciones cibernético.
>
> En este aspecto, es importante para trabajar en una infraestructura de datos espaciales que nos permita llevar el mundo abstracto de la red al concreto del posicionamiento geográfico de la infraestructura de comunicaciones e informática. […]
>
> La inteligencia en el ciberespacio conlleva el conocimiento de plataformas, sistemas operativos, redes de acceso, métodos de acceso múltiple, técnicas de validación de usuario, análisis de tráfico y perfilado de paquetes, factores que son necesarios para poder generar los elementos esenciales de información que permitan realizar las preguntas correctas para obtener la información que un comandante necesita para asegurar el uso y control de la red. Determinar de manera proactiva las capacidades, la psicología y las motivaciones de nuestros atacantes permitirá prevenir y anticipar ataques reales a las redes y a las actividades propias en el ciberespacio."[100]

Vemos entonces que sin importar el nombre con el que nos refiramos a la actividad, el objetivo de ella es descifrar lo virtual para obtener información pertinente al mundo físico y así apoyar los distintos tipos de operaciones (sean estas tradicionales o cibernéticas).

En consecuencia, y en miras de responder al objetivo que atañe a este capítulo, el próximo paso será responder los siguientes cuestionamientos: ¿cuál es el rol del sistema de inteligencia argentino en cuestiones cibernéticas tomando como base el marco legal? y ¿cómo funcionan operativamente los distintos instrumentos de este sistema y a qué forma de realizar inteligencia (anteriormente desarrolladas) responden sus operaciones? Al responder estos interrogantes, será posible enriquecer la investigación y confrontar la hipótesis propuesta**.**

---

[99] Puente, M. L. (1 de abril de 2018). Guía para entender la nueva geopolítica del ciberespacio. *Perfil.* (Consultado el 5 de diciembre de 2018 en https://www.perfil.com/noticias/elobservador/guia-para-entender-la-nueva-geopolitica-del-ciberespacio.phtml)

[100] Miguel, H. (15 de marzo de 2018). Mitos y realidades de la ciberdefensa. *Revista DEF* (consultado el 6/12/2018 en http://defonline.com.ar/mitos-y-realidades-de-la-ciberdefensa/)

B. Marco legal de la actividad de inteligencia

Para responder a nuestro primer interrogante, es necesario analizar no solamente las leyes vinculadas a la inteligencia, sino también, tener presente aquellas que hacen al sistema de seguridad interior y defensa nacional, ya que dichas leyes son relevantes a la hora de establecer los límites a los órganos que conforman la Agencia Federal de Inteligencia y a la vez, como vimos en el capítulo anterior, extrapolar dichos conceptos al ambiente cibernético. Estas divisiones pueden verse claramente reflejadas en las definiciones aportadas por la ley de Inteligencia Nacional, su modificatoria y el decreto 1311/2015 que establece la nueva Doctrina de Inteligencia Nacional.

Por su parte, la ley N° 27.126 (2015), modificatoria de la ley N° 25.520 de Inteligencia Nacional (2001), establece en su artículo segundo que la inteligencia nacional es "*la actividad consistente en la obtención, reunión, sistematización y análisis de la información específica referida a los hechos, riesgos y conflictos que afecten la Defensa Nacional y la seguridad interior de la Nación."* Mientras que la ley 25.520, en su artículo segundo, define como:

> "Inteligencia Criminal a la parte de la Inteligencia referida a las actividades criminales específicas que, por su naturaleza, magnitud, consecuencias previsibles, peligrosidad o modalidades, afecten la libertad, la vida, el patrimonio de los habitantes, sus derechos y garantías y las instituciones del sistema representativo, republicano y federal que establece la Constitución Nacional.
>
> Inteligencia Estratégica Militar a la parte de la Inteligencia referida al conocimiento de las capacidades y debilidades del potencial militar de los países que interesen desde el punto de vista de la defensa nacional, así como el ambiente geográfico de las áreas estratégicas operacionales determinadas por el planeamiento estratégico militar.
>
> Sistema de Inteligencia Nacional al conjunto de relaciones funcionales de los organismos de inteligencia del Estado Nacional, dirigido por la Secretaría de Inteligencia a los efectos de contribuir a la toma de decisiones en materia de seguridad exterior e interior de la Nación."

De esta forma, es posible apreciar que la división tajante entre seguridad interior y defensa nacional se hace eco de las cuestiones de inteligencia al establecer un sistema de inteligencia nacional desdoblado en tres agencias con responsabilidades propias y limitadas. Por su parte, el sistema de seguridad interior es el encargado de desarrollar la inteligencia referida a cuestiones criminales, mientras que, el sistema de defensa nacional se encargará únicamente de producir inteligencia en cuestiones referidas a la defensa

nacional y al instrumento militar. Por ley, estas agencias deben mantenerse separadas sin inmiscuirse en las tareas otorgadas a la otra.

Con un sistema de seguridad nacional dividido legalmente de forma tajante, las dificultades que ofrece el ciberespacio para desmembrar qué corresponde a seguridad interior y qué forma parte de la defensa nacional, merece un arduo trabajo. A modo de reducir la incertidumbre, el Decreto N° 1311/2015, establece en su anexo primero que se configura a la inteligencia nacional como un observatorio abocado a la gestión y producción de conocimientos sobre un conjunto de problemáticas relacionadas a la Defensa Nacional y la Seguridad Interior, entre las cuales, cabe destacar (de conformidad con el tema de tesis), en el ámbito de la seguridad interior *"las acciones que atenten contra la ciberseguridad, delitos contra la confidencialidad, la integridad y la disponibilidad de los sistemas informáticos, las redes o los datos, o parte de ellos, el uso fraudulento y la difusión ilegal de contenidos."* (folio 14). De esta forma, la Inteligencia Criminal se hace con la potestad de trabajar en cuestiones vinculadas a la seguridad de la información y la ciberseguridad, lo que atañe el hecho de que la Inteligencia Estratégica Militar no está habilitada para tratar estas cuestiones, dejando un vacío legal que más qué no decir nada nos permite interpretar que solamente las cuestiones vinculadas al sistema de defensa nacional en el ciberespacio serán objeto de consideración por parte de la última agencia en cuestión.

A la vez, esta norma, establece como destinatarios principales a: 1) el Presidente de la Nación, 2) los Ministerios de Defensa y Seguridad y 3) otros ministerios. De esta forma, los insumos aportados por la inteligencia nacional deben nutrir las políticas de defensa nacional y seguridad interior en base a problemáticas relevantes.

La normativa también distingue que, la Dirección Nacional de Inteligencia Criminal (de ahora en más, DINICRI), dependiente del Ministerio de Seguridad, tiene a su cargo la producción de inteligencia criminal a excepción de la referida a delitos criminales complejos, contra poderes públicos y el orden constitucional que quedarán bajo el manejo de la Agencia Federal de Inteligencia (de ahora en más, AFI), a menos que la misma agencia especifique lo contrario. Por su parte, la Dirección Nacional de Inteligencia Estratégica Militar (de ahora en más, DINIEM), tiene por objeto la producción de inteligencia estratégica militar, quedando, la producción de inteligencia operacional y táctica, en manos de los organismos de inteligencia dependientes de las Fuerzas Armadas. Esta división de tareas entre los distintos organismos dependientes de

la AFI supone, la cooperación institucional para el buen funcionamiento y obtención de los propósitos de la inteligencia nacional.

En este último punto, las entrevistas realizadas arrojan luz sobre la falta de cooperación entre las distintas entidades del sistema de inteligencia. Por su parte, mientras que la DINIEM y la DINICRI no entrelazan sus esfuerzos por cuestiones legales, ambas dependencias tienen una relación limitada con la AFI.[101]

C. Actividad del sistema de inteligencia nacional

Cuando hablamos de inteligencia como actividad, vemos que el proceso de investigación puede iniciarse de dos formas. La primera por requerimiento político, cuando se recurre a la inteligencia en busca de datos o antecedentes y se estimula cierta investigación. La segunda, se da cuando el sistema de inteligencia inicia una investigación a razón de su propia observación de lo que ocurre en el contexto. (Kent: 2016). A continuación veremos que los organismos del sistema de inteligencia en Argentina han iniciado el proceso de investigación de cuestiones cibernéticas de ambas formas, comprendiendo su deber de analizar la temática.

Este fenómeno se instala como eje de debate y análisis en el marco de la DINIEM antes que en la DINICRI. Aunque sin lugar a dudas, la cuestión era trabajada, desde hacía tiempo, por las dependencias de inteligencia de cada fuerza (armadas y de seguridad).

En el caso del Ministerio de Defensa, si bien la cuestión cibernética era un tema ya instalado, el Proyecto de Capacidades Militares (PROCAMIL) de 2010, elaborado en el marco del Estado Mayor Conjunto (EMCO), incluía las cuestiones de ciberdefensa como capacidades de inteligencia, lo cual fue nuevamente reflejado en el siguiente documento ministerial (PLANCAMIL de 2011), que incorporaba la ciberdefensa en el Área de Capacidad 3 (AC3) "Vigilancia, Reconocimiento e Inteligencia". (Albarracín y Eissa: 2019)

De forma paralela a la elaboración de dichos documentos, la cuestión cibernética surge como una preocupación para la DINIEM en 2011, bajo la dirección de Lourdes Puente Olivera, sin un requerimiento político formal, respondiendo directamente a la

[101] Según palabras del entrevistado civil Fuente C, *"durante el gobierno de Alfonsín, se había creado una instancia (legal) donde se hacían reuniones periódicas de la Central nacional de inteligencia. En ella se exponían los informes de inteligencia de cada agencia/dirección, lo cual era mucho más satisfactorio porque se compartía la información"*, hoy en día esto no sucede. Entrevista reservada con Fuente C (civil), 3 de septiembre de 2018, Buenos Aires, Argentina.

observación que la Dirección hacía sobre el contexto internacional, y en cumplimiento de la función que emana de los organismos de inteligencia de anticipar.[102]

En ese momento surge el interrogante sobre el rol y la responsabilidad de la inteligencia en materia cibernética, ante lo cual, el Ministerio de Defensa le solicita a la DINIEM realizar un relevamiento que tenga por objeto identificar las capacidades cibernéticas adquiridas con el objeto de coordinar esfuerzos.[103]

A lo largo del año 2012, la DINIEM inició un proceso de debate en el que participaron representantes de las Fuerzas Armadas y que tenía por objeto la definición conceptual de ciberdefensa, en miras de responder al interrogante planteado con anterioridad. El debate se concentró sobre todo en lo conceptual, porque dependiendo de las definiciones se iba a poder decidir quién se tenía que hacer cargo de qué y cuales iban a ser las funciones del sistema de defensa nacional en el ciberespacio.[104]

Este proceso concluyó con la elaboración de un documento elevado al Ministerio de Defensa en octubre de ese mismo año que obtuvo cierta reticencia por parte de la Dirección General de Planeamiento y Estrategia (DGPLA), por lo que el documento no logró obtener resultado alguno. Por el contrario, la DGPLA pujó para que las cuestiones de ciberdefensa no sean consideradas como una capacidad de inteligencia. (Albarracín y Eissa: 2019).

En medio de esta reticencia por parte de las autoridades del Ministerio, a fines del año 2012, el MINDEF sufrió un ataque cibernético que vulneró la seguridad de información confidencial. Para la Fuente G, este hecho fue altamente preocupante debido a que *"sacó a la luz proyectos de investigación y desarrollo, el estado real de las FFAA y de los sistemas de armas, información sobre cada uno de los trabajadores del MINDEF y el área en el que cada uno desempeñaba sus funciones, lo cual es sumamente crítico"*.[105]

Tras los hechos ocurridos el Ministerio de Defensa empieza a considerar peligroso el confundir operacionalmente los términos ciberinteligencia y ciberdefensa, lo que hacía necesario diferenciar medidas de seguridad de la información de las de ciberinteligencia, dilatando aún más el accionar de la DINIEM. (Albarracín y Eissa: 2019).

[102] Entrevistas reservadas con Fuente F y G (civiles), 18 y 20 de septiembre de 2018, Buenos Aires, Argentina.
[103] Entrevistas reservadas con Fuente F y G (civiles), 18 y 20 de septiembre de 2018, Buenos Aires, Argentina.
[104] Entrevista reservada con Fuente F (civil), 18 de septiembre de 2018, Buenos Aires, Argentina.
[105] Entrevista reservada con Fuente G (civil), 20 de septiembre de 2018, Buenos Aires, Argentina.

A pesar de ello, el sistema de inteligencia nacional comienza a creer oportuno el análisis de la cuestión cibernética. A partir del estudio de las Memorias Detalladas del Estado Nacional para los años de estudio (2007 - 2017), se puede apreciar que cuestiones referidas al crimen organizado y al terrorismo internacional están en la agenda de análisis del Sistema de Inteligencia Nacional (SIN) desde los primeros años del siglo XXI, no así las referidas al ambiente cibernético. Es a partir del año 2013 que estas memorias arrojan luz verde sobre la incumbencia del sistema de inteligencia argentino en el ciberespacio, cuando desde Jefatura de Gabinete de Ministros se refieren a los logros del SIN (en concordancia con el Plan de Inteligencia Nacional vigente) y detallan que la producción de inteligencia en materia de defensa nacional y seguridad interior involucró el profundo análisis de las ciberamenazas. (Jefatura de Gabinete de Ministros: 2014).

En consonancia con esto, en el año 2014 la Directiva Política de Defensa Nacional definió al ciberespacio como un ámbito transversal a los escenarios tradicionales de conflicto (mar, tierra, aire y espacio exterior), siendo esta la primera vez que Argentina definía conceptualmente al ciberespacio desde la óptica de la Defensa Nacional. Dicha conceptualización sería modificada en la siguiente DPDN del año 2018, la cual se refiere al ciberespacio como un quinto dominio de guerra.

La puesta en funcionamiento de la ley N° 27.126 y el Decreto N° 1311 (ambos de 2015), conllevaron la producción de inteligencia referente a la ciberseguridad y la ciberdefensa, de acuerdo al Plan de Inteligencia Nacional vigente. De esta forma, se delinearon escenarios definidos según las prioridades de asuntos estratégicos enmarcados en dicho plan.

La puesta en funcionamiento del Decreto 1311/2015 trajo aparejada la creación de la Dirección Operacional de Inteligencia sobre Ciberseguridad (DOC) en el seno de la AFI. Dicha Dirección, empezó a trabajar en noviembre de 2015[106] con la misión de producir *"inteligencia orientada al conocimiento de las acciones que atenten contra la ciberseguridad en el marco de la defensa nacional y la seguridad interior, y de los grupos nacionales o extranjeros responsables de llevarlas a cabo"* (Anexo 2, folio 66). Para ello, la DOC fue dotada de una Dirección de Inteligencia Informática encargada de detectar *"actividades relativas a riesgos y conflictos vinculados o derivados del uso de las tecnologías de la información y la comunicación"* (Anexo 2, folio 66) y una Dirección

[106] Bullentini, A. (1 de diciembre de 2015). "Predecir y prevenir ciberataques", en *Página 12* (consultado el 10 de diciembre de 2018 en https://www.pagina12.com.ar/diario/elpais/1-287308-2015-12-01.html)

de Inteligencia sobre Delitos Informáticos *"orientada al conocimiento de las actividades que pudieran configurar delitos informáticos en todas sus formas y modalidades"* (Anexo 2 folio 67).[107]

Por su parte, la producción de inteligencia nacional en materia de seguridad interior, estuvo signada al abordaje de temáticas tales como: *"Narcotráfico, Trata de Personas, Tráfico de Armas, Delitos Económicos y Financieros, Terrorismo y Atentados contra el Orden Constitucional, Ciberseguridad y Contrainteligencia Institucional y Criminal."* (Jefatura de Gabinete de Ministros: 2016, p. 509). De la misma forma, en el ámbito de la Defensa Nacional, la producción de Inteligencia se basó en temas referidos a: *"Presencia Militar Extra Regional, Capacidades y Potencial Militar de otros Estados, Conflictos Armados y Recursos Naturales, Ciberdefensa y Contrainteligencia Defensivo-Militar."* (Jefatura de Gabinete de Ministros: 2016, p. 509).

Tal como sucedió en el seno de la AFI, se puede especular que a partir de la nueva legislación vigente la DINICRI fue dotada de una mesa de trabajo destinada a desarrollar actividades de ciberinteligencia, especialmente aquellas destinadas al ciberpatrullaje[108]. Por otra parte, la DINIEM concentró sus actividades de inteligencia en el ciberespacio a modo de responder a los pedidos explícitos de la Dirección de Ciberdefensa.[109]

El cambio en la dirección de la DINICRI supuso una revitalización de las funciones anteriormente asignadas. Desde el año 2016 la mesa de trabajo de ciberinteligencia en el seno del MINSEG adquirió funciones dedicadas a realizar un análisis exhaustivo del ciberespacio que comprendió diversas técnicas de análisis propias de la actividad[110]que equivalen a las funciones arriba denominado IVR desde y para el ciberespacio.

Cabe mencionar, que todo lo referido a la interceptación de comunicaciones actualmente se encuentra en manos de la Corte Suprema de Justicia. Mientras la ley N° 25.520 establecía en su art. 21 la creación de la Dirección de Observaciones Judiciales como único órgano del Estado encargado de realizar interceptaciones (siempre que estas

[107] Cabe mencionar que el Ministerio de Defensa a través de su Jefatura de Gabinete y de la Dirección General de Ciberdefensa trabajó de forma coordinada con la AFI en la puesta en marcha del área de inteligencia mencionada. Entrevista reservada con Fuente J (civil), 14 de noviembre de 2018, Buenos Aires, Argentina.

[108] Jastreblansky, M. (10/12/2018). "Un monitoreo especial para controlar a los sectores violentos", en *La Nación*, Argentina (consultado el 4 de abril de 2018 en https://www.lanacion.com.ar/politica/un-monitoreo-especial-para-controlar-a-los-sectores-violentos-nid2200935)

[109] Entrevista reservada con Fuente J (civil), 14 de noviembre de 2018, Buenos Aires, Argentina.

[110] Entrevista reservada con Fuente K (civil). 20 de noviembre de 2018, Buenos Aires, Argentina.

sean autorizadas por la autoridad judicial competente), la ley N° 27.126, transfirió dicho órgano a la Procuración General de la Nación, quedando estas actividades bajo el paraguas de la Corte Suprema.

Por otra parte, el Decreto N° 656/2016, referido a la Agencia Federal de Inteligencia, facultaba al Director General de la AFI a aprobar su estructura orgánica y funcional a la vez que derogaba los artículos 2, 3, 4, 5, 6 y 7 y los anexos II, III, IV, V, VI y VII del Decreto N° 1.311, por lo que resulta casi imposible referirnos a la evolución de la estructura orgánica y funcional que se dio en el seno del sistema de inteligencia nacional a partir de esa fecha debido a que, a partir del decreto mencionado, se dejó de lado la publicación de las modificaciones, retomando el secretismo que atañe a los servicios de inteligencia.

A pesar de ello, podemos mencionar que, tanto en 2015 como en el año 2017, con la creación del Comité de Ciberseguridad, la Agencia Federal de Inteligencia fue invitada a participar de las reuniones de dicho Comité a través de su Dirección de Ciberinteligencia[111], lo cual supone una participación (no necesariamente operativa) por parte del sistema de inteligencia nacional en la definición de las políticas de ciberseguridad y ciberdefensa.

Con la creación de la Dirección Nacional de Investigaciones de Ciberdelitos, en el año 2018, en el marco del Ministerio de Seguridad, la DINICRI, encargada principal de detectar incidentes en el ciberespacio a través de métodos y herramientas propias a la ciberinteligencia y a partir de fuentes abiertas y cerradas, adquirió la tarea de elaborar y girar informes de inteligencia a dicha dependencia, alertando, de esta forma, sobre aquellos incidentes que se escapan a la Dirección de Investigaciones por los métodos y fuentes que esta dependencia está habilitada a utilizar.[112]

a. Formación

Como contraparte, fue a partir del cambio de gobierno que se impulsa la ciberseguridad como ámbito de formación de los agentes de inteligencia. A partir del año 2016 la Escuela Nacional de Inteligencia (ENI) modernizó su Programa de Formación de Agentes de Inteligencia con el objeto de profesionalizar, aún más, la formación de los ingresantes al sistema. De esta manera, con la colaboración de distintas Universidades a

[111] Entrevista reservada con Fuente J (civil), 14 de noviembre de 2018, Buenos Aires, Argentina.
[112] Entrevista reservada con Fuente D (civil), 11 de septiembre de 2018, Buenos Aires, Argentina.

nivel nacional, se convocó a alumnos y graduados, referidos por las instituciones académicas, a postularse para convertirse en agentes de inteligencia. (Jefatura de Gabinete de Ministros: 2017).

El día martes 5 de julio de 2016, Diario Perfil informaba respecto de los inicios del curso, replicando las palabras del Director de la AFI al mencionar que tanto la ENI como la AFI tienen por objeto proveer conocimiento para que el Presidente de la Nación pueda tomar las mejores decisiones y que, desde la modificación de la ley de inteligencia, el sistema tiene la misión de generar inteligencia referida a los delitos federales complejos. Ante esto, la formación de los aspirantes y la actualización de los conocimientos de los agentes ya insertos en el sistema, se enfocaría en áreas referidas a: legislación, doctrina y ciclo de inteligencia (recolección y análisis de información, calidad de información y medidas de seguridad) y delitos federales complejos tales como narcotráfico; trata de personas; tráfico de armas; terrorismo; ciberseguridad y lavado de dinero.[113]

A modo de continuar con la tarea de perfeccionamiento de personal y detección de posibles candidatos para ingresar al sistema de inteligencia, y en consonancia con los convenios establecidos con las Universidades, en 2017 se lanzó la Maestría en Ciberseguridad y Ciberdefensa, impartida en su conjunto por la ENI y la Facultad de Ciencias Económicas de la UBA. Dicha Maestría fue planificada por el Dr. Roberto Uzal en su ánimo de acercar las cuestiones cibernéticas a especialistas provenientes de distintas ramas disciplinarias, intentando contrarrestar la mentalidad de que la ciberseguridad es campo de estudio de las disciplinas informáticas. En virtud de ello, la Maestría logró una audiencia variada, proveniente de áreas relacionadas a los sistemas, la seguridad, la defensa y otras. La idea de esta Maestría (que es una de las únicas y la primera en su tipo en nuestro país) es nutrir a la población con conocimientos interdisciplinarios sobre el ciberespacio.[114]

[113] Diario Perfil. (5 de julio de 2016). La AFI lanzó un Programa de Formación de Agentes de inteligencia, en *Diario Perfil*, Buenos Aires, Argentina. (Consultado el 25 de noviembre de 2018 en https://www.perfil.com/noticias/politica/la-afi-lanzo-un-programa-de-formacion-de-agentes-de-inteligencia-20160705-0051.phtml)

[114] Entrevista reservada con Fuente G (civil). 20 de septiembre de 2018, Buenos Aires, Argentina.

Conclusiones parciales

Con el objeto de indagar sobre el rol de inteligencia en el trazado de las políticas públicas destinadas a los ámbitos de la ciberseguridad y la ciberdefensa, el presente capítulo nos iluminó respecto a los distintos procesos desarrollados en las agencias de inteligencia con el objeto de lograr el análisis de la cuestión cibernética por parte de los organismos de inteligencia que tienen como fin el nutrir a las políticas destinadas a la seguridad nacional.

Como vimos, a pesar de que la DINIEM fue quien comenzó a visualizar las cuestiones vinculadas al ciberespacio, lo cierto es que hasta fines de 2012 el accionar de la Dirección se centró en participar en el debate ministerial por definir la ciberdefensa, lo cual no obtuvo grandes resultados. A pesar de ello, el Ministerio de Defensa, a través de sus Directivas Políticas de Defensa Nacional de 2014 y 2018, logró establecer conceptualizaciones precisas de lo que significa el ciberespacio en el marco militar, aunque el definición mutó de una DPDN a la otra, lo cual significa un cambio de visión profundo en este sentido.

Respecto al proceso de involucramiento del sistema de inteligencia argentino en el ciberespacio, este comienza a cobrar impulso en el año 2013, luego de que el Ministerio de Defensa sea víctima de un ciberataque que vulneró la seguridad de una parte importante de sus documentos confidenciales. A partir de ello, según las memorias detalladas del Estado Nacional, los subsiguientes planes nacionales de inteligencia empezaron a incorporar las ciberamenazas como objeto de estudio de las agencias de inteligencia. Este profundo análisis de las ciberamenazas tiene la misión de servir de instrumento para desarrollar las políticas de ciberseguridad y ciberdefensa emanadas de los Ministerios de Seguridad y Defensa.

La nueva normativa de inteligencia implementada desde 2015 pone de manifiesto la necesidad del abordaje de ciberdefensa y ciberseguridad por parte de los organismos de inteligencia. Esto significó un avance en el impulso de la ciberinteligencia, ya que el Decreto 1311/2015 otorgó, por un lado, capacidades de ciberseguridad por parte de la DINICRI brindándole competencias de ciberpatrullaje y creó la Dirección Operacional de Inteligencia sobre el Ciberespacio, promoviendo el desarrollo de capacidades de ciberinteligencia en el marco de la AFI. Es posible suponer que al mismo tiempo que se creó estructuras dentro de la AFI destinadas a desempeñar tareas específicas de

ciberinteligencia, esto se haya replicado en los otros organismos parte del sistema de inteligencia nacional, aunque no podemos apreciar la fecha exacta en que esto da inicio.

El cambio de gobierno significó un reordenamiento de las capacidades de inteligencia en el ciberespacio. Por una parte, potenció las capacidades desarrolladas en la DINICRI, otorgándole mayores responsabilidades, lo cual resaltó con la adopción de la Dirección de Investigaciones de Ciberdelito en el Ministerio de Seguridad.

El año 2016 significó también un reordenamiento en la formación de agentes de inteligencia en el marco de la Escuela Nacional de Inteligencia, promoviendo la profesionalización de los mismos a través de la modificación del plan de estudios que incorporó temáticas vinculadas a las amenazas transnacionales entre las que podemos destacar la ciberseguridad.

A estos cambios se le sumó el Decreto 656/2016 que dejaba sin efecto gran parte de los lineamientos establecidos por el Decreto 1311/2015 y, a partir del cual, regresa el secretismo (podríamos decir que de forma estricta) a las cuestiones que atañen a la inteligencia nacional, dejándonos escasos recursos disponibles para estudiar la evolución del sistema a partir de esta fecha.

CONCLUSIONES GENERALES

El objetivo general que sirvió de lineamiento principal para esta investigación fue el de iluminar sobre los factores que diluyen la definición de una Estrategia Nacional de Ciberseguridad a modo de responder al interrogante planteado en el diseño de investigación de ¿cuáles son las causas que hacen a la falta de una Estrategia Nacional de Ciberseguridad en Argentina?

La hipótesis preliminar planteada en el inicio de esta tesis fue que "la falta de una ENCS en Argentina se debe a la incapacidad de definir los lineamientos conceptuales y la eficaz vinculación entre las normas y las políticas desarrolladas."

A fin de contrarrestar la hipótesis preliminar, el primer capítulo permitió visualizar que Argentina se ha visto afectada por enormes cuotas de actividad cibernética criminal, siendo uno de los países de la región más expuesto a esta problemática.

Si bien los problemas de seguridad internacional se plantean en el ámbito global, son los Estados, a partir de sus políticas domésticas, quienes proponen soluciones en el ámbito local que terminan afectando al ámbito global. En este sentido, la comunidad internacional ha tomado diversas medidas a fin de contrarrestar la cuestión cibernética que sirvieron de ejemplo para que Argentina adopte medidas comunes al resto de los Estados para empezar a delinear su sistema nacional de ciberseguridad.

Estas políticas adoptadas por Argentina, tratadas en el segundo capítulo, permiten vislumbrar el interés del Estado Nacional y de la elite política dominante en el período de estudio, por estimular la expansión y difusión de las TICs. Esta difusión tecnológica trajo aparejada la necesidad de establecer medidas de ciberseguridad y ciberdefensa con el objeto de mitigar y proteger al país de las vulnerabilidades provenientes del ecosistema que compone el ciberespacio.

A fin de iluminar las falencias de estas políticas, se analizó la estructura de la política doméstica. En este sentido, es posible apreciar que a fin de intentar prepararse ante el accionar delictivo en el ciberespacio se crearon diversas normativas destinadas a proteger la seguridad de la información y cooperar internacionalmente en el ámbito procesal.

Respecto a las políticas de ciberseguridad y ciberdefensa propiamente dichas, las funciones de ciberseguridad en el ámbito nacional se encuentran separadas entre los distintos organismos del Estado, haciendo que la toma de decisiones se encuentre dividida entre las distintas dependencias que poseen capacidades en el área.

De esta forma, encontramos un sistema dividido en tres: ciberseguridad, ciberdefensa y cibercrimen. Todas estas poseen distintas dinámicas y desarrollos paralelos. Por su parte, el Ministerio de Defensa empezó a articular la cuestión desde el año 2006, estructurando los resultandos con distinto grado de intensidad a lo largo del período de estudio. Es a partir del año 2015, cuando la creación de estructuras termina de cobrar forma, que las políticas empiezan a ser más operativas. En el caso de la ciberseguridad, desde sus inicios hasta la actualidad estuvo ligada a Jefatura de Gabinete de Ministros, siendo impulsada en el año 2011 a través del Programa ICIC. En materia de cibercrimen, aunque las investigaciones siempre estuvieron ligadas al ámbito del Ministerio de Justicia y Derechos Humanos, las políticas operativas son más recientes. Es a partir de 2018, con la creación de la Dirección de Investigaciones del Ciberdelito, que el Ministerio de Seguridad cobra mayor notoriedad en la temática.

Esto demuestra que las vulnerabilidades a las que nos enfrenta el ciberespacio sirvieron de puntapié inicial para que la administración nacional empiece a pensar en generar respuestas al fenómeno ciberespacial. Es un hecho que estas respuestas fueron planteadas sectorialmente, sin encontrar coordinación y unidad en las políticas destinadas al ciberespacio.

Tal como plantean Calam, et. al, los Estados que han desarrollado una única organización con responsabilidad general en cuestiones de ciberseguridad obtienen resultados más eficaces y ponen de manifiesto la necesidad de entrelazar los límites institucionales de los distintos departamentos, agencias y funciones para tratar de forma eficaz la ciberseguridad nacional.

Si los autores están en lo correcto, entonces el hecho de atacar sectorialmente el fenómeno ciberespacial sin una unidad en la coordinación que englobe las políticas de ciberseguridad, ciberdefensa y cibercrimen, son entonces menos eficientes.

Si bien el Programa ICIC surgió como coordinador de la ciberseguridad para todos los órganos de la Administración Pública Nacional, la modalidad de implementación de dichas recomendaciones no parece ser la adecuada al no plantearse como vinculante a todas las agencias gubernamentales salvo previa adhesión al programa, lo cual otorgaba la funcionalidad de que el Programa ICIC trabaje en conjunto con cada agencia según las necesidades que estas últimas presente. Siguiendo esta lógica, la implementación de la Política de Seguridad de la Información Modelo sólo se hizo efectiva en algunos casos particulares.

Esta necesidad de articulación de los organismos públicos en materia de ciberseguridad se reflejó en los intentos de crear una mesa de trabajo conjunto que obtenga como resultado la elaboración de una Estrategia Nacional destinada a la protección de las Infraestructuras de la Información y de la Ciberseguridad en 2015 y, tras su fracaso y el cambio de gestión nacional, la creación del Comité de Ciberseguridad en julio de 2017. Ambos grupos de trabajo reunieron a distintos organismos estatales vinculados a la mitigación de ciberamenazas. Por su parte, el Comité de Ciberseguridad se compuso por los Ministerios de Seguridad, Defensa y Modernización (actualmente Jefatura de Gabinete de Ministros), quienes se han visto obligados a trabajar en conjunto para la elaboración de una Estrategia Nacional de Ciberseguridad capaz de definir los lineamientos a seguir para la obtención de un ciberespacio cada vez más seguro.

Este Comité, además, cuenta con la participación activa del Ministerio de Justicia y Derechos Humanos, el Ministerio de Relaciones Exteriores y Culto y la Agencia Federal de Inteligencia, lo cual debería subsanar el hecho de que hasta la actualidad, la toma de decisiones en materia cibernética no se produjo de forma articulada.

A pesar del trabajo conjunto y de (ambos) esfuerzos por definir una ENCS, aún hoy (marzo de 2019), no se obtuvieron los resultados deseados.

En este sentido, y a fin de responder el último objetivo específico de esta investigación, el de indagar sobre el rol del sistema de inteligencia en el trazado de políticas públicas destinadas a los ámbitos de la ciberseguridad y ciberdefensa, se llevó a cabo un análisis de las funciones otorgadas por ley al sistema de inteligencia en el ciberespacio y su operatividad.

Dado que cuando hablamos de la actividad de inteligencia nos referimos a la producción de conocimiento oportuno para la adecuada toma de decisiones que tiene como fin prevenir y resolver aquellos conflictos que pudieran derivar en crisis, el fin último de la inteligencia es entonces servir de insumo para la toma de decisiones.

En este sentido, vemos que las agencias de inteligencia empiezan a indagar sobre las problemática a través de requerimiento político o por la propia observación y sistematización de la problemática.

En el caso de la defensa nacional, en el marco de la DINIEM la temática de defensa cibernética se instala por la propia observación del contexto en el año 2011, para luego ser, esta investigación, sustentada y respaldada por requerimiento político. Esta investigación primaria estuvo destinada a comprender y definir conceptualmente la

ciberdefensa e identificar los avances realizados en el ámbito del instrumento militar en materia cibernética para así lograr definir la división de tareas destinadas a la defensa cibernética. Más adelante, la DINIEM continuó con la producción de ciberinteligencia por requerimiento político.

En contraposición, en materia de seguridad interior, el ciberespacio se instala como unidad de análisis de la DINICRI y la AFI por requerimiento político a partir del año 2013, sin generar un proceso de debate en el que intervengan dichas entidades.

El accionar del sistema de inteligencia en el ciberespacio se acentúa en 2015 tras la adopción de nueva normativa. En el Decreto 1311 se define a la ciberseguridad dentro del ámbito de las actividades de inteligencia criminal, lo cual permite suponer que la inteligencia estratégica militar posee, a su vez, la capacidad de desarrollar actividades de inteligencia en el ciberespacio vinculadas estrictamente a lo propio de la defensa nacional.

En el caso de la AFI, el Decreto le otorga una estructura operacional vinculada estrictamente a la ciberinteligencia, otorgándole capacidades operativas en la materia.

En 2016, esto se vio potenciado en la modificación de los planes de estudio de la Escuela Nacional de Inteligencia, lo cual tuvo como objetivo la profesionalización de los agentes de inteligencia, incorporando la ciberseguridad como uno de los grandes ejes de análisis en la formación del personal de inteligencia.

A modo de cierre, y retomando el lineamiento principal de esta investigación, cabe resaltar que, a pesar del impulso de las políticas de ciberseguridad y ciberdefensa desarrolladas por nuestro país, la adopción de normativas pertinentes y el otorgar ciertas funciones de ciberinteligencia a las agencias de inteligencias nacionales, es preciso reconocer que no existe ningún documento oficial que declare a la seguridad del ciberespacio como interés vital de la Nación. Sin una definición de este interés por parte de las autoridades nacionales, será difícil guiar la tarea de inteligencia y las políticas de ciberseguridad y ciberdefensa en pos de la persecución de dicho interés.

En definitiva, si tomamos la primera premisa de la hipótesis que menciona la "incapacidad de definir los lineamientos conceptuales", vemos que en el caso de la ciberdefensa, el concepto ha mutado entre la Directiva Política de Defensa Nacional del año 2014 y el documento del año 2018. En el primer documento, el ciberespacio es definido como un ámbito transversal a los escenarios tradicionales de conflicto (mar, tierra, aire y espacio exterior), mientras que el documento que lo releva define al ciberespacio como un quinto dominio, lo cual supone visiones completamente diferentes

en el ámbito de la defensa nacional a la hora de actuar en este espacio. En el caso de la ciberseguridad, no se ha encontrado documentos oficiales que evidencien una definición oficial del término.

Respecto a la premisa que detenta la incapacidad de lograr una eficaz vinculación entre las normas y las políticas desarrolladas, vemos que en realidad, existen normas que se han adecuado por completo a las políticas de ciberdefensa y ciberseguridad. Es el caso de la división tajante en materia de seguridad y defensa que se ve reflejada en el ambiente cibernético, aunque esto trajo ciertas complejidades a la hora de su aplicación dado que el ciberespacio no permite una delimitación categórica tan estricta, sino que ofrece áreas grises en las que cuestiones de seguridad y defensa se mezclan de forma constante.

Vemos entonces que, el trabajo individual que han desarrollado las distintas agencias de gobierno vinculadas a la producción de políticas de ciberseguridad, ciberdefensa y cibercrimen, junto con la falta de elaboración de lineamientos conceptuales claros (a los cuales sirven las tareas de inteligencia estratégica), son, condicionantes de la no existencia de una Estrategia Nacional de Ciberseguridad.

A pesar de ambos intentos por vincular los esfuerzos nacionales, a partir del grupo de trabajo de 2015 y el Comité de Ciberseguridad creado en 2017, aún hoy el objetivo de elaborar una Estrategia Nacional de Ciberseguridad continúa sin llegar a puerto deseado. Una vez que esto llegue a concretarse, las oportunidades de reducir la incertidumbre y los riesgos y amenazas que plantea el ciberespacio para la Argentina serán cada vez mayores.

De esta manera, será objeto de análisis para una futura investigación el indagar sobre el contenido de la ENCS (una vez que se haga oficial), su proceso de elaboración de forma sistémica, pero también observar y reflexionar acerca de la implementación de dicha estrategia.

Otro punto de partida para un nuevo trabajo de estudio será el de indagar en profundidad el rol de la justicia en lo que se refiere a investigaciones que tienen como fin el procesar ciberdelitos y la aplicación del Convenio de Budapest en ese marco. Como vemos, el ciberespacio continúa siendo campo fértil de estudio.

REFERENCIAS BIBLIOGRÁFICAS

Libros:

Anónimo. (2009). Análisis de Inteligencia.

Albarracín Keticoglu, Ana y Sergio Eissa. (2019). Ciberdefensa en Argentina. Pujas en torno a su definición. En, Sol Gastaldi y Leandro Ocón (Eds.), *Ciberespacio, Estrategia y Defensa Nacional*, mimeo, Buenos Aires, Argentina.

Arquilla, John y David Ronfeldt. Cyberwar is coming! enArquilla, J. y D. Ronfeldt. (Eds.), *Athena's Camp: Preparing for Conflict in the Information Age* (pp 23-60) Santa Monica, CA, US: RAND Corporation, 1997. Recuperado de: https://www.rand.org/pubs/monograph_reports/MR880.html.

Dougherty, James y Robert Pfaltzgraff. (1993). *Teorías en pugna en las Relaciones Internacionales*. Argentina: GEL. ISBN: 950-694-292-7.

Ganuza Artiles, N. (2010). Situación de la ciberseguridad en el ámbito internacional y en la OTAN. En. Joyanes Aguilar, L. *Cuadernos de Estrategia N° 149. Ciberseguridad: retos y amenazas a la Seguridad Nacional en el ciberespacio*, (pp 166 - 214), España: IEEE.

Gómez Vieités, A. (2007). Enciclopedia de la seguridad informática. Alfaomega.

Kent, S. (2016). *Strategic Intelligence for American World Policy*, United States: Princeton Legacy Library.

Kuehl, Daniel (2009) From Cyberspace to Cyberpower: Defining the Problem. En Franklin D. Kramer, Stuart H. Starr, y Larry K. Wentz (Eds.), *Cyberpower and National Security* (pp 24-42).Washington, DC: Center for Technology and National Security Policy, National Defense University, Potomac Books, Inc. ISBN: 978-59797-423-3.

Li, J. and Daugherty, L. (2015). *Training Cyber Warriors: What can be learned from defense language training?* California, United States: Rand Corporation.

Lin, Herbert, Governance of Information Technology and Cyber Weapons. En Elisa D. Harris (Ed.), Governance of Dual-Use Technologies: Theory and Practice (pp 112-157). Cambridge, Mass.: Academy of Arts & Sciences. ISBN: 0-87724-110-4.

Lobell, S. (2009). Threat assessment, the state, and foreign policy: a neoclassical realist model. En. Lobell, S., N. Ripsman& J. Taliaferro. (2009). *Neoclassical Realism, the State and Foreign Policy*. Cambridge University Press. ISBN: 978-0-521-51705-8

MINDEF. (2015). *Libro blanco de la defensa.* Buenos Aires, Argentina: MINDEF.

Mitnick, Kevin y William Simón. (2007) *El Arte de la Intrusión: la verdadera historia de las hazañas de hackers, intrusos e impostores.* 1° ed. México, Alfaomega Grupo Editor, S.A. Abril de 2007. ISBN: 978-970-15-1260-9.

Morgenthau, Hans. (1990) Una teoría realista de la Política Internacional. En, Morgenthau. Política entre las Naciones: la lucha por el poder y la paz (pp 11-37). 6° ed., Buenos Aires, Argentina: GEL.

Rattray, G. L. (2016). An Environmental Approach to Understanding Cyberpower. On. Kramer, F., Starr, S. and Wentz, L. Cyberpower and National Security, (253 - 274), Washington, United States: Center for Technology and National Security Policy and National Defense University.

Salom Clotet, J. (2010). El ciberespacio y el crimen organizado. En. Joyanes Aguilar, L. *Cuadernos de Estrategia n° 149. Ciberseguridad. Retos y Amenazas a la Seguridad Nacional en el Ciberespacio*, (pp 130 - 164), España: IEEE.

Schwab, K. (2017). *La cuarta revolución industrial.* Ciudad Autónoma de Buenos Aires, Argentina: Debate. ISBN: 978-987-3752-69-8.

Singer y Friedman (2014). *Cybersecurity and Cyberwar. What everyone needs to know.* New York, United States: Oxford University Press. ISBN: 978-0-19-991809-6 (hardback) / 978-0-19-991811-9 (paperback).

Starr, Stuart. (2011) Developing a theory of cyberpower. En Tarek Saadawi y Louis Jordan (Eds.), *Cyber Infrastructure Protection* (pp 15-28). United States: Strategic Studies Institute, may 2011. ISBN: 1-58487-468-6.

Starr, Stuart. (2016) "Toward a Preliminary Theory of Cyberpower." En Kramer, Starr y Wentz (Eds.), *Cyberpower and National Security* (pp 43-88). Washington, DC: Center for Technology and National Security Policy, National Defense University, Potomac Books, Inc. ISBN: 978-59797-423-3.

Sun Tzu ([1958] 2015). *El Arte de la Guerra*. Traducida por Sergio Albano. Buenos Aires, Argentina: Gradifco. ISBN: 978-987-1093-45-8.

Taleb, N. (2018). *El cisne negro. El impacto de lo altamente improbable.* Buenos Aires, Argentina: Paidós.

Waltz, K. (1989). Teoría de la política internacional. Buenos Aires, Argentina: GEL.

Artículos Académicos:

Aranda Bustamante, G., Riquelme Rivera, J. y Salinas Cañas, S. (2015).La ciberdefensa como parte de la agenda de integración sudamericana.*ResearchGate*, enero de 2015, 100-110.

Barbé, E. (1987). El papel del realismo en las relaciones internacionales (la teoría de la política internacional de Hans J. Morgenthau). *Revista de Estudios Políticos (Nueva Época), julio – septiembre* (57), 149-176. Recuperado de https://dialnet.unirioja.es/servlet/articulo?codigo=26941

Calam, M., Chinn, D., Fantini Porter, J. y Noble, J. (september 2018). Asking the right questions to define government's role in cyberspace, *McKinsey&Company*. Recuperado de: https://www.mckinsey.com/industries/public-sector/our-insights/asking-the-right-questions-to-define-governments-role-in-cybersecurity

Eissa, S., Gastaldi, S.,Poczynok, I. y Zacarías Di Tullio, E. (2014). El ciberespacio y sus implicancias para la defensa nacional. Aproximaciones al caso argentino. *Revista Quilmes de Ciencias Sociales.* Segunda época, 6 (25), 181 – 198.

Flores, H. (2015, septiembre). Una visión de las amenazas ciberespaciales y la defensa.*Boletín del ISIAE. Recuperado de: http://www.cari.org.ar/pdf/boletin61.pdf*

Hernández, J. C. (27/2/2018). Estrategias Nacionales de Ciberseguridad en América Latina. *GESI*. Recuperado de: http://www.seguridadinternacional.es/?q=es/content/estrategias-nacionales-de-ciberseguridad-en-am%C3%A9rica-latina

Gastaldi, Sol y Candela Justribó (2014) La seguridad y la defensa en el ámbito ciberespacial. *EDENA*, informe de investigación, avance de trabajo n° 2, 1-15.

Justribó, Candela, Sol Gastaldi y Jorge A. Fernández. (2014) Las estrategias de ciberseguridad y ciberdefensa en Argentina: marco político-institucional y normativo. *EDENA*, informe de investigación, avance de trabajo n° 1, 1-17.

Justribó, Candela y Sol Gastaldi (2014). Investigando la Ciberdefensa. *EDENA*, informe de investigación, avance de trabajo n° 3, 1-7.

Justribó, Candela. (2014) Ciberdefensa: una visión desde la UNASUR.*IRI,* VII Congreso, 1-24.

Keohane, R. y Nye, J. (1998). Power and Interdependence in the Information Age. *Foreing Affairs*, 77 (5), 81-94.

Leiva E. (2015). *E*strategias Nacionales de Ciberseguridad: Estudio Comparativo Basado en Enfoque Top-Down desde una Visión Global a una Visión Local. *Revista Latinoamericana de Ingeniería de Software*, 3(4): 161-176, ISSN 2314-2642.

Marcelo de los Reyes. (2018). La inteligencia estratégica como instrumento fundamental para la toma de decisiones. Recuperado de https://es.scribd.com/document/392354912/La-Inteligencia-Estrategica-como-instrumento-fundamental-para-la-toma-de-decisiones

Niss, O. (2017). "Ciberseguridad y ciberdefensa en el Estado", mimeo, Rosario, Argentina.

Nye, J. (2010) CyberPower. *Belfer Center for Science and International Affairs, HARVARD Kennedy School*. Mayo de 2010.(Online). Recuperado de: http://www.belfercenter.org/sites/default/files/legacy/files/cyber-power.pdf

Rego, Miguel. (2012)Por un liderazgo claro para la Estrategia de Ciberseguridad Nacional. *Red Seguridad.* Septiembre de 2012. Recuperado de: http://www.redseguridad.com/instituciones/administracion/por-un-liderazgo-claro-para-la-estrategia-de-ciberseguridad-nacional

Torres Soriano, M. (8 de enero de 2018). El dilema de la interpretación en el ciberespacio. *Instituto de Estudios Estratégicos de España*. Recuperado de: http://www.ieee.es/Galerias/fichero/docs_opinion/2018/DIEEEO03-2018_Dilema_Ciberespacio_ManuelRTorres.pdf

Trentadue (2016). Módulo 1 Inteligencia Científico Tecnológica. MIEN, UNLP.

Von Heinegg, W. H. (2013). Territorial Sovereignty and Neutrality in Cyberspace. International L*aw Studies*, U.S. Naval War College, 89 (123), p 122 – 156.

Informes:

CICTE. (2012). *Declaración "Fortalecimiento de la Seguridad Cibernética en las Américas."* Recuperado de: https://www.sites.oas.org/cyber/Documents/Declaracion%20del%20Fortalecimiento%20de%20la%20Seguridad%20en%20las%20Americas.pdf

DGCD. (2015). Memoria 2015.

Jefatura de Gabinete. (2014). Memoria Detallada del Estado de la Nación 2013.

Jefatura de Gabinete. (2016). Memoria Detallada del Estado de la Nación 2015.

Jefatura de Gabinete. (2017). Memoria Detallada del Estado de la Nación 2016.

Kaspersky Lab. (2014). *Unveiling "Careto" – The Mask APT*. Recuperado de: https://kasperskycontenthub.com/wp-content/uploads/sites/43/vlpdfs/unveilingthemask_v1.0.pdf

KasperskyLab. (28/11/2017). Estadisticas generales 2017. Recuperado de: https://kasperskycontenthub.com/securelist/files/2017/12/KSB_statistics_2017_SP_final.pdf

KasperskyLab. (28/11/2017). Pronósticos de ataques cibernéticos en América Latina, 2018. https://securelist.lat/pronosticos-de-ataques-ciberneticos-en-america-latina-2018/85816/

Lewis, J. A. (2016). Experiencias avanzadas en políticas y prácticas de ciberseguridad: panorama general de Estonia, Israel, República de Corea y Estados Unidos. *BID.*

MINDEF. (2018). Ciberseguridad en el sector público. Recuperado de: https://www.itu.int/en/ITU-D/Regional-Presence/Americas/Documents/EVENTS/2018/20577/Discussion%20Public%20Sector%20Min%20Defensa.pdf

Security Radware. (2017). *Oplcarus 2017*. (6 de agosto de 2017). Recuperado de: https://security.radware.com/ddos-threats-attacks/threat-advisories-attack-reports/opicarus2017/

Observatorio de la ciberseguridad en América Latina y el Caribe. (2016). Ciberseguridad ¿Estamos preparados en América Latina y el Caribe? Recuperado de https://publications.iadb.org/handle/11319/7449?locale-attribute=es&

OEA/Trend Micro. (2015). *Reporte de Seguridad Cibernética e Infraestructuras Críticas de las Américas.*

UIT. (2017). *Global Cybersecurity Index.* Recuperado de: https://www.itu.int/dms_pub/itu-d/opb/str/d-str-gci.01-2017-pdf-e.pdf

UNODC. (2013). Estudio exhaustivo sobre el delito cibernético – borrador. Recuperado de: https://www.unodc.org/documents/organized-crime/cybercrime/Cybercrime_Study_Spanish.pdf

World Economic Forum. (2018). The global risk report 2018. Recuperado en: http://www3.weforum.org/docs/WEF_GRR18_Report.pdf

Fuentes electrónicas:

ANSES. (13/07/2016), "Conectar Igualdad ya superó las 100.000 notebooks entregadas en 2016". Recuperado de: http://noticias.anses.gob.ar/noticia/conectar-igualdad-ya-supero-las-netbooks-entregadas-en-1736

BA-CSIRT. Phishing. Recuperado de: www.ba-csirt.gob.ar

Bullentini, A. (1 de diciembre de 2015). "Predecir y prevenir ciberataques", en *Página 12*. Recuperado de https://www.pagina12.com.ar/diario/elpais/1-287308-2015-12-01.html

CCDCOE. "About us". Recuperado de https://ccdcoe.org/about-us/

CCDCOE. (24-28 Apr 2017). Locked Shields 2017. Recuperado de: https://ccdcoe.org/locked-shields-2017.html

CISCO. Internet of Everything FAQ. Recuperado de: http://ioeassessment.cisco.com/learn/ioe-faq

Cyber Ex International. (2018). Descripción. Recuperado de: https://www.cyberex.es/international/es/descripcion

CyberEx Internacional. (2019). Recuperado de: https://www.cyberex.es/international/es/resultado_2016

Davidovsky, S. (9/5/2018). Cuál es el objetivo de Aprender Conectados, el plan educativo que reemplaza a Conectar Igualdad, en *La Nación*. Recuperado de https://www.lanacion.com.ar/tecnologia/cual-es-el-objetivo-de-aprender-conectados-el-plan-educativo-que-reemplaza-a-conectar-igualdad-nid2132718

Diario Perfil. (5 de julio de 2016). La AFI lanzó un Programa de Formación de Agentes de inteligencia, en *Diario Perfil*, Buenos Aires, Argentina. Recuperado de https://www.perfil.com/noticias/politica/la-afi-lanzo-un-programa-de-formacion-de-agentes-de-inteligencia-20160705-0051.phtml)

ENISA. (2018). Cyber Europe. Recuperado de: https://www.enisa.europa.eu/topics/cyber-exercises/cyber-europe-programme

Estado Mayor de la Defensa de España (2018, 26 de octubre), "Equipos de siete naciones participan en el II Ejercicio del Foro Iberoamericano de Ciberdefensa", en *Estado Mayor de la Defensa de España,* Madrid (consultado el 29 de octubre de 2018 en http://www.emad.mde.es/EMAD/novemad/noticias/2018/10/Listado/181029-ni-foro-iberomaricano-ciberdefensa.html).

FIRST. "Mission." Recuperado de: https://www.first.org/about/mission

Fuerzasmilitares.org (2016, 25 de octubre), “Colombia ocupa segundo puesto de las Primeras Ciber Olimpiadas Militares de las Américas”, en *fuerzasmilitares.org*, Colombia (consultado el 13 de septiembre de 2018 en http://www.fuerzasmilitares.org/notas/colombia/fuerzas-militares/7153-cberolimpiadas-2016.html).

Fuerzas-armadas.mil (2018, 13 de septiembre), “Equipo del Comando Conjunto de Ciberdefensa logró clasificarse para las Ciberolimpiadas Militares 2018”, en *fuerzas-armadas.mil.ar*, Buenos Aires. Recuperado de: http://www.fuerzas-armadas.mil.ar/Noticia-2018-09-13-ciberdefensa-competencia.aspx

GFCE. “The GFCE Organization”. Recuperado de: https://www.thegfce.com/organization

Goujon, A. (7/1/2013). Anonymous dio de baja el sitio del INDEC en Argentina.*WeLiveSecurityEset.* Recuperado de: https://www.welivesecurity.com/la-es/2013/01/17/anonymous-dio-baja-sitio-indec-argentina/

Gutiérrez Amaya, C. (10/10/2014). Brasil, Chile y Argentina sufren el 80% del phishing en Latinoamérica. *WeLiveSecurityEset*. Recuperado de:https://www.welivesecurity.com/la-es/2014/10/10/brasil-chile-y-argentina-sufren-el-80-del-phishing-en-latinoamerica/

Infobae. (9/7/2012). Anonymous inició la Operación Quirófano y hackea páginas en Argentina. Recuperado de: https://www.infobae.com/2012/07/09/658114-anonymous-inicio-la-operacion-quirofano-y-hackea-paginas-argentina/

INVAP. Satélites ARSAT. Recuperado de: http://www.invap.com.ar/es/espacial-y-gobierno/proyectos-espaciales/satelite-arsat.html

InfoSecurity News. (octubre 2015). “Entrevista. Argentina – Ejercicio Nacional de Respuesta a Incidentes Cibernéticos”, en *infosecuritynews* Recuperado de: http://www.infosecurityvip.com/newsletter/entrevista_oct15.html

Infodefensa (2016, 3 de junio), “España y seis países latinoamericanos acuerdan un programa común de ciberdefensa”, en *Infodefensa*, Madrid. Recuperado de: http://www.infodefensa.com/es/2016/06/03/noticia-espana-latinoamerica-acuerdan-colaborar-ciberdefensa.html

ITU. (1/5/2018). CIRT Programme. Recuperado de: https://www.itu.int/en/ITU-D/Cybersecurity/Pages/Organizational-Structures.aspx

ITU. *Statistics. New data visualizationon Internet usersby región and country, 2010 – 2016* Recuperado de https://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx

Jastreblansky, M. (10/12/2018). "Un monitoreo especial para controlar a los sectores violentos", en *La Nación*, Argentina. Recuperado de: https://www.lanacion.com.ar/politica/un-monitoreo-especial-para-controlar-a-los-sectores-violentos-nid2200935

Jefatura Gabinete de Ministros. Recomendaciones de Ciberseguridad, en Argentina.gob.ar Recuperado de: https://www.argentina.gob.ar/modernizacion/infraestructuras-criticas-de-informacion-y-ciberseguridad/recomendaciones

Johnstone, L. (31/12/2012). Argentina Ministry of DefenseHacked, DocumentsleakedSiteDefaced. Recuperado de:https://www.cyberwarnews.info/2012/12/31/argentina-ministry-of-defense-hacked-documents-leaked-site-defaced/

KasperskyLab. (17/8/2016). Ataques financieros aumentaron un 16% en el segundo trimestre. Recuperado de: https://latam.kaspersky.com/blog/kaspersky-lab-ataques-financieros-aumentan-un-16-en-el-segundo-trimestre/7511/

Kaspersky Lab. Ciberamenazas y peligros en la red profunda (y oscura). Recuperado de: https://www.kaspersky.es/resource-center/threats/deep-web

KasperskyLab. (23/02/2018). Mapa de ciberataques en tiempo real. Recuperado de: https://cybermap.kaspersky.com/es/

La Nación. (1/2/2017). También hackearon 30 correos del Ministerio de Seguridad. Recuperado de: https://www.lanacion.com.ar/1980702-tambien-hackearon-30-correos-del-ministerio-de-seguridad

Miguel, H. (15 de marzo de 2018). Mitos y realidades de la ciberdefensa. *Revista DEF* Recuperado de http://defonline.com.ar/mitos-y-realidades-de-la-ciberdefensa/

NCSC. (11/5/2018). The National Cyber Security Centre. UK. Recuperado de: https://www.ncsc.gov.uk/

Norse. (23/02/2018). Mapa de ciberataques en tiempo real. Recuperado de: http://map.norsecorp.com/#/?geo=latAmer

Pagnotta, S. (7/8/2017). Confirman que fue phishing lo que permitió el robo de 3,5 millones en Argentina. *WeLiveSecurityEset.* Recuperado de:

https://www.welivesecurity.com/la-es/2017/08/07/confirman-phishing-robo-argentina/

PEN. Nueva capacitación en ciberdelito para fiscales especializados. Recuperado de: https://www.argentina.gob.ar/noticias/nueva-capacitacion-en-ciberdelito-para-fiscales-especializados

Puente, M. L. (1 de abril de 2018). Guía para entender la nueva geopolítica del ciberespacio. *Perfil*. Recuperado de: https://www.perfil.com/noticias/elobservador/guia-para-entender-la-nueva-geopolitica-del-ciberespacio.phtml

Schulkin, J. (24 de julio de 2018). "Expertos de la Universidad Internacional de Florida capacitarán a profesionales argentinos sobre ciberdelincuencia." *Infobae.* Recuperado de: https://www.infobae.com/tecno/2018/07/24/expertos-de-la-universidad-internacional-de-florida-capacitaran-a-profesionales-argentinos-sobre-ciberdelincuencia/

Schulkin, J. (3 de agosto de 2018). "Realizan simulaciones de respuesta a ataques cibernéticos en la Argentina antes del G20", en *Infobae.* Recuperado de:https://www.infobae.com/tecno/2018/08/03/simulaciones-de-respuesta-a-ataques-ciberneticos-en-la-argentina-antes-del-g20/

SecureList. (January 14, 2013). "Red October" Diplomatic Cyber Attacks Investigation. Recuperado de: https://securelist.com/red-october-diplomatic-cyber-attacks-investigation/36740/#1

Security radware. (6/8/2017). "Oplcarus 2017", en *securityradware.* Recuperado de: https://security.radware.com/ddos-threats-attacks/threat-advisories-attack-reports/opicarus2017/

Szklarz, E. (21 de diciembre de 2017), "Brasil promueve primer Ejercicio Iberoamericano de Defensa Cibernética", en *Diálogo-Américas.* Recuperado de: https://dialogo-americas.com/es/articles/brazil-organizes-first-ibero-american-cyber-defense-exercise

Team Cymru. (23/02/2018). Malicious activity map: world map. Recuperado de: http://www.team-cymru.org/visualizations/compromised_map/recent.mp4

Legislación y jurisprudencia argentina:

Jefatura de Gabinete de Ministros. (2011). Resolución N° 580.

Ministerio de Educación. (2018). Resolución N° 1410 Anexo 1.

Ministerio de Defensa. (2006). Resolución N° 346.

Ministerio de Defensa. (2013). Resolución N° 385.

Ministerio de Justicia y Derechos Humanos. (2016). Resolución N° 69.

Ministerio de Seguridad. (2018). Decisión Administrativa N° 564.

Ministerio de Seguridad. (2017). Resolución N° 1107-E.

Ministerio de Seguridad. (2018). Decisión Administrativa N° 299.

ONTI. (2013). Disposición N° 2.

PEN. (2006). Decreto N° 727.

PEN. (2010). Decreto N° 459.

PEN. (2014). Decreto N° 2645. Directiva de Política de Defensa Nacional

PEN. (2015). Decreto N° 13.

PEN. (2015). Decreto N° 1067.

PEN. (2015). Nueva Doctrina de Inteligencia Nacional. Decreto 1311.

PEN. (2016). Decreto N° 656.

PEN. (2016). Decreto N° 898.

PEN. (2016). Decreto N° 434.

PEN. (2018). Decreto N° 386.

PEN. (2018). Decreto N° 683.

PEN. (2018). Decreto N° 703. Directiva de Política de Defensa Nacional.

HCNA. (1988). Ley de Defensa Nacional. Ley N° 23.554

HCNA. (1992). Ley de seguridad interior. Ley N° 24.059

HCNA. (2000). Ley de protección de datos personales. Ley N° 25.326.

HCNA. (2001). Ley de firma digital. Ley N° 25.506.

HCNA. (2001). Ley de Inteligencia Nacional. Ley N° 25.520

HCNA. (2006). Ley N° 26.092

HCNA. (2008). Ley modificatoria del código penal – Ley de delitos informáticos. Ley N° 26.388.

HCNA. (2015). Ley modificatoria – Agencia Federal de Inteligencia. Ley N° 27.126

HCNA. (2017). Ley de adhesión al Convenio de Budapest. Ley N° 27.411

Jurisprudencia extranjera:

Congreso de Colombia. (2009). Ley 1273. Recuperado de: http://acueductopopayan.com.co/wp-content/uploads/2012/08/ley-1273-2009.pdf

Consejo de Europa. (2001). *Convenio sobre la ciberdelincuencia.*

White House of United States. (2011). *International Strategy for Cyberspace: Prosperity, Security and Opennes in a Networked World.*

Conferencias y Seminarios:

Borghello, C. y Temperini, M. (2013). Ciberseguridad Nacional Argentina: Craking de Servidores de la Administración Pública. En. Simposio Argentino de Informática y Derecho llevado a cabo en el marco de las Jornadas Argentinas de Informática (JAIIO) de la Sociedad Argentina de la Informática. Recuperado de: http://42jaiio.sadio.org.ar/proceedings/simposios/Trabajos/SID/03.pdf

Del Negro, R. (2016). Industria espacial y geopolítica. El caso de ARSAT. IX Jornadas de Sociología de la UNLP, 5 al 7 de diciembre de 2016, Ensenada, Argentina. En Memoria Académica. Disponible en: http://www.memoria.fahce.unlp.edu.ar/trab_eventos/ev.8845/ev.8845.pdf

Fuentes (entrevistas):

Entrevista reservada Fuente A (civil), 17/8/2018, Buenos Aires, Argentina.

Entrevista reservada Fuente B (civil), 31/8/2018, Buenos Aires, Argentina.

Entrevista reservada Fuente C (civil), 3/9/2018, Buenos Aires, Argentina.

Entrevista reservada Fuente D (civil), 11/9/2018, Buenos Aires, Argentina.

Entrevista reservada Fuente E (civil), 13/9/2018, Buenos Aires, Argentina.

Entrevista reservada Fuente F (civil), 18/9/2018, Buenos Aires, Argentina.

Entrevista reservada Fuente G (civil), 20/9/2018, Buenos Aires, Argentina.

Entrevista reservada Fuente H (militar), 3/10/2018, Buenos Aires, Argentina.

Entrevista reservada Fuente I (militar), 4/10/2018, Buenos Aires, Argentina.

Entrevista reservada Fuente J (civil), 14/11/2018, Buenos Aires, Argentina.

Entrevista reservada Fuente K (civil), 20/11/2018, Buenos Aires, Argentina.

ANEXO
ENTREVISTAS

FUENTE "A" – Entrevista reservada - 17 de agosto de 2018

Subsecretaría de Ciberdefensa

¿Hubo continuidad en las políticas de ciberdefensa con el cambio de gobierno?

No. Más bien rupturas, aunque no tan tajante. Hay una nueva concepción de ciberdefensa, lo cual supone un quiebre. Esto se refleja en las DPDN. La de 2014 definía al ciberespacio como un ámbito transversal, la actual se refiere a un nuevo dominio, lo que va de la mano con la concepción de que el ciberespacio es un quinto dominio, tal como lo plantea Estados Unidos y los países que forman parte de la OTAN.

Hubo un cambio brusco en las políticas de gobierno. Recién hoy hay una política de ciberdefensa. Durante el segundo mandato de Cristina se creó el Comando Conjunto de Ciberdefensa, Macri convirtió la Dirección de ciberdefensa en Subsecretaría, lo que le otorga mayor rango.

Antes de Aguad (tanto gobierno de Cristina como de Macri) no habían lineamientos claros en la materia, hoy sí. La DPDN de 2018 define que es competencia de defensa la protección de Infraestructuras Críticas.

Si bien aún hoy las IC no están definidas, hay una Comisión que está tratando de definirlas. (Están sacando muchas cosas del Homeland Security de EUA)

Están trabajando en dos concepciones de IC. Una que se refiere a las de carácter estrictamente militar y las otras referidas a garantizar la soberanía e independencia, su integridad territorial y proteger la vida y la libertad de sus integrantes.

¿Qué es el proyecto Núcleo Isoc& CSIRT/CERT para ciberdefensa?

Es un proyecto que se pretende hacer efectivo para el G20. La idea es construir un CERT nuevo, integrado por civiles y que dependa del MINDEF bajo la coordinación de la Subsecretaría. Va a tener la función de proteger las IC de la Defensa Nacional.

Por otra parte, la creación de un ISOC (Centro de Seguridad de la Información e Inteligencia Artificial) en el Comando Conjunto de Ciberdefensa. Este se encargará de proteger las IC propias del Instrumento Militar (dependiente de las FFAA).

La idea es articular información. Trabajar con otras agencias del gobierno teniendo cada uno sus funciones.

¿Cuál sería la diferencia con el Programa ICIC? ¿No es el CERT del Modernización el que actualmente se encarga de IC?

No queda claro. Se supone que el CERT de Modernización se va a encargar propiamente de la IC de la información. Lo que me cuesta verlo como una categoría aparte de IC, para mi es algo transversal a todas las IC.

Si el MINDEF se encarga de las IC y MINMOD de las IC de la información, ¿qué función queda para el MINSEG? El MINSEG es el encargado de prevenir y repeler los delitos cibernéticos.

¿Cómo afecta la nueva DPDN y el decreto 683 a la ciberdefensa? ¿El decreto 727/06 presentaba limitaciones para el accionar del sistema de ciberdefensa?

Con el decreto 727 había una limitación para el accionar de las FFAA. Al dejar atrás el concepto de agresión estatal externa, las FFAA pueden repeler agresiones en el ciberespacio. La nueva DPDN habilita a las FFAA a proteger las IC más allá del origen de la agresión.

Sólo para el caso particular de la ciberdefensa era necesaria la ampliación del decreto. Se podría haber hecho sólo para ese caso en particular sin la necesidad de habilitar una visión tan amplia en la que las FFAA puedan ser utilizadas para la lucha contra el narcotráfico y el terrorismo. Además, la presencia militar en fronteras hace años que se viene haciendo, por lo que el nuevo decreto todavía no cambió nada. ¿Responde el nuevo decreto a una excepcionalidad para el G20? De ser así se podría haber sacado un decreto de necesidad de urgencia una vez llegado el momento.

¿Existe algún tipo de instrumento que establezca los lineamientos estratégicos específicos de defensa cibernética?

Hay que escribir una estrategia, pero recién se está proyectando hacerlo.

El comité tripartito creado por Decreto 577/2017 (MINDEF, MINMOD y MINSEG) viene trabajando sobre una Estrategia Nacional de Ciberseguridad que no es para nada específica, sino que deja muchas cosas al aire. La idea es que cada parte escriba su propia estrategia, su propia visión de cómo va a desarrollar sus funciones respecto al ámbito cibernético.

Si una de las partes logra definir su estrategia específica para el ciberespacio antes de que salga la Estrategia Nacional de ciberseguridad, no va a pasar nada. Es tan amplio

lo que están escribiendo y tan poco concreto que es imposible que choque con las estrategias específicas de cada área.

La idea también es ampliar el Comité, para que empiece a estar integrada también por Cancillería, Justicia y Jefatura de Gabinete.

¿Existe algún manual de doctrina cibernética elaborado por el EMCO?

Hay pero de carácter secreto. El EMCO no lo comparte con la Subsecretaría. Sólo el Secretario tuvo acceso al documento, el resto no pudimos verlo.

El Comando no tiene buena relación con la Subsecretaría, ya que esta ejerce un control funcional. La Subsecretaría fue creada para regular el funcionamiento del Comando, por lo que genera roces.

¿Qué doctrina se utiliza para formar el personal?

En el Comando se utiliza esta doctrina elaborada por el EMCO y el Manual de Tallin, en la Subsecretaría se sigue el Manual de Tallin, ya que no se tiene acceso a la doctrina EMCO.

En la subsecretaría hace poco hubo una capacitación en ciberseguridad (cursos ainet). Vinieron de EUA a capacitarnos.

¿Cómo se compone el Comando y qué formación reciben sus profesionales?

Hay algunos civiles pero no un porcentaje significativo. El Comando se compone casi en su totalidad por personal militar y reciben formación militar.

Hay que ver los planes de estudio que tiene el Colegio Militar, las Escuelas Superiores y toda institución que forme parte de la UNDEF para poder ver la formación que reciben.

Existe una gran demanda de parte del Comando para obtener capacitación y visitas a CERTs internacionales.

El personal de ciberdefensa ¿participa en ejercicios conjuntos y combinados específicos del área? ¿Con qué países y con qué frecuencia?

Los ejercicios dependen del Comando.

Se está tratando de darle cada vez más relevancia al Foro Iberoamericano de Ciberdefensa. Ese es específico de ciberdefensa y participan únicamente las Fuerzas Armadas.

En este marco está Brasil, Argentina, España, Portugal y otros.

Se lanzó en 2016 en España. En la reunión de este año se planteó que en marzo/abril de cada año se va a desarrollar la reunión del Foro y en septiembre/octubre el ciberejercicio.

¿Con qué agencias de gobierno coopera el MINDEF en ciberdefensa?

Comité. Si bien formalmente está compuesto por MINMOD, MINDEF y MINSEG, también está participando de las reuniones Jefatura de Gabinete.

Fluvio Pompeo viene participando de las reuniones del Comité.

¿Hay algún tipo de acercamiento con el Congreso?

No. No se coopera con el Congreso. El único acercamiento que se produce es cuando piden que demos explicaciones de algo.

¿Existe cooperación con el sector privado y la academia? ¿Cómo se lleva a cabo?

Con el sector privado va a empezar a haber a través de los organismos reguladores. Una vez que se definan las IC (que van a ser las mismas que en cualquier país, a saber: energía, TICs, finanzas, sector nuclear, petróleo, gas, transporte…) se va a tener que empezar a trabajar en conjunto con las empresas que operan esas IC.

Con la academia existe cooperación con la UNLP ya que la Universidad cuenta con un CERT y está bastante avanzada en temas de ciberseguridad, pero todavía es incipiente esa cooperación, no sólo con la UNLP, sino con toda la academia.

En investigación y desarrollo todavía no hay nada.

¿Cuáles son los principales acuerdos internacionales específicos de ciberdefensa?

No hay. En realidad se trabaja a partir de acuerdos que son anteriores a la temática. En general, muchos de ellos plantean cooperar en determinados ámbitos de la defensa nacional y dejaban abierta la posibilidad de cooperar en ámbitos que se necesitaran a futuro, por lo que no hizo falta realizar acuerdos específicos ya que se suponen contemplados.

En general, se coopera con Chile, Brasil, Colombia y Estados Unidos. Se está trabajando también para agregar cooperación en defensa cibernética con España, en un acuerdo de 2006, aunque todavía no está cerrado.

Con Chile, por ejemplo, hay un grupo de trabajo. Además, un acuerdo sobre ciberdelito, ciberseguridad y ciberdefensa que data de 2018. Está la cooperación en

seguridad internacional denominada 2+2 porque participan los dos ministerios de cada país (MINDEF y MINSEG).[115]

Las FFAA, por su parte, tienen acuerdos internacionales propios.

¿Cuál es el principal lineamiento en el que se coopera?

La cooperación abarca todo lo que sea educación, investigación y sobre todo intercambio de información. Pero como el MINDEF aún no tiene el CERT esta cooperación es incipiente, sin CERT no se cuenta con información para intercambiar. Una vez que se ponga en marcha el CERT, se va a efectivizar la cooperación. Hoy es muy incipiente.

¿Qué porcentaje del presupuesto se destina al desarrollo de cibercapacidades y que tipo de capacidades se desarrollan?

Con el desarrollo del proyecto Núcleo ISOC & CSIRT/CERT se requiere de presupuesto que permita equipar estos centros. Esto no está contemplado en el presupuesto actual, aunque la administración asegura que no va a haber problemas en materia financiera para comprar los equipamientos necesarios.

El presupuesto para esto sale a través de planes militares.

¿El equipamiento está en proceso de compra? ¿Se llamó a licitaciones? ¿A qué país le estamos comprando?

Lo único que puedo decir es que está en proceso de compra. Se llamó a licitación y ya se asignó a quién se va a comprar, pero todavía no salió la licitación formal, aunque si se filtró en la prensa. No puedo mencionar ni a las empresas ni los países involucrados. (Si preguntas alguien te va a saber decir).

¿Cuáles fueron los momentos clave de la ciberdefensa en Argentina?

Es difícil marcar ciertos hechos como clave, darles ese grado de importancia. Fue importante la creación del Comando y más que nada cuando estuvo formada toda la estructura orgánica de la ciberdefensa.

Cabe reconocer que con Parodi aparecieron las definiciones concretas del sistema de ciberdefensa. Se le asignó mayor importancia. Antes no había claridad política. Incluso con Martínez había una lucha entre las distintas facciones que componen el PRO. Si bien Aguad es radical, tiene más aguante político. No le importa. Cuando tuvo que desplazar a figuras importantes, lo hizo.

[115] Memorandum de entendimiento sobre cooperación en materia de ciberseguridad, ciberdelito y ciberdefensa entre Argentina y Chile. 17 de mayo de 2018.

Desde que asumió Aguad que el objetivo de desarrollar la ciberdefensa está presente. Parodi tiene muchas definiciones sobre ciberdefensa. Está apostando a efectivizar.

Con Martínez, la Subsecretaría le pertenecía al pro y no tenía claridad política.

Parodi tiene definiciones concretas. Además tiene apoyo por parte del gobierno y de Aguad.

¿Cómo se trabaja con inteligencia?

Con la DNIEM hay cooperación por el manejo de la información. Además, inteligencia está involucrada concretamente en el proyecto. Pero, al tener requerimiento técnico se vuelve de carácter secreto.

Inteligencia se viene involucrando más en ciberdefensa recién ahora. Participa del Comité Tripartito.

¿Quién se encarga de la seguridad de la información del MINDEF?

Hay una dirección de informática que es la encarga de la seguridad de la información. Trabaja paralelamente a la Subsecretaría, lo cual carece de sentido. Se encuentra por fuera del sistema de ciberdefensa.

En el proyecto está contemplado trabajar más de cerca con esa dirección.

¿Cuál es el futuro de UNASUR?

UNASUR fue descartado por completo. Hace rato que los militares se dieron cuenta que la visión del gobierno actual no encajaba con lo que plantea el UNASUR, más la posición asumida ante el gobierno de Maduro. Es por eso que se pretende revitalizar y poner todos los esfuerzos en el Foro Iberoamericano.

¿Y el proyecto sobre fibra óptica? La verdad es que en UNASUR había un grupo de trabajo sobre defensa cibernética, pero los proyectos nunca llegaron a concluirse. Lo de fibra óptica quedó en el aire.

¿La influencia norteamericana en el sistema de ciberdefensa es del gobierno actual o viene de antes?

Viene desde antes. Más en cuestiones de ciberdefensa. Estamos trabajando mucho con lo que hace EUA.

Quería conocer tu opinión sobre el estado de la ciberseguridad en Argentina, las funciones de las FFSS y si hubo continuidad o cambio con el nuevo gobierno.

A partir de 2016 se dio mayor impulso a las cuestiones de ciberdelito. Se empezó a capacitar a las fuerzas de seguridad, brindando más herramientas.

Se creó el Instituto Conjunto en el que participan las cuatro fuerzas federales y se las capacita en ciberdelito. Lo bueno es que las fuerzas provinciales también participan del instituto y no se acota a las FF nacionales.

El ICSE tiene un efecto derrame sobre las fuerzas. Todo lo que hace es de carácter académico, las investigaciones, el desarrollo de laboratorios, etc.

El delito está cada vez más profesionalizados y es más fácil de cometer.

Hubo un cambio de paradigma, dado que el delito ya no se encuentra acotado al territorio nacional. Es posible ver que un atacante tiene un IP de Rumania por ejemplo, lo cual lo vuelve más complejo, es necesario capacitar a las FFSS para que entiendan que tipo de herramientas utiliza el atacante y porque el IP u otros datos figuran fuera del territorio.

Argentina, si bien participó desde los inicios de los Convenios de Budapest, recién ahora se convirtió en parte del Convenio. Este Convenio sirve para la integración y la colaboración con otros países, aunque todavía es incipiente.

¿Cómo afecta a las FFSS el convenio?

El convenio afecta más a lo judicial, sirve para la cooperación en investigaciones judiciales. Deberías hablar con gente de justicia.

¿Las FFSS cooperan internacionalmente?

Si, a partir de la creación del instituto se están organizando distintos seminarios que tienen el objetivo de capacitar a las fuerzas. Por ejemplo, a principio de año se realizó uno con Reino Unido. En breve comienza otro, pero todavía no es de público conocimiento. En la página del MINSEG se da aviso de estos cursos.

¿Cómo influyó el cambio de gobierno en cuestiones de ciberseguridad?

Hay otro enfoque con el cambio de gobierno. El ciberdelito tomó gran relevancia.

Por ejemplo, la ENI en conjunto con la UCA también lanzó una maestría en ciberdefensa, en la que el director es Uzal.

¿Cuál cree que es el sector más vulnerable?

Creo que las vulnerabilidades no discriminan por sector. Lo que pasa es que el sector privado ve a estas cuestiones como un gasto y no como una inversión. Recién cuando les ocurre un ataque empiezan a invertir, eso sí, no suelen denunciarlos.

Si te fijas en la página zone-h.org hace poco hackearon un dominio y terminaron cayendo varios. Tuvo efecto derrame, pasó hace un par de semanas. Hubo varios municipios afectados. El CERT de Banelco es muy interesante.

¿Que se hizo desde el gobierno nacional?

Se creó el Ministerio de Modernización y lo que antes era el Programa ICIC que estaba bajo la órbita de la ONTI pasó a estar en esa dependencia. Además, de avanzar con el programa se encarga de proveer recursos.

¿Las FFSS trabajan en conjunto con los CERT gubernamentales?

Las FFSS tienen su propio CSIRT que tiene la finalidad de establecer un sistema de alerta temprana. Es importante porque participan las cuatro fuerzas. Se creó el 12 de octubre de 2017, el dominio es csirt.minseg.gob.ar, fue creado por la resolución ministerial n° 1107.

También se creó la Dirección General de Ciberseguridad.

¿Hay alguna estrategia de ciberseguridad del ministerio?

Si. Justamente la Dirección de Ciberseguridad se encarga de establecer objetivos, metas, estrategias y todo lo relacionado con al ciberseguridad.

¿Dentro del IUPFA hay investigación de ciberseguridad?

Si, cada vez más. Es un tema que antes no atraía a las personas pero que hoy en día tienen cada vez más adeptos. De hecho hace poco me presentaron un proyecto para ser desarrollado a lo largo del año que viene.

En general son investigaciones académicas sobre el ciberdelito.

¿Existe una especialización por parte de las FFSS sobre los distintos tipos de delitos cibernéticos?

Si, por ejemplo la policía federal es especialista en cibercrimen, otra en grooming y así.

¿Cómo se desarrolla la formación de las FFSS?

Hace poco se lanzó el Programa de alto desempeño operativo. Si buscas, vas a encontrar porque salió en los medios.

Además existe una formación continua. Lo importante es hacerles entender cómo funciona la tecnología, brindándoles herramientas para que sean capaces de analizar tendencias y la evolución de todo lo relacionado a los ciberdelitos y a la innovación tecnológica.

Se los entrena también en técnicas de investigación.

¿Y en cuanto a lo forense?

En cuanto a la extracción forense, se los entrenar para que sean capaces de evitar la contaminación de pruebas, ya que es diferente la evidencia digital de la física. En este sentido, por resolución MS 234/2016 se lanzó un Protocolo de Actuación que pone especial énfasis a la capacitación en este sentido.

Además, últimamente se dio mayor impulso a la capacitación de amenazas transnacionales, entre ellas la ciberseguridad.

FUENTE "C" - Ángel Tello - 3 de septiembre de 2018.

Ex Viceministro de Defensa

¿Cómo limitaba el decreto 727/2006 a cuestiones de ciberdefensa? ¿Cómo afecta la creación del decreto 683/2018 y de la nueva DPDN a estas cuestiones?

En cuanto a la ley tengo una visión reduccionista dado que el decreto 727/2006 trata a las amenazas de origen externo sin interpretar la ley. En vez de hacer esto por decreto reglamentario en realidad era necesario modificar la ley.

En cuanto a la definición de agresión, la resolución de ONU al respecto se encuentra en revisión, por lo que este concepto quedaría limitado a lo que establecía taxativamente la resolución que por ser de Asamblea General no es de carácter obligatorio.

Por otra parte, la resolución abre la posibilidad de interpretación del Consejo de Seguridad, por lo que podría abarcar un espectro muy grande según los intereses de los miembros permanentes del CS de ONU.

En cuanto al nuevo decreto, hace una lectura amplia en cuanto a la magnitud y el origen de las amenazas. Mi crítica personal es que amplía las funciones de las Fuerzas Armadas al punto de que deja abierta la posibilidad de que están actúen en cuestiones de seguridad interior, lo cual no estoy de acuerdo.

Respecto a la nueva DPDN, introduce conceptos importantes, es un poco más completa. Habla de incertidumbre, por lo que estoy más en línea con lo que establece.

¿Le parece que introduce la necesidad de desarrollar capacidades en el ciberespacio?

En realidad eso es una mentira, porque en Argentina tenemos planeamiento por capacidades, lo cual pone un límite a las agresiones. El planeamiento por capacidades pretende definir el para qué.

En Argentina hay una negación de las hipótesis de conflicto, por ejemplo con Reino Unido. Se puede no decir públicamente de las hipótesis de conflicto pero es necesario que Argentina reconozca que tiene enemigos para poder desarrollar Fuerzas Armadas de acuerdo a las amenazas reales.

Pero más allá de todo esto, en nuestro país existe otro límite que es económico-financiero y las misiones propias de las FFAA.

¿Cómo actúa el Comando Conjunto de Ciberdefensa?

No llegué a visitarlo en mi paso por el Ministerio de Defensa. Pero cuenta con un sistema de alerta temprana. Depende del EMCO y tengo entendido que estaba muy bien puesto en Puerto Madero.

¿Cómo actúa el sistema de inteligencia en cuestiones de ciberseguridad?

Inteligencia tiene la tarea de realizar análisis y diagnósticos.

Antes en la guerra era de vital importancia el rol de los ingenieros, porque eran quienes se encargaban de desarrollar sistemas de armas, caminos, etc. Hoy esto cambió, además de ser el factor tecnológico (hardware) central para la guerra, los analistas de ciencias sociales, quienes se encargar de interpretar y asesorar, juegan hoy un rol central.

Es por esto que es de vital importancia el rol de inteligencia.

¿Y en cuanto a inteligencia dentro del MINDEF?

La DNIEM es muy limitada en cuanto al análisis. Además es limitada la relación con la AFI, se ocultan información. Pero esto sucede en todos los servicios de inteligencia alrededor del mundo dado que el manejo de información equivale a poder.

El sistema de inteligencia está compuesto por AFI, las Direcciones de ambos ministerios pero también cada fuerza de seguridad y armada cuenta con su propio sector de inteligencia.

Además, tanto el sector económico como el privado realizan inteligencia. Inteligencia comercial, financiera, etc. Es por eso que es difícil creer que la dirigencia política se haya desayunado la corrida cambiaria.

Durante el gobierno de Alfonsín, se había creado una instancia donde se hacían reuniones periódicas de la SIDE. En ella se exponían los informes de inteligencia de cada agencia/dirección, lo cual era mucho más satisfactorio porque se compartía la información.

En el caso de Francia, es interesante el Palacio de Versalles. Este Palacio cuenta con una habitación muy reducida en tamaño a la cual asistían los agentes de inteligencia para comentarle las novedades directamente al Rey. Esto no se delegaba como se hace ahora, por el valor de la información.

Hoy en día hay un problema. Las cosas no funcionan porque de gobierno a gobierno se elimina lo que hizo el anterior y se hacen cosas nuevas. Se elimina todo sin antes analizar si se lo puede hacer funcionar o no. Entonces, cuando las cosas nuevas no funcionan se las elimina y se intenta reemplazarlas. No hay continuidad. No hay control de nada.

¿Que hizo el Ministerio de Modernización en cuestiones de ciberseguridad?

Modernización lanzó una digitalización extrema. Un día llegaron al MINDEF y plantearon que todo tenía que ser digitalizado. Me pareció bien pero llega un momento en que absolutamente todo le llega a todos. Me opuse a que los documentos reservados sean digitalizados y me escucharon, por lo cual esos documentos continuaron estando en papel. Aunque así y todo resulta difícil que eso no se filtre. Es imposible que esto no suceda. Había un integrante de las FFAA que hacía referencia a esto diciendo que los documentos estaban seguros, que nadie fuera de América Latina se enteraría del contenido de ellos.

Otra cosa que hizo el Ministerio de Modernización fue la identificación por huella digital. Es bueno hasta que el personal asienta la huella al ingresar y al terminar la jornada, lo cual no asegura que durante todas esas horas el personal se encuentre en sus puestos de trabajo o dentro del Ministerio. Muchos asientan la huella, se van y vuelven casi a la hora de irse a casa.

¿Cómo afectan las medidas actuales? El hecho de que el Ministerio de Modernización deja de tener la jerarquía de Ministerio para pasar a ser una secretaría.

Hay que ver bien que es lo que se pretende hacer. De qué ministerio va a depender y si las funciones van a seguir estando bajo su órbita. Es muy reciente como para analizarlo ahora.

También es posible que Macri tenga que cambiar la ley de ministerios.

Sería lógico que el Comité de Ciberseguridad pase a estar comprendido por Jefatura de Gabinete.

¿A quién le compra armas y sistemas de inteligencia Argentina?

En general Argentina no compra armas. El presupuesto de defensa se compone en su gran mayoría por gastos de personal (sueldos, retiros, etc), lo cual deja poco margen de maniobra para adquisiciones.

En cuanto a inteligencia, es principal socio comercial es Israel.

En materia de defensa, lo poco que se compró en estos últimos años fueron los superestandar. Se compraron 5 con biónica de última generación más un simulador y repuestos que permiten reacondicionar otros cinco aviones, por lo que pasaríamos a tener 10 aviones de este estilo por un precio total de 12 millones de dólares, lo cual parece ser un regalo por parte de Francia.

También se estaba analizando comprar vehículos tipo Hammer a Estados Unidos y blindados.

En cuestiones cibernéticas se le compra a Israel.

Si te interesa el tema de armas hay un buen artículo que salió hoy en la Nación sobre los misiles supersónicos de China y la capacidad armamentística que está adquiriendo.

En cuestiones de ciberdefensa hay casos muy importantes, más allá del típico ejemplo de Stuxnet y las centrales nucleares de Irán.

Uno fue durante la guerra del Golfo, donde Estados Unidos logró cegar a Irak y literalmente los masacró. Lo cual no era necesario.

El segundo, en Mar del Plata. La cumbre a la que vino Bush. Mientras el avión presidencial de los Estados Unidos aterrizaba se cortaron todas las comunicaciones y fueron rehabilitadas una vez que el avión se encontraba en suelo argentino. Para esto, un portaaviones norteamericano estaba encallado en puerto y fue quien dirigió estos cortes.

¿Cómo se está desarrollando la Estrategia Nacional de Ciberseguridad?

Empezó con un proyecto muy ambicioso, muy detallista y se dieron cuenta de que no se podía seguir esos pasos por lo que ahora se está trabajando en conjunto con la OEA y sus recomendaciones.

El Comité cuenta con cinco Subcomités que fueron creados para elaborar planes específicos. En el caso del Ministerio de Seguridad, se está desarrollando un plan de lucha contra el ciberdelito para ser aplicado entre 2018 y 2020.

Se refiere específicamente en una política de ciberpatrullaje, la idea es hacer inteligencia de fuentes abiertas, de foros públicos y quitar el rótulo de inteligencia dado que choca con la percepción de la sociedad y la opinión pública.

La idea es que este protocolo no sea ciberinteligencia propiamente dicha.

Otro Subcomité está definiendo las IC, entre las que se encuentra ARSAT que actualmente está muy valuado a nivel político.

¿Cuáles son las capacidades adquiridas por el Ministerio de Seguridad?

El Ministerio cuenta con un SOC y un CSIRT que funcionan las 24 horas. El CSIRT está compuesto por las cuatro Fuerzas de Seguridad.

Esto va acompañado de campañas de concientización y cursos, entre ellos de e-learning que son abiertos a todo público, cursos específicos de programadores en lo que se trabaja con el ranking de vulnerabilidades de OWASP que visualiza los errores más comunes.

El CSIRT, por su parte, tiene funciones de seguridad informática y respuestas a incidentes. El SOC trabaja en la detección de amenazas.

El SOC sería un nivel 3 y el CSIRT un nivel 1.

¿Existe una especialización de las fuerzas de seguridad en cibercrimen?

Si. En general la Policía Federal se está haciendo cargo del ciberdelito exclusivamente en la web. Además se encarga de detectar todo lo relacionado a tenencia y distribución de pornografía infantil.

La PSA se especializa en forense informática y Gendarmería en investigación en el contexto de las causas.

Además, existe la opción de armas grupos por necesidad, es decir, según el caso. Se puede trabajar en conjunto con personal de las distintas fuerzas que estén capacitados en criptografía, forense, etc.

¿Existen tareas de concientización en temas de ciberseguridad desde la Dirección?

Si. De hecho estamos trabajando en eso. Hace poquito lanzamos un phishing para ver cómo reaccionan los usuarios. Es impresionante la cantidad de gente que fue víctima de esto. El paso siguiente es ponernos en contacto con esas personas para que tomen conciencia.

¿Con qué países se coopera internacionalmente?

Con varios países, diez aproximadamente. Entre ellos: Estados Unidos, Corea del Sur, España, Israel, Colombia, Brasil, China, Chile y estamos en tratativas con Japón.

En lo que es compra de material ¿el principal socio comercial es Israel?

Podríamos decir que sí, pero lo cierto es que todavía no compramos nada.

¿Cuál es el rol del Ministerio de Seguridad en la Cumbre del G20 en cuestiones de ciberseguridad?

En el G20 lo único que va a hacer el Ministerio en cuestiones de ciberseguridad son tareas de pentesting.

El Ministerio de Modernización va a ser el encargado de llevar a cabo el monitoreo.

¿Se desarrollan ejercicios conjuntos en cuestiones de ciberseguridad?

Todavía no, pero está contemplado que en algún momento se empiecen a realizar.

¿Crees que el gobierno actual tiene especial interés por la ciberseguridad? ¿Se dio mayor impulso a estas cuestiones? ¿Quién se encargaba de la ciberseguridad antes de que se cree la Dirección Nacional de Investigaciones de ciberdelito?

La Dirección es todavía muy nueva, fue creada en marzo. Anteriormente yo trabajaba algo en la PSA.

Es una temática de carácter estratégico para el gobierno pero no estoy seguro de que sea prioritaria. Si en 2016 se difundió los 100 objetivos prioritario del gobierno y la ciberseguridad estaba en esa lista, pero en el puesto número 74, lo que puede ser leído como que hay 73 prioridades antes o que compone los proyectos estratégicos del actual gobierno sin ocupar necesariamente el lugar número 74 porque todos los objetivos son igualmente importantes.

Hay que tener en cuenta también que el Ministerio de Seguridad fue mutando a lo largo del tiempo. Como entidad es relativamente nueva. Antes estaba con Justicia.

¿Se trabaja en conjunto con la DNICRI? ¿Quién se encarga de la seguridad de la información?

Si, se trabaja en conjunto. La DNICRI tiene una mesa de ciberseguridad. Si bien nosotros nos encargamos de detectar los incidentes en el ciberespacio, la Dirección de Inteligencia también, aunque utilizan distintos métodos, herramientas y tienen acceso a cuestiones que no son de carácter pública como lo que utilizamos nosotros. Lo cierto es que no estoy al tanto de cómo trabaja.

A veces nos llegan informes de inteligencia que nos muestran cosas que a nosotros se nos pasa por trabajar únicamente con fuentes abiertas, pero no sé qué hacen para conseguirlas.

¿Cómo afectó el Convenio de Budapest a la Dirección?

Budapest incentiva la cooperación internacional. Nació por el problema que supone la pornografía infantil.

El Convenio convoca a establecer una red 24/7 de detección, alerta, búsqueda de prófugos, etc. Además de comprometer a los Estados a legislar sobre ciberdelito.

El Convenio nos obliga a trabajar para poder participar de forma responsable en esa red y lo que es investigaciones penales.

¿Cuáles son los principales ejes en los que se forma a los profesionales de la Dirección?

Se los forma en métodos de investigación e inteligencia. Actualmente hay un curso que se está haciendo con Corea del Sur y otro con Estados Unidos.

Además se trabaja mucho con la OEA.

¿Cuáles son los ejes de trabajo conjunto con la OEA?

Actualmente estamos ejerciendo la presidencia del CICTE que si bien es el Comité Antiterrorismo, es quien impulsa las buenas prácticas y la elaboración de Estrategias Nacionales de Ciberseguridad en los países americanos.

Además de desarrollar foros y capacitaciones donde se intercambian indicadores de compromiso. En este sentido se trabaja con el SOC.

¿Cuáles son los antecedentes de la ciberseguridad que se desarrollaron durante el gobierno de Cristina?

El Programa ICIC principalmente que establecía un programa de buenas prácticas. Se hacía cargo de todo lo relacionado con la ciberseguridad y la implementación de la ISO 27.001.

Por otra parte, no había coordinación, es algo que recién ahora está en proceso de implementación.

Dentro de seguridad, quien tenía algo de responsabilidad en el tema era la Dirección de Crimen Organizado.

FUENTE "E" - Entrevista reservada - 13 de septiembre de 2018

Comité de Ciberseguridad

¿Cuáles fueron los cambios en las políticas para la ciberseguridad con el cambio de gobierno?

Con el gobierno anterior la discusión era a nivel táctico / operativo. No existía una buena concepción. Hoy hay más desarrollo sobre cibercrimen.

Antes se atacaba sectorialmente la cuestión, sin noción de tiempo ni dimensión. Los principales cambios se aprecian en que actualmente existe un orden, mayor conciencia, una estrategia, un organismo coordinador, mayor diálogo y una integración sistémica.

¿A qué se debe que se ataque sectorialmente la cuestión?

Cabe destacar que todos los países comienzan atacando sectorialmente en el ámbito cibernético. Incluso la NSA en Estados Unidos comenzó de esta forma.

Hay que reconocer que existe un incentivo negativo a la hora de invertir en estas cuestiones. Sin ciberseguridad no hay seguridad de la información. En Argentina, aproximadamente el 2% del PBI proviene del sector tecnológico. Además, estamos menos conectados que Chile (porcentualmente).

Por lo general el sector privado invierte más en estas cuestiones que el Estado.

En lo virtual existe algo similar al contrato social. Entre en juego las obligaciones del Estado para con la seguridad de los usuarios, la libertad y derechos de éstos últimos.

El Financial Times reportaba acerca del costo económico mundial del cibercrimen.

Volviendo a la pregunta anterior, hay que destacar algunas políticas implementadas por el anterior gobierno para la interconectividad en Argentina. Tal es el caso de TDA (televisión digital abierta), la ley de datos personales, ARSAT (con la propagación de fibras ópticas) que significan una digitalización del Estado. Si bien esto fue iniciativa del gobierno anterior, estas políticas tuvieron continuidad de forma más ordenada.

En cuanto a la ENCS, ¿Cuáles son las agencias de gobierno que participan del Comité más allá de los expuestos en la Resolución 577/2017?

Actualmente participan Jefatura de Gabinete de Ministros y los Ministerios de Relaciones Exteriores y Culto y Justicia y Derechos Humanos.

¿El Ministerio de Educación no participa del Comité?

Todavía no. Seguramente será invitado a participar más adelante, una vez que la Estrategia esté desarrollada y tenga que ser aplicada.

El Ministerio de Educación puede cumplir la tarea fundamental en cuestiones de concientización a la población sobre los usos de las TIC's.

¿Con qué frecuencia se reúne el Comité y cuando se planea hacer oficial la Estrategia?

Se reúne con gran frecuencia. Cabe destacar que el equipo que participa del Comité está haciendo un gran esfuerzo y trabajo para definir la ENCS.

Por otra parte, se planea que se haga oficial en noviembre, antes de la Cumbre de Presidentes del G-20.

¿Cómo se trabaja en conjunto con la OEA?

La OEA proporciona capacitación principalmente. A lo largo de todo el año se desarrollaron distintas capacitaciones en las que participó la OEA. Si te fijas en internet las acciones de Cancillería con la OEA, seguro aparecen las capacitaciones de ciberseguridad. Esto se desarrolló en el marco del Comité.

El CICTE proporciona expertise, ya que ayudo a desarrollar otras Estrategias en la región.

Sin lugar a dudas, es una estrategia pensada en términos nacionales mirando a la región.

Las estrategias de Chile, Colombia y Paraguay son un ejemplo de estrategias que fueron desarrolladas con recomendaciones de la OEA. Todas ellas sirven de modelo para la nuestra.

¿Cómo afecta la reciente modificación de la estructura del Estado al funcionamiento del Comité, dado que el Ministerio de Modernización deja de tener ese rango para ser una secretaría de Jefatura de Gabinete de Ministros?

En cuestiones operativas no cambia en nada. Modernización seguirá a la cabeza del proyecto y del Comité.

FUENTE "F" - Entrevista reservada - 18 de septiembre de 2018.

Ex Directora Nacional de Inteligencia Estratégica Militar

¿Cómo surge la cuestión de ciberdefensa y ciberseguridad en Argentina? ¿Cuál fue el rol de la DINIEM en este proceso?

Se origina con la ONTI que intentó concentrar todo lo relacionado con la ciberseguridad. Por su parte, las Fuerzas Armadas comenzaron antes. Lo hicieron cada una por separada.

Como las cuestiones de ciberseguridad requieren de la participación necesaria del sector privado, es muy difícil que inteligencia lleve a cabo el desarrollo de esta temática.

Mientras estuve en la DINIEM, empezamos a impulsar que se haga algo en el MINDEF, específicamente dentro del EMCO, pero no logramos nada, recién en 2014, mientras Jerónimo Morales Rins estaba a cargo de la Dirección, surge el Comando Conjunto de Ciberdefensa en el EMCO.

Por su parte, cada fuerza había avanzado en el desarrollo de la ciberdefensa, el Ejército era el más avanzado en estas cuestiones. Debe ser por ese motivo que hoy es quien está a cargo del Comando, por la experiencia que posee.

En cuanto a la ONTI, siempre fue incipiente, no lograba articular.

¿Las FFAA han desarrollado sus propias capacidades en ciberdefensa?

Si. Cada fuerza lo fue desarrollando en distintas áreas.

En Argentina tenemos el problema que a nivel tecnológico siempre estamos desactualizados, especialmente en nuestro sistema de defensa, ya que la Defensa hace años que se encuentra relegada.

Cuando se comenzó a desarrollar la cuestión, las capacidades no estaban estructuradas ni articuladas, cada fuerza contaba con capacidades aisladas. No estoy al tanto de la evolución de este tema desde que me fui de la Dirección.

Dentro de la DINIEM ¿qué se debatía respecto a la ciberdefensa?

Principalmente definiciones. El debate se concentró más en lo conceptual, porque dependiendo de esa definición se iba a poder decidir quién se tenía que hacer cargo de qué, cuales iban a ser las funciones de la defensa en el ciberespacio.

Hay un artículo escrito por Hugo Miguel en DEF sobre este tema.

¿La DINIEM trabaja en conjunto con la DNICRI en estos temas?

No. Si bien el límite de ciberseguridad y ciberdefensa es difícil y deberían cooperar, no se hace por una cuestión legal. La DINIEM tiene prohibido hacer inteligencia interna, por eso no puede trabajar en conjunto con la DINICRI. Esto no supera el hecho de que no existe un límite claro entre ciberseguridad y ciberdefensa.

Por su parte, la DINIEM no tiene un organismo vinculado a lo ciber, por lo menos no cuando yo estuve.

¿En qué se concentraron los esfuerzos del gobierno?

Los principales esfuerzos por parte de ambos gobiernos en cuanto al fenómeno cibernético se concentraron en la protección, en el desarrollo de capacidades defensivas, no ofensivas. La ciberinteligencia, por su parte, requiere de lineamientos específicos, de requerimientos que permitan desarrollar acciones de ciberinteligencia.

Para desarrollar tareas de ciberinteligencia tiene que estar claro el interés del Estado. En mi paso por la DINIEM, ese interés no estaba.

Es necesario distinguir que la ciberinteligencia no es el uso de herramientas digitales e informáticas en el ciclo de inteligencia, sino que es desarrollar las tareas propias de inteligencia en el ámbito del ciberespacio. Se relaciona con el espionaje y la protección de datos.

En inteligencia se utilizan muchas fuentes abiertas, hay poca información clasificada. La información se contrarresta con información proveniente de embajadas, organismos oficiales y funcionarios.

En 2012 no había requerimientos específicos del área cibernética.

En cuanto a la capacidad de incursión es necesario identificar hasta donde llega esa capacidad. En materia de ciberseguridad es más fácil porque hace referencia a la protección de sistemas y datos, pero como herramienta no queda claro el límite.

Por otra parte, para hacer inteligencia en el ciberespacio se requiere de profesionales formados, lo cual es difícil de conseguir ya que no es seguro de que existan y, fundamentalmente, que estén interesados en trabajar para el gobierno. En inteligencia

se requiere de lealtad, lo cual supone otro problema. Es complicada la articulación con el sector privado. Por lo general, muchos recursos humanos, por más vocación que tengan, terminan en manos de privados porque pagan mejor y tienen mejores condiciones de trabajo que con el sector público.

Por su parte, CITEDEF también tiene líneas de investigación en materia de ciberdefensa.

¿La falta de cooperación entre los sectores de inteligencia hace que se dupliquen esfuerzos?

Si. Siempre hay duplicación de esfuerzos.

La falla del sistema de inteligencia radica principalmente en que no queda claro el interés del Estado y en la falta de cooperación entre las distintas agencias del sistema.

A pesar de que SIDE/SI/AFI deben nuclear los esfuerzos de inteligencia, no existe una cooperación real.

¿Cómo fue la evolución de la ciberseguridad y la ciberdefensa en Argentina?

En la DINIEM comenzó por moda, no por necesidad. El tema estaba en boga a nivel internacional por lo que en Argentina se empezó a explorar el tema, no porque haya habido una preocupación real por el tema, no hubo un hecho importante ni conciencia.

Por otra parte, la DINIEM en 2011 tenía los niveles mínimos de seguridad, no estaba instalada en la conciencia de que el recurso humano es el eslabón más débil en la cadena de seguridad, por lo que hubo que trabajarlo de a poco.

En cuanto a la evolución del tema ciber en particular, se ve una evolución en lo organizacional y lo discursivo, hoy hay más conciencia de la temática.

Por otra parte, la ciberdefensa claramente tiene una dinámica distinta al cibercrimen. El segundo es más público y afecta directamente a un espectro más amplio de usuarios.

Es notable que hubieron más avances desde 2012 hasta 2017.

¿En qué año inteligencia empieza a trabajar la problemática del ciberespacio? ¿A qué causas responde? ¿Cómo se lo trabaja, desde lo conceptual, el desarrollo de capacidades u otras?

En 2011 no había prácticamente nada, la cuestión cibernética solo representaba una preocupación.

Para el sector de inteligencia había una confusión en cuanto a la responsabilidad que el sistema tenía en el ambiente cibernético.

Por otra parte, las cuestiones informáticas no estaban tan desarrolladas.

No es un tema que la política deje en manos de inteligencia o de las fuerzas. Es una problemática que se discute internacionalmente en foros y es muy difícil (para nuestro país) la participación de inteligencia en este tipo de dinámicas.

Es un problema en el que no basta con proteger los sistemas. En general, el sector privado es más capaz.

¿Cómo ha ido mutando el rol de inteligencia en cuestiones de ciberseguridad y ciberdefensa?

En 2011, por orden del Ministerio, la DINIEM empieza un relevamiento con el objeto de ubicar referentes y coordinar esfuerzos. En este sentido, hubo muchas reuniones que no lograron obtener frutos.

Era necesario darle capacidades a las FFAA que el sector político no estaba dispuesto a darles.

Fue necesario transmitir el problema al político, para lo cual era necesario analizar si estábamos siendo atacados.

Por otra parte, el ataque cibernético sufrido por el MINDEF en 2012/13 vulneró la seguridad de información confidencial, lo cual fue muy preocupante porque sacó a la luz proyectos de investigación y desarrollo, el estado real de las FFAA y de los sistemas de armas, información sobre cada uno de los trabajadores del MINDEF y en área en el que cada uno desempeñaba sus funciones, lo cual es sumamente crítico. Puricelli fue despedido por este incidente.

Rossi, por su parte, mostró una preocupación profunda por la cuestión de la ciberdefensa, aunque no logró entender el rol de esta.

Estuvo a favor de la utilización de open sources (software de código abierto) y el desarrollo propio, posicionándose en contra de las compras a occidentales. A pesar de que todos podemos estar a favor del desarrollo propio y demás, no tenía en cuenta la carencia de recursos con que cuenta la Defensa Nacional.

La dotación de capacidades vino de la mano de financiamiento de proyectos de software libre, sin tener en cuenta la seguridad necesaria., mientras que el Ejército argentino comenzaba con el desarrollo del vehículo zonda.

¿Existe una división tajante de las funciones que posee cada organismo de inteligencia respecto a la Ciberseguridad Nacional? ¿Cuáles son las funciones de cada organismo?

Dado que existe una división tajante entre seguridad y defensa, esto se replica en cuestiones de inteligencia. Por el contrario, el Decreto 683/2018 no pone fin a esta división ni ayuda a las cuestiones de inteligencia, dado que no modifica ni la ley de defensa nacional, ni de seguridad interior, ni de inteligencia nacional.

Por su parte, inteligencia criminal es más activa, mientras que inteligencia militar se encarga principalmente de la protección de datos.

Inteligencia aporta estadísticas, experiencia externa.

Inteligencia debe informar, pero tiene un costo político alto. Existe un vacío en la toma de decisiones, dado que se requiere de la presentación del panorama de la situación, no así el planteo de recomendaciones.

El sistema de inteligencia no es eficiente.

¿La DNIEM tiene una mesa de trabajo o alguna dependencia específica de ciberinteligencia?

Con Rossi, entre 2014 y 2015 se organizó una unidad de análisis dentro de la DINIEM.

¡Existe un solapamiento de funciones entre el EMCO, las FFAA, la DNIEM y el MINDEF?¿Quién se encarga de la seguridad de la información?

Por su parte, las FFAA se encargan de mantener los sistemas protegidos. Los sectores de inteligencia de cada fuerza desarrollan tareas de vigilancia.

Cada organismo se encarga de la protección de datos de cada uno.

En cuanto a la seguridad de la información, las direcciones de informática de cada fuerza y el EMCO son los encargados de mantener seguros estos recursos.

Inteligencia del Ejército bajo la conducción de Milani se encargaba de recopilar y buscar datos, tuvieron mayor desarrollo de capacidades, más presupuesto y recursos humanos disponibles.

En cuanto a las otras fuerzas, el desarrollo de la Fuerzas Aérea fue incipiente respecto a las demás, mientras la armada obtuvo un desarrollo intermedio.

En cuanto al EMCO y la DINIEM, cada una elabora sus planes. Cabe recordar que la ley de inteligencia es bastante restrictiva en este aspecto, es por esto también que existe una duplicación de esfuerzos, porque para la ley la conjuntes en inteligencia está restringida y no existe voluntad para que esto deje de ser así.

¿Cómo se han venido construyendo capacidades dentro de cada fuerza, del Comando Conjunto, en la DNIEM y el MINDEF?

El MINDEF tiene estructura sobre ciberdefensa. El gobierno anterior había pensado al CCCD (dentro del EMCO) para ser ocupado por jóvenes alejados de los centros de poder de las FFAA que sean formados por el Comando para desarrollar tareas de relevamiento.

¿Cómo se desarrolla la formación de estos profesionales?

Por lo general los profesionales de comunicación y seguridad de la información son los que sirven al área de ciberdefensa, pero por lo general esto depende del presupuesto. Dentro de las FFAA existe una discusión constante por temas presupuestarios y conceptuales.

¿La utilización del Manual de Tallin responde a lineamientos políticos?

En realidad no está mal que se utilice este Manual para la formación de agentes cibernéticos. El Manual de Tallin fue fabricado por y para Estados digitales, si bien no estamos a ese nivel, es necesario que en el proceso de formación de nuestros profesionales, estos lo tengan en cuenta y sepan adaptarlo a las necesidades del contexto nacional.

¿Cómo afectó la creación del MINMOD a cuestiones de seguridad de la información y de las TIC's?

Lo cierto es que por un lado las políticas como gobierno abierto son buenas para lograr mejores estándares de transparencia, pero esto no está fiscalizado por el sector de inteligencia, por lo que puede ser preocupante la implementación de estas políticas sin los niveles de seguridad adecuados.

¿El sector de inteligencia trabaja en conjunto con el Comité de Ciberseguridad?

El Comité solicitó esfuerzos por conocer la vulnerabilidad a la que se encuentra expuesta la APN, por tal motivo aumentó el relevamiento de información. El análisis de redes es fundamental para ver el panorama nacional e identificar las puertas de entrada.

Se replanteo el problema.

Hoy en día los sistemas de inteligencia de todo el mundo se enfrentan al problema de las fakenews.

¿Cómo afecta la adhesión al Convenio de Budapest?

Hay que tener en cuenta que justicia hace inteligencia sin una formación en inteligencia. Se encarga de resolver.

El Convenio de Budapest afecta pero no hay que perder de vista las seis reservas que hizo Argentina a la hora de firmar el Convenio. En realidad es algo más emblemático, si no te adherís quedas mal ante la comunidad internacional. ¿Quién está dispuesto a no firmar un convenio para cooperar en materia de procesamiento judicial ante incidentes cibernéticos? ¿Cuál sería el objetivo de hacer esto? Lo veo más bien como una formalidad.

¿Cuáles son los principales objetivos de la Maestría de Ciberseguridad y Ciberdefensa que está desarrollando la ENI con la UBA?

En general existe una delegación del problema cibernético al informático, con esta maestría se intenta contrarrestar esta mentalidad e implantar una visión de las distintas áreas de estudio para que los estudiantes se formen en cuestiones cibernéticas.

La Maestría se inició gracias al Dr. Uzal (oficial del ejército), quien se acercó a la ENI y a la UBA con el plan de estudios. Dado que la ENI ve con buenos ojos acercarse a la comunidad, la maestría hizo de buen incentivo para la formación en materia ciber.

Esta maestría cuenta con un 20% de profesionales provenientes de los ámbitos de seguridad y defensa, mientras que entre el 70 y el 80% provienen de ramas muy variadas, por lo que se aspira a la formación de gerentes, a transmitir el problema a la población en general desde las visiones de cada ciencia sobre el ciberespacio, por lo que la Maestría posee cierta complejidad.

Debe existir una adecuación entre el sector público y el privado. Por lo general, el privado es el que más sabe, el que más invierte y más se capacita. En cambio, el Estado es quien identifica la problemática.

Esta fue una de las primeras iniciativas en cuanto a la formación en Argentina.

Por otra parte, fue Macri quien empezó con la profesionalización de los agentes en materia cibernética y otras amenazas en la ENI, antes no hubo mucho en inteligencia, ya que se encontraba restringida y tenía cierta dependencia ideológica.

La SIDE, por ejemplo, trabajaba para el gobierno de turno.

FUENTE "H" - Entrevista reservada - 3 de octubre de 2018.

Comando Conjunto de Ciberdefensa

¿Cómo se problematiza la cuestión de defensa cibernética en Argentina?

En el 2000 se registró el primer ataque masivo en el ámbito cibernético (no en Argentina). Durante el siglo XXI, el contexto internacional fue aumentando la dependencia de las redes de información, ya que se generó mayo interacción y vínculo, por lo que surgió un nuevo espacio de confrontación.

Tradicionalmente, la defensa era realizada en cuatro espacios conocidos (tierra, mar, aire y espacio exterior), hoy el ciberespacio constituye el quinto ambiente de operaciones.

En Argentina, el CCCD realiza operaciones cibernéticas permanentes y coordina las acciones con los comandos cibernéticos de las Fuerzas Armadas. Además, realiza campañas de concientización para las academias de las FFAA (se concentra en la concientización de los RRHH del sistema de Defensa Nacional).

El CCCD fue creado en mayo de 2014 y depende directamente del EMCO. Desde ahí ha venido desarrollando vínculos alrededor del mundo. En este sentido, el Comando estudia los avances realizados por distintos países alrededor del mundo para analizar sus aspiraciones. En este sentido, se visualizaron los avances realizados por Alemania (tiene una fuerza cibernética dotada de los especialistas del área de comunicaciones e informática de todas las fuerzas, constituyéndose en una fuerza similar a la Aérea, el Ejército y la Armada), Australia, China, Corea del Norte, Corea del Sur, Estados Unidos, Estonia, Francia, Colombia, la OTAN y otros.

A nivel internacional, desde 2015 hasta la actualidad ha desarrollado reuniones bilaterales con Japón, Estados Unidos, España, Italia, Uruguay, Brasil, Israel, Chile, Colombia, Perú y Alemania.

¿Cuáles fueron los principales objetivos de estas reuniones?

El objetivo principal es conocer cómo afrontan las cuestiones de ciberdefensa los otros países.

Además, generar vínculos e intercambio de experiencias en el ambiente cibernético.

En 2016, El Comando de España inició el Foro Iberoamericano de Ciberdefensa. El objetivo fue el de compartir información sobre la organización de la ciberdefensa en cada país y la forma en que cada uno resolvió sus problemas.

Un problema que se reflejó entre todos los participantes fue la carencia de RRHH capacitados en esta temática.

En la reunión del Foro de este año que se desarrolló en Argentina, se adoptó una carta de intención en la cual, los países parte del Foro se comprometieron a desarrollar todos los años una reunión en marzo y un ciberejercicio en octubre.

¿Dónde y cuándo se desarrollará el próximo ciberejercicio?

Está fijado para fin de mes en Madrid.

Además, Portugal se comprometió a elaborar un documento de procedimientos para el Foro, para paliar cuestiones referidas a las invitaciones de las FFAA de cada país al ciberejercicio y a la reunión, las obligaciones del país anfitrión y presidente protémpore del Foro y otras cuestiones.

Por otra parte, Italia pidió adherirse al Foro.

¿Cómo se decide cuáles son las sedes de cada encuentro?

Los países se postulan y el presidente pro témpore (que es el país sede de la reunión por el lapso de un año), a través de comunicaciones informales paralelas, establece el calendario del año siguiente, junto con las sedes para empezar con los preparativos.

Además, Argentina participa de las Ciber Olimpiadas organizadas por Colombia.

Las ciber olimpiadas cuentan con dos etapas. Una online (a distancia) y otra presencial. En la primera etapa de la Olimpiada realizada este año, Argentina logró clasificar para participar de la etapa presencial.

¿Cómo trabaja el Comando con la Subsecretaría?

El Comando trabaja en conjunto con la Subsecretaría de Ciberdefensa, poseen contacto permanente. Por su parte, el CCCD coordina las acciones con las FFAA. Cada fuerza cuenta con una dirección de ciberdefensa.

La Subsecretaría, por ejemplo, fue la encargada de negociar los acuerdos con Rafael para la adquisición de material. El partner nacional de Rafael es la UNLP, quien está encargada de desarrollar la capacitación de RRHH para la utilización del material que se está adquiriendo. Los cursos empezaron a desarrollarse hoy en el Comando.

¿Qué Facultad de la UNLP es la encargada de la capacitación?

No lo sé con exactitud, aunque calculo que la Facultad de Ingeniería.

¿Cómo trabaja en conjunto el CCCD con las FFAA?

Existe dialogo constante entre el Comando y los Centros de Ciberdefensa de cada Fuerza. No hay una relación orgánica, pero todos los días se produce intercambio de información, difusión de eventos y alertas de incidentes.

¿El CCCD desarrolló doctrina para la formación de sus agentes?

Lo que elaboró es un reglamente propio y un manual de procedimientos técnicos que es utilizado por el Comando y las FFAA. Este manual es una guía que da instrucciones al personal sobre cómo actuar ante un incidente cibernético.

¿Se trabaja con el Manual de Tallin?

Si, pero el Manual de Tallin se usa para que el personal conozca cómo afecta el DI (derecho internacional) al ambiente cibernético, aunque ante la inexistencia de acuerdos internacionales sobre este tema, este manual no establece cuestiones obligatorias.

Tallin representa cuestiones políticas y estratégicas, no cuestiones técnicas.

Recordemos que la misión del Comando es la conducción de operaciones cibernéticas para garantizar la seguridad del ciberespacio. El Manual de Tallin se utiliza únicamente para que el personal conozca sobre las implicancias del DI en el ciberespacio.

¿Cómo se estructura el sistema de ciberdefensa nacional?

A la cabeza del sistema de Defensa se encuentra el Presidente de la Nación, seguido por el Ministro de Defensa Nacional. De éste depende, por un largo el EMCO, y por otra parte la estructura propia del Ministerio.

Por debajo del EMCO se encuentra el CCCD (posee un Estado Mayor y un Jefe de EM), quien cuenta con un Centro de Operaciones de Ciberdefensa (COC) y un Centro de Ingeniería de Ciberdefensa (CIC).

Por debajo del Ministerio, se encuentra la Secretaría de Ciberdefensa, quien cuenta con contactos permanentes con el CCCD.

Por su parte, el COC se encarga de desarrollar actividades operacionales (es un SOC), mientras que el CIC se encarga de tareas de forense. Ambos centros son aún incipientes. Recordemos que esta estructura fue creada hace apenas cuatro años.

El Estado Mayor del CCCD cuenta con la conducción de las operaciones de ciberdefensa, además de contar con tareas exclusivamente administrativas.

El COC es de respuesta inmediata, mientras que el CIC brinda apoyo de ingeniería y gestión del conocimiento de las TICs.

¿Cuál es el presupuesto con el que cuenta el Comando para la compra de equipamiento?

El tema del presupuesto y la compra de insumos son provista por el Ministerio de Defensa. Lo que son las soluciones tecnológicas y la compra a Rafael del ISOC y el CSIRT vienen de ahí.

El equipamiento actual fue provisto por el MINDEF al momento de la creación del Comando. Desde el amueblamiento hasta el software y hardware.

En 2014, el Comando realizaba tareas de planeamiento. En 2015 se le otorgó el nuevo predio en el que funciona aún hoy (Puerto Madero), en 2016 se comienza con el entrenamiento del personal y en 2017/18 realiza operaciones cibernéticas.

A futuro se espera contar con una organización importante o una fuerza propia como la desarrollada por Alemania.

La rigidez de las políticas para ingresar al ámbito militar resulta perjudiciales a la hora de contratar personal. Además, las políticas del gobierno de redistribución de los recursos humanos, suponen más limitaciones para encontrar personal.

¿Cómo afecta la nueva DPDN a las funciones del Comando?

Nos sorprendió ver la importancia que le dio la nueva DPDN a cuestiones de ciberdefensa. De hecho, contamos 23 menciones sobre la temática a lo largo de todo el documento, lo que supone un incremento respecto a la DPDN anterior. Ahora bien, como se traducirá esto a los efectos prácticos todavía no lo sabemos. En realidad la DPDN no constituye una norma, sino una visión estratégica.

Hasta ahora, las funciones de Comando son las de coordinar a las FFAA, establecer criterios rectores, generar una doctrina y concientización dentro del sistema de Defensa Nacional.

¿Cómo afecta el Decreto 683/2018?

En realidad para el ámbito de la ciberdefensa no modifica mucho.

¿No cree que al modificarse el concepto de agresión estatal externa por el de agresión externa el sistema de ciberdefensa amplía sus capacidades?

La verdad es que a partir de esa modificación, se amplían sólo algunos márgenes, se da la posibilidad de desarrollar operaciones ofensivas, si, pero actualmente las funciones del Comando continúan siendo las mismas que antes.

Aunque por otra parte, se llamó al Comando a participar de los JJOO de la juventud. Todavía no le asignaron el rol al personal que participará de los JJOO. Recibirán capacitación.

¿Cuáles serán las funciones del Comando en la Cumbre del G-20?

En realidad la mayor responsabilidad del operativo de seguridad recaerá sobre el Ministerio de Seguridad. En cuanto al ámbito cibernético, el CCCD se encargará de tareas de comando aeroespacial y redes.

¿Existe cooperación con la academia y el sector privado?

Con la academia dependiente de las Fuerzas sí. Hace poco la CONEAU nos aprobó un plan de formación para capacitar RRHH provenientes de las FFAA.

Respecto al sector privado, no. Sólo existe vinculación con algunas empresas que nos quieren vender soluciones tecnológicas. La verdad es que nos reunimos con ellas y vemos que es lo que tienen para ofrecer pero no tenemos capacidad de tomar esas decisiones.

¿Realizan tareas de investigación y desarrollo dentro del Comando?

Si. De hecho el COC desarrolló un simulador de ciberdefensa. Existe la necesidad de desarrollar tecnología dentro del ámbito militar.

¿Cuántas son las redes que protege el Comando?

Son 4 y requieren del trabajo conjunto entre el Comando y las distintas FFAA, dada su distribución a lo largo de todo el país y que el Comando es relativamente nuevo mientas que las FFAA, sus redes y sistemas de armas son mucho más antiguos, por lo que es necesario adecuar las TIC's.

¿Cuáles son los próximos pasos para la ciberdefensa?

El próximo paso es el polo de ciberdefensa que se está desarrollando en Martelli. La idea es dejar Puerto Madero y que la Subsecretaría, el Comando y los SOC de cada fuerza trabajen en conjunto y en un único espacio físico.

¿Hay fecha para esto?

No. Hoy está en proceso de construcción ese centro y no se sabe cuánto tiempo durarán las obras. No tenemos fecha para salir de Puerto Madero.

Fuente I - Entrevista reservada - 4 de octubre de 2018

Comando Conjunto de Ciberdefensa – COC

¿Cómo opera el COC?

El Centro de Operaciones de Ciberdefensa utiliza open sources, es decir, trabaja con osint y tiene por objeto analizar la correlación de eventos. Para esto, trabaja con un playbook a partir del cual las fuentes humanas deben analizar los eventos a partir de una checklist.

Dentro del COC se poseen funciones de primer y sólo algunas de segundo nivel. En cuanto al primer nivel, su rol es defensivo y de detección. En cuanto a las funciones de segundo nivel, se cruzan datos para ver si el riesgo es real y analizar el nivel del riesgo. A partir de ello se decide si se trata de un evento o un incidente y, en caso de ser un incidente, se comparten alertas a las FFAA. Por lo general, existen alertas diarias.

El CIC es el encargado de realizar el resto de las funciones de segundo nivel. Entre estas funciones se encuentran el análisis técnico, forensia y resiliencia.

El nivel tres, por su parte, es el que debe encargarse de detectar el origen del ataque, es decir, su atribución. La Subsecretaría de Ciberdefensa es la encargada del nivel tres.

En este sentido, para el Manual de Tallin, los ciberataques son considerados de forma similar a un acto de guerra.

¿Cómo funciona el simulador?

El simulador es de desarrollo propio y lo que busca es replicar los hechos para así poder obtener respuestas.

Es similar a los simuladores que se utilizan en los ejercicios combinados. Un ejemplo de ello es el que proporcionará INDRA en el ciberejercicio que se desarrollará en España a fin de mes. Lo mismo pasa en las ciberolimpiadas.

En el ciberejercicio de Brasil del año pasado, por ejemplo, el simulador no funcionó todo el tiempo. Esto puede pasar por distintos motivos, desde fallas técnicas a saturación por la cantidad de usuarios, etc.

Al haber desarrollado nuestro propio simulador, nos proporciona cierta ventaja comparativa en cuanto al entrenamiento.

¿Quienes participan de los ciberejercicios que se realizan en el marco del Foro Iberoamericano de Ciberdefensa y de las Ciberolimpiadas de Colombia?

Se forman grupos para que participen de estos eventos. Con respecto al Foro, participan miembros del COC.

En las Ciberolimpiadas, en cambio, participa un grupo compuesto por miembros del COC y del CIC.

¿Qué es lo que intenta proporcionar la nueva tecnología adquirida de Rafael?

El sistema de Rafael busca influir en lo que es la fase de correlación. Al adquirir un ISOC se está adquiriendo Inteligencia Artificial. El proceso de implementación de esta tecnología se hará bajo la supervisión constante de recursos humanos**¿Qué protege el CCCD?**

El Comando tiene por objeto la protección de las IC del Instrumento Militar.

De esta forma, se protegen las redes militares, que por lo general son bastante seguras ya que cuentan con pocos nodos de comunicación. El principal problema es que en algún punto las redes pasan por terceros y no se encuentran bajo el dominio estrictamente militar, por lo que es necesario proteger las entradas a dichas redes.

¿Cómo se relacionan con las FFAA? ¿Realizan ejercicios conjuntos?

Con las fuerzas existe un flujo de información cotidiano. Se trabaja en conjunto con los SOC de cada fuerza. Además, existen alertas diarias.

Además, existen reportes semanales.

Aún no realizamos ejercicios conjuntos pero por el hecho de que estamos trabajando constante y cotidianamente con la realidad.

FUENTE J - Entrevista reservada - 14 de noviembre de 2018

Ex Director General de Ciberdefensa – MINDEF

¿Cuál fue el proceso de creación de la Dirección General de ciberdefensa en el MINDEF?

La creación de la Dirección General de Ciberdefensa en 2015 (DGCD) se creó como instrumento ministerial de control político sobre el creado Comando Conjunto de Ciberdefensa y en reemplazo de la Unidad de Coordinación de Ciberdefensa dirigida por el Jefe de Gabinete de Asesores del Ministerio de Defensa.

La decisión tomada por el Ministro Rossi en 2013 fue jerarquizar y crear elementos de solución para la problemática planteada a nivel internacional con la proliferación de los llamados ataques cibernéticos y por supuesto las FFAA debían formalizar la necesaria generación de la capacidad.

¿Cómo se internacionalizó la cuestión de ciberdefensa?

En 2013 la cooperación internacional cobra mayor fuerza con Rossi, quien en un principio vivita Brasil y se crea la Declaración Conjunta bilateral que da marco a la cooperación bilateral en materia de defensa cibernética.

Por otra parte, en ese entonces existía la Unidad de coordinación, de la que participaba personal proveniente del EMCO (de comunicaciones y jefatura 2 de inteligencia), cuadros civiles y representantes de las FFAA. Por su parte, inteligencia propuso pensar la ciberdefensa de forma transversal para proteger las redes. La unidad de coordinación, por su parte tuvo una visión más amplia en la que prevalecía la prevención y mitigación.

Bajo la conducción de Rossi, se destinó recursos a la DINIEM destinados a la ciberdefensa, estos gastos reservados sirvieron para la compra y puesta en valor del edificio de puerto madero en 2014, donde actualmente funciona lo referido a la ciberdefensa. Además, en 2013 se dio la adhesión al programa ICIC.

Por su parte, de DGCD dependía directamente del Ministerio.

Por otra parte, la internacionalización de la ciberdefensa se dio en el UNASUR. Bajo el paraguas de las reuniones de dicho organismo, Argentina organizó un seminario en 2014.

Además, se desarrollaron acciones con Brasil, Paraguay y Bolivia (principalmente en el área de capacitación y firma de convenios), y acciones bilaterales con España.

En 2016, con el cambio de gobierno, se pierde operatividad, entre otras cosas, por falta de presupuesto. Entre otras cosas, se empieza a negociar G2G para la compra de insumos que finalizaría con la compra a la empresa Rafael Systems en 2018.

En cuanto a la OEA, hasta 2015 la relación fue prácticamente nula. En 2016 empiezan las capacitaciones en este marco. Se hizo efectiva la propuesta de concientizar.

¿Cómo se desarrollaron dichas negociaciones? ¿Hubo proyectos de investigación y desarrollo?

Norberto se empezó a contactar con las embajadas. Se pretendía llevar adelante una compra conjunta con Modernización y Seguridad, aunque esta idea no prosperó.

En 2016 estaba la propuesta de compra y desarrollo propio. Hay que tener en cuenta que el ciclo de vida tecnológico es de cinco años. Un plan de tecnología propia requiere de RRHH capacitados, por lo que primero es necesario invertir en esto.

En cuanto a proyectos de I+D hubieron varios, entre ellos el desarrollo de un sistema operativo Linux para la Defensa.

¿Cuáles fueron los principales puntos/ejes de debate en el proceso de creación de la Dirección? (Funciones, relación con el Comando Conjunto de Ciberdefensa, relación con las FFAA, cuestiones conceptuales, otras)

Las misiones y funciones pueden encontrase en la Decisión Administrativa, pero las más importantes eran la de control funcional del CCCD, la de relación con los demás organismos del estado en materia de Ciberseguridad y la gestión de la Seguridad de la Información. Cabe mencionar que el MINDEF no tenía en ese momento un área de Seguridad Informática absolutamente necesaria en cualquier organización de ese tamaño.

La relación con las FFAA fue siempre muy positiva. Desde un primer momento nos propusimos conducir el proceso desde lo político y se logró. Se pusieron metas ambiciosas como la puesta en valor de un antiguo geriátrico de la ARA en desuso y se lo transformó en el edificio de Ciberdefensa, se lo equipó de tecnología, mobiliario y se instaló allí el nuevo CCCD y la DGCD.

Se acompañó el plan estratégico de desarrollo de la capacidad planteado por el Comando y se procuró compatibilizar y armonizar el trabajo y las relaciones de las tres fuerzas y el EMCO.

La mayor problemática planteada desde lo normativo fue la incapacidad planteada por las fuerzas en el momento de la realización de una forensia para detectar al agresor

en un ciberataque ya que en la mayoría de los casos el origen o salto último se generaba y se genera en infraestructuras locales.

Desde lo conceptual la discusión era referida a la ciberdefensa directa o indirecta, a la capacidad de ataque en definitiva. De todos modos era una discusión que no cambiaba la situación ya que no era del momento. El esfuerzo se centró en madurar la capacidad. Si bien determinados intereses preferían sumar Ciberdefensa a una u otra área de capacidad de las fuerzas la creación del CCCD subsanó buena parte de la discusión.

¿Cuáles fueron las capacidades asignadas a la Dirección en materia tecnológica? ¿Tuvo una partida presupuestaria especial ante su creación?

La DGCD creada en 2015 no tuvo partida presupuestaria propia, no obstante tuvo todos los recursos económicos necesarios para su funcionamiento a partir de la asignación de recursos de áreas concurrentes. En materia tecnológica se sumó presupuesto del EMCO y del MINDEF con el objetivo de la compra del equipamiento necesario para instalar el Centro de Ciberdefensa en Puerto Madero. Si bien era el primer paso, pero fue el suficiente para esa etapa.

¿Cómo operó la Dirección durante el gobierno de Cristina Fernández de Kirchner?

En 2015, la DA 15 conforma la estructura de ciberdefensa. Brinda la capacidad de establecer actividades de concientización y divulgación, investigación y desarrollo y operaciones.

La DGCD operó con mucho apoyo ministerial e interactuando con otros ministerios de manera coordinada. En 2015 se llevaron a cabo acciones en distintas líneas: Capacitación y Concientización, Difusión Territorial, Cooperación Internacional (UNASUR, OTAN), Diseño de Políticas de Seguridad de la Información adhesión a ONTI, Implementación de los primeros procesos de Seguridad en IAF y DNIEM, Instalación del primer CSIRT monitoreando la red del MINDEF, Organización de Seminarios Internacionales, Nacionales, Desarrollo del Sistema Operativo Linux para la Defensa, Diseño de la Maestría en Ciberdefensa, Desarrollo e instalacipon de un laboratorio de Forensia en la Escuela Superior Técnica del EA, Desarrollo de una HoneyPot en el Instituto Universitario Aeronáutico, etc.

En cuanto a actividades de capacitación y concientización se desarrollaron diversos seminarios y charlas en Universidades y empresas con el objeto de concientizar a usuarios y agentes de la APN.

En cuanto a actividades operativas, se desarrollaron operaciones para proteger las redes del Ministerio a través del CSIRT. Por otra parte, se implementó la normativa, entre ellas, la política modelo en el Comité, la DINIEM y el IAF.

En materia de I+D, se brindó recursos al IUA (en cordoba) y a la Escuela Superior Técnica del Ejército. En el primero se desarrolló una red honeypot y en el segundo un laboratorio forense. Además, se impulsó la creación de una Maestría en ciberdefensa que no logró definirse.

¿Cómo se relaciona la Dirección con el CCCD y cuáles son los vínculos que tiene con los sectores de las FFAA especializados en defensa cibernética?

La DGCD si bien no tiene funciones de conducción formal sobre el CCCD y las Direcciones de Ciberdefensa de las FFAA, sí existe una relación funcional y una definición política ministerial sobre las fuerzas. En lo operativo se realizaron reuniones permanentes para la coordinación de acciones entre las fuerzas y para la implementación de los planes que se acordaban entre ellas. Además se hicieron reuniones especiales en Córdoba y Mar del Plata donde se trabajaban tanto temas operativos como de estrategia, donde se reunía a más de 30 miembros de las FFAA.

¿Cuáles fueron los principales cambios en el funcionamiento de dicho órgano con el cambio de gobierno? ¿Sus funciones siguieron siendo las mismas? ¿Hubo algún tipo de inversión anterior a las actuales compras a la empresa Rafael?

La gestión del nuevo gobierno a partir de diciembre de 2015 diseña una nueva estructura creando la Subsecretaría de Ciberdefensa pero dependiendo de la Secretaría de Ciencia, Tecnología y Producción para la Defensa, con dos Direcciones Generales debajo. De esta manera se des jerarquiza el órgano de Ciberdefensa a partir de la dependencia de una secretaría, que además no era la adecuada a las misiones delegadas. Esto conllevó un sinnúmero de problemas, desde funcionales hasta burocráticos.

Durante 2016 no se le asignó presupuesto y en 2017 se le asignaron pesos argentinos ciento ochenta mil.

No hubo ninguna compra en esos dos años y ninguna acción.

En 2017, con la llegada de Aguad, la compra se desarticuló, y concluyo mucho después de lo esperado.

¿Cómo se creó el Comité de Ciberseguridad y cómo es la Estrategia que se está desarrollando?

En 2016, Norberto propuso la creación de un Comité de Ciberseguridad, desde el que se trabajara la compra conjunta de materiales. En 2017 se crearon grupos de trabajo en el marco del Comité (creado a mediados de 2017) entre los que se encontraba el de concientización y capacitación que desarrolló una encuesta a nivel nacional de las necesidades de capacitación.

Del Comité participan nic ar (cancillería), AFI, jefatura de gabinete y a veces comunicaciones.

La estrategia en si es básica. Se la podría comparar con la que se desarrolló en Paraguay.

¿Cuáles fueron los planes de concientización y formación en ciberdefensa de la Dirección? ¿Fueron impulsados por el actual gobierno o se desarrollaron antes? ¿Hacia quienes estaba dirigido (sólo al ámbito militar)? En cuanto a los planes de formación, ¿sólo fue contemplado el sistema educativo de las Fuerzas Armadas y del Ministerio (hoy UNDEF)?

El plan de concientización y capacitación se ejecutó en la gestión anterior, hasta diciembre de 2015 a través de seminarios realizados en distintas ciudades del país donde se coorganizaba con universidades locales y cámaras empresarias. Se invitaba a estudiantes, empleados públicos y público en general. Se daban charlas, tanto civiles como militares lo que generó un muy buen clima de relación entre los miembros de las fuerzas y la ciudadanía, sobre todo en los estudiantes que asistían.

Se propició la concreción de la Maestría de Ciberdefensa armada por la EST y por el IUA. Se realizaron charlas en la UNDEF y capacitaciones especiales para miembros de las FFAA.

A partir de enero de 2016 me hago cargo del área de Capacitación y Concientización de la Subsecretaría, pero lamentablemente fueron muy pocas las charlas internas que pudimos dar. Las demás actividades fueron de planificación pero la falta de presupuesto hizo imposible alguna acción.

En 2017 se creó el Comité Nacional de Ciberseguridad y grupos de trabajo entre los Ministerios de Modernización, Defensa y Seguridad. Nuestro grupo, el de Capacitación y Concientización, tuvo reuniones mensuales en donde se avanzó en el diseño de un plan de formación a partir de una encuesta que realizamos en la APN y se organizaron 4 charlas abiertas a la comunidad sobre la temática.

¿Qué significa la compra de un CERT/CSIRT para la Subsecretaría de Ciberdefensa? ¿Sería la primera vez que cuentan con este tipo de tecnología o representa una modernización de lo ya existente?

Es una modernización de lo ya existente. El EA ya contaba con un CSIRT y el CCCD estaba armando uno con software libre al igual que la anterior DGCD. La definición de utilizar software abierto (Software Libre / Open Source) o no es sí una decisión estratégica. Cabe mencionar que un CSIRT es apenas uno de los elementos que se necesitan para equipar un centro de Ciberdefensa.

En la definición de la estrategia de ciberseguridad que está proyectando el Comité de Ciberseguridad se espera que el MINDEF se encargue, no sólo de proteger las IC del IM, sino también de proteger las IC de la defensa nacional, lo cual estaría en manos de la Subsecretaría. A partir de esto, me gustaría saber ¿cuáles son las funciones operativas que tuvo la Subsecretaría desde sus inicios hasta la actualidad? Es decir, ¿cuenta con un centro de operaciones o sus funciones recaen en el nivel estratégico?

Las funciones principales del elemento político (antes Dirección y ahora Subsecretaría) son de definición de estrategias y de control funcional. No operativas, que siempre se delegaron al instrumento militar. A excepción del comienzo de la DGCD donde se armó un área operativa provisoria ya que el CCCD todavía no estaba operativo.

FUENTE K - Entrevista reservada - 20 de noviembre de 2018.

Dirección Nacional de Inteligencia Criminal

¿Existen mesas de ciberseguridad en las FFSS y en el DINICRI?

Si, cada fuerza está especializada en algún tipo de ciberamenaza.

Por otra parte, dentro del MINSEG, la DINICRI cuenta con un área de sistemas que brinda soporte técnico y algunos trabajos específicos. A partir de 2016 esta mesa tuvo funciones más específicas. Cabe destacar que el área de sistemas es distinta a la mesa de ciberseguridad y, por ende, cumplen distintas funciones. El cambio de gobierno supuso más crecimiento en el área.

¿Cuál es la función de esta mesa de ciberseguridad para el G20?

Principalmente la de ciberpatrullaje.

¿Existe cooperación entre las FFSS y la DINICRI?

Existen reuniones informarles. Las FFSS tienen funciones más operativas que la DINICRI.