Revista ESTRATEGIA

TERCERA ÉPOCA

NÚMERO 6

CENTRO DE ALTOS ESTUDIOS NACIONALES
Colegio de Defensa del Uruguay
República Oriental del Uruguay
2019

Revista ESTRATEGIA

TERCERA ÉPOCA
NÚMERO 6
ISSN 0797-4604

Centro de Altos Estudios Nacionales

República Oriental del Uruguay

2019

La Revista Estrategia es la publicación del Centro de Altos Estudios Nacionales que a modo de instancia de reflexión académica, en un contexto de pluralismo y diversidad de opiniones responsables, ofrece sus páginas a profesionales, investigadores, docentes, estudiantes y público en general, nacionales y extranjeros, vinculados a temas relacionados a los altos intereses Nacionales, la Estrategia suprema de conducción del Estado, la Seguridad y la Defensa Nacional.

Asistente editorial: Claudia Fernández.

Centro de Altos Estudios Nacionales
Víctor Haedo 2020 – C.P. 11.600
Telefax: (598) 2401 8944 – 2401 8385 - 2408

E – mail: calen@mdn.gub.uy
calen.revistaestrategia@mdn.gub.uy

http://www.calen.edu.uy

Montevideo – República Oriental del Uruguay

CONTENIDO

EDITORIAL

En esta edición de la Revista Estrategia presentamos a nuestros lectores a un grupo de especialistas que escriben sobre asuntos de actualidad e históricos, que comprenden un conjunto de artículos relacionados con el eje temático "Infraestructuras críticas y ciberseguridad", establecido para el año 2018, y temas históricos-estratégicos como el pensamiento estratégico del General Artigas que aspiramos resulten de interés y de amena lectura.

En estas páginas se aborda en primer término el tema planteado en el eje temático citado. El artículo de la Magíster en Ciencia Política Rosario Rodríguez plantea, que las infraestructuras consideradas críticas a partir de su valoración estratégica frente a eventuales amenazas que afectan la seguridad de los Estados requieren de una mirada integral, con énfasis en la colaboración interinstitucional de manera que permita su protección. Las alianzas posibles entre el crimen organizado y el terrorismo presentan un nuevo desafío a resolver por los países y exigen estrategias que demanden el apoyo principalmente del sector Defensa así como de otros actores de la sociedad.

Por su parte, el Coronel Magíster Gustavo Vila considera a las Tecnologías de la Información y Comunicaciones como una de las fuerzas más poderosas que se hallan detrás de la evolución de las sociedades contemporáneas. A su vez, los Estados dependen del funcionamiento confiable de sus infraestructuras críticas para el logro de sus Objetivos Nacionales. En la actualidad, las ciberamenazas explotan la complejidad y conectividad de los sistemas de infraestructura crítica, colocándolos en una posición de vulnerabilidad y riesgo. Por lo que entiende, que es necesario un adecuado marco de seguridad en el ciberespacio, a fin de contribuir decisivamente a la seguridad nacional.

La discusión dicotómica de responsabilidades, en las que tareas que son propias de la Defensa Nacional empiezan a ser asignadas a Seguridad Pública, es el tema de la contribución del Coronel Magíster Mario Moreira quien afirma que la protección de Infraestructura crítica o estratégica no escapa a este debate. En su ensayo realiza un análisis normativo y estratégico identificando diferencias, citando una infraestructura crítica relacionada con la ciberseguridad a ser protegida.

Por otro lado, el Ingeniero Enrique Morales plantea la conveniencia de establecer una estrategia energética nacional a largo plazo. Realiza aportes para la elaboración de dicha estrategia según el método CALEN, procurando el logro del desarrollo socio-económico del país como un Objetivo Fundamental. Basándose en los escenarios delineados, señala posibles infraestructuras críticas que puedan ser necesidades estratégicas a futuro.

Desde otra perspectiva, el Oficial de Estado Mayor del Ejército de Chile Alejandro Amigo Tossi, manifiesta que la amenaza digital es uno de los riesgos primordiales para la seguridad de los países desarrollados y en vías de desarrollo. Sostiene que este fenómeno es uno de los retos a la seguridad nacional y uno de los principales desafíos a la protección de organizaciones estatales y privadas en todo el mundo. Por lo tanto, propone los tópicos que podrían incluirse en la apreciación nacional sobre la ciberamenaza a la seguridad nacional de su país y por último, las consideraciones en relación con este peligro incluidas en las Estrategias de Seguridad Nacional de ciertas potencias occidentales.

Finalmente, el Coronel e Ingeniero Militar en Informática Pablo Camps nos plantea que el ciberespacio como quinto dominio de la interacción humana ha dado lugar a la aparición de recientes formas de intimidación creadas por individuos, organizaciones o Estados que buscan aprovecharse esta nueva forma virtual de interactuar. En su artículo, se centra en el grado de seguridad y capacidad de defensa en el ciberespacio de la República Oriental del Uruguay, presentando las nuevas amenazas identificadas por la legislación nacional, detallando las estructuras más importantes encargadas de prevenir o repeler un eventual ataque y por último discutiendo la situación actual del país en cuanto a una estrategia de ciberseguridad.

En segundo término, en este número tratamos temas históricos-estratégicos, como el desarrollado por el Profesor en Historia Daniel Torena quien nos sitúa en el Río de la Plata a comienzos del S XIX, cuando esta región era profundamente disputada por su importancia estratégica y geopolítica, al igual que por sus ricas tierras, por las Grandes Potencias Coloniales de la Gran Bretaña y Portugal, que se la querían arrebatar al Imperio Español. Nos acerca así, a la política anglo-portuguesa instrumentada en tal sentido en la época de la Patria Vieja.

Asimismo, el Coronel Mario Abella nos ilustra sobre el protagonismo que tuvo el General José Artigas junto al Pueblo Oriental, desde el año 1811 hasta 1820, en un período histórico de inexorable valor geopolítico en la región, mojón fundamental para la conformación de nuestro Estado-Nación, la República Oriental del Uruguay.

El debate sobre estos temas es, sin duda, mucho más profundo de lo que aquí conseguimos reflejar. No obstante, ofrecemos estas páginas, cuya lectura deseamos despierte su interés, con la certeza de estar contribuyendo a una discusión necesaria para el presente y futuro de nuestro país.

LA PROTECCIÓN DE INFRAESTRUCTURAS CRÍTICAS COMO UN ASPECTO DE LA SEGURIDAD INTEGRAL DEL ESTADO

María del Rosario Rodríguez Cuitiño[1]

RESUMEN

Los países tienen sectores que se encontrarían en riesgo, si cesaran de funcionar deliberadamente por actos terroristas, acarreando perjuicios para el país y su población. Las infraestructuras consideradas críticas a partir de su valoración estratégica frente a eventuales amenazas que afectan la seguridad de los Estados requieren de una mirada integral, con énfasis en la colaboración interinstitucional de manera que permita su protección. Las alianzas que puedan darse entre el crimen organizado y el terrorismo no deben desdeñarse y presentan un nuevo desafío a resolver por los países y exigen estrategias que requieren el apoyo principalmente del sector Defensa así como de otros actores de la sociedad.

Palabras clave: infraestructuras críticas, crimen organizado, terrorismo, España, Uruguay

Introducción

El presente artículo analiza las infraestructuras críticas atendiendo a su vulnerabilidad frente a eventuales riesgos y amenazas que sufren los Estados y procura explorar en torno a qué herramientas se requieren para su defensa. Para ello, considera el caso de España abordando el desafío del terrorismo internacional y realiza una mirada a Uruguay enfrentando las amenazas de crimen organizado y los actos terroristas, analizando en términos de Seguridad y Defensa Nacional, cuáles han sido las respuestas de estos países en torno a la protección de infraestructuras críticas como un sector estratégico a valorar y al establecimiento de políticas frente a esta problemática a situarse en un primer plano en la agenda pública.

Las sociedades actuales dependen para su funcionamiento de un sistema de servicios que posibilitan la producción y gestión de diversos sectores tanto de instituciones estatales como privadas. Entre ellos se identifican los que son prestados por las infraestructuras críticas,

1 Magíster en Ciencia Política (UDELAR). Docente del CALEN-Colegio de Defensa. Diplomada como Asesora en Defensa (INJUDE), Ministerio de Defensa Nacional. Fue Asesora del Secretario del Consejo de Defensa Nacional y Subdirectora Académica del CALEN. Ha publicado artículos sobre Seguridad y Defensa en Uruguay y en el exterior.

cuyo daño puede aparejar consecuencias negativas sobre la seguridad de las personas y la seguridad estatal, requiriendo estas infraestructuras protección y prevención de sus países, frente a amenazas originadas deliberadamente por el hombre, provocadas por la naturaleza o por una falla técnica.

Qué son las infraestructuras críticas

Para Rodríguez (2016) se trata de estructuras estratégicas denominadas "críticas" porque requieren por su importancia, ser protegidas. Caro Bejarano (2011) busca conceptualizarlas refiriendo a la prestación de servicios básicos imprescindibles que son necesarios proteger porque sin ellos no existe capacidad de subsistencia, al impedir el funcionamiento normal de esos servicios. En este sentido, lo define como:

> cualquier interrupción no deseada, ya sea debida a causas naturales, técnicas, ya sea por ataques deliberados, tendrían graves consecuencias en los flujos de suministros vitales o en el funcionamiento de los servicios esenciales, aparte de ser una fuente de perturbaciones graves en materia de seguridad. (Caro Bejarano, 2011, p.2)

Esta autora distingue entre infraestructuras estratégicas y críticas, lo que contribuye en su comprensión. En este sentido, plantea que infraestructuras estratégicas refieren a aquellos intereses públicos y privados que pueden ser atacados deliberadamente del punto de vista físico o cibernético y sobre los que se encuentran servicios considerados esenciales para la sociedad, "englobando aquellas instalaciones, redes, sistemas y equipos físicos y de tecnología de la información sobre las que descansa el funcionamiento de los servicios esenciales" (Carabias, 2013, p.10). En tanto, infraestructuras críticas son estructuras estratégicas que requieren de un particular resguardo y "cuyo funcionamiento es indispensable y no permite soluciones alternativas, por lo que su perturbación o destrucción tendría un grave impacto sobre los necesarios servicios que prestan a la sociedad" (Carabias, 2013, p.10). Se cataloga como "crítico" el impacto que pueden tener esos ataques en aquellas prestaciones básicas para la sociedad que ponen en peligro la seguridad de sus habitantes y del Estado como tal.

Aunque consideremos que pueden suceder eventos no intencionales que afecten una infraestructura crítica, como ser los puramente accidentales, o los producidos por los desastres naturales, son preocupantes las amenazas para la seguridad, con voluntad de incidir y de pretender imponerse, especialmente atentados terroristas y crimen organizado transnacional, que con sus acciones pueden afectar y poner en peligro determinados servicios prestados a la sociedad. En consecuencia, la valoración de infraestructuras críticas para su protección frente a estas amenazas ocupa actualmente un lugar relevante en la agenda de los gobiernos. Es probable que los países tengan un plan de respuesta ante accidentes, pero es necesario incluir las siguientes interrogantes al pensar en infraestructuras críticas: ¿Sabemos cómo proteger y actuar ante daños intencionales? ¿Qué actores deben intervenir en estas situaciones? Los elementos en que deben enfocarse los Estados y sus organizaciones tienen que ver en: a) Cómo se entiende el valor de la infraestructura crítica y su importancia para considerarla estratégica; b) Qué ámbitos de significancia son los que deben atenderse para proteger infraestructuras; c) Cómo se va a responder a las eventuales amenazas. Las políticas y estrategias deben en primer

lugar, definir cuáles son las infraestructuras críticas y luego en elaborar un plan de acción de respuesta estatal para protegerlas. Fundamentalmente, habrá que atender a reconocer si esos planes de acción se apoyan en un concepto de respuesta integral, coordinando entre las diferentes entidades intervinientes.

Dentro de las infraestructuras críticas se incluyen los servicios energéticos, de transporte y de agua. Se trata de la seguridad física de la infraestructura pero también de "la seguridad de las tecnologías de la información y las comunicaciones" (Caro Bejarano, 2011, p.2). Un ataque cibernético puede "hackear" el sistema informático afectando por ejemplo, redes bancarias y las finanzas del país. Pero el ciberterrorismo puede afectar la seguridad aérea ante un ataque al "software" de aeronaves privadas que impactara deliberadamente en un aeropuerto con pérdidas humanas y materiales. La interdependencia es un elemento clave entre los servicios brindados y la tecnificación, cuya perturbación acarrearía peligrosas consecuencias en la población. Como mencionan Miranzo y del Río (2014) existe una gran dependencia de nuestras sociedades con las infraestructuras críticas, pues cualquier catástrofe sobre ellas, acarrearía graves perjuicios para la seguridad y funcionamiento de los Estados, y el bienestar sanitario y económico de las personas.

Medidas tomadas por España para prevenir y responder frente a riesgos en sus infraestructuras críticas

España es un buen ejemplo en definir respuestas frente al terrorismo internacional, con políticas de seguridad para combatirlo, incluidas las vinculadas a reducir fragilidades en las infraestructuras críticas, a partir de estrategias a nivel mundial y de medidas tomadas en el ámbito europeo. Luego de los atentados del 11S, las acciones tomadas en materia de seguridad dieron lugar al combate contra el terrorismo, constituyéndose en el primordial componente de las estrategias de seguridad y defensa (Aznar, Berenguer, Diez y Laborie, 2013). Es así que surgen varios instrumentos normativos, entre ellos, las Resoluciones del Consejo de Seguridad 1368 (2001) que afirma que todo acto de terrorismo internacional constituyen una amenaza para la paz y la seguridad internacionales, y 1373 (2001) que establece disposiciones sobre el financiamiento del terrorismo. La Estrategia Global de las Naciones Unidas contra el Terrorismo (Asamblea General, 2006) se transforma "en un instrumento único para intensificar las iniciativas nacionales, regionales e internacionales de lucha contra el terrorismo" de manera de sumar los esfuerzos en un enfoque hacia la seguridad cooperativa.

Desde el Consejo Europeo se aprueba el Plan de Acción sobre la Lucha contra el Terrorismo (2001) y la Estrategia Europea de Seguridad - Una Europa segura en un mundo mejor (2003). No obstante, el terrorismo dirige un duro golpe a España en los atentados del 11M en Madrid, lo que llevó a desarrollar mecanismos de prevención ante amenazas y protección de sus habitantes, bienes físicos y cibernéticos. Ese mismo año la Unión Europea resolvió, a través del Consejo Europeo, exhortar a la Comisión Europea y al Alto Representante a confeccionar una estrategia global sobre protección de infraestructuras críticas. En 2004 la Comisión propone al Consejo y al Parlamento Europeo medidas para luchar contra el terrorismo, a través de cuatro comunicaciones, una de ellas sobre "Protección

de las infraestructuras críticas en la lucha contra el terrorismo", que plantea la interconexión existente en las infraestructuras críticas europeas del ámbito público y privado, definiéndolas como:

> aquellas instalaciones, redes, servicios y equipos físicos y de tecnología de la información cuya interrupción o destrucción tendría un impacto mayor en la salud, la seguridad o el bienestar económico de los ciudadanos o en el eficaz funcionamiento de los gobiernos de los Estados miembros (COM/2004/0702 final).

Posteriormente el Consejo Europeo suma en 2005 el Libro Verde sobre un Programa Europeo para la Protección de Infraestructuras Críticas (PEPIC) y la red de información sobre alertas en infraestructuras críticas (CIWIN) como una herramienta de apoyo al PEPIC. El Libro Verde procura proteger las infraestructuras críticas europeas atendiendo a sus efectos transfronterizos mediante la comunicación, coordinación y cooperación entre los Estados miembros, en el ámbito nacional y de la Unión Europea, público y privado. Enfatiza que las infraestructuras críticas comprenden "los recursos físicos, servicios y sistemas de tecnologías de la información, redes y elementos de infraestructura cuya interrupción o destrucción tuviera grave impacto en la salud, la seguridad o el bienestar económico o social" (COM/2005/0576 final), instando a crear listas de infraestructuras críticas por los Estados miembros en su territorio, analizar sus vulnerabilidades, riesgos y presentar soluciones para su protección. En tanto, la red de información es un instrumento de comunicación sobre amenazas y alertas inmediatas, adoptando medidas de seguridad de los Estados miembros y preparando el nivel de respuesta según el nivel de alarma.

La Estrategia de la Unión Europea de Lucha contra el Terrorismo adoptada por el Consejo Europeo (2005) también fue pensada a partir de los atentados terroristas en Madrid. Su compromiso estratégico para brindar una respuesta global al terrorismo frente a atentados físicos y electrónicos, está pensado sobre cuatro pilares: prevenir, proteger, perseguir y responder, actuando a nivel nacional, europeo e internacional. Su fin es proteger la infraestructura crítica europea, debiendo los Estados miembros actualizar sus normas y mecanismos nacionales, mejorando su capacidad de respuesta frente a un atentado, brindando seguridad en las fronteras, transporte y otras infraestructuras fronterizas, dada la gran interdependencia entre éstas.

Una nueva Directiva de la Unión Europea en 2008 sobre la estrategia global contra el terrorismo internacional identifica las infraestructuras críticas europeas (ICE), mejorando la protección de éstas desde el ámbito comunitario, por entenderlo insuficiente desde los Estados miembros, aunque sean éstos y los operadores de ICE quienes tienen la responsabilidad de protegerlas. Se enfoca en los sectores energéticos y de transportes valorando la necesidad de incorporar otros ámbitos como ser tecnologías de la información y comunicaciones. Además, distingue entre infraestructura crítica e infraestructura crítica europea, apreciando el impacto de su incidencia según la interdependencia entre diversos sectores y las infraestructuras. Según esta Directiva:

> se entenderá por "infraestructura crítica", el elemento, sistema o parte de este situado en los Estados miembros que es esencial para el mantenimiento de funciones sociales vitales, la salud, la integridad física, la seguridad, y el bienestar social y económico de la población y cuya perturbación o destrucción afectaría gravemente a un Estado

> miembro al no poder mantener esas funciones; "infraestructura crítica europea" o "ICE", la infraestructura crítica situada en los Estados miembros cuya perturbación o destrucción afectaría gravemente al menos a dos Estados miembros (Directiva del Consejo de la Unión Europea 2008/114/CE).

Finalmente, se destaca en 2013 la creación por la agencia policial de la Unión Europea, Europol, del Centro Europeo de Cibercriminalidad, que asiste a las unidades de cibercrimen de países en su combate contra el crimen organizado transnacional y el terrorismo. Teniendo en cuenta estos antecedentes, España colocó a las infraestructuras en un primer plano, aprobando la Secretaría de Estado de Seguridad en 2007, el Plan Nacional para la Protección de las Infraestructuras Críticas[2], el primer Catálogo Nacional de Infraestructuras Estratégicas, y el Acuerdo sobre Protección de Infraestructuras Críticas. La finalidad del Plan fue proteger las infraestructuras físicas, las tecnologías de la información y las comunicaciones que brindan servicios esenciales a la sociedad, ante amenazas o ataques intencionales, poniendo en marcha las capacidades operativas estatales y la coordinación con operadores críticos. Este Plan fue revisado en 2016[3]. El Catálogo[4] clasificó áreas estratégicas para proteger y prevenir amenazas contra ellas: agua, energía, alimentación, sistema financiero, salud, industria nuclear, tecnologías de la información y las comunicaciones, transporte, administración, espacio, industria química e investigación. Cada uno de estos sectores valora sus infraestructuras críticas, eliminando sus vulnerabilidades mediante un plan estratégico de protección.

Al elaborar su primera Estrategia de Seguridad Nacional (2011), España ubica a los temas de seguridad en primer plano. Para Aznar et al (2013) es el documento de planificación estratégica al más alto nivel político. La Estrategia fue necesaria para analizar riesgos y amenazas para la seguridad española, teniendo en cuenta escenarios de incertidumbre frente a ataques terroristas, ciberataques y crimen organizado, que dañen intereses nacionales, señalando que el terrorismo y los ciberataques dañan infraestructuras críticas, suministros y servicios críticos que sustentan la vida de la sociedad, debiendo garantizarse su bienestar y la economía del país[5]. También se aprobaron normas para la protección de infraestructuras críticas definiendo esta protección como:

> el conjunto de recursos, servicios, tecnologías de la información y redes, que en el caso de sufrir un ataque, causarían gran impacto en la seguridad, tanto física como económica, de los ciudadanos o en el buen funcionamiento del Gobierno de la Nación. (Ley 8/2011, Artículo 2, Literal k).

Según Caro Bejarano (2011) son medidas que conjugan coordinación entre instituciones públicas, operadores o propietarios de infraestructuras críticas buscando mejorar la seguridad global. Todas estas disposiciones significaron un avance en la valoración estratégica de infraestructuras críticas y muestran el proceso de maduración de respuesta ante el terrorismo en distintos niveles y sectores, pensando la integralidad, la coordinación y la

2 El Plan fue categorizado como un documento clasificado

3 Fue revisado por la Instrucción de la Secretaría de Estado de Seguridad 01/2016

4 Esta información se encuentra a resguardo en el Ministerio del Interior, siendo su responsable la Secretaría de Estado de Seguridad.

5 Apartado "Infraestructuras, suministros y servicios críticos"

cooperación. Esta primera Estrategia inicia un proceso consolidado a nivel nacional y en su relación al entorno europeo, indicando el propio documento que para aumentar la capacidad de recuperación de activos e infraestructuras críticas se requiere avanzar en herramientas para proteger instalaciones, invocar razones de seguridad para fortalecer sectores críticos y cooperar instituciones públicas y operadores de infraestructuras.

En 2013 se impulsó la Estrategia de Seguridad Nacional que reconoce amenazas y riesgos, y la Estrategia de Ciberseguridad Nacional para ataques cibernéticos. España ya contaba con dispositivos de prevención y respuesta para los incidentes de ciberseguridad pero actuaban de manera independiente; en la actualidad hay presentes diferentes instituciones con distintos niveles estratégicos-sectoriales de planificación y operación que trabajan bajo un enfoque integral. Los Centros de Seguridad nacionales en red para proteger los sistemas de información son equipos de respuesta para dichos incidentes que actúan mediante el Centro Nacional de Protección de Infraestructuras y Ciberseguridad. La Oficina de Coordinación Cibernética (Secretaría de Estado de Seguridad) es la encargada de la coordinación técnica-operativa con la Comunidad Europea y Estados miembros en el ámbito de la ciberseguridad y con los Centros de Respuesta a Incidentes Cibernéticos (CSIRT) nacionales.

La Estrategia de Seguridad 2013 fue sustituida en 2017; su revisión obedeció a cambios "significativos" en el escenario internacional, contemplando entre las amenazas y desafíos al terrorismo transnacional y los ciberataques. El ciberespacio como "espacio común global" es considerado vulnerable frente a actividades ilícitas que pongan en riesgo la seguridad nacional y de los habitantes. Las infraestructuras críticas son definidas como "infraestructuras estratégicas cuyo funcionamiento es indispensable y no permite soluciones alternativas" (Estrategia de Seguridad 2017 "Un proyecto compartido de todos y para todos") siendo los sectores estratégicos: administración, agua, alimentación, energía, espacio, industria química, industria nuclear, instalaciones de investigación, salud, sistema financiero y tributario, sector TIC y transporte.

El Centro Nacional de Protección de Infraestructuras y Ciberseguridad sustituye al Centro Nacional de Protección de Infraestructuras Críticas, siendo la ciberseguridad un objetivo estratégico del Ministerio del Interior. Así se abarca a la amenaza cibernética, empleando "la innovación como elemento fundamental de fortalecimiento de la seguridad, en particular del crimen organizado y del terrorismo" para el combate de los delitos electrónicos en la "evolución de la delincuencia hacia entornos digitales" (Real Decreto 770/2017). Este Centro[6] promueve, coordina y supervisa las políticas de protección de infraestructuras críticas españolas y de ciberseguridad. Además, desde el 2014 el Ministerio cuenta con el Centro de Inteligencia contra el Terrorismo y el Crimen Organizado (CITCO), encargado de la recepción, integración y análisis de la información estratégica en la lucha contra el crimen organizado, el terrorismo y el radicalismo violento y de la evaluación de la amenaza terrorista contra el Sistema de Protección de Infraestructuras Críticas.

6 Depende del Secretario de Estado de Seguridad, quien también dirige el Sistema Nacional de Protección de las Infraestructuras Críticas y las políticas de ciberseguridad.

El ejemplo español demuestra que frente a las amenazas transnacionales, las estrategias para prevenir ataques a sectores críticos consisten en elaborar planes integrales de respuesta multisectorial, basados en coordinación interinstitucional y cooperación internacional.

La protección de las infraestructuras críticas en el ámbito uruguayo

A los países les cuesta mucho enfrentarse a los desafíos para garantizar la seguridad, siendo un reto adicional el crimen organizado y el terrorismo en el ciberespacio (Gazapo 2017), fundamentalmente si tenemos en cuenta los riesgos que presentan los vínculos entre el terrorismo internacional y el crimen organizado transnacional (Resolución del Consejo de Seguridad de ONU 1373/2001) y los reportes anuales de la Oficina de las Naciones Unidas contra la Droga y el Delito (UNDOC) que plantean el financiamiento de actividades terroristas mediante fondos del crimen organizado.

Enfrentar amenazas con los instrumentos policiales y militares a su disposición no es suficiente ya que se requiere una solución integral del conjunto de la sociedad (Rodríguez 2017). En los últimos años Uruguay presenta una visión moderna de la Defensa Nacional que comprende a todos los sectores del quehacer nacional, incluida la Seguridad, en una concepción multisectorial y multidimensional y contiene aspectos de la seguridad humana, pues busca generar las condiciones para el bienestar presente y futuro de la población. Además, se aprecian estrategias que procuran garantizar la seguridad de infraestructuras críticas. Esa visión se encuentra en la Ley Marco de Defensa Nacional 18.650 (2010) que define a la Defensa Nacional como:

> el conjunto de actividades civiles y militares dirigidas a preservar la soberanía y la independencia de nuestro país, a conservar la integridad del territorio y de sus recursos estratégicos, así como la paz de la República, en el marco de la Constitución y las leyes, contribuyendo a generar las condiciones para el bienestar social, presente y futuro de la población. (Artículo 1º).

También se aprecia en la aprobación por el Consejo de Defensa Nacional[7] de la "Política de Defensa Nacional. Un Uruguay integrado a la región y abierto al mundo" (2014)[8], documento de más alto nivel gubernamental que determina el proceso de planificación de la Defensa Nacional, siendo este Consejo el que analiza las amenazas que pudieran afectar al país, trabajando junto con su Secretario, el Coordinador de los Servicios de Inteligencia del Estado y la Comisión Interministerial de Defensa Nacional. Partiendo de la definición de Defensa Nacional, este documento consideró el escenario internacional, regional y nacional, atendiendo el contexto geopolítico y estratégico, conceptualizando a las amenazas como "…todas aquellas acciones reales o percibidas que poseen un potencial intrínseco de afectar

7 El Consejo de Defensa Nacional forma parte del Sistema de Defensa Nacional. Es un órgano asesor y consultivo del Presidente de la República en temas de Defensa, integrado por el propio Presidente y los Ministros de Defensa Nacional, Interior, Relaciones Exteriores y Economía y Finanzas.

8 La Política de Defensa Nacional fue aprobada por el Decreto 105/014

negativamente los intereses y objetivos nacionales." (Política de Defensa Nacional, 2014, p.21), señalando el aspecto dinámico en el estudio de éstas al establecer que "La naturaleza de las actuales amenazas y el elevado grado de incertidumbre existente, producto de la velocidad con que los cambios ocurren, exigen énfasis en la actividad de análisis y en la capacidad de pronta respuesta de los diferentes sectores del Estado." (Política de Defensa Nacional, 2014, p. 3).

En ella, el Estado uruguayo identificó una serie de eventuales obstáculos que podría enfrentar entre 2014-2030: el deterioro del medio ambiente; la aparición de pandemias; el crimen organizado (incluido el crimen cibernético); los actos terroristas; el espionaje y los ataques cibernéticos; la inestabilidad democrática en la región; el surgimiento de guerras extra-continentales; el agravamiento de conflictos regionales; las crisis económicas; y la apropiación y el control indebido de los recursos estratégicos. Entre sus lineamientos estratégicos para la Defensa destacamos: proteger y fortalecer las infraestructuras vitales y estratégicas para Uruguay, que proveen de los servicios y recursos esenciales, como ser la energía, el agua, el transporte y las comunicaciones; prevenir las acciones del crimen organizado; proteger de ciberataques y los datos de la gestión pública y privada, nacional y en su caso, regional; y participar en ámbitos regionales e internacionales relacionados con políticas de seguridad y defensa.

La Política Militar de Defensa aprobada en 2016[9] complementa a la Política de Defensa Nacional. Ésta fija lineamientos para que la Política Militar de Defensa establezca los medios preventivos que atenúen o eviten riesgos y amenazas. De hecho, las Fuerzas Armadas, instrumento militar de la Defensa, pueden colaborar con la seguridad pública dentro de un marco específico, en emergencias nacionales, en infraestructuras vitales y estratégicas del país[10]. Han sido definidas como "la rama organizada, equipada, instruida y entrenada para ejecutar los actos militares que imponga la Defensa Nacional" (Ley Marco de Defensa Nacional, 2010, Artículo 18), pudiendo emplearse para combatir al crimen organizado y al terrorismo, apoyando a las fuerzas de seguridad a enfrentar las amenazas y ser usadas ante entornos de eventual ataque terrorista. Pueden proteger infraestructuras críticas manteniendo las condiciones de seguridad necesarias para el desarrollo económico y social del país; disuadir o neutralizar espionajes o ataques cibernéticos y desarrollar y emplear medios militares en conjunto y coordinación con las instituciones involucradas, para apoyar la prevención, disuasión y/o combate al terrorismo[11]. La Política Militar de Defensa determina que las Fuerzas Armadas tienen capacidad para combatir y prevenir el terrorismo si así se dispusiera, conformando unidades especialmente adiestradas, y entre sus acciones están la seguridad de las líneas de comunicaciones terrestres, marítimas e instalaciones portuarias, la seguridad de las líneas de navegación aérea y de la infraestructura aeronáutica, y la protección de infraestructuras críticas. A éstas las define como "las que aseguran el funcionamiento de los servicios básicos y sostienen los sistemas de producción del país" (Política Militar de Defensa, 2016, Lineamientos del empleo del instrumento militar, Numeral 2), mencionando que están ubicadas en el espacio terrestre, siendo el ámbito de responsabilidad del Ejército, lo que no

9 La Política Militar de Defensa fue aprobada por Decreto 129/016
10 Síntesis introductoria de la Política Militar de Defensa
11 Objetivos de la Defensa Militar

excluye que existan otras infraestructuras críticas en áreas con competencia de la Armada y la Fuerza Aérea, que también ejercen tareas de seguridad pública.

Como medidas tomadas ante un eventual ataque terrorista, se aprobaron diversas leyes para prevención y control de lavado de activos y financiamiento del terrorismo, además de la Estrategia Nacional contra el Terrorismo (2017) como un instrumento de rápida respuesta para prevenir, proteger y perseguir acciones violentas enmarcadas como terroristas que afecten a la seguridad de la población. En ese ámbito surge el Centro Nacional Coordinador Contra el Terrorismo (CENACOT)[12] con un Coordinador[13] que asesora, coordina, planifica y supervisa los aspectos vinculados con la Estrategia Nacional contra el Terrorismo. También el Poder Ejecutivo elaboró un proyecto de ley antiterrorista que refiere al ciberespacio utilizado por los grupos terroristas mediante tecnologías de la información para impactar aún más sus ataques. Para Rodríguez (2018) el terrorismo es una amenaza para el país por atentados o por el generar redes que afecten a otros países de la región, siendo imprescindible la cooperación con estos países y la coordinación entre las entidades públicas y con operadores privados.

Por otra parte, concordando con Realuyo (2016), el ciberespacio abre nuevas posibilidades en el accionar del crimen organizado, obteniendo enormes ingresos, por lo que allí también debe actuar el Estado. Cuando la tecnificación del crimen organizado se manifestó en 2017 con el ciberataque mundial mediante el virus Ransonware, Uruguay tomó medidas preventivas coordinando entre las diversas instituciones responsables de las áreas de seguridad informática, incluido el Ministerio de Defensa. El impacto de ese ciberataque con un programa denominado "WannaCry", que bloqueó miles de computadoras personales o de trabajo en red y exigió un pago para devolver el acceso a la información ubicada en archivos digitales, dejó varios países afectados en infraestructuras como hospitales, transporte y comunicaciones y miles de víctimas en el mundo. Es importante señalar que en Uruguay, la alerta y respuesta acerca de tecnologías de la información está a cargo de la Agencia de Gobierno Electrónico y Sociedad de la Información y del Conocimiento (AGESIC)[14], órgano fiscalizador en seguridad de la información, estando entre sus objetivos fortalecer el ecosistema de ciberseguridad y desde allí fortalece a las instituciones. Cuenta con el Centro Nacional de Respuesta a Incidentes de Seguridad Informática (CERTuy)[15] que protege los sistemas de información que soportan los activos de información críticos estatales. Según datos estadísticos, el Centro respondió 1684 incidentes de seguridad informática, duplicando su número en relación a 2016. El CERTuy coordina con el Centro de Respuesta a Incidentes de Seguridad de la empresa estatal de telecomunicaciones (SCIRT de ANTEL). La política de ciberseguridad asentada en la Política de Seguridad de la Información[16] se implementó en los centros de datos usados por el Estado (Administración Central) que contienen sistemas informáticos que puedan representar un riesgo para el organismo. En esta línea, el Ministerio de Defensa Nacional dispone desde 2015 de un Equipo de Respuesta a Incidentes de Seguridad Informática de Defensa(D-

12 Ambos son aprobados por el Decreto 180/017

13 La figura del Coordinador del CENACOT recae actualmente en el Secretario del Consejo de Defensa Nacional quien es a su vez, el Jefe del Estado Mayor de la Defensa

14 Depende de Presidencia de la República

15 Creado por Ley No. 18.362, Artículo 73

16 La Política de Seguridad de la Información fue aprobada por el Decreto 92/014

CSIRT)[17], siendo el primer centro creado en el ámbito de la Defensa Nacional que atienda la ciberdefensa y que incluye a las Fuerzas Armadas (Camps:2016, 274) y ataques sobre infraestructuras críticas y servicios esenciales. Este Centro trabaja de forma coordinada con el CERTuy, vinculándose con organismos regionales en la materia. En el caso del Ministerio del Interior, se atienden los delitos informáticos-financieros, a través de la Dirección General de Lucha contra el Crimen Organizado e INTERPOL[18].

Esta perspectiva institucional indica que se han dado importantes pasos que permiten avanzar hacia la primera Estrategia Nacional de Ciberseguridad. Sin contar aún con dicha Estrategia, Uruguay se destaca en su respuesta frente al cibercrimen por su alto grado de desarrollo en sus políticas de ciberseguridad, por fomentar en la sociedad una conciencia de seguridad cibernética, dispone de estudios cibersecuritarios y cuenta con centros de respuestas a incidentes y medidas de protección a infraestructuras críticas (Gazapo, 2017). Teniendo presente que para enfrentar un eventual ataque se requiere de estructuras conjuntas e integradas, se identifican a las estructuras de ciberdefensa militares bajo el accionar del Estado Mayor de la Defensa (Camps, 2016).

En resumen, la protección de infraestructuras críticas como un aspecto de la seguridad integral del Estado requiere una respuesta entre todos los sectores involucrados. Desde su lugar, las distintas organizaciones tienen que contribuir a planificar estrategias pensadas a mediano y largo plazo, y coordinar líneas de acción para responder a las crisis que afecten al país. El éxito estará en la prevención y cooperación entre las diversas instituciones y en la coordinación de planes multisectoriales (Rodríguez, 2016, p. 1).

Conclusiones

Analizar el itinerario histórico llevado adelante por España muestra un proceso de maduración respecto de determinadas infraestructuras, adecuando sus políticas de seguridad con las pautas mandatadas desde la Unión Europea para contrarrestar al terrorismo y al crimen organizado. Los antecedentes europeos reseñados influyeron en el modelo español siendo determinantes para definir sus infraestructuras, valorarlas estratégicamente, considerarlas críticas y catalogarlas, los ámbitos relevantes para atender su protección y los planes de respuesta interinstitucionales ante eventuales amenazas del terrorismo, el crimen organizado y al cibercrimen.

Sería muy útil para Uruguay seguir similar hoja de ruta, teniendo en cuenta que su desarrollo en este tema fue significativo. Para enfrentar y minimizar el impacto que pueden tener esos ataques, el contar con un Catálogo de Infraestructuras Críticas y con una Estrategia Nacional de Ciberseguridad como lo ha hecho España, permite seguir avanzando en los planes de respuesta sectoriales y en un plan nacional de respuesta que tenga en cuenta también el ámbito estatal y el privado, con operadores de algunas de estas infraestructuras críticas En este mismo sentido, es necesaria la revisión constante de dichos planes ante escenarios de seguridad muy cambiantes.

17 Este Equipo de Respuesta fue creado por el Decreto 36/015
18 Dicha información surge del Decreto 298/016

La Estrategia Española de Seguridad Nacional 2017 mira hacia América Latina, considerando en su planeamiento geoestratégico a futuro, ser actor entre esta región y la Unión Europea, y ubicando en prioridad, políticas de cooperación hacia esta región. En consecuencia, el vínculo entre los Colegios de Defensa iberoamericanos significa terreno fértil para fomentar aún más los lazos de cooperación en Seguridad y Defensa. Uruguay puede mirar a España para que le aporte su experiencia en construcción de estrategias y sus lecciones aprendidas para prevenir y atenuar amenazas. En este sentido, también contribuye la participación en ámbitos regionales e internacionales dedicados al intercambio de información y discusión de políticas vinculadas al crimen organizado y al terrorismo. Del mismo modo, es valioso propiciar ejercicios que simulen escenarios de riesgos vinculados a prevención y protección de infraestructuras críticas, poniendo en práctica las herramientas de que dispone el país, los roles y responsabilidades de cada organización involucrada, la formulación de políticas y la planificación de respuestas interinstitucionales que puedan ser válidos en un escenario real.

La definición actual de la Defensa Nacional en Uruguay, que comprende la concepción de Seguridad, presenta un enfoque integral y de acción multisectorial que se torna favorable para responder a eventuales amenazas. Implementar políticas para proteger infraestructuras críticas demanda una visión que permita usar todos los recursos de la sociedad. Pensar la Defensa Nacional como una política de Estado, permite llevar adelante políticas públicas con una adecuada coordinación interinstitucional entre diversos organismos, que vayan más allá de orientaciones políticas de corto plazo. Responder y superar cualquier crisis con éxito mediante los esfuerzos coordinados de las organizaciones basados en un concepto integral representa un valioso reto para los países.

Referencias

Aznar, F., Berenguer, F., Diez, J., y Laborie, M. (2013). Los conceptos de Seguridad y Defensa de España. En Conceptos sobre Seguridad y Defensa de los países iberoamericanos. Desde la óptica de sus Colegios de Defensa. Centro de Altos Estudios Nacionales-Colegio de Defensa del Uruguay (comp.): Montevideo, pp. 285-317.

Camps, P. (2016). Ciberdefensa y ciberseguridad: Nuevas amenazas a la seguridad nacional, estructuras nacionales de ciberdefensa, estrategias de ciberseguridad y cooperación interagencias en este ámbito. En Ciberdefesa e cibersegurança: novas ameaças á Segurança Nacional / Organizador José Cimar Rodriguez Pinto. Río de Janeiro: ESG, pp. 265-278.

Carabias, J (2013). La seguridad de las infraestructuras críticas. El caso español. Revista Atenea Seguridad y Defensa, Año V, Nº 46, pp. 6-8.

Caro Bejarano, M. (2011). La protección de las infraestructuras críticas. Documento de Análisis 021/011. Revista del Instituto Español de Estudios Estratégicos, pp.1-7.

España (2011). Estrategia Española de Seguridad. Una responsabilidad de todos. Madrid: Gobierno de España. Recuperado de http://www.realinstitutoelcano.org/wps/wcm/connect/c06cac0047612e998806cb6dc63

29423/EstrategiaEspanolaDeSeguridad.pdf?MOD=AJPERES&CACHEID=c06cac0047612e998806cb6dc6329423

-------- (2011b). Ley 8/2011 de 28 de abril de 2011. Protección de Infraestructuras Críticas.

España. Centro Nacional de Protección de Infraestructuras y Ciberseguridad. Recuperado de http://www.cnpic.es/Presentacion/index.html

España (2013). Presidencia del Gobierno. Estrategia de Seguridad Nacional. Un proyecto compartido. Madrid:Departamento de Seguridad Nacional. Recuperado de http://www.lamoncloa.gob.es/documents/seguridad_1406connavegacionfinalaccesiblebpdf.pdf

España (2013). Gabinete de la Presidencia del Gobierno. Estrategia de Ciberseguridad Nacional. Madrid: Departamento de Seguridad Nacional. Recuperado de http://www.dsn.gob.es/es/estrategias-publicaciones/estrategias/estrategia-ciberseguridad-nacional

España (2016). Instrucción de la Secretaría de Estado de Seguridad 01/2016. Nuevo Plan de Protección de Infraestructuras Críticas. Madrid: Secretaría de Estado de Seguridad.

España (2017). Real Decreto 770/2017 de 28 de julio de 2017. Estructura Orgánica Básica del Ministerio del Interior. Recuperado de https://www.boe.es/boe/dias/2017/07/29/pdfs/BOE-A-2017-9013.pdf

España. Ministerio del Interior (2017). La ciberseguridad, objetivo estratégico del Ministerio del Interior. Madrid: Gobierno de España. Recuperado de http://www.interior.gob.es/prensa/noticias/-/asset_publisher/GHU8Ap6ztgsg/content/id/7640082

España. Ministerio del Interior. Secretaría de Estado de Seguridad. Centro de Inteligencia Contra el Terrorismo y el Crimen Organizado (CITCO). Gobierno de España. Recuperado de http://www.interior.gob.es/el-ministerio/directorio/servicios-centrales/secretaria-de-estado-de-seguridad1

España (2017). Estrategia de Seguridad Nacional. Un proyecto compartido de todos y para todos. Madrid: Presidencia del Gobierno de España. Recuperado de http://www.lamoncloa.gob.es/serviciosdeprensa/notasprensa/presidenciadelgobierno/Documents/2017-1824_Estrategia_de_Seguridad_Nacional_ESN_doble_pag.pdf

Fresneda, C. (13 de mayo de 2017). Europol reconoce que el ciberataque es de un “nivel sin precedentes”.El Mundo.
Recuperado de:
http://www.elmundo.es/economia/2017/05/13/5916d88a268e3e253e8b45de.html

Gazapo, M. (2017). Ciberespacio: el nuevo campo de actuación del crimen organizado en América Latina. En El crimen organizado en América Latina: manifestaciones, facilitadores y reacciones. Sampó y Troncoso (comp.). Instituto Universitario General Gutiérrez Mellado, pp. 335-361.

Gómez de Ágreda, A. (2016). El modelo de ciberseguridad y ciberdefensa en España. En Ciberdefesa e cibersegurança: novas ameaças á Segurança Nacional / Organizador José Cimar Rodriguez Pinto. Río de Janeiro:ESG, pp.147-177.

Miranzo, M. y del Río, C. (2014). La protección de infraestructuras críticas. Unidad de Investigación sobre Seguridad y Cooperación Internacional. Revista de la Unidad de Investigación sobre Seguridad y Cooperación (UNISCI). Discussion Papers. Nº 35 (Mayo / May 2014), pp. 339-352. Recuperado de http://revistas.ucm.es/index.php/UNIS/article/viewFile/46435/43628

Oficina de las Naciones Unidas contra la Droga y el Delito (UNODC) (2004). Convención de las Naciones Unidas contra la Delincuencia Organizada Transnacional y sus Protocolos. Nueva York: Naciones Unidas. Recuperado de https://www.unodc.org/pdf/cld/TOCebook-s.pdf

Organización de Naciones Unidas (2001). Resolución 1368. Nueva York: Consejo de Seguridad.

-------- (2001b). Resolución 1373. Nueva York: Consejo de Seguridad.

.------- (2006). Resolución A/RES/60/288. Estrategia Global de las Naciones Unidas contra el Terrorismo. Nueva York: Asamblea General.

Realuyo, Celina B. (2016), "La futura evolución de las organizaciones criminales transnacionales y la amenaza para la seguridad nacional de los EE. UU.", Perry Center Ocassional Paper, enero 2016, William J. Perry Center for Hemispheric Defense Studies, National Defensa University.

Rodríguez Cuitiño, M. (16 de marzo de 2016). ¿Estamos preparados para proteger infraestructuras críticas? Revista Diálogo Político. Montevideo: Fundación Konrad Adenauer Uruguay. Recuperado de http://dialogopolitico.org/actualidad/estamos-preparados-para-proteger-infraestructuras-criticas/

Rodríguez Cuitiño, M. (2018). La lucha contra el crimen organizado y el terrorismo en Uruguay: Un desafío a enfrentar. Revista de Estudios en Seguridad Internacional. Vol. 4. Nº1. pp. 55-70.

Unión Europea (2001). Plan de Acción sobre la Lucha contra el Terrorismo. Bruselas: Consejo Europeo.

-------- (2003). Estrategia Europea de Seguridad (EES) - Una Europa segura en un mundo mejor. Bruselas: Consejo Europeo.

------- (2004). Lucha contra el terrorismo: preparación y gestión de las consecuencias. COM (2004) 701 final. Comunicación al Consejo y al Parlamento Europeo. Bruselas: Comisión de las Comunidades Europeas. Recuperado de https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=celex:52004DC0701

------- (2004b). Prevención, preparación y respuesta a los ataques terroristas. COM (2004) 698 final. Comunicación al Consejo y al Parlamento Europeo. Bruselas: Comisión de las Comunidades Europeas. Recuperado de https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=celex:52004DC0698

-------- (2004c). Prevención y la lucha contra la financiación del terrorismo a través de medidas para mejorar el intercambio de información, aumentar la transparencia y mejorar la trazabilidad de las transacciones financieras. COM (2004) 700, final. Comunicación al Consejo y al Parlamento Europeo. Bruselas: Comisión de las Comunidades Europeas. Recuperado de https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=celex:52004DC0700

------ (2004d). Protección de las infraestructuras críticas en la lucha contra el terrorismo. COM (2004) 702, final. Comunicación al Consejo y al Parlamento Europeo. Bruselas: Comisión de las Comunidades Europeas. Recuperado de https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=celex:52004DC0702

Unión Europea (2004). Europol. Recuperado de https://www.europol.europa.eu/es

-------- (2005). Libro verde sobre un programa europeo para la protección de infraestructuras críticas. COM(2005) 576 final. Bruselas: Comisión de las Comunidades Europeas. Recuperado de https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=celex:52005DC0576

-------- (2005b). Estrategia de la Unión Europea de Lucha contra el Terrorismo. Bruselas: Consejo de la Unión Europea. Recuperado de http://register.consilium.europa.eu/doc/srv?f=ST+14469+2005+REV+4&l=es

------- (2008). Directiva 2008/114/CE del Consejo. Identificación y designación de infraestructuras críticas europeas y la evaluación de la necesidad de mejorar su protección. Bruselas: Consejo de la Unión Europea. Recuperado de https://eur-lex.europa.eu/legal-content/ES/ALL/?uri=celex:32008L0114

Uruguay. Administración Nacional de Telecomunicaciones, Centro de Respuesta a Incidentes de Seguridad (CSIRT). Recuperado de http://www.csirt-antel.com.uy

Uruguay. Presidencia de la República. Agencia para el desarrollo del Gobierno de Gestión Electrónica y la Sociedad de la Información y del Conocimiento. Estadística de Incidentes 2017. Montevideo: Centro Nacional de Respuesta a Incidentes de Seguridad Informática. Recuperado de https://www.cert.uy/inicio/novedades/alertas_y_vulnerabilidades/estadistica+de+incidentes+2017

Uruguay. Poder Ejecutivo. Ministerio de Defensa Nacional. Equipo de Respuesta a Incidentes de Seguridad Informática de Defensa. Recuperado de https://www.mdn.gub.uy/?page_id=2070

Uruguay coordina defensa y adopta primeras medidas ante ciberataque (17 de mayo de 2017). La República. Recuperado de http://republica.com.uy/coordina-defensa.

Uruguay. Poder Legislativo (2008). Ley 18.362 de 6 de octubre de 2008. Creación de Centro Nacional de Respuesta a Incidentes de Seguridad Informática (CERTuy) en la Agencia

para el Desarrollo del Gobierno de Gestión Electrónica y la Sociedad de la Información y del Conocimiento (AGESIC). Montevideo: Asamblea General.

------- (2010). Ley 18.650 de 19 de febrero de 2010. Marco de Defensa Nacional. Montevideo: Asamblea General.

Uruguay. Poder Ejecutivo (2014). Decreto 92/014. Estandarización de los nombres de dominio de la Administración Central para todos los servicios vinculados con internet. Montevideo: Presidencia de la República.

---------- (2014b). Decreto 105/014. Política de Defensa Nacional. Montevideo: Presidencia de la República.

Uruguay. Poder Ejecutivo (2015). Decreto 36/015. Creación del Centro de Respuesta a Incidentes de Seguridad Informática en el Ministerio de Defensa Nacional (D-CSIRT). Montevideo: Presidencia de la República.

Uruguay. Poder Ejecutivo (2016). Decreto 129/016. Política Militar de Defensa. Montevideo: Presidencia de la República.

Uruguay. Poder Ejecutivo. (2016). Decreto 298/016. Reglamentación del art. 27 de la Ley 19.315 relativo a los cometidos de la Dirección General de Lucha contra el Crimen Organizado e INTERPOL. Montevideo: Presidencia de la República.

Uruguay. Poder Ejecutivo (2017). Decreto 180/017. Estrategia Nacional Contra el Terrorismo. Montevideo: Presidencia de la República.

LOS CIBERATAQUES COMO AMENAZAS A LAS INFRAESTRUCTURAS Y RECURSOS CRÍTICOS DE UN ESTADO

Gustavo Vila[1]

RESUMEN

Las Tecnologías de la Información y Comunicaciones (TIC) son una de las fuerzas más poderosas que se hallan detrás de la evolución de las sociedades contemporáneas. A su vez, los Estados dependen del funcionamiento confiable de sus infraestructuras críticas para el logro de sus Objetivos Nacionales (OONN). En la actualidad, distintos tipos de ciberamenazas explotan la creciente complejidad y conectividad de los sistemas de infraestructura crítica, colocando a éstos en una posición de vulnerabilidad y riesgo. Debido al rol protagónico de aquellos en la vida diaria de todas las personas, se hace necesario lograr un adecuado marco de seguridad en el ciberespacio, como una forma de contribuir decisivamente a la seguridad nacional.

Palabras clave: Infraestructura crítica, Terrorismo, Ciberseguridad, Amenazas, Defensa Nacional.

1 - Introducción

En el mes de Junio de 1982, un satélite de reconocimiento de EEUU detectó una enorme explosión en un gasoducto de Siberia. La causa fue una falla en el sistema de control informático del gasoducto, el cual había sido robado por espías soviéticos de una compañía de Canadá. Los soviéticos desconocían que la CIA había manipulado el software para que, luego de un tiempo, el sistema se resetease y permitiese la generación de presiones insoportables para las uniones y soldaduras de las tuberías, sin que se disparasen las alarmas del sistema. Esta puede ser considerada la primera demostración de los efectos de una "bomba lógica" en una infraestructura crítica (The Economist, 2010).

Las TIC son una de las fuerzas más poderosas que se hallan detrás de la evolución de las sociedades contemporáneas y los Estados dependen del funcionamiento confiable de sus infraestructuras críticas para el logro de sus Objetivos Nacionales (OONN) e Internet fue

[1] El Magister Gustavo Vila es un Coronel retirado del Arma de Infantería del Ejército Nacional. Es Oficial Diplomado de Estado Mayor, egresado del Curso de Altos Estudios Nacionales (CALEN), Licenciado en Ciencias Militares con orientación en Estrategia (IMES), y Magister en Estrategia Nacional.

diseñado para la comodidad y fiabilidad, no para la seguridad. Sin embargo en un mundo interconectado, Internet brinda a la par oportunidades y amenazas en relación con las infraestructuras críticas: ningún pasaporte es necesario en el ciberespacio, un dominio que constituye un bien público mundial impuro[2]. Las ciberamenazas explotan la creciente complejidad y conectividad de los sistemas de infraestructura crítica, colocando a los mismos en una posición de vulnerabilidad y riesgo. Debido a su rol protagónico en la vida diaria de las personas, se hace necesario lograr un adecuado marco de seguridad en el ciberespacio, como una forma de contribuir decisivamente a la seguridad nacional. Un ejemplo de lo anterior lo constituye la situación caótica que supondría la interrupción de la energía eléctrica o anomalías en el sistema económico-financiero, mediante ataques informáticos desarrollados por Estados, organizaciones o personas (Saavedra, 2015) (Sancho, 2016). Si bien las computadoras e Internet han transformado la economía y han dado grandes ventajas cualitativas a los ejércitos de las grandes potencias, no es menos cierto que la tecnología digital tiene su contracara: los riesgos a ciberataques por parte de actores estatales y no estatales, constituyendo una amenaza compleja, difusa y potencialmente muy peligrosa[3] (Martin, 2016).

2 - Desarrollo

2.1 – Globalización, terrorismo y nuevas amenazas

El ciberespacio es un dominio virtual donde se llevan adelante complejas actividades "on line" asociadas al proceso de globalización en el que nos hallamos insertos; este quinto dominio ha sido generado por las TIC y en él coexisten las personas y las computadoras, y constituye el campo de batalla de la ciberguerra. En el ciberespacio no hay un límite geográfico claro y el teatro de operaciones son las redes globales interconectadas (Sancho, 2016). Este dominio se caracteriza por permitir ocultar la identidad y ubicación de las personas, en tanto que es omnipresente en algunos lugares e inexistente en otros, permitiendo aumentar la velocidad, volumen y alcance de los Estados y las personas, requiriéndose para su acceso de medios de tratamiento automático de información y conexiones de datos. La Junta de Estado Mayor Conjunta de los EEUU define al ciberespacio como "Un dominio global dentro del entorno de información consistente en las redes interdependientes de tecnología de información, infraestructura y datos, incluidos Internet, las redes de telecomunicaciones, los sistemas informáticos, así como los procesadores y controladores allí insertados" (DoD, 2016, p. 58).

---

[2] Los bienes públicos mundiales pueden ser puros e impuros. Un bien público mundial puro es aquel donde hay imposibilidad que exista rivalidad y exclusión en su uso o consumo. Uno impuro en cambio, es aquel en el cual existe rivalidad y/o exclusión en su uso o consumo. El ciberespacio encaja en esta última categoría," […] presentando deficiencias en cuanto a su oferta, cobertura, disponibilidad, calidad y seguridad. […] las autoridades nacionales tienen una importante responsabilidad en la regulación de la existencia, uso, y condiciones de funcionamiento del ciberespacio…" (Santo, 2016, P 48).

[3] Existen muchas "áreas oscuras" y a diferencia de la guerra convencional, no hay una normativa específica al respecto. En el caso de la OTAN, el vacío pretendió ser llenado con el llamado "Manual de Tallin", el cual en sus 302 páginas, proporciona 95 "reglas" a partir de la legislación que aplica a los conflictos convencionales, adaptados al ciberespacio y a la ciberguerra. Bajo esta óptica un hacker puede ser considerado un blanco legítimo si representa una amenaza para el país que sufre la agresión cibernética, ante la posibilidad que cause lesiones o muerte de personas, o bien daños o destrucción de infraestructura crítica, pudiendo en consecuencia ser objeto de ataques para su neutralización (El Mundo, 2013).

La actual globalización supone tanto ventajas como riesgos[4]. Al hablar de actores hostiles en el ciberespacio se debe hablar de Estados y organizaciones, y dentro de éstas adquieren especial significación las organizaciones terroristas. Hoy el ciberespacio es uno de los campos de batalla en la guerra contra el terrorismo y las infraestructuras críticas constituyen blancos altamente redituables; a su vez las TIC pueden llegar a constituirse en armas de destrucción y desinformación masiva. El ciberterrorismo ya está entre nosotros y resulta posible y altamente probable que las TIC sigan siendo utilizadas por actores no estatales para alcanzar sus objetivos (Martin, 2016). El empleo del ciberespacio por organizaciones terroristas ha dado origen al término "ciberterrorismo" el cual es definido por el Ministerio de Defensa de España (2010) como "un ciberataque para causar la inutilización o interrupción de redes de ordenadores o comunicaciones para generar temor o intimidar a la sociedad con un objetivo ideológico" (p. 348).

Hoy los grupos terroristas utilizan Internet para llegar a sus seguidores y difundir su mensaje, pero sus capacidades para lanzar ciberataques sobre infraestructuras y recursos críticos siguen siendo muy limitadas. Esta ausencia de ciberataques por organizaciones terroristas puede interpretarse como el resultado de la falta de habilidades técnicas apropiadas dentro de los grupos para desarrollar virus informáticos o la incapacidad para infiltrar agentes en las infraestructuras críticas, pero esta circunstancia puede cambiar muy rápidamente. Actualmente se han detectado una serie de grupos de hackers que trabajan para diferentes organizaciones terroristas, así como un sinnúmero de amenazas[5] (Europol, 2018). Si bien las organizaciones terroristas no disponen de capacidades creíbles para lanzar un ciberataque masivo, algunos

[4] Desde el punto de vista de las TIC la globalización puede ser considerada a partir de tres aspectos: la conectividad, la fiabilidad y la vulnerabilidad. En relación con la conectividad, Saavedra (2016) señala que personas dispersas por todo el mundo pueden reunirse virtualmente como nunca antes; si bien las ventajas del mundo on line son muy frecuentemente rescatadas, no es menos cierto que a la par de las ventajas existen una serie de debilidades. Nuestra sociedad y los servicios públicos esenciales (SSPPEE) que constituyen la infraestructura crítica y permiten nuestra vida cotidiana sin sobresaltos, son cada vez más "on line-dependientes". La creciente conectividad a través de una Internet insegura multiplica las vías para un ciberataque; a su vez, la creciente dependencia en las computadoras aumenta el daño que pueden causar (The Economist, 2010). En este contexto, la fiabilidad está dada por la capacidad de las organizaciones que habiendo detectado una vulnerabilidad en sus sistemas, rápidamente aplica parches y medidas defensivas. El problema es que el grado de fiabilidad es variable: existen organizaciones que reparan y refuerzan sus sistemas rápidamente, otras no son capaces de darse cuenta que están utilizando un software vulnerable, en tanto que otras ni siquiera son capaces de bajar las actualizaciones de seguridad del software que utilizan. En lo que refiere a la vulnerabilidad, esta se incrementa proporcionalmente a la reducción de las barreras de acceso al ciberespacio al existir dispositivos de muy bajo costo que combinan comunicaciones, acceso a la web, así como capacidades de video. Esta conectividad, a través de la Internet de las Cosas (IoT), ofrece un sinnúmero de oportunidades a personas y organizaciones con las habilidades y medios técnicos adecuados. Mayor conectividad significa mayor vulnerabilidad, resultando particularmente expuestos las redes eléctricas, instalaciones nucleares, los oleoductos de gas y petróleo, y los bancos y el sistema financiero en general (The Economist, 2010).

[5] El Estado Islámico (EI) disponía de la Hacking División, también conocida por la denominación de Ciber Califato, la cual incorporaba a cualquier grupo hacker que se identificase con la organización terrorista. En un momento la Hacking División llegó a contar con varias organizaciones, siendo las más importantes el Ciber Ejército del Califato (Caliphate Cyber Army), el Ciber Ejército Islámico (Islamic Cyber Army) y los Hijos del Ejército del Califato (Sons of the Caliphate Army). Estas organizaciones trabajaban en el ciberespacio atacando websites, recopilando información sobre los sistemas de energía eléctrica y las industrias, y realizando reclutamiento en Facebook y Twitter.

estudios sugieren que estos grupos pueden estar tratando de "tercerizar" estas capacidades. Para ello,

> en lugar de tratar de desarrollar su propia capacidad y herramientas, algunos grupos terroristas ahora se orientan hacia mercados criminales en línea, utilizando los servicios de la industria del crimen para comprar el acceso a las capacidades que ellos mismos carecen. Si esto es cierto, es probable que la efectividad de los grupos ciberterroristas aumente, tal vez en el corto plazo (Europol, 2018, p. 15).

A los efectos de amplificar los efectos sobre la opinión pública, debido al poco impacto que genera un ciberataque en el mundo virtual (el cual muchas veces es ocultado por quién lo recibe), es posible amplificar los efectos de aquel conduciendo al mismo tiempo un ciberataque contra infraestructuras críticas que produzcan efectos en el mundo real, en lo que se denomina un "ataque híbrido", pudiendo afectar alguno de los servicios públicos esenciales (SSPPEE) como ser el agua potable, la energía eléctrica, las represas o los sistemas de comunicaciones (Europol, 2018).

2.2 – La guerra cibernética y las ciberamenazas

Dentro de las llamadas "nuevas amenazas"[6] encontramos **la guerra cibernética o ciberguerra,** la cual es un conflicto en el ciberespacio. Ésta puede ser definida como "el uso de capacidades basadas en la red de un Estado, para interrumpir, denegar, degradar, manipular o destruir información residente en computadores y redes de ellos, o los propios ordenadores y las redes de otro Estado" (Leiva, 2018, p. 27).[7] Debido a ello, en la ciberguerra no proteger las redes propias equivale a dejar abierta la puerta de calle de nuestra casa; la securitización de una red en cambio equivale a cerrar con llave: no impide los robos, pero los dificulta.

Asociados con el concepto de ciberguerra se encuentran los conceptos de ciberseguridad y ciberdefensa.

- **Ciberseguridad.** Puede definirse como "Prevención de daños, protección y restauración de equipos, sistemas de comunicaciones electrónicas, servicios de comunicaciones electrónicas, comunicación alámbrica y comunicación electrónica, incluyendo la información contenida en el mismo, para asegurar la disponibilidad, integridad, autenticación, confidencialidad y no rechazo" (DoD, 2016, p. 57). Ella es un proceso mediante el cual se protege a través de la prevención, detección y respuesta contra los diferentes tipos de amenazas a las infraestructuras críticas, los sistemas de información y de comunicaciones, negándole su uso a terceros. La seguridad

[6] El Decreto 105/14 Política de Defensa Nacional de la ROU señala como obstáculos que podrían devenir en amenazas al deterioro del medio ambiente; las pandemias; el Crimen Organizado (y dentro de éste la modalidad de crimen cibernético); el terrorismo; la materialización del espionaje y los ataques cibernéticos; la inestabilidad democrática en la región; el surgimiento de guerras extracontinentales; el agravamiento de conflictos regionales; las crisis económicas; y la apropiación y el control indebido de los recursos estratégicos (Poder Ejecutivo, 2014).

[7] La diferencia entre la ciberguerra y la guerra convencional en lo que a efectos sobre el adversario refiere, es ínfima. Una de las principales diferencias la constituye el medio ambiente operacional, que en este caso lo constituye el ciberespacio. En este tipo de conflicto el soldado es el *cracker*, quién busca vulnerabilidades en nuestros dispositivos y sistemas, del mismo modo que el comandante enemigo busca las vulnerabilidades en nuestro despliegue, o el ladrón busca las vulnerabilidades en nuestros domicilios.

informática se lleva adelante con tres objetivos: asegurar la disponibilidad, confidencialidad e integridad de los sistemas y la información (Saavedra, 2015).

- **Ciberdefensa.** Es la "aplicación de medidas de seguridad para proteger las los diferentes componentes de los sistemas de información y comunicaciones de un ciberataque" (Ministerio de Defensa, 2010). Comprende tanto medidas de defensa activas, pasivas, proactivas, preventivas y reactivas para asegurar el uso propio del ciberespacio y negarlo al enemigo o a otras organizaciones.

En función de lo anterior, y tal como lo señala Camps (2016), podemos atribuirle a la ciberseguridad un carácter más preventivo, es decir evitar que se produzca el ciberataque, en tanto que la ciberdefensa tiene un carácter más reactivo, es decir la reacción una vez producido al ataque.

Los actores capaces de materializar un ataque informático son variados y García et al. (2016) señalan que el ataque puede ser realizado por una variedad de elementos hostiles que incluyen crackers, delincuentes comunes, atacantes internos, personal descontento, personal realizando actividades no autorizadas (acceso a Internet), servicios de inteligencia extranjeros, crimen organizado, terroristas, entre otros. Por ello una **ciberamenaza** es:

> Cualquier circunstancia o evento con el potencial de impactar negativamente sobre las operaciones de la organización (incluyendo su misión, funciones, imagen o reputación), recursos, y otras organizaciones a través de Tecnología de la Información (TI) y/o un Sistema de Control Industrial (SCI), a través del acceso, destrucción, divulgación, modificación de información o denegación de servicio, de forma no autorizada (DoE, 2012).

En el Anexo 3 se realiza una caracterización de las amenazas.

Las TIC han generado el ciberespacio, el quinto dominio de interacción humana[8], y a partir de 1998[9] un nuevo campo de batalla de dimensiones planetarias. Este nuevo dominio ha inducido la aparición de nuevas amenazas materializadas por individuos, organizaciones o Estados que buscan defender sus intereses a través de herramientas cibernéticas (Camps, 2016). Por su parte Santo (2016) y Parraguez (2017), señalan que una cantidad creciente de países identifican los ataques cibernéticos como una amenaza igual o mayor que la representada por un ataque terrorista debido a sus afectaciones a la seguridad nacional y sus implicaciones en todos los campos de poder nacional. Un ciberataque (o ataque cibernético) es definido por el Ministerio de Defensa (2010) de España como una "forma de ciberguerra/ciberterrorismo donde combinado con un ataque físico o no se intenta impedir el empleo de los sistemas de información del adversario o el acceso la misma".

[8] El primer dominio lo constituye la tierra, el segundo el mar, el tercero el aire, el cuarto el espacio, y el quinto el ciberespacio.

[9] En 1998, la organización insurgente Ejército de Liberación Tigres de Tamil Ealam (LTTE – Liberation Tigers of Tamil Ealam, también conocida como los "*Tigres Tamiles*") que operaba en Sri Lanka, atacó con correos masivos sedes diplomáticas del gobierno de Sri Lanka con un promedio de 800 correos diarios, a lo largo de dos semanas, saturando sus redes. El mensaje decía "Somos los Tigres Negros de Internet y estamos haciendo esto para desorganizar sus comunicaciones" (Martin, 2016). Esta acción fue el primer ciberataque por parte de una organización irregular contra el sistema informático de un país.

2.3 – Los Activos Críticos Nacionales (ACN) como objetivos potenciales.

2.3.1 – Qué son las Infraestructuras y Recursos Críticos (IRRC) y los ACN?

Cada Estado y dentro de éste, cada organización debe definir y determinar aquellas **Infraestructuras y Recursos Críticos (IRRC)** que constituyen sus **Activos Críticos Nacionales (ACN).** La legislación de Perú a este respecto, resulta muy ilustrativa acerca del vínculo entre IRRC y ACN.

- El Decreto Supremo N° 106-2017-PCM define la infraestructura como "Conjunto de estructuras, instalaciones u obras que componen un Activo Crítico Nacional – ACN, que son esenciales e imprescindibles para el normal desarrollo o funcionamiento de un país." (Poder Ejecutivo del Perú, 2017).
- El mismo decreto anterior define los recursos como "Conjunto de elementos tangibles o intangibles, disponibles de una Nación, que componen un Activo Crítico Nacional – ACN, permiten atender una necesidad o alcanzar un objetivo y son esenciales e imprescindibles para el normal desarrollo o funcionamiento de un país" (Poder Ejecutivo del Perú, 2017).
- Finalmente se define un ACN como:

  recursos, infraestructuras y sistemas que son esenciales e imprescindibles para mantener y desarrollar las capacidades nacionales, o que están destinados a cumplir dicho fin. La afectación, perturbación o destrucción de dichos activos no permite soluciones alternativas inmediatas, generando grave perjuicio a la Nación. (Poder Ejecutivo, 2017).

Cada Estado debe determinar cuáles son los ACN a ser protegidos y establecer políticas o estrategias para la protección de los mismos. España, por ejemplo, definió las bases de su política de protección de infraestructura crítica a través de la Ley de Protección de Infraestructuras Críticas PIC 8/2011, Real Decreto 704/2011. Allí son definidos doce sectores estratégicos en donde cada organismo encargado de sector debe identificar los correspondientes ACN. Estos sectores incluyen Administración, Espacio, Industria Nuclear, Industria Química, Instalaciones de Investigación, Agua, Energía, Salud, Tecnologías de la Información y Comunicaciones, Transporte, Alimentación, Sistema Económico y Financiero. A su vez España divide sus ACN como infraestructuras estratégicas y críticas.

- Infraestructura estratégica son las instalaciones, redes, sistemas, equipos físicos y tecnología de la información de los que depende el funcionamiento de los SSPPEE.
- Infraestructura crítica son aquellas instalaciones estratégicas cuya operatividad resulta indispensable y no permite otras alternativas, para el funcionamiento de los SSPPEE (BOE, 2018).

2.3.2 – Las agresiones a los ACN y los posibles agresores

Como señala Uzal (2017), "los componentes de la Infraestructura Crítica de un estado nación constituyen blancos potenciales y altamente valorados por diversos tipos de organizaciones ciberterroristas." Las plantas e instalaciones modernas disponen de sistemas de

producción y de control automatizados, resultando fundamental el papel que cumplen los Controladores de Lógica Programable (PLC[10], por su sigla en inglés) y los Sistemas de Supervisión, Control y Adquisición de Datos (SCADA[11], por su sigla en inglés), los cuales a su vez constituyen elementos vulnerables dentro de las infraestructuras críticas.

- Un PLC es una computadora de uso específico, la cual es empleada para el control en los procesos automatizados de naturaleza electromecánica (por ejemplo el control de la maquinaria de una instalación o en líneas de montaje).
- Un SCADA es un software de control de producción, el que intercomunicado con los diferentes componentes de la instalación, permite el control de todo el proceso, brindando información en tiempo real a los operadores.

Ambos interactúan entre sí, permitiendo el SCADA el gerenciamiento integral de una instalación a partir de los datos provenientes de los PLC instalados.

Los ciberataques buscan afectar el funcionamiento normal de los PLC y los SCADA[12]. Mediante la modificación de los programas de los PLC de una instalación se logra distorsionar el funcionamiento de determinados componentes electromecánicos de la misma (por ejemplo calderas, centrifugadoras, transformadores, etc.) sometiéndolos a condiciones de funcionamiento anormales que lleven a su explosión, rotura, incendio o cualquier otra forma de degradación. Esta acción hostil sobre los PLC se complementa con una acción similar sobre los SCADA, de forma que el sistema de información muestre en sus pantallas datos falsos, que oculten el ataque que está teniendo lugar, y en cambio simulen que el funcionamiento de la instalación se está realizando en condiciones operativas normales[13] (Uzal, 2017) (The Economist, 2010).

[10] Programmable Logic Controller.

[11] Supervisory Control and Data Adquisition.

[12] Si bien los ciberataques a los ACN no pueden impedirse, Uzal (2017) señala que es posible mitigar sus efectos a través de la adopción de una serie de medidas como ser *firewalls*, *honey pots*, o Sistemas de Detección de Intrusiones (IDS). El *firewall* es un filtro que controla las comunicaciones que pasan de una red a otra, y que en virtud de su configuración, permite o impide el paso del flujo. Una subred que ha sido aislada por firewalls recibe el nombre de Zona Desmilitarizada (DMZ, por su sigla en inglés) y en ella se ubican los servidores críticos de la instalación. Los *honey pots* son sistemas de información falsos (también llamados "*sistemas señuelos*") que buscan confundir a los agresores acerca de la ubicación de los verdaderos sistemas de información, atrayendo los ciberataques y facilitando su detección y eventual identificación de los perpetradores. Los IDS se ubican en la Intranet del ACN (también llamada Red de Área Local o LAN) con la finalidad de monitorear todo el tráfico en la red, buscando detectar patrones anormales o sospechosos y dar una alerta temprana, logrando reducir el riesgo de ataques.

[13] Un ejemplo típico del desarrollo y los riesgos de un ciberataque sobre ACN lo constituyó el ataque del año 2010 con virus Stuxnet sobre la infraestructura nuclear de Irán. Inicialmente el virus fue introducido por una persona, utilizando un pen drive USB, en una o varias de las computadoras de las instalaciones del programa nuclear iraní. Una vez dentro del sistema, el virus escaneó todas las computadoras con sistema operativo Windows que estaban conectadas a la red en busca de los PLC que controlaban las centrifugadoras. En este caso, el PLC que fue blanco del ataque, era aquel que controlaba la velocidad de las centrifugadoras. Luego de infectar los PLC, el virus permaneció latente e indetectable durante casi un mes, replicándose a sí mismo y permitiendo a los hackers hacerse con el control de las centrifugadoras y obtener información acerca de la operación normal del sistema. Con las centrifugadoras fuera de control, Stuxnet reprodujo los datos de su funcionamiento normal en el SCADA, engañando a los operadores iraníes acerca del funcionamiento real de los sistemas. Así el virus permaneció indetectado durante meses para los operadores de la fábrica, en tanto que las centrifugadoras se autodestruían gradualmente. Stuxnet resultó tan bien diseñado que incluso cuando los operadores de las centrifugadoras se percataron de que las cosas estaban fuera de control, un código les impidió el apagado de las máquinas. Finalmente y luego de varios meses, debido a las tensiones extremas

En la actualidad, los vacíos legales en lo relacionado con el uso del ciberespacio, así como la indefinición respecto de las actividades criminales,

> […] es aprovechado por países o grupos con un gran desarrollo en cuestión de cibercomandos, ciberguerra y ciberespionaje, para que desde el anonimato y a través del ciberespionaje o ciberataques, tomen información sensible de países u organismos antagónicos o causen daño a la infraestructura crítica para obtener o incrementar su poder económico, tecnológico o militar (García et al, 2016, p. 201).

Hoy el ciberespacio es un campo de batalla más[14].

2.4 – La defensa de los ACN contra los ciberataques

La defensa informática debe tener como principal objetivo la defensa de los datos, los cuales se hallan en toda la infraestructura crítica pública y privada, debido a los serios trastornos a la seguridad nacional en los diferentes planos que puede generar su afectación (Artiga, 2016). En teoría cada Estado se da sus propios estándares de ciberseguridad, los cuales son determinados por la legislación aplicable a través de directivas, políticas, normas, instrucciones, regulaciones y procedimientos para asegurar la preservación de los datos cumpliendo con los requisitos de confidencialidad, integridad y disponibilidad de la información.[15] Actualmente en el campo de la protección de los ACN, lo difícil es determinar qué defender más que cómo defenderlo, de ahí la necesidad de determinar cuál es la infraestructura crítica que resulta vital para el normal funcionamiento del país.

Los bajos estándares en los procedimientos de ciberseguridad en un entorno complejo de redes y comunicaciones amplio y abierto facilitan que un equipo de hackers competente, trabajando para un Estado u organización, tengan altas probabilidades de éxito, particularmente cuando el blanco son por ejemplo, las redes de energía eléctrica (Saavedra, 2016). El sector energético en general, y particularmente las plantas de generación y las redes de distribución eléctrica, constituyen tal vez el sector más sensible de cualquier sociedad moderna, debido a los efectos en cascada que cualquier disfunción puede llegar a generar. En caso de ocurrencia de un ataque de estas características el mismo supondrá una afectación mayor a la seguridad nacional caracterizada por pérdidas humanas, distorsiones en la vida de las personas por la paralización o degradación de los SSPPEE, problemas de seguridad pública y enormes perjuicios a las actividades económico-financieras y productivas.

---

a que fueron sometidas, cerca de 1.000 centrifugadoras del programa nuclear de Irán se desintegraron. Todavía hoy se desconoce con certeza quién o quiénes fueron responsables de la creación de Stuxnet, pero las pruebas apuntan a grupos de hackers trabajando para Israel y los EEUU. La empresa de seguridad Symantec considera que se habrían utilizado entre 5 y 10 expertos en software, durante un período de aproximadamente 6 meses (Holloway, 2015) (BBC, 2015) (ABC, 2017).

[14] Actualmente cualquier operación militar es precedida y se realiza simultáneamente con actividades de ciberespionaje y una serie de ciberataques a los sistemas de comando, comunicaciones, control e inteligencia y a la infraestructura crítica del enemigo, buscando afectar su capacidad de combatir y la moral de su población.

[15] Confidencialidad para preservar las restricciones establecidas en restricciones de acceso y divulgación de la información, incluyendo medios para la protección de la propiedad y confidencialidad de la información. Integridad para proteger la información contra la modificación y/o destrucción no autorizada y garantizar la autenticidad de la misma. Disponibilidad buscando asegurar el acceso seguro, confiable y a tiempo a la información y al uso de la misma (DoE, 2012).

Todavía no existe conciencia cabal de los riesgos que suponen los diferentes tipos de ciberamenazas a la seguridad nacional. Los cambios en el medio ambiente estratégico y en el campo de las TIC han sido tan grandes y acelerados que los actores públicos y privados no han evaluado sus efectos ni medido sus consecuencias. La defensa contra un ciberataque es una tarea que debe ser desarrollada en forma conjunta por el Gobierno Nacional y el sector privado de la sociedad y las estrategias de ciberseguridad "apuntan tanto a la protección de la sociedad contra las ciberamenazas perjudiciales, como al refuerzo del desarrollo social y económico, a partir de un entorno seguro de tecnologías de la información y comunicaciones" (Parraguez, 2017).

2.5 – Caso de la ROU: una breve aproximación

2.5.1 – El marco jurídico-legal

En el año 2010 fue aprobada la Ley 18.650, Ley Marco de Defensa Nacional (LMDN) de nuestro país. La misma fue complementada en el año 2014, por el Decreto 105/014, el cual aprobó la Política de Defensa Nacional (PDN). Este último documento define el escenario estratégico actual y el futuro, determina los Intereses Nacionales (IINN), y a partir de éstos incluye los objetivos permanentes y estratégicos de la Defensa Nacional (DN) y los posibles obstáculos a enfrentar en su materialización. Dentro de los obstáculos se menciona el Crimen Organizado y dentro de éste se incluyen:

> […] delitos como el narcotráfico, tráfico ilegal de armas, el lavado de activos, la trata de personas, la corrupción y los ataques cibernéticos, entre otros". Posteriormente se establece como obstáculo para los objetivos de la DN la "materialización del espionaje y los ataques cibernéticos (Poder Ejecutivo, 2014).

También se establece a texto expreso que:

> En la actualidad se da en forma reiterada el espionaje por parte de Empresas, Organismos o estados extra-regionales a los gobiernos de la región, las empresas públicas, así como a empresas privadas u organismos de la sociedad civil con el fin de captar ilícitamente información para obtener ventajas económicas y el control político, militar o social, en el plano estratégico de los países (Poder Ejecutivo, 2014).

Finalmente, en el mismo sentido, este decreto establece como lineamiento estratégico "Proteger al Uruguay de ataques cibernéticos y preservar la reserva de datos producto de la gestión estatal y privada, tanto a nivel nacional como regional, en cuanto esta última corresponda" (Poder Ejecutivo, 2014).

2.5.2 – La arquitectura de ciberseguridad de la ROU

La responsabilidad de la conducción de la ciberseguridad en nuestro país recae en la Presidencia de la República, y dentro de ella, específicamente en la Agencia de Gobierno Electrónico y Sociedad de la Información (AGESIC)[16]. Su brazo operativo lo constituye el

[16] La estructura comprende un Consejo Directivo Honorario, una Dirección Ejecutiva (conformada por el Director Ejecutivo y la Directora Adjunta) del cual dependen cinco Consejos Asesores. Por debajo existen cinco áreas operativas (Seguridad de la Información; Organismos y Procesos; Servicios de Apoyo; Ciudadanía Digital; Tecnología y una Secretaría General (Poder Ejecutivo, 2006). El organismo fue creado en el año 2005 a través de la Ley 17.930 y reglamentado por el Decreto en el año 2006 por el Decreto 205/006 (Camps, 2016) (Poder Legislativo, 2005). Este

Centro de Respuesta de Incidentes de Seguridad Informática del Uruguay (CERTuy), el cual tiene por misión "Proteger los activos de información críticos del Estado y promover el conocimiento en seguridad de la información de manera de prevenir y responder a incidentes de seguridad" (CERTuy, 2018a).[17] Dependiendo del CERTuy se hallan los Equipos de Respuesta a Incidentes de Seguridad Informática (CSIRT - *Computer Security Incident Response Team*). [18]

En lo que refiere a incidentes informáticos, en el primer semestre de 2017 se atendieron un total de 457, lo que supone un incremento del 9% respecto de igual período del año anterior. El aumento de los incidentes pudo haberse debido a la existencia de nuevos sistemas de detección, y al aumento en la confianza en el CERTuy por parte de los miembros de las comunidades objetivo (CERTuy, 2018b). El siguiente gráfico representa los porcentajes por categorías de los incidentes.

organismo participa en la formulación de políticas en materia información, conocimiento y desarrollo informático, liderando la estrategia de implementación de Gobierno Electrónico como base de un estado eficiente y centrado en el ciudadano, impulsando la sociedad de la información y del conocimiento y el buen uso de las TIC (Poder Legislativo, 2006). AGESIC realiza diversas actividades de capacitación teniendo como brazo operativo en ciberseguridad al Centro de Respuesta de Incidentes de Seguridad Informática del Uruguay (CERTuy - *Computer Emergency Response Team – Uruguay)*

[17] Dentro de las tareas del CERTuy se destacan el prevenir y responder a incidentes de seguridad informática; proponer y asesorar normas y procedimientos de seguridad; brindar alertas informáticos; coordinar los planes de recuperación y realizar los análisis post ataques; fomentar las buenas prácticas y la creación de Equipos de Respuesta ante Incidentes de Seguridad Informática (CSIRT); interacción con organismos similares de otros Estados (Poder Ejecutivo, 2009a) (Poder Ejecutivo, 2009b) (CERTuy, 2018a). Este centro está conformado por un grupo de expertos responsables del desarrollo de medidas preventivas y reactivas ante incidencias de seguridad en los sistemas de información. Dentro de la comunidad objetivo del CERTuy se encuentran el gobierno, salud, orden público, servicios de emergencia, energía, telecomunicaciones, transporte, suministro de agua potable, ecología y ambiente, agro-industria, banca y servicios financieros, y en general cualquier sector que afecte a más de un 30% de la población (CERTuy, 2018a).

[18] Los CSIRT corresponden a las diferentes comunidades objetivo, y dentro de sus servicios hallamos algunos de naturaleza reactiva (alertas y manejo de incidentes) y otros proactivos (anuncios, detección de incidentes, y desarrollo de técnicas y herramientas); asimismo, brindan capacitación y entrenamiento, análisis de riesgos, consultorías en seguridad y actividades de concientización de la comunidad en temas de seguridad informática (CSIRT-ANTEL, 2018). En función de su misión, en caso de incidentes informáticos, el CERTuy coordina con el CSIRT – ANTEL, el CSIRT del Ministerio de Defensa Nacional (MDN) o con otros equipos de respuesta del sector público o privado (Camps, 2016).

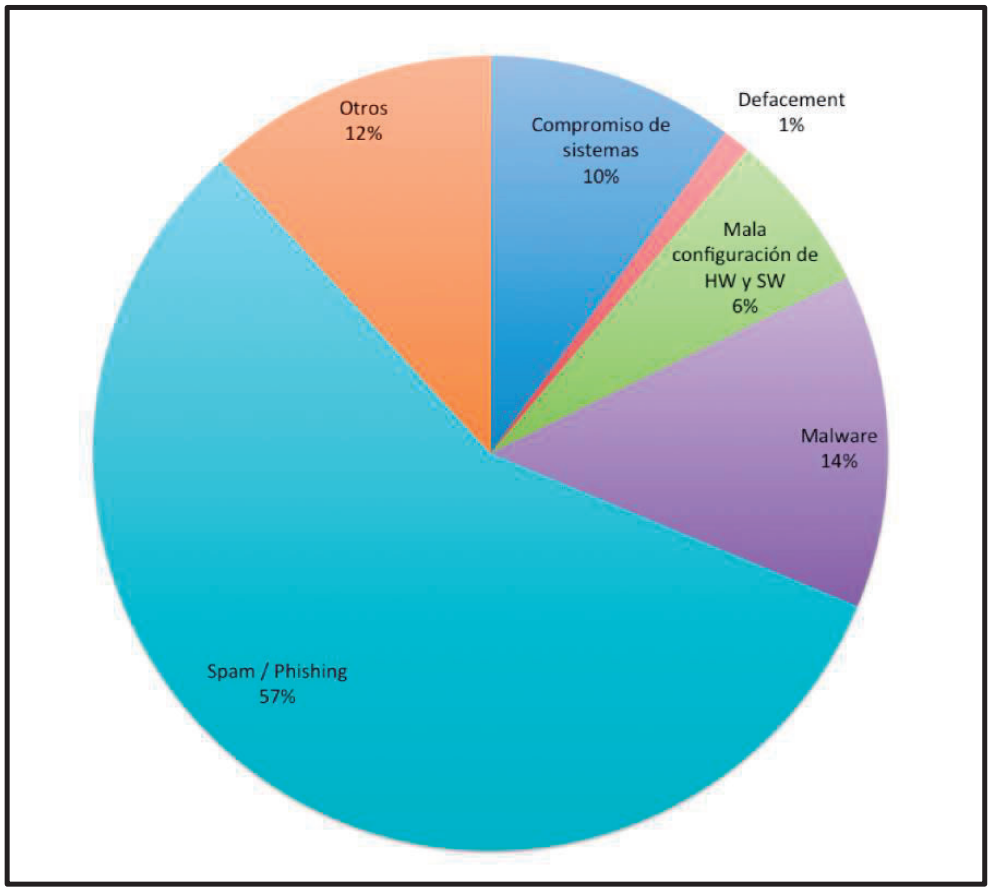

Figura 1 Discriminación de incidentes informáticos en la ROU durante el primer semestre del año 2017. CERTuy

2.5.3 – Planes y estado del arte en ciberseguridad y protección de ACN

La ROU incluyó a la ciberseguridad/ciberdefensa en su PDN aprobada en el año 2014, pero comenzó a desarrollar la estructura organizacional para poder enfrentar incidentes informáticos a partir del año 2008 con la creación del Centro Nacional de Respuesta a Incidentes de Seguridad Informática (CERTuy)[19]. Actualmente no se posee una Estrategia Nacional de Ciberseguridad, pero se está trabajando en ella, existiendo los recursos humanos, los organismos y los marcos legales para poder desarrollarla[20].

[19] El CERTuy fue creado en el año 2008 a través de la Ley 18.362. Dicha ley le asigna las tareas de prevención y respuesta en caso de incidentes informáticos. Con posterioridad, en el año 2009 el Decreto 451/009 reglamenta la citada ley y define las responsabilidades del CERTuy (Camps, 2016).

[20] A los efectos de poder desarrollar el Plan Estratégico de Protección de ACN capaz de integrarse a una Estrategia Nacional de Ciberseguridad, existe una serie de actividades mínimas a ser desarrolladas:

- Creación de un Centro Nacional para la Protección de los ACN.
- Definir los ACN y su grado de importancia crítica desde el punto de vista de la seguridad nacional.
- Realizar un Estudio de Seguridad de cada ACN.
- Designación de un Responsable de Seguridad y Enlace por cada ACN.
- Determinar las amenazas, vulnerabilidades y riesgos de cada ACN.
- Desarrollar planes generales y de contingencia en los diferentes niveles para la actuación antes, durante y después de una crisis. Como mínimo los planes deberían comprender:

Recientemente el Banco Interamericano de Desarrollo (BID) llevó a cabo un estudio sobre el estado de la madurez en seguridad cibernética en América Latina y el Caribe, sobre la base de cinco áreas y cuarenta y nueve indicadores. Las cinco áreas incluyeron: política y estrategia de seguridad cibernética; cultura cibernética y sociedad; educación, formación y competencias en seguridad cibernética; marco jurídico y reglamentario; normas, organizaciones y tecnologías.

Cada uno de los indicadores fue evaluado individualmente para cada país de la región, contando con cinco niveles de madurez: inicial, formativo, establecido, estratégico y dinámico, siendo puntuados de 1 a 5. En este estudio del BID la ROU fue muy bien evaluada en las diferentes áreas, siendo uno de los países pioneros de la región a este respecto, presentando una serie de vulnerabilidades que deberían ser corregidas a la brevedad es especial en lo que respecta a:

- Desarrollo de la correspondiente estrategia nacional, con énfasis en lo que refiere a contenidos y a la estrategia de defensa cibernética.
- En materia legal, en lo que se relaciona con el derecho sustantivo y procesal de ciberdelincuencia, donde existen carencias importantes.
- Adhesión a las normas, poniendo especial atención en lo que refiere a su aplicación por los operadores y a la existencia de un conjunto de normas y prácticas mínimas aceptables.
- Protección de infraestructura crítica, destacándose todo lo relacionado con la identificación, organización, coordinación y gestión de riesgos.
- Gestión de crisis, poniendo acento en la planificación (donde existen vacíos importantes) y evaluación.
- Mejoramiento de las tecnologías de seguridad cibernética.

La ROU debe determinar en primer lugar cuáles son sus ACN necesarios para su seguridad nacional, y en segundo lugar, desarrollar la necesaria planificación estratégica que contemple aquello que debe ser protegido y que acciones deben ser realizadas en caso de ataque. Como señala Camps (2016), si bien la ROU carece de:

> una estrategia de ciberseguridad nacional, ha sido evaluado positivamente en un reciente informe conjunto del Banco Interamericano de Desarrollo y la Organización de Estados Americanos. De igual forma se carece de una organización conjunta a nivel Fuerzas Armadas que tenga como cometido específico repeler ataques cibernéticos que afectan la seguridad nacional o eventualmente realizarlos como respuesta a un ataque anterior (p. 276).

3 – Conclusiones

La tecnología informática nos ha dado la posibilidad de resolver un sinfín de tareas cotidianas de una manera práctica y veloz, ocupando cada vez mayores espacios en la vida comunitaria. Esta "*sociedad de la información*" a la par de generar oportunidades, genera

- Plan Estratégico de Protección de ACN.
- Planes Estratégicos Sectoriales.
- Planes de Seguridad del Operador.
- Planes de Protección Específicos a cada ACN.
- Planes de Crisis y de Apoyo Operativo para cada ACN.

riesgos y amenazas, los cuales son directamente proporcionales al grado de dependencia digital de esa sociedad. Es en este entorno donde se llevan a cabo actividades ilícitas de naturaliza diversa por parte de actores estatales, organizaciones e individuos que pueden afectar los ACN, vulnerando nuestra seguridad nacional y generando perjuicios de diferente naturaleza y gravedad a la sociedad. Los conflictos actuales se han caracterizado por el empleo cada vez más frecuente del ciberespacio como un campo de batalla. Es debido a estas ciberamenazas que los Estados deben adecuar su normativa jurídico-legal, sus organizaciones, capacidades y estrategias a los nuevos tiempos marcados por la aceleración de la globalización y un sistema internacional anárquico.

No puede existir seguridad de los ACN si no existe una política pública de ciberseguridad y no podrá existir una política pública de ciberseguridad si no existe una Cultura de Seguridad y Defensa en la sociedad. En la ROU, si bien la responsabilidad política en materia de ciberseguridad recae en los tres poderes del Estado, se destacan especialmente los roles del Ministerio del Interior y Ministerio de Defensa Nacional, tal cual lo establece el Decreto 105/014 que determina la Política de Defensa Nacional de la República, alineado con la LMDN Nro. 18.650.

En lo que refiere específicamente a nuestro país, se desprenden una serie de consideraciones. En primer lugar, la ROU, aún con las carencias constatadas, se encuentra mucho mejor preparada en materia de protección de ACN/IRRC que la mayoría de los países de la región. En segundo lugar, para mantener y consolidar la anterior condición se estima necesario:

- Incrementar la formación de recursos humanos altamente especializados para trabajar en el campo de las TIC.
- Incrementar la formación de los niños y jóvenes en su paso por el Sistema Educativo Nacional (SEN) en el dominio de las habilidades y destrezas informáticas.
- Actualizar y completar la legislación vigente.
- Continuar desarrollando la infraestructura nacional de comunicaciones e informática.
- Potenciar los mecanismos de ciberseguridad de los ACN y de respuesta ante incidentes informáticos.

En tercer lugar, a partir de los recursos humanos, materiales y económicos a disposición de los actores públicos y privados, es necesario proceder a la formulación de políticas, programas y proyectos que permitan diseñar una Estrategia Nacional de Ciberseguridad integral, capaz de prevenir o minimizar las vulnerabilidades señaladas en los obstáculos y amenazas a los OONN definidos por la Política de Defensa Nacional.

Con el tiempo necesario, recursos económicos, contactos personales y adecuada motivación, un adversario decidido siempre será capaz de penetrar cualquier sistema. Si bien hasta el momento los grupos terroristas han utilizado las TIC fundamentalmente para propaganda y comunicaciones, y por incapacidad o por decisión propia no han llevado a cabo ciberataques contra ACN, esta situación podría variar en el corto o mediano plazo en virtud de la óptima ecuación costo-beneficio que supone un ataque de esta naturaleza.

Referencias

ABC. (2017, 13 de Mayo). The internet of hacked things. Recuperado de http://www.abc.net.au/news/2015-10-07/four-corners-internet-of-hacked-things/7778954

Artiga, R. (2016). El Ciberespacio y la Seguridad Nacional en El Salvador. En J. Rodriguez Pinto (Ed), *Ciberdefesa e Ciberseguranca: Novas Ameacas a Seguranca Nacional*. (P 99-129). Río de Janeiro, Brasil: ESG.

Baltodano, E. (2010). Malware: Software malicioso. En J. Villasuso (Ed). *Ciberseguridad en Costa Rica.* (P 268-274) San Jose, Costa Rica: Universidad de Costa Rica.

BBC. (2015, 11 de Octubre). El virus que tomó el control de mil máquinas y les ordenó autodestruirse. Recuperado de https://www.bbc.com/mundo/noticias/2015/10/151007_iwonder_finde_tecnologia_virus_stuxnet

BID (2016). *Ciberseguridad: ¿estamos preparados en América Latina y el Caribe?* Recuperado de https://www.agesic.gub.uy/innovaportal/file/5396/1/ciberseguridad-estamos-preparados-en-america-latina-y-el-caribe.pdf

Boletín Oficial del Estado (BOE) de España (2018). *Ley de Protección de Infraestructuras Críticas PIC 8/2011, Real Decreto 704/2011*.

Recuperado de https://www.boe.es/buscar/pdf/2011/BOE-A-2011-7630-consolidado.pdf

Camps, P. (2016). Ciberdefensa y Ciberseguridad: Nuevas Amenazas a la Seguridad Nacional, estructuras nacionales de ciberdefensa, estrategias de ciberseguridad y cooperación interagencias en este ámbito. En J. Rodriguez Pinto (Ed). *Ciberdefesa e Ciberseguranca: Novas Ameacas a Seguranca Nacional*. (P 265-278). Río de Janeiro, Brasil: ESG.

Carozo, E. (2013). Centro de respuesta de incidentes informáticos. ¿Para qué? *Revista de Seguridad*.

Recuperado de https://revista.seguridad.unam.mx/numero-16/centro-de-respuesta-incidentes-inform%C3%A1ticos-para-qu%C3%A9

Carozo, E., Martínez, C. , Vidal, L. , Betarte, G. , Blanco, A. , Cota, E. , Pérez, J. (2006). *CERTuy: Hacia un CSIRT Nacional*.

Recuperado de https://iie.fing.edu.uy/eventos/telcom2006/trabajos/mvdtelcom-013.pdf

Centro Argentino para las Relaciones Internacionales (CARI). (2013). *Ciberdefensa-Ciberseguridad. Riesgos y amenazas.*

Recuperado de http://www.cari.org.ar/pdf/ciberdefensa_riesgos_amenazas.pdf

CERTuy (2018a). *Qué es el CERTuy?*

Recuperado de https://www.cert.uy/inicio/institucional/que_es_el_cert/

CERTuy (2018b). *Estadisticas de incidentes en el primer semestre de 2017*.

Recperado de

https://www.cert.uy/inicio/novedades/alertas_y_vulnerabilidades/estadisticas+de+incidentes+en+el+primer+semestre+de+2017

CSIRT-ANTEL (2018). *Servicios del CSIRT de ANTEL*.

Recuperado de http://www.csirt-antel.com.uy/node/4

Department of Defense (DoD) (2015). *The DoD Cyber Strategy*. Washington, USA: Autor.

Department of Defense.(DoD) ((2016). *JP 1-02 Dictionary of Military and Associated Terms*. Washington, USA: Autor.

Department of Energy (DoE). (2012). *DOE/OE-0003 Electricity Subsector Cybersecurity Risk Management Process*.

Recuperado de https://www.energy.gov/sites/prod/files/Cybersecurity%20Risk%20Management%20Process%20Guideline%20-%20Final%20-%20May%202012.pdf

Diaz, H (2018). Capítulo 2: Infraestructura crítica vulnerable a la ciberguerra. En Centro de Estudios Estrategicos de la Academia de Guerra de Chile (Ed), *La Ciberguerra. Sus impactos y desafíos*. (P 45-59). Santiago de Chile, Chile: Academia de Guerra.

El Comercio (2018, 19 de Setiembre). ¿Cuál es la diferencia entre un hacker y un cracker?

Recuperado de https://elcomercio.pe/tecnologia/actualidad/diferencia-hacker-cracker-noticia-490674

El Mundo (2013, 20 de Marzo). La OTAN pone en su punto de mira a los 'hacktivistas' como objetivos militares.

Recuperado de http://www.elmundo.es/elmundo/2013/03/20/navegante/1363780082.html

El Observador (2017, 16 de Mayo). Detectan posible vínculo de Corea del Norte con ciberataques masivos. Recuperado de https://www.elobservador.com.uy/detectan-posible-vinculo-corea-del-norte-ciberataques-masivos-n1071692

Europol (2018). *Terrorism Situation and Trend Report*.

Recuperado de https://www.europol.europa.eu/activities-services/main-reports/european-union-terrorism-situation-and-trend-report-2018-tesat-2018

García, J. y Mondragón, J. (2016). La Ciberseguridad y Ciberdefensa en el contexto de México. En J. Rodriguez Pinto (Ed). *Ciberdefesa e Ciberseguranca: Novas Ameacas a Seguranca Nacional*. (P 178-206). Río de Janeiro, Brasil: ESG.

Hirane, C. (2016). Ciberespacio. Bien Publico Mundial en tiempos de globalización: Política pública de ciberseguridaduna necesidad imperiosa y la Ciberdefensa como desafío del Siglo XXI. En J. Rodriguez Pinto (Ed). *Ciberdefesa e Ciberseguranca: Novas Ameacas a Seguranca Nacional*. (P 41-79). Río de Janeiro, Brasil: ESG.Holloway, M. (2015). *Stuxnet Worm Attack on Iranian Nuclear Facilities*.

Recuperado de http://large.stanford.edu/courses/2015/ph241/holloway1/

Homeland Security (2018a). *Critical Infrastructure Sectors*.

Recuperado de https://www.dhs.gov/critical-infrastructure-sectors

Homeland Security. (2018b). *National Infrastructure Protection Plan*.

Recuperado de https://www.dhs.gov/national-infrastructure-protection-plan

IMPO. (2006). *Decreto 205/006 Funcionamiento de la AGESIC*.

Recuperado de https://www.impo.com.uy/bases/decretos/205-2006

Interpol (2016). *Informe Anual de 2016*. Recuperado de https://www.interpol.int/es/Centro-de-prensa/Publicaciones2/Informes-anuales/2016

Joint Chief of Staff (2018). *JP 3-12 Cyberspace Operations*. Washington DC, USA: Autor.

Joyanes, L. (2010). Introducción. Estado del Arte de la Ciberseguridad. En Ministerio de Defensa (Ed). *Cuaderno de Estrategia Nro 149. Ciberseguridad. Retos y amenazas a la Seguridad Nacional en el Ciberespacio*. (P 13-46). Madrid, España: Ministerio de Defensa.

Koble, M. (2018). *La diferencia entre el phishing y spoofing*.

Recuperado de https://techlandia.com/diferencia-phishing-spoofing-info_241711/

Leiva, R (2018). Capítulo 1: Aparece la Ciberguerra. En Centro de Estudios Estrategicos de la Academia de Guerra de Chile (Ed), *La Ciberguerra. Sus impactos y desafíos*. (P 23-44). Santiago de Chile, Chile: Academia de Guerra.

Marowsky, C. (2018). Capítulo 5: Efectos de los riesgos y amenazas de la ciberguerra en la infraestructura crítica. En Centro de Estudios Estrategicos de la Academia de Guerra de Chile (Ed), *La Ciberguerra. Sus impactos y desafíos*. (P 107-128). Santiago de Chile, Chile: Academia de Guerra.

Martin, G. (2016). *Understanding Terrorism. Challenges, Perspectives, and Issues*. London, United Kingdom: Sage.

Martin, P. (2015). *Inseguridad cibernética en América Latina: Líneas de reflexión para la evaluación de riesgos*.

Recuperado de http://www.ieee.es/Galerias/fichero/docs_opinion/2015/DIEEEO79-2015_InseguridadCibernetica_AmericaLatina_PaulE.Martin.pdf

McAfee (2018). *Threat Landscape Dashboard*.

Recuperado de https://www.mcafee.com/enterprise/en-us/threat-center/threat-landscape-dashboard.html

Ministerio de Defensa (2010). *Cuaderno de Estrategia Nro 149. Ciberseguridad. Retos y amenazas a la Seguridad Nacional en el Ciberespacio.* Madrid, España: Autor.

National Institute of Standards and Technology (NIST). (2018). *Framework for Improving Critical Infrastructure Cybersecurity*.

Recuperado de https://doi.org/10.6028/NIST.CSWP.04162018

OWASP. (2016). *Ingeniería social: hacking psicológico*.

Recuperado de https://www.owasp.org/images/2/27/02_INGENIER%C3%8DA_SOCIAL.pdf

Parraguez, L. (2017). *The State of Cybersecurity in Mexico: An Overview.*

Recuperado de https://www.wilsoncenter.org/publication/the-state-cybersecurity-mexico-overview

Poder Ejecutivo. (2017). *Decreto Supremo que aprueba el Reglamento para la Identificación, Evaluación y Gestión de Riesgos de los Activos Críticos Nacionales (ACN). Nro 106-2017-PCM*.

Recuperado de https://busquedas.elperuano.pe/normaslegales/decreto-supremo-que-aprueba-el-reglamento-para-la-identifica-decreto-supremo-n-106-2017-pcm-1585361-1/

Poder Ejecutivo. (2014). *Decreto 105/014. Política de Defensa Nacional*.

Recuperado de https://www.impo.com.uy/bases/decretos/105-2014

Poder Ejecutivo (2009a). *Decreto 451/009 Funcionamiento y organización del CERTuy*. Recuperado de https://www.agesic.gub.uy/innovaportal/v/298/1/agesic/decreto-n%C2%B0-451_009-del-28-de-setiembre-de-2009.html

Poder Ejecutivo (2009b). *Decreto 452/009. Política de Seguridad de la Información*. Recuperado de https://www.agesic.gub.uy/innovaportal/v/299/1/agesic/decreto-n%C2%B0-452_009-de-28-de-setiembre-de-2009.html

Poder Legislativo (2010). *Ley 18.650. Ley Marco de Defensa Nacional*.

Recuperado de https://legislativo.parlamento.gub.uy/temporales/leytemp6292733.htm

Poder Legislativo (2005) *Ley 17.930. Creación de AGESIC*.

Recuperado de http://agesic.gub.uy/innovaportal/v/700/1/agesic/creacion_de_agesic.html

Saavedra, B (2017). *Big Data. Too big to ignore for Latin America and the Caribbean*. Washington DC, USA: CHDS.

Saavedra, B. (2016). *Critical infrastructure in Latin America: connected, dependent, and vulnerable*. Washington DC, USA: CHDS.

Saavedra, B. (2015). *Cybersecurity in Latin America and the Caribbean: the state of readiness for the defefnse of cyberspace.* Washington DC, USA: CHDS.

Symantec. (2018). *Resumen Ejecutivo. Informe Sobre Amenazas para la Seguridad en Internet.*

Recuperado de https://www.symantec.com/content/dam/symantec/mx/docs/reports/istr-23-executive-summary-mx.pdf

The Economist (2010). War in the Fifth Domain. *Autor*.

Recuperado de https://www.economist.com/briefing/2010/07/01/war-in-the-fifth-domain

The White House. (2018). *Presidential Policy Directive / PPD-21-- Critical Infrastructure Security and Resilience.* Recuperado de https://obamawhitehouse.archives.gov/the-

press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resilience

The White House (2013). *Executive Order 13636 of February 12, 2013 Improving Critical Infrastructure Cybersecurity.*

Recuperado de https://www.gpo.gov/fdsys/pkg/CFR-2014-title3-vol1/pdf/CFR-2014-title3-vol1-eo13636.pdf

Uzal, R. (2017). *Ciberterrorismo: Aportes para la protección de infraestructura crítica*. Recuperado de http://espacioestrategico.blogspot.com/2017/03/ciberterrorismo-aportes-para-la.html

Uzal, R. (2015). *El Problema de la Ciber Atribución: Aportes para una estrategia de Ciber Defensa*.

Recuperado de http://www.cari.org.ar/pdf/boletin61.pdf

Wikipedia. (2018a) *Rootkit.* Recuperado de https://es.wikipedia.org/wiki/Rootkit

Wikipedia. (2018b) *Programa espía*.

Recuperado de https://es.wikipedia.org/wiki/Programa_esp%C3%ADa

Wikipedia. (2018c). *Cookies (informática).*

Recuperado de https://es.wikipedia.org/wiki/Cookie_(inform%C3%A1tica)

Wikipedia. (2018d). *Phising*. Recuperado de https://es.wikipedia.org/wiki/Phishing

Wikipedia (2018e). Suplantación.

Recuperado de https://es.wikipedia.org/wiki/Suplantaci%C3%B3n

Wikipedia. (2018f). *Ataque de denegación de servicios*.

Recuperado de https://es.wikipedia.org/wiki/Ataque_de_denegaci%C3%B3n_de_servicio

LA PROTECCIÓN DE INFRAESTRUCTURAS CRÍTICAS O ESTRATÉGICAS, ¿RESPONSIBILIDAD DE SEGURIDAD PÚBLICA O DE DEFENSA NACIONAL?

Mario Moreira[1]

RESUMEN

En la República Oriental del Uruguay, en los últimos años hemos asistido a la discusión dicotómica de responsabilidades, en las que tareas que son propias de la Defensa Nacional empiezan a ser asignadas a Seguridad Pública. La protección de Infraestructura crítica o estratégica no escapa a esta discusión.

El presente trabajo pretende incorporar un punto de vista a esta discusión, sobre la base del análisis normativo y estratégico. Luego de identificar estas diferencias, el trabajo citará una infraestructura crítica relacionada con la Ciberseguridad a ser protegida.

Palabras clave: Estratégica, Crítica, Defensa Nacional, Seguridad Pública.

Hacia una definición de Infraestructura crítica

El presente trabajo es orientado conceptualmente en la definición de la Ley de Protección de Infraestructura Estratégica en España, la cual determina que son:

Infraestructuras estratégicas: las instalaciones, redes, sistemas y equipos físicos y de tecnología de la información sobre las que descansa el funcionamiento de los servicios esenciales;

E **Infraestructuras críticas:** las infraestructuras estratégicas cuyo funcionamiento es indispensable y no permite soluciones alternativas, por lo que su perturbación o destrucción tendría un grave impacto sobre los servicios esenciales (B.O.E. 102, 2011, Art. 2).

1 Coronel del Arma de Ingenieros del Ejército de Uruguay. Diplomado en Estado Mayor, con especialización y cursos en Defensa realizados en la Escuela de Defensa de Argentina y el Centro William Perry de Estados Unidos. Instructor de Estrategia, Licenciado en Ciencias Militares, Magíster en Educación, Magíster en Estrategia Nacional.

El enfoque normativo

En la R.O.U. entendemos que la "Defensa Nacional comprende el conjunto de actividades civiles y militares dirigidas a preservar la soberanía y la independencia de nuestro país, a conservar la integridad del territorio y de sus recursos estratégicos, así como la paz de la República, en el marco de la Constitución y las leyes; contribuyendo a generar las condiciones para el bienestar social, presente y futuro de la población (Ley 18.650, 2010, Art. 1). Con la promulgación de esta norma jurídica, se asignó la protección de los recursos estratégicos a la Defensa Nacional.

En la Política de Defensa Nacional fueron incluidos como Interés y Objetivo Estratégico de la Defensa Nacional, la protección de los recursos estratégicos renovables y no renovables que determine el Poder Ejecutivo; mencionándose expresamente en el Escenario Estratégico de la Defensa Nacional; que los conflictos entre estados tienden a desaparecer, aunque menciona que los recursos naturales, particularmente los energéticos darán lugar a la competición geopolítica entre Estados (Dec. 105/014, 2010, p. 17).

Es importante destacar que en la Política de Defensa Nacional, encontramos la primera aproximación a la definición de que Recursos Estratégicos son necesarios proteger, incluyéndose dentro de estos, los recursos energéticos, minerales, alimenticios, agua potable y biodiversidad (Dec. 105/014, 2010, p.25).

En la Política Militar de Defensa se coloca como objetivo estratégico para la Defensa Militar, el de emplear los medios militares para proteger la bioseguridad, los recursos naturales estratégicos renovables, no renovables y las infraestructuras críticas, a fin de asegurar las condiciones de seguridad necesarias para el desarrollo económico y social del país contemplando las seguridad jurídica de los actores económicos (Dec. 129/016, 2016, p.11).

En el año 2016, con la publicación de la Política Militar de Defensa, encontramos la primera referencia a la infraestructura crítica, dentro de los lineamientos para los cuales se decide emplear a la Defensa Militar. Este lineamiento se refiere a la integridad territorial, expresando que dentro de las acciones que llevarán a cabo las Fuerzas Armadas para asegurar la integridad territorial, se incluyen la protección de infraestructura crítica (Dec. 129/016, 2016, p.15).

En la Política Militar de Defensa se concibe a los recursos, como un sistema, es decir con los aspectos que los tornan estratégicos y sus entornos operativos. Se menciona que en el caso de los recursos naturales, el sistema se compone del recurso en sí mismo, más los medios de extracción que lo hacen explotable, las vías de comunicaciones que los hacen transportables, las industrias asociadas que lo hacen utilizable, los puertos que lo tornan comercializable, los medios de transporte que lo hacen llegar a los usuarios, el personal capacitado que hace posible la cadena de eventos anterior, entre otros (Dec. 129/016, 2016, p.17).

Asociando el concepto de Recurso Natural con un interés estratégico en una visión sistémica, podemos definir que el mismo se encuentra indisolublemente asociado a la infraestructura estratégica que permite su explotación, transporte, industrialización y transporte interno hasta llegar al usuario final.

Para la Seguridad Pública en la Ley Orgánica Policial se le asigna a la Policía Nacional como Policía Administrativa, el cometido de participar en los operativos que determinen las

autoridades competentes, en casos de grave riesgo, catástrofe o en materia de protección del medio ambiente y recursos naturales (Ley 19.135, 2015, Art. 2, Lit. h).

No existe referencia normativa a la infraestructura crítica; aunque el Decreto de Creación y Reglamentación de la Guardia Republicana, menciona dentro de las tareas asignadas a esta fuerza, la custodia de las vías de comunicaciones terrestre y otros centros de interés, encontrándose en fase de desarrollo un marco conceptual tendiente a la tarea de protección de infraestructura crítica (Dec. 259/011, 2011, Art. 2º).

Como conclusión preliminar del Marco Normativo vigente para la Defensa Nacional y la Seguridad Pública en nuestro país, podemos determinar que la protección de infraestructura estratégica y/o crítica es tarea de la Defensa Nacional, en el concepto amplio, ya que existe más de un factor del Potencial Nacional que está orientado a la protección de los mismos.

Si nos centramos exclusivamente en la dicotomía Defensa Militar/Policía Nacional, podemos determinar que es una tarea asignada normativamente a la Defensa Militar.

Acerca de la Concepción Estratégica

El presente artículo es realizado para una publicación cuya temática se orienta a la Estrategia Nacional, por lo tanto a partir de ahora el mismo se centrará en la descripción de la relación fines/medios que es necesaria para la protección de infraestructura crítica o estratégica. Es importante destacar que nuestro marco normativo, habla de infraestructura crítica y recursos estratégicos, pero no habla de infraestructura estratégica.

En una primera aproximación a la categorización de infraestructura a proteger, deberíamos considerar la diferencia que hace referencia el marco normativo español que fuera citado al inicio del artículo; donde la infraestructura estratégica está referida a las instalaciones, redes, sistemas y equipos físicos y de tecnología de la información sobre las que descansa el funcionamiento de los servicios esenciales.

Entendiéndose por servicio esencial, el servicio necesario para el mantenimiento de las funciones sociales básicas, la salud, la seguridad, el bienestar social y económico de los ciudadanos, o el eficaz funcionamiento de las Instituciones del Estado y las Administraciones Públicas (B.O.E. 102, 2011, Art. 2).

Asociada a esta definición encontramos las áreas estratégicas, siendo éstas las que producen, distribuyen o brindan un servicio esencial. En cuanto a nuestro país, el enfoque que se le da a lo que es un servicio esencial, se asocia específicamente al derecho laboral, no vinculándose áreas y/o infraestructuras críticas.

La Infraestructura Crítica desde el plexo normativo español es aquella infraestructura estratégica cuyo funcionamiento es indispensable y no permite soluciones alternativas, por lo que su perturbación o destrucción tendría un grave impacto sobre los servicios esenciales

Henry Mintzberg (1993) definía que lo estratégico está relacionado con la sustentabilidad o existencia de una organización; desde el punto de vista Estratégico Nacional si la infraestructura se encuentra asociada a reestablecer el normal funcionamiento de un servicio esencial, estamos considerando a la misma como ***"Infraestructura Estratégica"***; pero si estas

están asociadas a un servicio esencial, el cual no posee alternativas en cuanto se produzca una perturbación o destrucción, estamos hablando de ***"Infraestructura Critica"***.

Desde el punto de vista estratégico las definiciones adquieren valor en cuanto es asociada la finalidad que se persigue, con los medios que se emplean para protegerla, materializando la adecuada relación de los fines con los medios que pregona la Estrategia.

En el Art. 1 de la Ley Marco de Defensa Nacional, se establece como finalidad de la Defensa Nacional, contribuir a generar las condiciones para el bienestar social, presente y futuro de la población. En esta finalidad está presente la sustentabilidad y la existencia del objeto a proteger, integridad territorial, infraestructura crítica y estratégica; así como los recursos estratégicos vistos en forma sistémica, que permitan asegurar esa condición de bienestar social a la población.

En el concepto amplio de Defensa Nacional que se emplea en la República Oriental del Uruguay, los medios a ser empleados son el conjunto de actividades civiles y militares; aunque podríamos inferir conjunto de actividades estatales o de todos los factores del Potencial Nacional[2].

Específicamente encontramos que la Defensa Militar tiene asignada[3] la protección de infraestructura crítica, o sea aquella que está relacionada con la existencia del Estado como tal y su función de garantizar los servicios esenciales para los cuales no se poseen alternativas.

Se podría inferir que cuando se habla de infraestructura estratégica, estamos hablando de un nivel menor de importancia, donde se pone en juego la sustentabilidad del accionar del Estado como tal y consecuentemente el involucramiento de la Defensa Nacional es menor.

Si lo analizamos desde el punto de vista de la finalidad estratégica, la Seguridad Pública está relacionada con todos los instrumentos que cuenta el Estado para asegurar el desarrollo de la vida en sociedad, en la acepción de convivencia en sociedad y lo que se pretende es que no se vulnere el derecho de la persona en la acepción de seguridad ciudadana (Dec. 105/014, 2014, p.13).

Al igual que la Defensa Nacional, el concepto de Seguridad Pública en su sentido amplio emplea todos los medios con los que cuenta el Estado, para asegurar el normal funcionamiento de los servicios esenciales como salud, seguridad, bienestar social y económico.

El concepto de Seguridad Pública es asociado como finalidad al derecho de las personas y la convivencia en sociedad, lo que hace que sus medios sean empleados en la sustentabilidad del accionar del Estado.

Del análisis anterior podemos inferir que en nuestro país desde el punto de vista de la finalidad estratégica, la Seguridad Pública está orientada a asegurar la sustentabilidad del Estado en cuanto a la infraestructura estratégica que brinda los servicios esenciales, y la Defensa Nacional debería orientarse a la protección de la Infraestructura Crítica que pongan en riesgo el accionar del Estado como tal, en aquellos casos que por daño o deterioro de esa infraestructura el Estado, no se posea medios como para sustituirlo.

2 El Potencial Nacional es dividido en campos para su análisis, cuantificación y estudio. En el caso de la República Oriental del Uruguay el mismo se subdivide en cinco factores: Político, Militar, Científico Tecnológico, Psicosocial y Económico.

3 Es un lineamiento de la Defensa Militar, incluido en el Dec. 129/016, Política Militar de Defensa.

Adicionalmente desde el punto de vista estratégico, es responsabilidad de la Defensa Nacional, la protección de los Recursos Estratégicos y toda la Infraestructura Crítica o Estratégica que se encuentre relacionada con su explotación, industrialización, transporte, almacenamiento y distribución.

Acerca de la infraestructura de los recursos estratégicos y su regionalización para la Defensa Nacional

En la bibliografía que ha sido citada, se ha mencionado que los recursos estratégicos a ser protegidos por la Defensa Nacional son los recursos energéticos, minerales, alimenticios, agua potable y biodiversidad (Dec. 105/014, 2010, p.25).

El recurso natural, es considerado para la Defensa Nacional y particularmente para la Defensa Militar, categorizado como un sistema (Dec. 129/016, 2016, p.17). Asociando el concepto de Recurso Natural en una visión sistémica con un interés estratégico, podemos definir que el mismo se encuentra indisolublemente asociado a la infraestructura estratégica que permite su explotación, transporte, industrialización y transporte interno hasta llegar al usuario final.

En una visión sistémica, el objeto a proteger por la Defensa Nacional recurso e infraestructura estratégica, desde el punto de vista moderno de la geopolítica debería permitir regionalizar el espacio geográfico de nuestro territorio en sus tres dimensiones; espacio terrestre, marítimo y aéreo del Estado Uruguayo, coincidente con las áreas de responsabilidad de la Defensa Nacional, en la cual se divide el territorio de nuestro país (Ley 18.650, 2010, Art. 5). Para comenzar el análisis es necesario conceptualizar el espacio geográfico, desde la perspectiva estratégica, como un concepto de mayor amplitud, "...el espacio delimitado, con contenidos fisiográficos, biogeográficos y antropogeográficos, considerados estáticamente y en la dinámica de sus interacciones, de naturaleza política, económica, psicosocial y para la Defensa Nacional" (Campos, G., 2002, p. 228).

Desde el punto de vista geopolítico para la Defensa Nacional, surgen las siguientes regionalizaciones de recursos e infraestructuras estratégicas (Moreira, M., 2016, págs. 111-116):

Espacios geográficos dinámicos, los cuales en consonancia con la definición de espacio geográfico citada anteriormente, es sustentable política, económica, jurisdiccional y administrativamente por el Estado. Desde el punto de vista de los recursos estratégicos y la infraestructura estratégica este tipo de espacios geográficos agrupa infraestructuras que están relacionadas con la sustentabilidad del Estado desde el punto de vista energético, en cuanto que se asegura el bienestar presente y futuro de la población.

Espacios geográficos dinámicos emergentes, son aquellos espacios que son considerados a partir de la posesión de recursos, los cuales necesitan un desarrollo de infraestructura para comenzar a ser explotados. En nuestro país hace unos pocos años atrás, se realizó la proyección de la mega minería con característica de minería a cielo abierto, siendo el hierro el recurso que estaba en consideración. Toda la infraestructura proyectada y construida en función de este proyecto, debería ser caracterizada como infraestructura estratégica, siendo posicionada geográficamente en un espacio dinámico emergente.

Espacios geográficos decadentes, volviendo a la consideración dinámica del espacio geográfico, son aquellos espacios que han perdido peso relativo en función que se han abandonado por la pérdida de interés que existe en ellos. Desde el punto de vista de las infraestructuras estratégicas, aquellas que en el párrafo anterior fueron categorizadas como emergentes, al haberse abandonado el proyecto en la dinámica de la geopolítica, hoy es un espacio geográfico regionalizado como decadente, el cual contiene toda la infraestructura relacionada con el proyecto allí posicionada.

Espacios geográficos de reserva, son aquellos sectores del espacio geográfico cuya posesión de recursos es catalogada como reserva. Por ejemplo, porciones del espacio que poseen reservas de agua que tienen impacto antropogeográfico. Toda la infraestructura estratégica destinada a mantener y explotar ese espacio de reserva, es regionalizada en el espacio geográfico como espacio de reserva.

Desde el punto de vista de los recursos mencionados en la Política de Defensa Nacional, citamos como ejemplo los reservorios de agua que alimentan la Planta de OSE de Paso Severino que abastecen al 60 % de la Población del Uruguay, siendo esta infraestructura estratégica regionalizada en espacios geográficos de reserva. La restante infraestructura estratégica destinada a la obtención del recurso, industrialización, traslado, almacenamiento y distribución final del agua, es posicionada en un espacio geográfico dinámico.

Espacios geográficos enclaves, entendiéndose a estos como las porciones del territorio nacional de importancia estratégica porque su contacto con el exterior, le permite generar grados de sustentabilidad.

Es en este sentido que lo primero que se debería determinar es aquel recurso y su infraestructura estratégica asociada, que pueda ser categorizada como crítica, o sea que en caso de sufrir una perturbación el país como tal no posee un medio sustitutivo.

Al poseer nuestro país una categorización geopolítica dependiente de recursos del extranjero, particularmente en lo que se refiere al petróleo, la infraestructura que permite la llegada del petróleo a nuestro país, su refinamiento, almacenaje y distribución de grandes proveedores, son regiones que incorporan desde el punto de vista de la Defensa Nacional infraestructuras críticas.

Asociado a lo anteriormente expuesto desde el punto de vista geopolítico, surge otra construcción hacia la regionalización del espacio geográfico, que son aquellas infraestructuras críticas que se regionalizan en áreas enclaves, siendo éstas las que permiten al país desde el punto de vista de los recursos el contacto para la subsistencia. O sea, sobre la base de la categorización de país petróleo dependiente, toda la infraestructura que permite la llegada de este recurso de otras regiones a nuestro país, deberían configurarse cómo áreas enclaves.

Esta regionalización del espacio geográfico por parte de la Defensa Nacional, en función de las Infraestructuras asociadas a recursos estratégicos, contribuye a responder a la pregunta con la cual iniciáramos el trabajo, ya que Seguridad Pública regionaliza espacios en función del delito o índices delictivos.

Esta primera aproximación a regionalización del espacio geográfico en función de las infraestructuras críticas o estratégicas, conduce a una segunda línea de razonamiento, la cual está vinculada con la competición geopolítica entre Estados, por la posesión de esos recursos.

Este aspecto queda claramente definido en la Política de Defensa Nacional donde se menciona que, los recursos naturales y particularmente los energéticos, darán lugar a la competición geopolítica entre estados, en gran parte, producto de un acentuado aumento de la demanda, asociado al crecimiento demográfico (Dec. 105/014, 2010, p.25).

En consonancia con lo expuesto anteriormente la regionalización para la Defensa Nacional del país, tomando recursos e infraestructura estratégica, que esté relacionada con la producción de energía o la posesión de recursos, la que pudiese dar lugar a la competición geopolítica entre Estados, es pasible de ser mencionada como una región a ser incluida como hipótesis de conflicto. A nivel internacional del pensamiento político y geopolítico contemporáneo, relacionado con la afirmación anterior, podemos citar a Michael Klare (2003) y su obra "Guerras por los recursos: el futuro escenario del conflicto global".

Sabido es que en lo relativo a la producción energética, nuestro país comparte represas hidroeléctricas binacionales; así como redes de interconexión, que hasta la fecha son enmarcadas en acuerdos de cooperación. Si somos coherentes con la precisión que realiza la Política de Defensa Nacional, esta infraestructura estratégica si se asocia a la competición geopolítica entre Estados, debería dar origen a la formulación de Hipótesis de Conflicto.

Lo anteriormente expuesto no quiere decir que sea un conflicto en el cual el medio preponderante de la Defensa Nacional que actúe sea el Factor Militar o la Defensa Militar; sino en este caso adherimos al concepto de Beaufre de Estrategia Ampliada, en el cual se menciona que un Estado en la contraposición de intereses con otro Estado, utiliza todos los medios del potencial nacional para solucionar el conflicto (1965, p.79). Se entiende necesaria realizar esta aclaración, ya que en nuestro país la competición geopolítica entre Estados, siempre se razona en función de la confrontación bélica.

Uno de los aspectos emergentes e innovadores de la Ley Marco de Defensa Nacional y la normativa que se fue publicando sobre la temática en años sucesivos, refieren a tres tiempos estratégicos, paz, crisis y conflicto armado.

De las afirmaciones anteriores surgen dos orientaciones conceptuales a ser empleadas en la planificación estratégica de la Defensa Nacional:

- queda eliminada la dialéctica paz/guerra del pensamiento relacionado a la Defensa Nacional que imperó históricamente en nuestro país,
- asociado al Art. 1 de la Ley 18.650, la Defensa Nacional es concebida en el pensamiento estratégico de Beaufre, como Estrategia Ampliada, conjunto de actividades civiles y militares.

En este caso las hipótesis de conflicto son identificadas por la Defensa Nacional, a través del Consejo de Defensa Nacional, acorde a lo establecido en la Ley Marco de Defensa Nacional, Art. 12, en el que se determina que Compete al Consejo de Defensa Nacional asesorar sobre la Defensa Nacional. Tiene entre otros cometidos:

A. Analizar las amenazas que pudieran poner en riesgo la soberanía e independencia de la República, así como afectar gravemente los intereses nacionales, proponiendo en tales casos las medidas y/o acciones que se estimen necesarias para su resolución.

B. Analizar y proponer las hipótesis de conflicto.

C. Sugerir la adopción de estrategias, aprobar los planes y coordinar las acciones necesarias para la defensa.

D. Realizar propuestas sobre asuntos relacionados con la defensa que, por afectar a varios organismos del Estado, exijan un tratamiento conjunto (Ley 18.650, 2010, Art. 12).

El método a utilizarse para la configuración de Hipótesis de Conflicto, según Karl Popper, debería ser de corte deductivo, planteando el conflicto en función de la relación fines/medios, para extraer conclusiones para cada uno de los actores, buscando determinar las relaciones lógicas entre ellas (1997, p. 39).

Afirmamos que es de corte deductivo porque busca a través de enunciados anteriormente aceptados, "deducir enunciados singulares o predicciones".

Estas hipótesis de conflicto a ser formuladas, como menciona el literal B), del Artículo 12 de la Ley Marco de Defensa Nacional, en cuanto a la protección de Infraestructuras Críticas, deberían seguir las orientaciones conceptuales emergentes que surgen de la nueva corriente de pensamiento imperante en nuestro país.

En primer término debería considerar los tiempos estratégicos de crisis y conflicto armado. Se excluye la paz, porque en este tiempo habitualmente los Estados comparten intereses en función de las infraestructuras estratégicas en la cuales coparticipan y cooperan.

En los tiempos estratégicos de crisis y conflicto armado, la protección de la infraestructura estratégica por parte de la Defensa Nacional, debe formularse en una concepción de Estrategia Ampliada. Una eventual hipótesis de conflicto, considerando el bien a proteger a la infraestructura estratégica que podría provocar una competición geopolítica entre Estados, debería configurarse de la siguiente forma:

Tabla 1

Protección de Infraestructura Crítica en función de tiempos estratégicos

TIEMPO ESTRATÉGICO	DENOMINACIÓN DEL MODO ESTRATÉGICO	ACTUACIÓN DE LOS FACTORES POLÍTICO Y ECONÓMICO	ACTUACIÓN DE LA DEFENSA MILITAR
CRISIS	INDIRECTO	Preponderante, llevan adelante la negociación y realizan las principales acciones estratégicas.	Nula o si participa es como respaldo al accionar de los otros factores.
CONFLICTO ARMADO	DIRECTO	En apoyo al esfuerzo de la Defensa Militar y buscando legitimar el accionar de ésta.	Se hace uso del empleo de la fuerza, el cual puede ser desde leve a integral.

Nota: Elaboración propia.

Cuando se hace referencia a los modos estratégicos y a la evolución de la formulación de la hipótesis de conflicto en forma integral, la misma obedece a la existencia de una metodología de análisis estratégico, que aplica la teoría de los principios de las relaciones internacionales, para describir en la relación fines/medios, como cada actor participa en el conflicto (Objeto de estudio de la estrategia).

Es posible comparar mediante esta metodología, la aplicación de los principios o teorías rivales sobre la base de la percepción de la aplicación de un actor sobre otro, "variando la intensidad", como afirma Khan, sobre la base del análisis racional de las barreras que cada actor va superando. Conceptos de escalar y "desescalar" conflictos, muy utilizados en el ambiente estratégico (1980, p.123).

Para estos conceptos podemos identificar tres teorías o conjuntos de principios que se agrupan en las siguientes corrientes de pensamiento estratégico, en cuanto a la formulación de hipótesis de conflicto relacionadas con la protección de recursos e infraestructura estratégica:

- La inspirada en el pensamiento de Clawsewitz, vinculando a la estrategia con la guerra, para el caso de otros actores estratégicos el uso de la violencia en todas sus formas como única forma de solución del conflicto.

- La inspirada en Beaufre y preponderante en nuestro país, que vincula todos los medios disponibles para la solución de conflictos; no necesariamente aquellos que generan violencia.

- La corriente Anglosajona, que vincula situaciones de paz y tensión, utilizando medios; pero que es una solución intermedia a las dos anteriores.

De lo anteriormente expuesto en cuanto a la formulación de hipótesis de conflicto relacionadas con la protección de recursos e infraestructura estratégica por parte de un Estado, ante la eventual competición geopolítica sobre los mismos, se puede concluir parcialmente que esto es tarea de Defensa Nacional, desde el punto de vista normativo y estratégico, en cuanto a la concepción y operacionalización de las mismas en función de tiempos y medios.

Conclusiones

Desde el punto de vista normativo en este artículo se estableció como responsabilidad de la Defensa Nacional la protección de infraestructura crítica, siendo ésta la infraestructura que el Estado no posee alternativas como tal ante deterioro o daño; así como toda aquella infraestructura relacionada con los recursos estratégicos incluidos en la Política de Defensa Nacional y su concepción sistémica. Esta responsabilidad está asociada a la finalidad de la Defensa Nacional de asegurar el bienestar social presente y futuro del conjunto de la población.

Desde el punto de vista Estratégico si la infraestructura afecta la existencia del accionar del Estado como tal, también es responsabilidad de la Defensa Nacional.

En cambio la Seguridad Pública, tiene un marco de actuación más restrictivo en cuanto a Infraestructura Estratégica; y debería ser empleada solo para asegurar que no se vulneren los derechos de las personas y la convivencia en sociedad, manteniéndose su accionar en el plano táctico u operativo, sin tener impacto a nivel Estratégico Nacional.

Sólo podría considerarse aquella infraestructura estratégica que posea impacto en los servicios esenciales; siendo los que afectan la seguridad los primordiales como punto de atención para la Seguridad Pública.

Desde el punto de vista de la publicación para la cual realizamos el aporte, especializada en Estrategia Nacional, podemos concluir que la protección de infraestructura estratégica, cuando pasa el límite que afecta el derecho de la persona y la convivencia en sociedad, comenzando a afectar el accionar del Estado como tal en cuanto a la sustentabilidad; así como la protección de la infraestructura crítica siendo ésta la que ante daño o deterioro el Estado no tiene capacidad de sustituirla y la infraestructura asociada a los recursos estratégicos (Minerales, energéticos, alimenticios, agua y biodiversidad con una visión sistémica), es responsabilidad exclusiva de la Defensa Nacional en el sentido amplio.

Asociada a la conclusión anterior es posible determinar que la Infraestructura Nacional puede ser categorizada de la siguiente manera según la finalidad de la protección y los medios a emplearse:

Tabla 2

Categorización de Infraestructura Crítica en función de la finalidad y los medios a emplearse

Tipo de Infraestructura	**Finalidad de la Protección**	**Medios a emplearse**
Estratégica	Asegurar la sustentabilidad del Estado, en cuanto a brindar a la población la salud, la seguridad, el bienestar social y económico de los ciudadanos, o el eficaz funcionamiento de las Instituciones del Estado y las Administraciones Públicas.	Seguridad Pública Cuando se comienza a afectar las condiciones de bienestar social presente y futuro de la población, pasa a ser un problema de Defensa Nacional.
Crítica	Aquella que afecta la existencia del Estado como tal; o que ante daño o deterioro no exista alternativa	Defensa Nacional
Relacionada con los recursos estratégicos (Agua, alimenticios, minerales, energéticos y biodiversidad)	Proteger el recurso como tal, la infraestructura de explotación, traslado, industrialización y distribución.	Defensa Nacional

Nota: Elaboración propia.

Considerando la categorización mencionada anteriormente, entendemos conveniente mencionar que el país como tal, debería dictar un Marco Normativo al respecto; así como la Concepción Estratégica de las acciones que permitan materializar esta protección.

Dentro de las diferencias sustanciales que se presentaron en la segunda parte del trabajo, están las relacionados con los criterios de regionalización, que utilizan la Defensa Nacional y la Seguridad Pública, mientras esta última regionaliza en función del delito, la Defensa Nacional

es el único instrumento que posee el Estado para regionalizar la protección de la infraestructura crítica o estratégica relacionada con los recursos estratégicos que posee el país.

Pudimos determinar que la regionalización cuando se vincula con espacios enclaves, que aseguran el funcionamiento del país, asociado a un recurso energético que no se posee y que proviene de un ámbito externo, incluiría todo lo relativo a las infraestructuras críticas.

En cambio las restantes regionalizaciones que se hagan en Defensa Nacional, relacionadas con espacios geográficos dinámicos, dinámicos emergentes, de reserva o decadentes, van a integrar a esos espacios infraestructuras estratégicas.

Si consideramos la competición geopolítica entre Estados sobre recursos, que orientan estratégicamente a enunciar hipótesis de conflicto para la defensa de los mismos, se concluye que esta actividad de análisis geopolítico/estratégico se mantiene dentro de la órbita de la Defensa Nacional, a través del Consejo de Defensa Nacional. Los tiempos estratégicos y los modos estratégicos implican la participación en diferentes grados de la Defensa Nacional como tal, no visualizándose el empleo de la Seguridad Pública en esta tarea.

Ejemplo de análisis de una Infraestructura Crítica, asociada a Ciberseguridad

En el año 2017, investigadores del observatorio de Defensa que funciona en el C.AL.E.N. identificaron el Data Center de ANTEL, ubicado en la Ciudad de Pando, Canelones, como la principal infraestructura crítica a proteger.

A continuación citamos los principales indicadores a tomar en cuenta en cuanto a esa infraestructura crítica (C.AL.E.N., 2017):

Indicador- Data center certificado Tier III en diseño y construcción: TIER es una certificación o "clasificación" de un Data Center en cuanto a su diseño, estructura, desempeño, fiabilidad, inversión y retorno de inversión. TIER III: Cuenta con redundancia en sus infraestructuras. Cuenta con varias fuentes alternativas de electricidad y refrigeración en caso de emergencia. Las operaciones de mantenimiento no requieren que el Centro esté offline en ningún momento. Disponibilidad del 99,982 %.

Indicador- Software y hardware de seguridad: Triple control de seguridad para el ingreso. Más de 200 cámaras de vigilancia, equipamiento con vidrios blindados, detectores biométricos de huellas dactilares y puertas blindadas similares a las que se usan en las bóvedas de bancos.

El sistema de monitoreo continuo del aire y detección de humo, puertas corta fuegos. En caso de detectarse un foco ígneo, se utilizará un gas especial que desplaza el oxígeno de la sala y no daña los equipos.

La seguridad de la información incluye varias etapas de redundancia para asegurar el acceso a los datos de las empresas, contingencia y continuidad del servicio.

Indicador- Software: Centro de monitoreo las 24 horas.

Indicador- Headend 3.0 (HD - 4k - realidad virtual): **Headend 3.0**: Se trata de una infraestructura de última generación para proveer servicios convergentes para plataformas

audiovisuales sobre Internet y televisión en sus distintas modalidades. Estos servicios tecnológicos están diseñados para ofrecer prestaciones de gestión y distribución de videos en HD, 4K y realidad virtual. Con estas herramientas se podrán emitir en la mejor calidad disponible señales en directo, así como también una amplia gama de ofertas de servicios de vídeo bajo demanda. **HD**: La alta definición (AD), más conocida como HD o HQ (siglas del inglés High Definition o High Quality, respectivamente), es un sistema de imagen, vídeo o sonido con mayor resolución que la definición estándar, alcanzando resoluciones de 1280×720 píxeles y 1920×1080 píxeles. **4k**: 4K es un tipo de resolución de pantalla que tiene cerca de 4000 píxeles de resolución horizontal. Existen fundamentalmente dos tipos de resolución 4K que se diferencian por su relación de aspecto: por una parte, el DCI 4K como estándar emergente para resolución en cine digital y en infografía, de relación 17:9, y por otra parte el 4K UHDV (2160p) usado en la industria de la televisión digital, de relación 16:9. **Realidad virtual:** La realidad virtual (RV) es un entorno de escenas u objetos de apariencia real. La acepción más común refiere a un entorno generado mediante tecnología informática, que crea en el usuario la sensación de estar inmerso en él.

Indicador- Free Cooling Indirecto: Solución de Free Cooling Indirecto. Este es un sistema de enfriamiento que aprovecha las bajas temperaturas que se dan en el ambiente para enfriar una estancia o equipo. Se trata de una solución de eficiencia energética que garantiza un ahorro de energía y un funcionamiento responsable de los sistemas de acondicionamiento térmico.

Indicador-Energía directa: El sistema de energía es ecológico. Dos subestaciones independientes brindan combustible suficiente como para funcionar durante una semana sin energía exterior de ningún tipo. La energía es de 12 megawatts de potencia, equivalente en consumo energético a una ciudad de 14.000 habitantes, la mitad de Pando.

La información anterior construida en función de indicadores nos permite evaluar desde el punto de vista técnico esta infraestructura, la cual posee mecanismos y medios propios de protección, como son las fuentes de energía que aseguran su funcionamiento, un sistema de enfriamiento, los indicadores de seguridad para software y hardware. Con estos indicadores y sobre la base de la información incluida en el cuadro 2 del artículo, esta infraestructura es categorizada como estratégica.

Cuando se considera que esta infraestructura aloja todos los servidores de los organismos públicos e instituciones del Estado Uruguayo, su categorización cambia a infraestructura estratégica y por lo tanto la responsabilidad de protección, debería recaer sobre la Defensa Nacional.

Referencias

Beaufre, A., (1965), *Introducción a la Estrategia*, Madrid, España, Instituto de Estudios Políticos.

B.O.E., (2011), *Boletín Oficial Español, No. 102*, que contiene la Ley 8/2011, Ley de Protección de Infraestructuras Críticas, Madrid, España.

C.AL.E.N., (2017), *Artículo acerca de indicadores de Ciencia y Tecnología que permiten identificar una Infraestructura Estratégica*, Montevideo, Uruguay, Centro de Altos Estudios Nacionales.

http://calen.edu.uy/pdf/observatorio_2017/_02_indicadores_de_ciencia_y_tecnologia.pdf

Campos, G. (2002), Manual de inteligencia Estratégica, Buenos Aires, Argentina, Escuela Superior de Guerra.

Dec. 105/014, (2014), *Política de Defensa Nacional*, Montevideo, Uruguay.

Dec. 129/016, (2016), *Política Militar de Defe*nsa, Montevideo, Uruguay.

Dec. 259/011. (2011), *Decreto de Creación de la Guardia Republicana*, Montevideo, Uruguay.

Kahn, H. (1980), *Onescallation*, Washington, Estados Unidos, Reston Publishing.

Klare, M. (2003), *Guerra por los recursos. El futuro escenario del conflicto global*, Barcelona, España, Urano Tendencias.

Ley 18.650, (2010), *Ley Marco de Defensa Nacional*, Montevideo, Uruguay.

Ley 19.135, (2015), *Ley Orgánica Policial*, Montevideo, Uruguay.

Mintzberg, H.; Quinn, B. (1998), *El Proceso Estratégico. Conceptos, contextos, casos. 2ª. Edición*, México, Prentice Hall Hispanoamericana, S.A.

Moreira, M, (2016), *Impacto de la Política de Defensa Nacional en la Planificación de la Defensa Militar*, Tesis de Maestría, Montevideo, Uruguay, Centro de Altos Estudios Nacionales.

Popper, K. (1997), La lógica de la Investigación científica, Madrid, España, Tecnos.

ESTRATEGIA ENERGÉTICA URUGUAY 2050 – ALGUNOS ELEMENTOS CLAVE A CONSIDERAR EN DIAGNÓSTICO Y POLÍTICA

Enrique Morales Rodríguez[1]

RESUMEN

Partiendo del desarrollo socioeconómico del país como un Objetivo Fundamental, en este trabajo se asume el suministro energético, en particular el eléctrico, como un insumo crítico de dicho desarrollo, fundamentando esta premisa. Sobre esta base, y analizando los antecedentes del tema, se manifiesta la conveniencia de establecer una estrategia energética nacional a largo plazo (año 2050). Se realizan algunos aportes parciales para la elaboración de dicha estrategia según el método CALEN, procurando el logro del Objetivo Fundamental señalado, simultáneo con otros Objetivos de Estado ya establecidos o comprometidos. En base a los escenarios delineados, se señalan posibles infraestructuras críticas que puedan ser necesidades estratégicas a futuro.

Palabras clave: estrategia energética, Uruguay 2050, fase diagnóstico, fase política, elementos clave.

Antecedentes

El desarrollo socioeconómico de un país, es un Objetivo Fundamental en cualquier Estrategia Nacional y en el Uruguay, de hecho está reconocido como Interés Nacional Estratégico por la actual Política de Defensa.

El suministro energético, en cualquier país y circunstancia, siempre es un insumo esencial de dicho desarrollo aunque su nivel de influencia depende del modelo de desarrollo. Dicho suministro, comprende energía en diversas formas. Dentro de éstas, el componente eléctrico es el único que, en todo el mundo ha duplicado su participación en los últimos 40 años (Morales, 2017 e International Energy Agency-OCDE, 2016), como se observa en Figura 1[2], debido a la expansión vertiginosa de la población y penetración en ésta de actividades sólo impulsables por electricidad –herramientas informáticas- y, en otras actividades, residenciales o industriales, la irrupción de la electricidad como vector energético limpio y eficiente en

1 Ing. Enrique Morales Rodríguez: Ingeniero Químico y Químico Farmacéutico (UDELAR). Especializado en Tecnología Nuclear y Seguridad Nuclear en Argentina. Se desempeñó en la actividad privada, en las áreas de minería de oro, irradiación ionizante y otras. Docente e Investigador en Facultades de Química e Ingeniería. Docente del C.A.L.E.N. (C y T) desde 2014.

2 Tomada de International Energy Agency-OCDE, 2016.

sustitución de la quema de combustibles en condiciones contaminantes e ineficientes (Figura. 3).

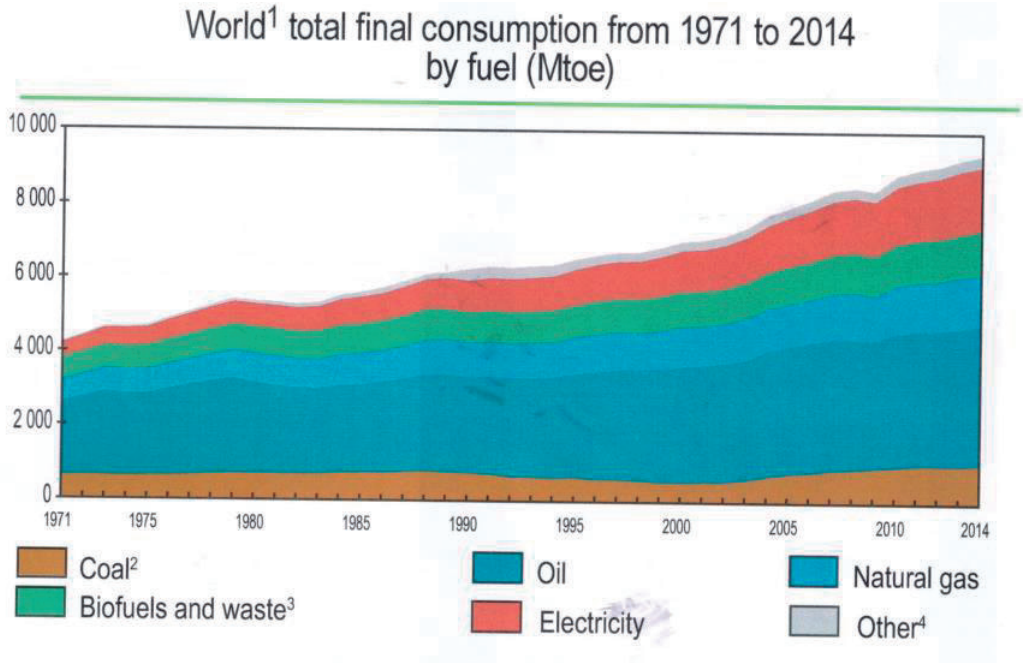

Figura 1. Consumo final total mundial de 1974 a 2014 por combustible (Mtoe). ©ECD/IEA 2016 Key world energy statistics, IEA.

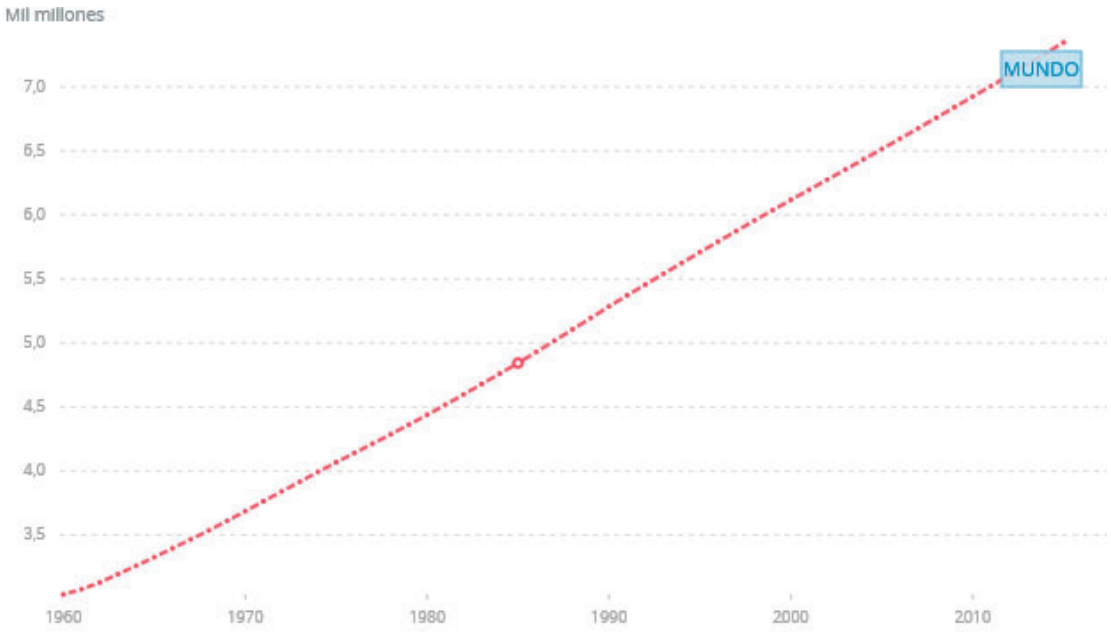

Figura 2. Población Mundial. International Energy Agency-OCDE, 2016.

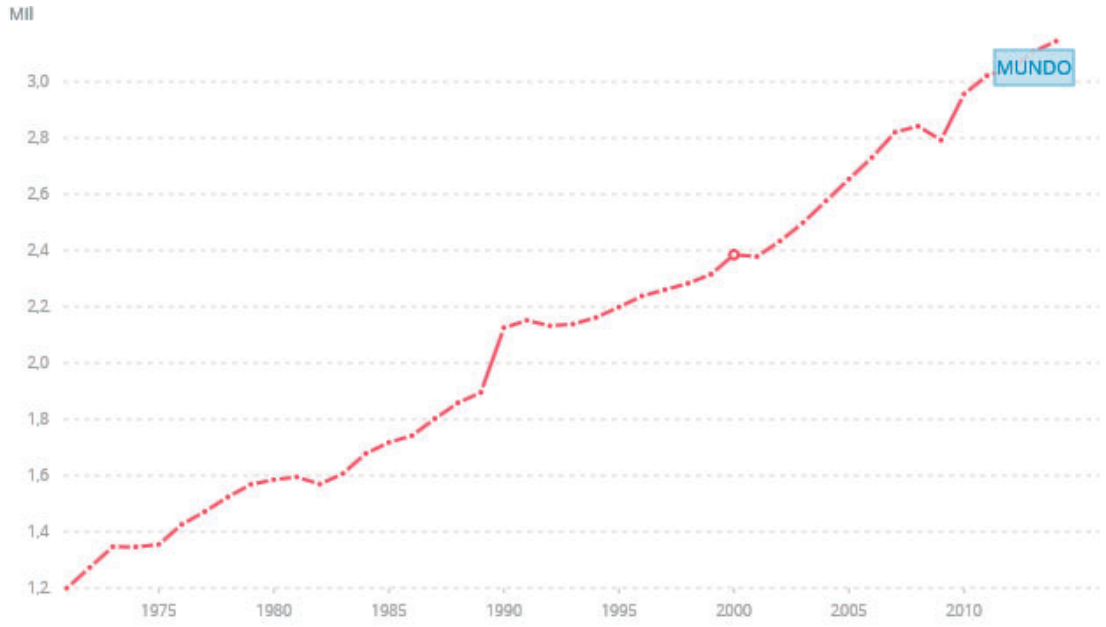

Figura 3. Consumo eléctrico per cápita (kW*hr/año).
Datos del Banco Mundial: http://datos.bancomundial.org/indicador

Uruguay no ha sido excepción, por el contrario en nuestro país entre 1975 y 2015, el consumo eléctrico, más que se quintuplicó, representando actualmente el 21%-10% en 1975- del consumo energético total, que a su vez también más que se duplicó en ese período (DNE - MIEM, 2017), como surge de la Tabla 1.

Tabla 1
Consumo final energético uruguayo 1965 – 2016

ktep / *ktoe*	1965	1975	1985	1995	2000	2005	2010	2011	2012	2013	2014	2015	2016
Leña y carbón vegetal	355,8	389,4	495,8	456,1	403,0	444,5	524,2	559,3	543,3	549,9	538,2	519,0	**519,0**
Firewood and charcoal	21%	21%	29%	21%	16%	19%	15%	15%	15%	14%	13%	12%	**11%**
Residuos de biomasa	15,1	27,2	46,2	46,0	35,0	41,5	645,6	625,8	626,8	690,7	900,9	1157,6	**1.227,5**
Biomass wastes	1%	1%	3%	2%	1%	2%	18%	17%	17%	18%	22%	26%	**27%**
Carbón mineral	5,1	1,2	0,3	0,3	0,4	0,9							
Coal	0%	0%	0%	0%	0%	0%							
Derivados del petróleo	1.164,1	1.209,3	920,4	1.274,5	1.438,5	1.234,5	1.521,0	1.582,2	1.589,0	1.680,4	1.689,4	1.690,2	**1.760,0**
Oil products	69%	67%	53%	58%	58%	52%	43%	43%	43%	44%	41%	38%	**38%**
Biocombustibles							8,8	22,0	29,4	43,8	52,8	78,8	**85,2**
Biofuels							0%	1%	1%	1%	1%	2%	**2%**
Gas natural					30,2	73,5	45,7	50,0	46,9	46,6	42,8	43,7	**47,7**
Natural gas					1%	3%	1%	1%	1%	1%	1%	1%	**1%**
Derivados del carbón	22,6	16,7	0,9	0,2	0,1	0,9	0,3	0,3	0,2	0,2	0,1	0,1	**0,2**
Coal products	1%	1%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	**0%**
Electricidad	118,5	173,7	271,1	429,8	552,2	556,7	772,7	800,3	823,8	847,2	871,3	906,2	**955,7**
Electricity	7%	10%	16%	19%	22%	24%	22%	22%	23%	22%	21%	21%	**21%**
Solar											2,6	2,9	**3,3**
											0%	0%	**0%**
TOTAL	1.681,2	1.817,5	1.734,7	2.206,9	2.459,4	2.352,5	3.518,3	3.639,9	3.659,4	3.858,8	4.098,1	4.398,5	**4.598,6**
	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	**100%**

Nota: tomada de (DNE - MIEM, 2017)

En el Uruguay, es bien clara la correlación entre desarrollo y consumo energético, medida por el indicador intensidad energética global: (consumo final energético) / PBI, expresado en toneladas equivalentes de petróleo (tep) por millón de dólares (constantes de 2005) de PBI. Este indicador, en el año 2005 se situó en 5,7 tep / (MU$S 2005) y en 2016 fue de 6,9 tep / (MU$S 2005) (DNE - MIEM, 2017), dando cuenta de distintos escenarios de desarrollo industrial. De cualquier manera, entre 1997 y 2016, dicho indicador no osciló más de un 21%, a lo largo de 20 años y diversas situaciones, variación muchísimo menor al crecimiento del PBI de 62% en el mismo período (DNE - MIEM, 2017), por lo que se puede concluir que un desarrollo económico significativo del país, en cualquier escenario, estará siempre asociado a un gran aumento en el consumo energético. En base a esta y otras tendencias actuales (demográficas, p. ej.) y a la esperada concreción de Objetivos Fundamentales del Estado, se puede considerar muy probable para el futuro un escenario de cierto aumento de la población, erradicación de la pobreza asociada a un desarrollo socioeconómico continuo y difusión universal del "estilo de vida digital", lo que conduciría a una demanda eléctrica en permanente aumento hasta 2050 (Morales, 2017 y Morales Rodríguez, 2012)

En la medida que la cobertura apropiada de esta demanda, responde a Objetivos Fundamentales y de Estado, la infraestructura necesaria para lograr dicha cobertura –ya sea de propiedad pública o no- constituye una infraestructura crítica para el país, y como tal la trataremos en este trabajo.

Actualmente existe en el país y está implementada, una Política Energética, definida hasta 2030 (MIEM - DNE, 2009). Esta se plantea como objetivo general diversificar la matriz energética, fomentando la participación de fuentes autóctonas, en particular las renovables: se fijó un objetivo de 15% de renovables no convencionales en la generación eléctrica para 2015, lo que se ha logrado; para 2020 la Política plantea llegar al nivel óptimo en el uso de éstas. También se plantea intensificar la participación del gas natural en la matriz a precios competitivos, aunque este último planteo, en lo referido a generación eléctrica, hoy no esté tan claro por razones de notoriedad. Entre los objetivos particulares, se cuenta también la integración energética con países de la región, en lo que efectivamente se ha avanzado, con la interconexión con Brasil vía conversora de Melo. Nuestras represas hidroeléctricas, son la principal fuente de generación eléctrica renovable, a la vez que firme (se puede disponer de ellas en todo momento, aunque con dependencia del clima) y flexible (se adapta a la demanda). Para reducir la vulnerabilidad de estas fuentes a fenómenos de sequía, UTE contrató en 2013 un seguro climático por U$S 450 millones, que le permiten adquirir o generar (termoeléctrica) potencia firme si la hidraulicidad cae por debajo del 60% del promedio anual. La generación eléctrica por biomasa en las megaplantas de celulosa, permite el autoconsumo en estas importantes industrias privadas a la vez que vierten ciertos excedentes -unos 400 GW*hr/año lo que es cerca del 3% del consumo nacional- de energía firme a la red de UTE. Se han incorporado, de acuerdo a lo previsto, nuevas fuentes de generación renovable, como los parques eólicos y solares, que en 2016 alcanzaron participaciones de 22% y 1% respectivamente en la matriz eléctrica (DNE - MIEM, 2017), la complementariedad de dichas fuentes con la generación térmica, permite minimizar el uso de ésta en casos de escasez de generación hidroeléctrica. La naturaleza intermitente de estas fuentes, frecuentemente origina excedentes

de generación, que actualmente se están exportando, con ingreso de divisas, a países vecinos, aprovechando las interconexiones históricas y recientes, como se observa en la Figura 4[3].

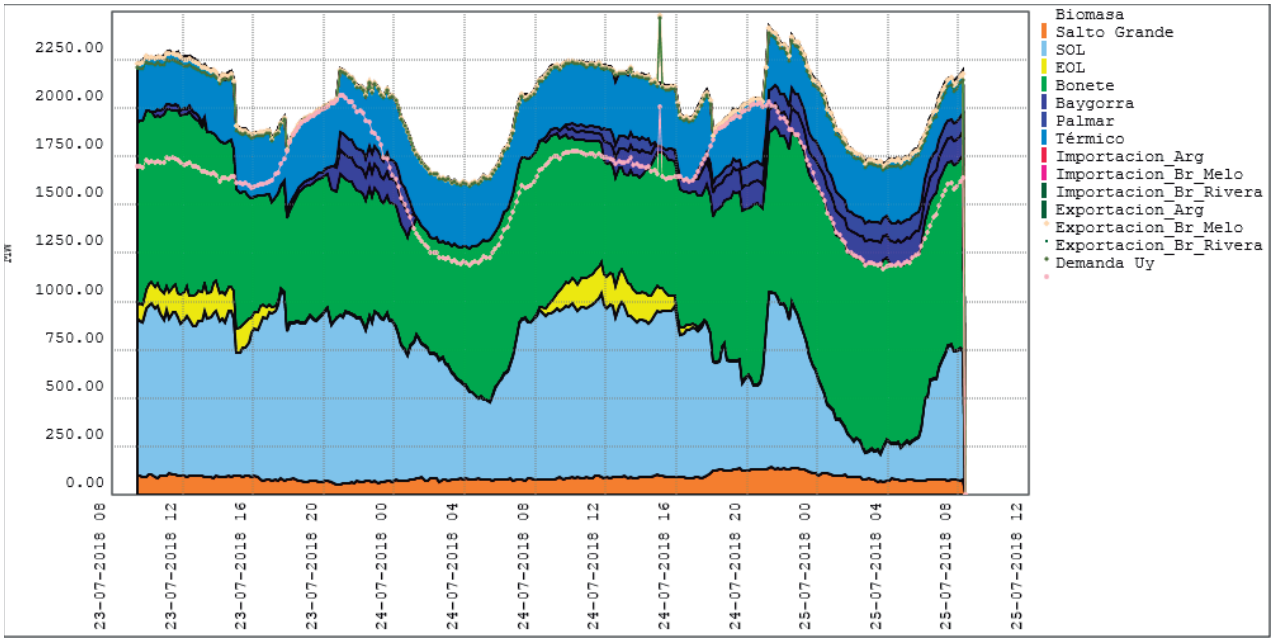

Figura 4. Despacho de cargas Uruguay 23-24/7/2018. "Despacho últimas 48 horas" www.adme.com.uy, el 25/7/2018

En la medida que las decisiones en el sector Energético en general llevan un tiempo considerable para implementarse y una vez implementadas, su naturaleza impone mantenerlas vigentes también durante mucho tiempo, la definición en los próximos años de una estrategia energética nacional hasta el 2050, sería en mi opinión, de enorme importancia.

Por supuesto que la definición de dicha estrategia sería de gran complejidad por la enorme cantidad de factores técnicos, políticos, económicos y escenarios a considerar. Pensando en que dicha estrategia se fuera a elaborar según el método de Planificación Estratégica del CALEN, en este trabajo procuraremos analizar algunos de los muchos factores clave a considerar en las primeras Fases, o sea en las de Diagnóstico y Política, como aporte parcial a la elaboración de tal compleja definición.

Algunos elementos clave de Fase Diagnóstico

De acuerdo a lo antes mencionado, el *Horizonte Temporal* abarcará hasta el año 2050, período para el cual suponemos que la demanda eléctrica tendrá un crecimiento continuo.

El *Alcance* del tema, naturalmente consistirá en el *Sistema* de gestión eléctrica uruguayo, tanto en su configuración actual como en otras que puedan ser necesarias en el futuro y todas las implicancias estratégicas nacionales de estos sistemas actuales o hipotéticos.

3 Tomada de la web de la Administración Nacional del Mercado eléctrico "Despacho últimas 48 horas" www.adme.com.uy, el 25/7/2018

Los escenarios de posibles configuraciones a futuro de dicho Sistema estudiados en este trabajo, incluyen el uso de fuentes de generación eléctrica del tipo de las ya existentes en Uruguay así como de otras usadas en el mundo.

Ambiente externo

Amenazas:

- Muchos insumos energéticos usados actualmente o potencialmente necesarios para el futuro –petróleo, gas natural-, no son recursos propios del país, por lo que se deben obtener de proveedores externos, con riesgo de afectación del desarrollo nacional en caso de precios y/o salidas de divisas insostenibles para el país o conflictos geopolíticos con los proveedores.
- La importación directa de electricidad desde países vecinos, aun siendo socios dentro del MERCOSUR, en cierta medida implica una amenaza similar a la anterior, si bien más manejable.
- La generación eléctrica mediante ciertas fuentes, como la nuclear, implica la adquisición de tecnología e insumos –no el uranio en sí, que es bastante accesible- a un club de proveedores muy exclusivo, lo que en ciertas situaciones puede conducir a riesgos similares a los mencionados en los parágrafos anteriores. Por otra parte, la viabilidad económica, así como la disponibilidad de modelos comerciales de reactores nucleares, en general ocurre para potencias altas, por lo que la adaptación a un país de las características de Uruguay necesitaría un exhaustivo análisis. Existen propuestas técnicas de diseños innovadores de reactores, como los Small Modular Reactors, que podrían integrarse más fácilmente a una red como la uruguaya, pero para un país con nula experiencia en el área nuclear como Uruguay, gestionar una tecnología aún no madura internacionalmente puede crear desafíos imposibles de abordar en plazos razonables. También se debe tener en cuenta que, si toda o la mayor parte de una inversión en generación nuclear se hace a costa exclusivamente de insumos importados, el egreso de divisas puede ser una amenaza similar a la antes descrita.
- El funcionamiento continuo de ciertas fuentes, en algunos escenarios, puede requerir interacción con los países vecinos, por ejemplo, para absorber en sus redes excedentes de generación eólica y/o solar si la penetración de estas fuentes en la red uruguaya está por encima de determinados límites. En estos casos, la certeza del suministro interno puede depender de la capacidad técnica de estos países para interactuar en las condiciones adecuadas, o de un acuerdo político muy sólido que lo garantice en cualquier situación, trasladando el costo al país vecino con el que se acuerde.

Oportunidades:

- El Green Climate Fund, previsto en el Acuerdo de Paris, puede ayudar a solventar inversiones en el área energética –asociadas a generación eléctrica libre de carbono- que serían inaccesibles o muy dificultosas para el Estado.
- Organismos internacionales, como el O.I.E.A. o estatales de países vecinos, están en condiciones y en principio dispuestos a prestar asistencia técnica en caso de que Uruguay deba realizar determinadas transiciones en el área energética.
- Similarmente a lo ocurrido con la represa de Salto Grande, no se debe descartar que ciertas usinas eléctricas puedan instalarse en asociación con países vecinos,

aprovechando una importante economía de escala pero manteniendo la independencia del país.

Ambiente interno

Debilidades:

- La geografía del país, no permite la instalación de nuevas hidroeléctricas –al menos, de gran porte- y la capacidad máxima de generación de las represas en funcionamiento, alcanza 1538 MW (DNE - MIEM, 2017). La capacidad máxima de generación por biomasa actual es de 425 MW, (DNE - MIEM, 2017). Es de prever la instalación de todavía una nueva megaplanta de celulosa, posiblemente la última, que también tendría autoconsumo por generación con biomasa e inyectaría nuevos excedentes a la red de UTE, que optimistamente se podrían considerar cercanos al 7% del consumo nacional actual. La suma de todo lo anterior sería el techo de producción de las fuentes de generación renovable y firme actuales y previstas.
- La gestión continua de fuentes renovables variables –a altas penetraciones- sin dependencia de conexión con redes extranjeras, requiere disponibilidad de instalaciones de almacenamiento. Las hidroeléctricas reversibles son hoy la opción más habitual en el mundo y en Uruguay en principio sería factible instalar algunas de ellas, pero esta factibilidad y/o los impactos que implique, deben analizarse en el escenario 2050, con la cantidad y/o características que esto signifique.
- Algunas fuentes de generación de base que podrían ser necesarias en el futuro como la nuclear, requieren, además de las usinas en sí mismas y aun siendo éstas privadas, una infraestructura paralela del Estado –técnica, legal, institucional- destinada a asuntos de su exclusiva competencia: gestión de residuos, seguridad, regulación, que garantice el funcionamiento de las usinas en condiciones adecuadas. De entrar en este camino, Uruguay todavía tendría muchos temas pendientes al respecto.

Fortalezas:

- La actual Política Energética permite gestionar el suministro por varios años más -salvo situaciones externas y/o internas extremas- por lo que, en principio se dispone de tiempo para delinear e implementar una estrategia a 2050.
- Las fuentes actualmente en uso muy probablemente podrían ser parte de una estrategia energética a 2050, facilitando la implementación de ésta, en la medida que son Medios Disponibles.

Análisis del poder

De los cinco factores del Poder Nacional, estimo que a efectos de una Estrategia Energética a 2050, sería imprescindible la participación de tres de ellos: Político, Económico y Científico-Tecnológico. De un análisis detallado podría surgir la necesidad de participación también del factor Psicosocial en la medida que para gestionar apropiadamente decisiones tan significativas, es necesario que cuenten con un consenso social sólido. En principio, el factor Militar no participaría en la definición estratégica, aunque probablemente sea necesario su

aporte a futuro en la etapa de Gestión, fundamentalmente en la protección de infraestructuras críticas asociadas a generación eléctrica.

El factor Político, sería necesario a efectos de autorizar inversiones estatales –o licitaciones a privados que las realicen- en el área energética, de características aptas para el logro de Objetivos Nacionales. Cierto tipo de infraestructuras energéticas, por otra parte, también podrían requerir un marco legal específico.

El factor Económico, es el que solventará las inversiones mencionadas, o asegurará que las inversiones privadas sean positivas para la Economía del país.

El factor Científico-Tecnológico, interactuando con el Económico, debería establecer, como primer paso, la participación óptima de las distintas fuentes de generación en el conjunto del sistema eléctrico. Posteriormente, debería definir las características técnicas de nuevas fuentes que se incorporen (a efectos de garantizar la seguridad y soberanía del país) aun cuando dichas fuentes sean propiedad y/u operadas por privados. Naturalmente, en este caso, también será necesaria la estricta supervisión del Estado en la etapa de Gestión, en lo que intervendría nuevamente el factor C y T; la participación de este factor sería mucho mayor todavía si las inversiones fueran estatales.

Planes en vigencia

Los *Planes en Vigencia*, corresponden a las decisiones en el área energética ya ejecutadas. Estas, de acuerdo a la política vigente hasta 2030 incluyen el uso preponderante de generación renovable, procedente de nuestras represas hidroeléctricas, la biomasa y los existentes parques eólicos y solares.

Lo más razonable es suponer que dichas fuentes en uso –que a efectos de Planificación Estratégica son *Medios Disponibles y Potenciales*- sigan en funcionamiento en la estrategia a 2050, aunque sea necesario el agregado de otras fuentes o estructuras complementarias.

En la medida que en la actualidad existe una Política Energética definida y en funcionamiento, no se analizarán *Necesidades* estratégicas para el momento actual, sino hacia el futuro, en el Horizonte Temporal señalado.

Algunos elementos clave de Fase Política

- Los Objetivos de esta planificación estratégica, naturalmente deben ser consistentes con los Objetivos Fundamentales nacionales y con otros del Estado. Tomaremos en base a ello como Objetivo la definición de un sistema de gestión eléctrica que permita satisfacer la demanda nacional con seguridad -durante todo el Horizonte Temporal a 2050- y sin menoscabo de otros Objetivos Fundamentales u Objetivos del Estado. Entre estos últimos, consideraremos algunos aplicables al tema, contenidos en la actual Política de Defensa: desarrollo económico, cultural y social del país, la protección del Ambiente, los recursos naturales estratégicos, y otros, como los definidos en algunos de los Objetivos de Acuerdos Internacionales ratificados por Uruguay, que constituyen pues un compromiso del Estado uruguayo. Los Objetivos del Desarrollo Sustentable, aprobados por unanimidad en la Asamblea General de ONU (ONU, 2015) y el Acuerdo

del Clima de Paris, también aprobado en 2015 (ONU - UNFCC, 2015), son los compromisos internacionales de Uruguay más relevantes a efectos de la definición de la estrategia energética.

Elaboración de escenarios

Los diversos escenarios a considerar están asociados a muy diversos eventos. De éstas, uno de los más significativos, es la demanda o consumo eléctrico uruguayo a futuro, o sea en escenarios a 2050.

Para pronosticar esta demanda a 2050 se pueden emplear diversos métodos, de los que resumimos a continuación algunos resultados.

Como se mencionó, la demanda eléctrica uruguaya está en crecimiento desde hace más de 40 años –salvo mesetas temporales, provocadas por crisis financieras o restricciones técnicas (Morales Rodríguez, 2012)- en forma continua. Actualmente es de 13.886 GW*hr/año y desde hace unos 15 años, el ritmo de crecimiento acumulativo es del 1,5% anual -2,8% en los últimos 6 años- (DNE - MIEM, 2017 y Morales Rodríguez, 2012) si se descuenta el autoconsumo de las grandes industrias de celulosa, como se observa en la Tabla 2.

Tabla 2
Matriz eléctrica uruguaya 2002 – 2016

GWh	2002	2003	2004	2005	2010	2011	2012	2013	2014	2015	2016
Térmica (fósil)	26,4	6,6	1.076,8	956,3	1.165,0	2.627,1	3.748,6	1.859,5	729,8	962,7	464,4
Thermal (fossil)	0%	0%	18%	12%	11%	25%	35%	16%	6%	7%	3%
Térmica (biomasa)	0,0	0,0	27,3	24,5	1.089,8	1.127,5	1.313,4	1.448,0	1.893,3	2.388,4	2.432,7
Thermal (biomass)	0%	0%	0%	0%	10%	11%	12%	12%	15%	17%	18%
Hidráulica	9.535,3	8.529,5	4.780,7	6.683,6	8.407,2	6.478,9	5.420,9	8.205,9	9.649,1	8.266,0	7.842,2
Hydropower	100%	100%	81%	87%	78%	63%	51%	70%	74%	60%	56%
Eólica					69,9	111,3	112,5	144,1	732,7	2.065,1	2.994,3
Wind					1%	1%	1%	1%	6%	15%	22%
Solar									3,4	48,7	151,9
									0%	0%	1%
TOTAL	9.561,7	8.536,2	5.884,8	7.664,4	10.732,0	10.344,9	10.595,4	11.657,5	13.008,3	13.730,8	13.885,6
	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%

Nota: Tomada de (DNE - MIEM, 2017)

Pensando en una simple proyección de esta tendencia, para 2030 se podría esperar una demanda de 18.200 Gw*hr/año y para 2050 de 28.000 Gw*hr/año.

Una proyección más sólida puede surgir teniendo en cuenta la evolución de la población nacional y del consumo eléctrico per cápita. El Instituto Nacional de Estadística prevé para 2050 una población de 3:700.000 habitantes (INE, 2014). Asumiendo el logro del Objetivo

Fundamental del desarrollo socioeconómico generalizado, el consumo per cápita por cierto también aumentaría, lo tomaremos de 5.000 kW*hr/año (Morales, 2017); esta cifra se basa en los 4.000 kW*hr/año hoy el mínimo asociable a un Índice de Desarrollo Humano alto (> 0,9 (Pastermak) y una conservadora evolución de éste (Morales, 2017). De todo lo anterior surgiría un consumo eléctrico nacional –sin incluir el autoconsumo de una eventual nueva megaplanta de celulosa- de 18.500 GW*hr/año a 2050 (Morales, 2017); se observa que la proyección anterior se correlaciona relativamente bien con esta en el mediano plazo (2030) pero no en el largo plazo a 2050. Este resultado, por cierto se debe tomar como un escenario favorable, en lo que refiere a los Objetivos Nacionales y, en opinión del autor, el más probable.

Otros escenarios que conduzcan a distintos eventos de demanda, se pueden elaborar pensando en una descollante mejora en la eficiencia energética-eléctrica. En este caso, podría lograrse el mismo nivel de desarrollo, consumiendo menos energía. Pensando que la intensidad energética eléctrica (consumo eléctrico nacional / PBI) disminuyera a un ritmo de 3,5% anual, la demanda nacional a 2050 sería de 15.500 GW*hr/año, suponiendo un continuo crecimiento –suposición compatible con un alto desarrollo socioeconómico- del PBI a 4% anual. Este escenario naturalmente sería muy favorable, pero poco probable, ya que en el mundo no se ha logrado este ritmo de mejora en los últimos 40 años (Morales, 2017), salvo en regiones que parten de un desarrollo muy reducido y, en condiciones favorables, avanzan bastante rápido.

En un escenario de escaso crecimiento y persistencia del subdesarrollo, la demanda a 2050 también sería bastante menor, posiblemente del orden de 14.500 GW*hr/año; este es un escenario poco probable y por cierto muy desfavorable, en la medida que no incluye el logro de los Objetivos del Desarrollo Sustentable.

Definidos los escenarios de demanda, se debe tener en cuenta la Debilidad señalada en Fase Diagnóstico: la capacidad total de generación propia y firme es de 1963 MW[4]. Esta capacidad quedaría saturada muy probablemente antes de 2030 (Morales Rodríguez, 2012 y Morales, 2017), como se ilustra en Figura 5, salvo en escenarios poco probables o muy desfavorables para los Objetivos Nacionales.

[4] Funcionando a plena carga las 24 horas, 365 días al año, esta capacidad permite generar entonces, como máximo absoluto unos 17.200 GW*hr/año

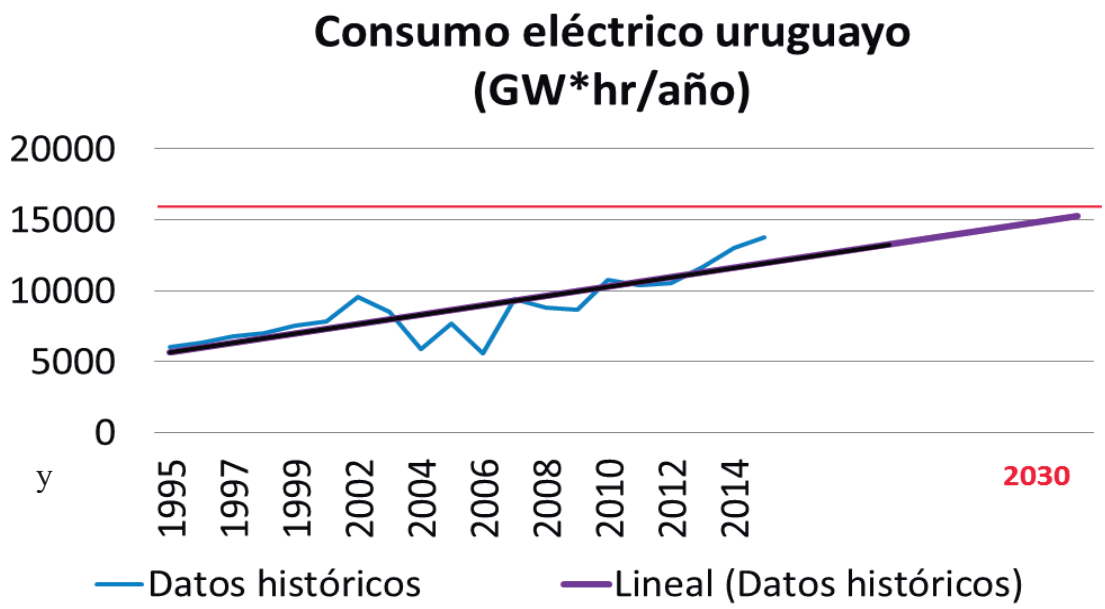

Figura 5. Proyección lineal de demanda comparada con capacidad de generación firme. Morales, 2017.

En caso de instalarse la mencionada nueva megaplanta de celulosa, su aporte a la red, equivaldría aproximadamente al crecimiento del consumo durante tres años, lo que daría unos años extra para nuevas decisiones. De cualquier manera, para 2050, un escenario desfavorable muy probable, sería el de no poder cubrir la demanda necesaria para el logro de Objetivos Fundamentales, salvo agregados o modificaciones al sistema actual; las instalaciones y dispositivos asociados a estas modificaciones serán infraestructuras críticas para el país. A continuación daremos una mirada a ciertas implicancias estratégicas de algunos de estos posibles agregados o modificaciones.

Considerando la capacidad de generación de las usinas termoeléctricas (650 MW), operables con fuel-oil o gas natural, actualmente disponibles y el aporte de la central de ciclo combinado de Punta del Tigre (530 MW) en construcción, se podría cubrir esta demanda con Medios Disponibles y Potenciales, pero consumiendo adicionalmente 650.000 (toneladas G.N.)/año en 2030 y 975.000 (toneladas G.N.)/año en 2050 (Morales, 2017); esto suponiendo que a 2050 se mantenga la capacidad eólica y solar actuales (1300 MW) que se complementan bien con la generación térmica, y evitarían el consumo de otras 470.000 (toneladas G.N.)/año. Aun considerando precios relativamente bajos para estos combustibles importados (≈300 U$S/ton G.N.), el flujo de divisas ya luego de 2030 podría ser insostenible (Morales Rodríguez, 2012), por representar la generación termoeléctrica por sí sola, un déficit comercial permanente del 3-5% de las exportaciones actuales.

Esta situación, sería un escenario extremadamente desfavorable, por el freno a largo plazo que pondría en el desarrollo económico y por tanto, social del país. Paralelamente al problema económico, se debe recordar que Uruguay ha ratificado el Acuerdo de París sobre el Clima (ONU - UNFCC, 2015), y por tanto, la reducción de emisiones de gases de efecto invernadero a futuro, debe ser tomada como un Presupuesto Básico. Suponiendo de manera muy optimista que fuera viable económicamente el consumo de gas natural antes mencionado, las emisiones asociadas en 2050 serían de unas 2:700.000 ton CO2/año (Morales, 2017), que comparadas con las totales actuales de Uruguay (6:300.000 ton CO2/año (DNE - MIEM, 2017),

implicarían un aumento de emisiones de casi 50%, sólo debido a la generación termoeléctrica. El choque con un Presupuesto Básico y el impacto socioeconómico, son eventos tan desfavorables en mi visión, que una estrategia que incluya una generación de base térmica de tal magnitud no sería admisible, salvo un escenario de grandes mejoras en el comercio exterior y en el que fuera viable contar en el país con otros medios, como la Captura y Almacenamiento de Carbono (International Energy Agency, Noviembre 2016) a gran escala. En este momento, no podemos asignar probabilidades a un escenario como este.

En el supuesto que la proporción de generación por renovables variables avanzara a un 30% en 2050, el consumo de fósiles podría quedar en un nivel razonable de unas 230.000 ton G.N./año[5]. En este supuesto de tan alta penetración de renovables a 2050, el consumo de combustibles fósiles podría reducirse aún más y ser casi nulo, si se logra un acuerdo con países vecinos para intercambiar la exportación de excedentes de generación variable por importación de potencia firme cuando se requiera, a través de las interconexiones ya existentes. Pero tanto esto último como lo primero (gestión de una red con 30% de renovables variables) como se ha dicho, dependería de la permanente capacidad de redes vecinas (Brasil, Argentina) y voluntad de sus autoridades, como mínimo de absorber los excedentes de generación variable[6] y, en el segundo caso, también de suministrar potencia firme. No sería posible en este momento, prever la probabilidad de lograr un acuerdo permanente de este tipo y/o de otras implicaciones estratégicas que éste pudiera tener (saldos económicos de los intercambios, por ejemplo), requeriría un análisis geopolítico y técnico-económico detallado.

Sin depender de redes vecinas, se podría lograr el funcionamiento de la red nacional en dicha configuración si se dispone de medios de gestión masiva (almacenamiento flexible) de los excedentes de un 30% de generación variable, usando medios bien conocidos y maduros, como el almacenamiento en baterías o en centrales hidroeléctricas reversibles. La viabilidad de estas opciones a nivel nacional dependerá seguramente de la magnitud de energía a gestionar; hemos considerado para este trabajo un nivel de excedentes a almacenar de 1,1 GW*hr/día[7] en 2050, y la necesidad de almacenarlo durante 4 días, período normal para el Uruguay de días consecutivos con exceso de sol/viento en algunas temporadas y de déficit en otras temporadas. Esto implicaría entonces tener capacidad –lo asumimos como una estimación mínima básica- para gestionar en forma flexible unos 4,4 GW*hr. Las baterías de litio, actualmente las más eficientes, tienen para aplicaciones macro como los coches eléctricos, precios –en base a la energía acumulada- en el orden de 500 U$S/(kW*hr). Si bien existen proyecciones a la baja de estos precios (Dept. of Energy - USA, 2017), algunas referencias pronostican dificultades ante un uso masivo (Morales, 2017). Con precios actuales la inversión necesaria inicial de stock de baterías, sería de unos U$S 2200:000.000, sin considerar costos de reciclado permanente en

[5] Este consumo sería del orden de magnitud de las 111.400 ton fuel-oil/gas-oil para generación termoeléctrica actuales (DNE - MIEM, 2017).

[6] Estos excedentes existen ya actualmente, con 23% de generación variable, según lo visto en Antecedentes.

[7] extrapolado con el 33% de aumento previsto del consumo, de los 0,8 GW*hr/día promedio diario exportado en 2018, calculado por el autor a partir de datos de la Administración del Mercado Eléctrico: 173 GW*hr exportados al 24/7/2018, www.adme.com.uy

caso que éste fuera técnicamente posible[8]. Se debería analizar la favorabilidad de este escenario desde el punto de vista económico. A nivel global, la alternativa más usual para gestionar generación variable, más bien es el de las hidroeléctricas reversibles y existen en el mundo ejemplos de instalaciones de este tipo con capacidad para gestionar 4,4 GW*hr y más, como la de Rocky Mountain, USA (Morales, 2017), pero se debería comprobar si existen en Uruguay todas las formaciones geográficas que lo permitan, con impacto económico y ambiental aceptable. Según versiones de prensa (Diario El País - Montevideo, 2015), UTE habría ubicado ya unas tres posibles localizaciones en el Norte uruguayo (Cerro Largo, Tacuarembó, Rivera) para estas hidroeléctricas reversibles, entre ellas una en Cuchilla Negra (Rivera), con capacidad para almacenar 300 MW durante varias horas; la probabilidad o certeza de que un escenario de uso de esta tecnología sea favorable, queda pues pendiente de la confirmación oficial de que éste sea efectivamente un Medio Potencial.

Como otra fuente de generación posible[9], hemos analizado la generación nuclear. Siendo la nuclear una fuente de generación de base (inflexible), su máxima participación posible, dependerá de las características de una red, en lo que refiere a oscilaciones de la demanda. Para estimar esta participación, hemos supuesto que el perfil de demanda uruguaya actual, con variaciones de 112% entre máximo y mínimos (potencia mínima promedio de 800 MW, setiembre-octubre; máximo de demanda: 1700 MW pico nocturno, invierno (Adm. Mercado Eléctrico, 2017) se mantenga para el consumo a 2050; este supuesto es conservador, ya que si se espera mayor industrialización del país, la demanda tenderá más bien a aplanarse. Sobre la base de la potencia mínima actual -extrapolada a 1065 MW en 2050- una central nuclear de 500 MWe podría funcionar sin dependencia de gestión por redes extranjeras, aunque representando el 23% de la demanda total del S.I.N. lo que podría traer algunas complejidades de gestión, al menos con los criterios actuales (Morales Rodríguez, 2012). Esa central nuclear, permitiría evitar la mayor parte de las emisiones por generación termoeléctrica antes vistas (Morales, 2017). Respecto al flujo de divisas, esa opción en principio también evitaría gran parte de los egresos corrientes por importación de combustible, ya que el costo de combustible nuclear es del orden del 10% del equivalente en petróleo (Morales Rodríguez, 2012), pero las inversiones requeridas son enormes y las dificultades estratégicas para construir y gestionar esa instalación, como se mencionó en los capítulos de Fase Diagnóstico son especialmente serias para un país como Uruguay. Pese a ello, y como también se vio en los capítulos de Diagnóstico, existen algunas Oportunidades en el Ambiente Externo y en el futuro pueden surgir otras que faciliten esa opción, en particular relacionadas al financiamiento por el Green Climate Fund, por tratarse de generación libre de CO2; no existen antecedentes al respecto, por lo que no le asignaremos probabilidad. Los países vecinos de Argentina y Brasil, tienen gran experiencia en el área nuclear, y teóricamente –no consideramos tampoco, probabilidades para este escenario- serían posibles acuerdos de cooperación; también se podría con certeza, contar con la cooperación multilateral del O.I.E.A. para asesorar (misiones C.O.R.R. del OIEA IAEA) en preparación previo al inicio de la construcción. Existen también otras oportunidades ciertas de cooperación multilateral como el Banco de Uranio de Bajo Enriquecimiento (IAEA, 2017)

[8] La probabilidad de un escenario en que efectivamente se logre una gestión técnica adecuada por baterías, con Medios Disponibles para el país, deberá entonces ser estudiada, junto con la favorabilidad económica, en todos los posibles contextos globales a futuro.

[9] Esta fuente, a efectos estratégicos no es un Medio Disponible ni Potencial, ya que no estaría disponible en forma previsible.

creado por el O.I.E.A. en Agosto 2017, con sede en Kazajstán, destinado a asegurar suministro continuo de uranio enriquecido para fines exclusivamente energéticos, principalmente a países en vías de desarrollo.

NECESIDADES:

De acuerdo a lo visto, surgiría la necesidad cerca de 2030 de introducir cambios al sistema eléctrico uruguayo, que perduren hasta 2050 o más allá. Se han señalado las principales alternativas posibles, todas las cuales implican escenarios estratégicos de amplia complejidad.

En siguientes entregas de la revista procuraremos seguir avanzando en el abordaje de dichos escenarios, buscando además una actualización permanente de éstos.

Referencias

Diario El País - Montevideo. (24 de Febrero de 2015). Recién en diez años se deberá acumular energía eólica.

Adm. Mercado Eléctrico. (2017). Informe Anual 2017. Montevideo.

Dept. of Energy - USA. (2017). Cost and Price Metrics for Automotive Lithium-ion Batteries.

DNE - MIEM. (2017). Balance Energético Nacional 2016. Montevideo.

IAEA. (29 de Agosto de 2017). IAEA LEU Bank reaches Milestone with Storage Facility Inauguration in Kazakhstan.

IAEA. (s.f.). Construcion Readiness Review. Vienna.

INE. (2014). Estimaciones y proyecciones de la población de Uruguay - Revisión 2013. Montevideo.

International Energy Agency. (Noviembre 2016). 20 Years of Carbon Capture and Storage. Accelerating Future Deployment. Paris.

International Energy Agency-OCDE. (2016). Key World Energy Statistics. París.

MIEM - DNE. (2009). Política energética 2005-2030. Montevideo.

Morales Rodríguez, E. (2012). Un Uruguay nuclear? Respuestas sobre seguridad y regulación estatal. Saarbrücken: Editorial Académica Española.

Morales, E. (2017). Perspectivas de la energía nuclear en el contexto de mitigación del cambio climático. VI Encuentro Regional de Ingeniería Química. Montevideo.

ONU - UNFCC. (2015). Conference of the Parties. Twenty-first session. Paris.

ONU. (2015). 17 Sustainable Development Goals. New York.

Pastermak, A. (s.f.). Rep. UCRL-ID-140773. Lawrence Livermore National Laboratory.

CONSIDERACIONES SOBRE LA CIBERAMENAZA A LA SEGURIDAD NACIONAL ∞*

Alejandro Amigo Tossi[1]

RESUMEN

La ciberamenaza es uno de los principales riesgos para la seguridad de los países desarrollados, como también de los Estados en vías de desarrollo como el nuestro. Este fenómeno es uno de los retos a la seguridad nacional que exige la adopción de un enfoque integral en su análisis, que contemple los aspectos que han transformado a los actores y acciones maliciosas de este ámbito en uno de los principales desafíos a la seguridad de organizaciones estatales y privadas en todo el mundo. Estados, hackers, hacktivistas y cibercriminales han sido protagonistas de diversos actos que han configurado una nueva dimensión para la seguridad nacional e internacional. El propósito de este artículo es proponer los tópicos que podrían incluirse en la apreciación nacional sobre la ciberamenaza a la seguridad nacional de Chile, basado en ciertas definiciones conceptuales, los ciberataques que han afectado a organismos del gobierno de Chile e instituciones de la defensa y por último, las consideraciones sobre la ciberamenaza incluidas en las Estrategias de Seguridad Nacional de ciertas potencias occidentales.

Palabras clave: Seguridad Nacional, Defensa Nacional, Ciberespacio, Ciberamenaza, Planificación nacional.

∞ Este artículo fue publicado en la Revista Política y estrategia Nro. 125 (2015). Editada por: Academia Nacional de Estudios Políticos y estratégicos (ANAPE) Chile.

*Fecha de recepción: 220914
Fecha de aceptación: 040615

[1]Oficial de Estado Mayor, Ejército de Chile. Master of Arts in Security Studies, Georgetown University. Magíster en Conducción Militar, Academia de Guerra, Ejército de Chile. Licenciado en Ciencias Militares, Escuela Militar. Autor del blog "Ciberestrategia" https://ciberestrategia.wordpress.com/. Actualmente es parte del Grupo de Planificación Estratégica de la Dirección de Operaciones del Ejército de Chile. alejandroamigotossi@gmail.com.

NATIONAL SECURITY IMPLICATIONS OF CYBER THREATS ABSTRACT

ABSTRACT

Cyber threat is one of the main risks for security in development countries, as well in States on the development path, such as ours.
This phenomena is a challenge to national security, that needs the adoption of a paramount approach in its analysis, that have to consider all the aspects that had transformed the actors and malevolent actions in this environment in one of the most important challenges to the security of governmental as well as private organizations all over the world. States, hackers, cyber activists and cybercriminals has been main actors in several situations that had shaped a new dimension for international and national security. The purpose of this article is to propose topics that could be included in the national assessment for cyber threats to the Chilean national security, based upon several conceptual definitions, cyberattacks already executed to state and military organization's in Chile, and lastly, considerations over cyber threats included in the National Security Strategies of some western powers.
Key words. National Security, National Defense, Cyberspace, cyber threats, national Planning.

Introducción

La ciberamenaza forma parte de los riesgos a la seguridad nacional de los países desarrollados, pero también afecta a los Estados en vías de desarrollo, donde organizaciones estatales y empresas privadas han incorporado en sus procesos de funcionamiento las nuevas tecnologías que emplean el ciberespacio. Este último es el caso de Chile, donde el uso masivo de internet y redes informáticas es un aspecto fundamental en todos los ámbitos del quehacer nacional. El Estado chileno es el país latinoamericano con mayores avances en gobierno electrónico según la Encuesta de Desarrollo del Gobierno Electrónico de las Naciones Unidas[2]. Además, de acuerdo con el UN E-Government Development Survey, Chile es el país con la mayor evolución digital en la región[3]. Estos antecedentes hacen evidente que la ciberamenaza es parte de los retos a la seguridad nacional, exigiendo un análisis integral que defina los riesgos que en este dominio el país enfrentará en el corto y mediano plazo y que considere los últimos acontecimientos nacionales y la experiencia de ciertos países que están a la vanguardia en esta área. El propósito de este artículo es desarrollar un breve análisis de la ciberamenaza a la seguridad nacional de Chile, teniendo como referencia ciertas nociones básicas sobre la temática, los ataques que han acaecido sobreobjetivos nacionales y la apreciación estratégica de

[2]http://unpan3.un.org/egovkb/datacenter/CountryView.aspx
[3]Economist Intelligence Unit & IBM. "Digital economy rankings 2010: Beyond e-readiness". 2010. p. 4.

la amenaza procedente del ciberespacio por parte de tres potencias occidentales. A partir de esta revisión, se propone la consideración de ciertos temas en la apreciación que el Estado chileno debiera desarrollar sobre esta amenaza. El artículo se divide de la siguiente manera. En primer lugar, se desarrolla un breve marco teórico para conceptualizar los actores y fenómenos en el ámbito de la ciberamenaza que debieran considerarse para el análisis de la realidad nacional. En segundo lugar, se describen algunos ciberataques que han afectado a organismos del gobierno de Chile e instituciones de la defensa, como evidencias de la amenaza actual procedente del ciberespacio. En tercer lugar, se analiza el contenido sobre la ciberamenaza en las Estrategias de Seguridad Nacional de ciertas potencias occidentales que en el ámbito de la defensa podrían ser referentes para Chile. Por último, como conclusión, se proponen algunos aspectos que deberían ser contemplados en la evaluación de la ciberamenaza a la seguridad nacional.

Conceptualización de la ciberamenaza

El ámbito donde se desarrollan y actúan las ciberamenazas es el ciberespacio, el cual entenderemos como un dominio interactivo compuesto por redes digitales que se utilizan para almacenar, modificar y comunicar información; incluyendo internet y otros sistemas de información que apoyan a las organizaciones, empresas, infraestructuras y servicios[4]. Por tanto, los ciberactores son aquellos elementos que llevan a cabo algunas de las acciones explicadas más adelante en el dominio del ciberespacio. Los ciberactores que perpetran operaciones maliciosas contra Estados, sus instituciones y organizaciones privadas es posible separarlos en cinco grupos: actores estatales con cibercapacidades como parte de sus activos de defensa, terroristas, elementos del crimen organizado, hacktivistas[5] y hackers patriotas[6]. En el caso de los actores estatales, un ejemplo es el indicado por el reporte de la empresa norteamericana de ciberseguridad Mandiant que identifica como "APT-1" a un grupo situado en China que contaría con el apoyo del gobierno chino y posee diversas similitudes con una unidad del Ejército Popular Chino. Según este informe, esta unidad es capaz de desarrollar una avanzada y persistente amenaza a intereses norteamericanos[7].Otro caso, es el ataque a los sistemas computacionales de la empresa Sony, supuestamente por parte del Estado Norcoreano según EE.UU., que incluso resultó en ciberataques de respuesta por parte de la potencia norteamericana[8]. El ciberespacio es un dominio al cual los terroristas buscarán expandir las acciones de terror para el logro de sus objetivos políticos. El bloqueo de las emisiones del canal francés TV5 el mes de abril pasado, por parte de un grupo que proclamó su lealtad al Estado Islámico, es un ejemplo de este tipo de hechos[9]. En cuanto al crimen organizado, un reporte de la empresa McAfee, señala que este es un negocio ilícito donde los riesgos, que asumen los responsables, son bajos en comparación con las exorbitantes ganancias, y que sus operaciones implican pérdidas globales anuales

[4]UK Government. "The UK Cyber Security Strategy". Noviembre 2011.

[5]Término utilizado para describir a los hackers que su principal objetivo es realizar activismo mediante acciones en redes y sistemas informáticos.

[6]Término utilizado para describir a los hackers que realizan ataques a otros Estados que son percibidos como adversarios por parte de sus propios Estados.

[7]Mandiant. "APT1 Exposing One of China's Cyber Espionage Units". Intelligence Report. 2014.

[8]http://www.bloomberg.com/politics/articles/2015-03-17/north-korea-web-outage-was-response-to-sonyhack-lawmaker-says. Último acceso el 19 de marzo de 2015.

[9]http://www.independent.co.uk/news/uk/home-news/bbc-says-feared-isis-cyber-attack-during-live-news-broadcast-was-actually-operational-error-10167537.htmlÚltimo acceso el 2 de junio de 2015.

aproximadas de 400 billones de dólares la economía mundial[10] . Los hacktivistas como "Anonymous" llevan a cabo ataques a sitios web como protestar en defensa de ciertos derechos civiles en el contexto de conflictos intraestatales o de tipo global. Nuestro país ha sido víctima de la acción de este último grupo, y algunos casos serán mencionados más adelante. Por último, los hackers patriotas han participado en el contexto de crisis interestatales, donde realizan ataques sin ninguna dirección o patrocinador, con el único fin de apoyar a sus respectivas naciones en la prosecución de los objetivos[11]. El rol de estos últimos en la agresión rusa contra Georgia en el año 2008, se concentró en ataque a sitios web gubernamentales e incluso superó el periodo de tiempo en que Rusia hizo uso de la fuerza[12]. Es importante además mencionar la acción conjunta entre Estados y actores no estatales patrocinados por los primeros, donde la diferencia entre ambos se vuelve difusa. Algunos Estados han utilizado hackers de orientación nacionalista y hacktivistas para ocultar su responsabilidad y evitar la consiguiente atribución[13]. Estos actores no estatales con el apoyo financiero y técnico de un aparato estatal, aumentan sus capacidades y logran ejecutar acciones con altas probabilidades de infligir graves daños a objetivos más relevantes. Los casos de ataques atribuidos a China por parte de EE.UU. hacia organizaciones privadas y estamentos estatales de esa nación, son ejemplos recientes de este fenómeno[14].

Otro punto son las técnicas que utilizan los ciberactores y los objetivos por alcanzar en el marco de sus acciones contra las redes y sistemas informáticos de organismos estatales y privados. Dentro de las técnicas encontramos la acción de virus o troyanos en sistemas informáticos, denegación del servicio en sitios web, robo de información sensible, fraude, eliminación de la información en computadores y bases de datos y la inutilización o control remoto de sistemas de control de infraestructura crítica. El ataque del virus Stuxnet, atribuido a EE.UU. e Israel, que destruyó entre 1.000 a 6.000 máquinas centrífugas que enriquecían uranio en plantas nucleares de Irán[15], es una demostración de la última técnica señalada. En cuanto a los objetivos de los ciberataques, más allá de las actuales acciones en contra de redes computacionales, bases de datos y sistemas de correos corporativos, en un futuro previsible las acciones más riesgosas serán ataques contra infraestructuras civiles vitales (centrales nucleares, represas, sistemas de distribución de energía, servicios básicos, etc.) no necesariamente en el contexto de los conflictos armados, y acciones contra redes y/o sistemas de información de las Fuerzas Armadas durante crisis o conflictos[16]. En cuanto a los métodos empleados para afectar los intereses de un país, es posible separarlos en dos tipos: la explotación de redes informáticas y ataques propiamente tal. La explotación corresponde a actividades de espionaje a redes del gobierno, industria de defensa y Fuerzas Armadas con el objetivo de alcanzar un dominio de la información desde tiempo de paz. Esta superioridad incluso podría otorgar a potenciales

[10]McAfee & Center for Strategic and International Studies. "Net Losses: Estimating the global cost of Cybercrime". 2014.
[11]Carr, Jeffrey. "Inside Cyber Warfare". O'Reilly Media, Inc., 2010. p. 15.
[12]http://www.foxnews.com/story/2008/08/13/russian-hackers-attack-georgia-in-cyberspace/
[13]Ibid. p. 115. Último acceso el 11 de agosto del 2014.
[14]http://www.washingtonpost.com/world/national-security/2014/03/24/74aff686-aed9-11e3-96dc-d6ea14c099f9_story.html
[15]http://www.washingtonpost.com/world/national-security/stuxnet-was-work-of-us-and-israeli-experts-officials-say/2012/06/01/gJQAlnEy6U_story.html. Último acceso el 22 de agosto del 2014.
[16]Clarke, Richard y Knake, Robert. "Cyber War, the next threat to National Security and what to do about it". Ecco Editorial, 2010. p. 107.

enemigos la ventaja de incrementar su preparación para enfrentar ciberataques de represalia. Adicionalmente, la explotación tendrá como propósito preparar futuros ataques contra redes informáticas o sistemas que controlan actividades industriales vitales en caso de crisis o conflictos de baja intensidad. Los ciberataques corresponden a denegaciones de servicio, introducción de virus, malware y/o troyanos que causarán pérdida de información o impedirán el normal servicio de redes, servicios web y de correo, y sistemas informáticos. La evidencia internacional demuestra que los ataques más importantes son "denegación de servicio" contra redes gubernamentales y sitios web de empresas privadas para interrumpir o deshabilitar su funcionamiento normal; ataques destinados a borrar o destruir información vital en entidades privadas o estatales y ataques para degradar o alterar sistemas de control industriales. Además, los sistemas de mando y control y redes institucionales de las Fuerzas Armadas, serán vulnerables a ataques destinados a reducir la capacidad de la fuerza militar para dirigir y controlar las operaciones en los otros dominios de la guerra. La complejidad de las acciones en el ciberespacio dificultan la defensa y disuasión contra estas operaciones. La atribución de un ataque va más allá de determinar el origen de los autores. La acción de identificar al o los responsables de un ciberataque debe relacionarse con el contexto de una crisis o con anteriores acciones similares. El caso del destructivo virus Shamoon en las redes informáticas de la petrolera estatal saudí Aramco y su consecuente atribución por parte de EE.UU. y Arabia Saudita al Estado de Irán[17], es un ejemplo donde un escenario estratégico de confrontación entre potencias regionales sirvió de base para especular sobre el supuesto responsable. Sin embargo, en caso de que la atribución sea correcta, será complejo ejecutar una acción de respuesta o procurar una sanción internacional, debido a la ausencia de normas reconocidas globalmente en el dominio del ciberconflicto. Además, la ambigüedad de la evaluación de un ciberataque como uso letal de la fuerza de acuerdo con el derecho internacional, significará un desafío adicional para que el Estado afectado planifique algún tipo de respuesta. Por último, un aspecto relevante son los propios usuarios de los sistemas informáticos. Esta amenaza interna estará siempre presente a pesar del nivel de seguridad alcanzado en las propias redes, y podrá comportarse como un facilitador de un ataque o simplemente en ejecutor de acciones maliciosas. Los casos de Snowden y Manning, en la Agencia de Seguridad Nacional norteamericana y el Ejército de EE.UU. respectivamente, son ejemplos del alcance y daño que pueden provocar la acción de "insiders".

Chile bajo la ciberamenaza

Chile, en su condición de sociedad abierta, interconectada con el mundo y con un alto grado de avance digital, tiene una mayor exposición a los riesgos en el ámbito de las redes y sistemas informáticos, que previsiblemente se irán consolidando como parte de las amenazas que afectarán a la seguridad nacional. Por ejemplo, un evento organizado por Naciones Unidas sobre ciberseguridad y desarrollo entregó como conclusión que los países en vías de desarrollo como Chile tienen un mayor riesgo de ser blanco de ciberataques y que el impacto económico y consecuencias contra la infraestructura crítica, el sistema bancario, los sistemas nacionales de salud, el gobierno y bancos de datos de la industria y servicios podrían ser de alto impacto[18]. Es

[17]http://www.nytimes.com/2012/10/24/business/global/cyberattack-on-saudi-oil-firm-disquiets-us.html?_r=2 Último acceso el 16 de septiembre del 2014.

[18]http://www.un.org/apps/newsstory.asp?Cr=cyber&NewsID=40692#.UXR6xitAQW9. Último acceso 21 de abril del 2014.

decir, un sostenido crecimiento económico, la adopción de tecnologías de informática y computación avanzadas y el creciente uso de internet son las condiciones ideales para un incremento de la ciberamenaza. Lo anterior, es respaldado por un informe de KasperskyLab, el cual señala que Chile ocupa el puesto número uno de los países latinoamericanos que son víctimas de ciberataques[19]. A la fecha, los principales ciberataques contra intereses nacionales han sido acciones de actores no estatales en apoyo a movimientos civiles de protesta, operaciones destinadas a robar información o cometer delitos y por último, espionaje de correos electrónicos de instituciones de la defensa nacional. Uno de los primeros episodios ocurrió en el año 1995, con el hackeo del sitio web de la "Cumbre de Presidentes de América", donde el dominio fue intervenido y reemplazado por propaganda en contra de la reunión internacional[20]. Luego, en 1996 fue saboteada la red informática del Servicio de Impuestos Internos y perturbado su funcionamiento, con el consiguiente daño en su nivel de confianza pública[21]. Durante los últimos cinco años ha existido un incremento en los tres tipos de ataques mencionados en el párrafo anterior, lo que ha incrementado la atención pública sobre el tema. Con respecto a hacktivistas que han apoyado movimientos de protesta, el actor principal ha sido el actor no estatal "Anonymous Chile". Esta franquicia nacional ha sido responsable de ataques contra sitios web de organizaciones públicas y privadas, donde los dominios han sido víctimas de "denegación de servicio" y su contenido ha sido sustituido por propaganda contra políticas gubernamentales o empresas involucradas con cuestiones ambientales. Los principales ejemplos de estos casos son los siguientes:

- Junio del 2011, "Operación Andes libre" atribuida por Anonymous. En respuesta a la supervisión del Estado en el contenido de la web en territorio nacional. Sus acciones fueron la denegación de servicio de sitios web gubernamentales relacionados con el tema[22].

- Julio del 2012, "Operación Chile 2012" atribuida por Anonymous. Su objetivo fue la defensa de una serie de derechos cívicos y la denuncia de ciertas políticas ambientales del gobierno. Sus acciones fueron la denegación de servicio de sitios web del gobierno y empresas privadas relacionadas con proyectos hidroeléctricos[23].

En relación a las acciones destinadas a robar información, estas han correspondido a ataques contra sitios web del gobierno y actividades cibercriminales contra individuos. El principal ejemplo del primer caso, fue el robo de información privada de seis millones de personas desde las bases de datos de organismos públicos, que fueron subidos a internet el día siguiente. Los sitios web atacados fueron el Ministerio de Educación, la Dirección General de Movilización Nacional y el Servicio Electoral de Chile[24]. En cuanto a ataques orientados a instituciones de la defensa nacional, durante el mes de agosto del año 2014, se conoció una acción de hackers peruanos que vulneraron la ciberseguridad de la Fuerza Aérea de Chile y

[19]http://www.emol.com/noticias/tecnologia/2012/09/13/560281/chile-entre-los-paises-que-sufre-masciberataques-en-america-latina.html. Último acceso 18 de abril del 2014

[20]http://www.policia.cl/paginas/brigadas/bg-bricib/bg-bricib.htm. Último acceso el 14 de abril del 2013.

[21]Ibíd. Último acceso el 14 de abril del 2014.

[22]http://elcomercio.pe/actualidad/791354/noticia-anonymous-lanzara-ciberataques. Último acceso el 17 de abril del 2014.

[23]http://www.latercera.com/noticia/nacional/2012/07/680-475213-9-anonymous-lanzo-operacion-operacionchile2012-contra-sitios-chilenos.shtml. Último acceso el 17 de abril del 2014.

[24]http://news.bbc.co.uk/hi/spanish/latin_america/newsid_7395000/7395288.stm. Último acceso el 15 de abril del 2014.

filtraron cientos de correos electrónicos de la institución. Dentro de la información revelada se encontraban detalles de negociaciones entre la institución y empresas de defensa para la compra de armamento, radares y el desarrollo de overhaul de sistemas de armas institucionales[25].

La ciberamenaza según las potencias occidentales

La ciberamenaza representa un aspecto relevante en las estrategias de seguridad nacional de algunas de las principales potencias occidentales. Para demostrar lo anterior, se analizarán brevemente las versiones de Estados Unidos, Reino Unido y Australia, con el objetivo de identificar aspectos que debiera considerar una apreciación sobre la ciberamenaza hacia los intereses de Chile. En general, estos documentos contienen una descripción global del fenómeno, que considera algunos tópicos que no forman parte del debate nacional, y plantean una interacción entre el tema en comento y otros fenómenos transnacionales. Aunque los textos reflejan la realidad de cada país en su dimensión nacional, regional e internacional, es importante que nuestra nación considere estas referencias para ser incluidas en nuestro escenario estratégico.

La Estrategia de Seguridad Nacional de EE.UU., 2010

La estrategia de EE.UU. en su versión 2010, consideró la ciberamenaza como parte de los retos a uno de sus principales intereses nacionales, la "seguridad". El documento declara que la ciberamenaza es uno de los más complejos desafíos para su estabilidad interna[26]. El texto describe claramente que las fortalezas de Estados Unidos en diversas áreas, son al mismo tiempo, su principal debilidad frente a ciberenemigos.

> "… nuestras redes gubernamentales son constantemente sondeadas por intrusos… adversarios podrían utilizar vulnerabilidades para interrumpir el suministro en una escala masiva. En el internet y comercio electrónico… cibercriminales generan cientos de millones de dólares de pérdidas a empresas y consumidores, como también el robo de valiosa propiedad intelectual"[27].

Este párrafo contiene dos aspectos principales. Primero, para los EE.UU. la ciberamenaza se centra en la defensa nacional, la seguridad pública y la economía; ámbitos donde han ocurrido los principales acontecimientos en el ciberespacio. Segundo, confirma que cuanto más alto el nivel de desarrollo de un país, más peligrosa es la ciberamenaza en contra de sus intereses nacionales y la seguridad nacional. Posteriormente, el documento norteamericano declara que sus ciberamenazas comprenden hackers individuales, grupos delictivos organizados, redes terroristas y Estados que disponen de avanzada tecnología en esta área[28]; incorporando a los grupos terroristas en los actores que operan activamente en el ciberespacio. En resumen, el contenido de la estrategia estadounidense permite deducir algunos aspectos que

[25]http://www.elmostrador.cl/pais/2014/08/14/hackers-peruanos-vulneran-seguridad-de-la-fach-y-filtrancientos-de-correos-electronicos-de-la-institucion/ Último acceso el 15 de agosto del 2014.
[26]El Presidente de Estados Unidos. "The United States National Security Strategy", 2010. p. 27.
[27]Ibid.
[28]Ibid.

deberían ser parte de la apreciación nacional sobre la temática. En primer lugar, la importancia de señalar claramente cuáles son los ámbitos del nivel nacional que podrían ser los principales objetivos de la ciberamenaza. En segundo lugar, la importancia de asumir que el avance del país hacia el desarrollo incrementará los riesgos en este ámbito. En tercer lugar, la necesidad de identificar los potenciales ciberactores según la realidad nacional.

Estrategia Nacional de Seguridad del Reino Unido, 2010

La Estrategia Nacional de Seguridad del Reino Unido contempla la ciberamenaza como uno de los riesgos prioritarios a su seguridad, en el mismo nivel del terrorismo, las crisis militares internacionales y los desastres naturales. El documento señala que la amenaza en cuestión no es un riesgo futuro, sino que en la actualidad el gobierno, el sector privado y los ciudadanos están bajo ataques sostenidos, por parte de Estados hostiles o de organizaciones criminales[29]. La Estrategia en uno de sus párrafos declara lo siguiente: "La actividad en el ciberespacio seguirá evolucionando como una amenaza directa a la seguridad y economía del país, mientras sigue perfeccionándose como un medio de espionaje y crimen, y continúa creciendo como un facilitador del terrorismo, así como un arma militar para uso de los Estados y, posiblemente, otros actores"[30]. Esta declaración acerca de la ciberamenaza tiene dos aspectos relevantes. El Reino Unido la considera como uno de los activos de la defensa que serán empleados por actores estatales en caso de crisis o conflicto militar. Además, es evaluada como una herramienta disponible para las redes terroristas, que podrían atacar su territorio o intereses en el extranjero. Por otra parte, el documento declara que los ataques en el ciberespacio podrían tener un efecto potencialmente devastador y que el gobierno, la fuerza militar, ciertos objetivos industriales y económicos (incluyendo los servicios críticos), podrían verse perturbados por adversarios que cuenten con la tecnología necesaria[31]. En síntesis, la estrategia del Reino Unido contiene algunos puntos que sería significativo explicitar en el caso nacional. En primer lugar, la importancia de considerar la relación que existe entre redes terroristas y/o subversivas y el ciberespacio como un medio para influenciar las acciones del Estado de Chile. En segundo lugar, la ciberamenaza debe ser considerada como parte del inventario bélico que podría ser utilizado en el contexto de un conflicto. En tercer lugar, la importancia de asumir los efectos devastadores que un ciberataque podría tener en contra de bienes económicos vitales o servicios públicos en el futuro cercano.

La Estrategia Nacional de Seguridad de Australia, 2012

Este documento, al igual que los otros dos casos, puntualiza a la ciberamenaza como uno de los principales riesgos para su seguridad. La estrategia afirma que la ciberactividad maliciosa es una creciente, y siempre cambiante, amenaza a la seguridad nacional a través de actividades terroristas, el crimen organizado y el espionaje[32]. El documento australiano declara que si las acciones en el ciberespacio con intención de causar daños no se controlan, tienen el

[29]HM Government. "The United Kingdom National Security Strategy", 2010. p. 29.
[30]Ibid.
[31]Ibid. p. 30.
[32]Gobierno de Australia. "The Australian National Security Strategy". 2012. p. iii.

potencial de socavar la confianza en la estabilidad social y económica y la prosperidad de la nación[33]. El texto además explica que la dependencia de internet y sistemas informáticos ha incrementado la exposición de Australia al ciberespionaje. El documento asume que las actividades de espionaje colocan una serie de intereses nacionales en riesgo, incluyendo: información gubernamental clasificada, información comercial con consecuencias directas para la economía, propiedad intelectual y datos privados de los ciudadanos[34]. En otra sección se señalan otras actividades maliciosas en el ciberespacio tales como: servicios de inteligencia extranjeros que utilizan el internet para infiltrarse en los sistemas propios, coordinación de grupos extremistas y radicalización de nuevos reclutas y el internet como medio para promover el odio y la división entre grupos de la sociedad[35]. En conclusión, el documento australiano contiene los siguientes temas que podrían incluirse en el proceso de análisis nacional. En primer lugar, la importancia de describir las consecuencias a largo plazo de que el país sea un objetivo permanente de los ciberataques. En segundo lugar, la importancia de evaluar en forma precisa los objetivos principales de las actividades de ciberespionaje. Finalmente, que la inclusión de otras actividades maliciosas en internet, además de los ciberataques, es relevante para una completa evaluación de la amenaza que en este dominio enfrentará el Estado chileno.

Conclusión

La evaluación nacional de la ciberamenaza debe considerar como referencias, entre otros aspectos, el estado del arte sobre el tema, los acontecimientos nacionales e internacionales y la estimación de referentes internacionales. En cuanto al contenido, el documento al menos, debería referirse a los actores, objetivos, métodos, complejidad, inminencia y la multidimensionalidad del tema. La defensa nacional debe definir con precisión la amenaza que Chile ya está enfrentando y la que probablemente afrontará en un futuro próximo. Aunque nuestros intereses nacionales y escenario estratégico poseen particularidades, si el Estado Chileno continúa avanzando hacia el desarrollo, la evidencia internacional permite asumir que enfrentará con mayor frecuencia la acción de algunos de los ciberactores mencionados. La estimación de la ciberamenaza será la principal guía para planificar la respuesta nacional, por tanto esta debería incluir los siguientes conceptos. En primer lugar, convendría considerar el amplio espectro de actores que han desarrollado acciones contra el Estado Chileno, principalmente hacktivistas y cibercriminales, y los que han protagonizado incidentes en el nivel internacional. Además, debería incorporar la interacción entre los diferentes actores, tanto la relación entre Estados y grupos no estatales y estos últimos con otras amenazas emergentes. En segundo lugar, correspondería analizar todos los métodos y objetivos que se han identificado en los últimos eventos y así permitir la programación de distintas respuestas nacionales. Por último, se debe catalogar la ciberamenaza entre actividades de explotación de redes, ciberespionaje, cibercrimen y ataques propiamente tal a redes informáticas y/o sistemas de control industrial. Un enfoque integral que incluya todos estos aspectos, permitiría comprender la complejidad del fenómeno y los retos que plantea a nuestra nación. La apreciación tendría que ser priorizada conforme a la realidad nacional y su probable evolución. Es decir, los ciberataques o el espionaje que han afectado a organizaciones estatales y empresas privadas debieran ser considerados

[33]Ibid. p. 11.
[34]Ibid. p. 16.
[35]Ibid. p. 40.

como los de mayor riesgo e inminencia. Asimismo, los acontecimientos que están ocurriendo en otras regiones del mundo deberían ser incluidos como potenciales peligros que pudieran materializarse en el futuro cercano. Por último, sería relevante indicar los principales intereses nacionales que serían objetivos potenciales de acciones en el ámbito del ciberespacio, tanto en tiempo de paz como en crisis o conflicto. Además, señalar los efectos previsibles que la ciberamenaza podría tener contra activos económicos vitales y servicios públicos, con el objetivo de generar las medidas preventivas, de respuesta y remediales con respecto al tema. Este breve análisis y consecuentes proposiciones buscan ser un aporte para desarrollar una evaluación actualizada y completa sobre la ciberamenaza que enfrenta y afrontará el Estado chileno. Una apreciación realista y contextualizada sobre este nuevo dominio en el escenario de seguridad nacional e internacional facilitaría la respuesta nacional. En el ciberespacio la ventaja está de lado del que ofende y los Estados deben ser previsores para disminuir esa brecha.

Referencias

CARR, Jeffrey. “Inside Cyber Warfare”. O’Reilly Media, Inc., 2010.

CLARKE, Richard y Knake, Robert. “Cyber War, the next threat to National Security and what to do about it”. Editorial Ecco, 2010.

Economist Intelligence Unit & IBM. “Digital economy rankings 2010: Beyond e-readiness”. 2010.

Gobierno de Australia. “TheAustralianNational Security Strategy”. 2012.

Gobierno del Reino Unido. “The United Kingdom National Security Strategy”. 2010.

Gobierno del Reino Unido. “The UK Cyber Security Strategy”. Noviembre 2011.

Mandiant. “APT1 Exposing One of China’s Cyber Espionage Units”. Intelligence Report. 2014.

McAfee & Center for Strategic and International Studies. Net Losses: Estimating the global cost of Cybercrime. 2014.

Ministerio de Defensa de Chile. “Estrategia Nacional de Seguridad y Defensa de Chile”. 2012.

Presidencia de Estados Unidos. “TheUnitedStatesNational Security Strategy”. 2010.

Sitios web

http://diario.elmercurio.com/detalle/index.asp?id=%7B37c95938-4e8b-48d9-97e2-886d3d3668df%7D

http://elcomercio.pe/actualidad/791354/noticia-anonymous-lanzaraciberataques.

http://news.bbc.co.uk/hi/spanish/latin_america/newsid_7395000/7395288.stm.

http://unpan3.un.org/egovkb/datacenter/CountryView.aspx

http://www.bloomberg.com/politics/articles/2015-03-17/north-korea-web-outagewas-response-to-sony-hack-lawmaker-says.

http://www.elmostrador.cl/pais/2014/08/14/hackers-peruanos-vulneranseguridad-de-la-fach-y-filtran-cientos-de-correos-electronicos-de-lainstitucion/

http://www.emol.com/noticias/tecnologia/2012/09/13/560281/chile-entre-lospaises-que-sufre-mas-ciberataques-en-america-latina.html.

CIBERDEFENSA Y CIBERSEGURIDAD: NUEVAS AMENAZAS A LA SEGURIDAD NACIONAL, ESTRUCTURAS NACIONALES DE CIBERDEFENSA, ESTRATEGIAS DE CIBERSEGURIDAD Y COOPERACIÓN INTERAGENCIAS EN ESTE ÁMBITO*

Pablo Camps[1]

RESUMEN

Las nuevas tecnologías de la información y de las comunicaciones dieron origen al ciberespacio. El mismo constituye el quinto dominio de interacción humana, y cada día se hace más extenso albergando más información y brindando más y más servicios. Como resultado, este nuevo espacio ha dado lugar a la aparición de nuevas amenazas creadas por individuos, organizaciones o Estados que buscan aprovecharse esta nueva forma virtual de interactuar. Las actividades ilícitas en este medio pueden causar efectos muy importantes a la víctima y reportar importantes beneficios al perpetrador, quien además muchas veces no puede ser identificado.

Los Estados, como garantes de la seguridad y tranquilidad de sus habitantes han debido adaptar sus estructuras y marcos normativos para prevenir y enfrentar este nuevo escenario donde las fronteras no son claras, y los actores pueden no identificarse claramente.

El presente trabajo se enfoca en la situación de la República Oriental del Uruguay en lo referente a su grado de seguridad y capacidad de defensa en el ciberespacio.

Para ello, se presentan inicialmente las nuevas amenazas identificadas por la legislación nacional, para pasar luego al detalle de las estructuras más

*Este artículo fue publicado en el libro de Ciberdefesa e Cibersegurança: Novas Ameaças à Segurança Nacional (2016) editado por la Escuela Superior de Guerra de Brasil.

[1]Coronel de Artillería; Ingeniero Militar en Informática (I.M.E.S. 2001); Ingeniero en Informática (Universidad Católica 2006); Licenciado en Ciencias Militares (I.M.E.S. 2009); Diplomado en Estado Mayor; Actualmente es Jefe del Departamento de Sistemas de Información del Ministerio de Defensa Nacional.

importantes encargadas de prevenir o repeler un eventual ataque. Finalmente se discute la situación actual del País en cuanto a una estrategia de ciberseguridad.

Palabras clave: Ciberespacio, Ciberseguridad, Ciberdefensa, Uruguay, Nuevas tecnologías.

Introducción

Para referirnos a la ciberseguridad y la ciberdefensa debemos comenzar por definir ambos términos para evitar ambigüedades. De acuerdo con el Consejo Argentino de Relaciones Internacionales[2] la ciberdefensa es un "conjunto de acciones de defensa activas, pasivas, proactivas, preventivas y reactivas para asegurar el uso propio del ciberespacio y negarlo al enemigo o a otras inteligencias en oposición". Por su parte la ciberseguridad es definida como el "conjunto de acciones de carácter preventivo que tienen por objeto el asegurar el uso de las redes propias y negarlo a terceros". Si bien las definiciones tienen parte común, podemos diferenciar un término del otro considerando que la ciberseguridad se refiere más a lo preventivo para evitar que se tenga lugar un ataque, mientras que la ciberdefensa se identifica más con lo reactivo frente a un ataque.

Otro elemento que puede llegar a crear interrogantes es que tipo de estructuras deben articularse por parte de los estados para tener una adecuada seguridad en el ciberespacio. Sobre este punto, considerando que una cadena es tan frágil como su eslabón más débil, las soluciones más efectivas serán las que se establezcan estructuras robustas partiendo desde individuos que operan equipos en el ciberespacio formados y concientizados sobre la importancia de la seguridad, pasando por equipos con adecuados niveles de seguridad, software seguro y correctamente configurado y equipos de monitoreo y respuesta capaces de detectar amenazas y prevenir ataques antes de que ocurran o de que causen mayores daños en caso de concretarse.

El ciberespacio llegó para quedarse, y cada vez se extiende más en el actual mundo globalizado. Este nuevo ámbito de interacción humana está abierto a los diferentes actores que pueden ser tanto atacantes como víctimas. En este medio, los ataques pueden ser de alta complejidad patrocinados por estados o empresas privadas, pueden venir de grupos organizados con fines terroristas o activistas, de organizaciones delictivas o de simples individuos. Pueden ser dirigidos o genéricos y atacar blancos gubernamentales, empresariales o particulares con objetivos dispares según el caso. Lo blanco y lo negro no son la norma en este espacio donde priman los grises y no es siempre fácil determinar si un ataque es un delito común, un acto terrorista o un ataque que puede afectar la seguridad nacional, y lo que es peor aún no siempre se puede identificar al atacante.

[2]CONSEJO ARGENTINO DE RELACIONES INTERNACIONALES (2013)

Nuevas amenazas
Generalidades

Desde la llegada de las nuevas tecnologías de la información, se ha buscado a través de ellas facilitar tareas a sus usuarios, brindarle nuevos servicios y posibilidades muy variadas. Así fue posible progresivamente el procesamiento automático de la información, y posteriormente la comunicación entre computadores utilizando redes que se extendieron más y más hasta cubrir todo nuestro planeta. La creación de Internet, marca sin lugar a dudas un hito trascendente en la evolución delas nuevas tecnologías, pero el crecimiento exponencial en lo que a procesamiento y comunicaciones digitales se refiere ha alcanzado niveles no imaginados hace tan solo un par de décadas. En nuestros días es cada vez más común hablar de dispositivo inteligentes, utilizando un concepto tradicionalmente asociado exclusivamente con el ser humano. De esta forma además de los teléfonos inteligentes que son de accesibilidad casi universal en el mundo desarrollado, agregamos los televisores inteligentes, las señales de tránsito inteligentes, vehículos inteligentes, y muchos dispositivos o aparatos que incluyen ese adjetivo en su descripción, y que basan las prestaciones que brindan en las tecnologías de la información y de las comunicaciones.

El amplio y vertiginoso crecimiento en torno a las tecnologías de la información paulatinamente abrió un nuevo espacio para el desarrollo de las actividades humanas: el ciberespacio. Éste se constituyó de acuerdo con la revista The Economist[3] en el quinto dominio de interacción humana luego del terrestre, marítimo, aéreo y espacial.

Pero es conveniente especificar a qué nos referimos cuando hablamos de ciberespacio. Existen al respecto múltiples definiciones pero en general coinciden en que abarcan los medios que basados en las tecnologías de la información y las comunicaciones son utilizados para brindar algún servicio. Acorde a lo anterior, y función de lo que se planteará más adelante es conveniente puntualizar que Internet no es el ciberespacio, aunque constituye una parte muy importante de él.

Este nuevo ámbito virtual de interacción humana, que inicialmente fue abierto y buscó hacer disponible información y nuevas posibilidades, resultó campo fértil para que actividades mal intencionadas o ilícitas comenzaran a desarrollarse al igual que anteriormente lo hacían en el mundo real. En tal sentido las tradicionales amenazas mutaron su forma y ámbito de actuación, pasando ahora a accionar en el ciberespacio.

Términos como ciberdelito, cibercrimen, ciberactivismo, ciberterrorismo, ciberespionaje, ciberataque, ciberseguridad entre otros surgen como analogía a los anteriores y pasan a constituirse en nuevas amenazas en el ámbito cibernético.

Como consecuencia de la aparición de estas nuevas amenazas, los Estados han debido encarar primeramente una transformación de sus estructuras y crear nuevas organizaciones para enfrentarlas. De igual forma, los marcos normativos han debido ser actualizados para perseguir y dar captura a quienes utilizan este nuevo ámbito para cometer actividades ilícitas. La República Oriental del Uruguay, al igual que las demás naciones, se encuentra en este proceso, y ha realizado importantes avances en la materia.

[3]THE ECONOMIST (2010)

Normativa Nacional

La Ley 18.650[4] fue aprobada en el año 2010 y constituye luego de la Constitución de la República el Marco para la Defensa Nacional del País. La misma define en su artículo 1º la Defensa Nacional como sigue:

> La Defensa Nacional comprende el conjunto de actividades civiles y militares dirigidas a preservar la soberanía y la independencia de nuestro país, a conservar la integridad del territorio y de sus recursos estratégicos, así como la paz de la República, en el marco de la Constitución y las leyes; contribuyendo a generar las condiciones para el bienestar social, presente y futuro de la población.

Destaca en la definición realizada por la norma el carácter civil y militar de la defensa, lo que involucra y compete a todos los ciudadanos de la República. Además especifica finalmente su objetivo que es contribuir a generar las condiciones para el bienestar de la población. Se entiende naturalmente que cualquier actividad o acto que atente contra ese bienestar será objeto de la Defensa Nacional.

La norma[5] a continuación establece en su artículo 2º las características de esa Defensa Nacional:

> La Defensa Nacional constituye un derecho y un deber del conjunto de la ciudadanía, en la forma y en los términos que se establecen en la Constitución de la República y en las leyes. Es un bien público, una función esencial, permanente, indelegable e integral del Estado. En su instrumentación confluyen coordinadamente las energías y los recursos del conjunto de la sociedad.

En este caso, se establece que la Defensa constituye un derecho y deber para toda la ciudadanía, y determina que el estado es el único que puede cumplir esa función. Con estas definiciones realizadas en su primer capítulo, la ley encuadra los conceptos fundamentales sobre su asunto.

El País aprobó además por decreto presidencial en el año 2014 su Política de Defensa Nacional[6]. Este documento comienza definiendo el escenario estratégico actual y el escenario futuro, pasando luego a establecer los intereses nacionales que inspiran al País como preámbulo de la determinación de los objetivos permanentes y estratégicos de la Defensa Nacional.

Una vez establecidos los objetivos mencionados, se identifican los posibles obstáculos a enfrentar, dentro de los cuales se menciona el Crimen Organizado. Dentro de este se incluye[7]: "[…] delitos como el narcotráfico, tráfico ilegal de armas, el lavado de activos, la trata de personas, la corrupción y el crimen cibernético, entre otros".

[4]PODER LEGISLATIVO (2010)
[5]Ibid.
[6]PODER LEGISLATIVO (2014)
[7]Ibid. Pág. 22.

De igual forma se establece más adelante en el citado documento que otro posible obstáculo para lograr los objetivos de la Defensa Nacional es la materialización del espionaje y los ataques cibernéticos. A este respecto se establece que:

> En la actualidad se da en forma reiterada el espionaje por parte de Empresas, Organismos o Estados extra-regionales a los gobiernos de la región, las empresas públicas, así como a empresas privadas u organismos de la sociedad civil con el fin de captar ilícitamente información para obtener ventajas económicas y el control político, militar o social, en el plano estratégico de los países.

La Política de Defensa Nacional, finalmente establece sus lineamientos estratégicos, diferenciando los aspectos nacionales de los internacionales. Entre los primeros incluye: "Proteger al Uruguay de ataques cibernéticos[8] y preservar la reserva de datos producto de la gestión estatal y privada, tanto a nivel nacional como regional, en cuanto esta última corresponda". El lineamiento especificado encauza las actividades de ciberdefensa o ciberseguridad que pueda realizar el País.

Como corolario de las normas presentadas, el Uruguay es encuentra próximo a aprobar su Política Militar de Defensa. La misma se encuentra en etapa de borrador actualmente, pero incluirá sin lugar a dudas lineamientos para el empleo de los recursos militares en el ámbito cibernético, alineados con el marco legal ya aprobado.

Estructuras Nacionales y Cooperación
Situación General del País

De acuerdo con los datos publicados por el Banco Mundial[9], 61,5 de cada 100 habitantes del país son usuarios de Internet. Este guarismo, que resulta bastante alto en la región, se debe a la promoción por parte del estado de diferentes políticas que favorecen el acceso a través de medios tanto alámbricos como inalámbricos. En este sentido, además se han aprobado diferentes normas que han procurado desarrollar el gobierno electrónico, a la vez que garantizar un adecuado nivel de seguridad.

En lo relativo a garantizar el mencionado nivel de seguridad, algunas de las medidas adoptadas incluyen el desarrollo de una legislación que acompañe el desarrollo de las nuevas tecnologías, la capacitación de quienes las utilizan[10], la creación de políticas de seguridad cibernética[11] en todos los organismos estatales, y la capacidad de detección y respuesta a incidentes cuando ocurran.

A continuación, se detallarán las principales agencias del país actualmente responsables de la ciberseguridad y ciberdefensa, encargadas de prevenir un ataque y eventualmente llevar adelante una defensa si se materializa el mismo. Si bien como se detallará

[8] Ibid. Pág. 23.
[9] BANCO MUNDIAL (2016)
[10] En todos los niveles educativos y etarios.
[11] El Decreto del Poder Ejecutivo 452/2009, estableció que todos los organismos estatales deben desarrollar su política de seguridad cibernética.

más adelante, no existe a la fecha una estrategia nacional definida para la materia, la Agencia para el Desarrollo del Gobierno de Gestión Electrónica y la Sociedad de la Información y el Conocimiento (AGESIC) dependiente de la Presidencia de la República, a través del Centro Nacional de Respuesta a Incidentes de Seguridad Informática (CERTuy) constituye el primer escalón encargado de la seguridad y defensa cibernética del país.

A nivel de los ministerios de Defensa Nacional y del Interior, existen también organizaciones encargadas de brindar la seguridad y defensa cibernética. En el caso del primer ministerio mencionado, se explican sus características más adelante. En el caso del Ministerio del Interior, la Unidad de Delitos Cibernéticos de la Policía Nacionales es el organismo que tiene a su cargo la investigación de los delitos cibernéticos.

La Agencia para el Desarrollo del Gobierno de Gestión Electrónica y la Sociedad de la Información y del Conocimiento (AGESIC)

De acuerdo a lo establecido en su propia web, AGESIC "fue creada en diciembre de 2005 con la denominación "Agencia para el Desarrollo de Gobierno Electrónico" (Artículo 72 - Ley Nº 17.930) y su funcionamiento fue reglamentado en junio de 2006 (Decreto 205/006)"[12]. Su misión es:

> Liderar la estrategia de implementación del Gobierno Electrónico del país, como base de un Estado eficiente y centrado en el ciudadano, e impulsar la Sociedad de la Información y del Conocimiento como una nueva forma de ciudadanía, promoviendo la inclusión y la apropiación a través del buen uso de las tecnologías de la información y de las comunicaciones.

La agencia está organizada en base a seis áreas dependientes de una Dirección Ejecutiva, y veintiuna divisiones que dependen de una de las áreas, o directamente de la dirección. Una de las áreas es la de Seguridad de la Información como puede observarse en la Figura 1.

Del área de Seguridad de la Información dependen las divisiones de Gestión de Seguridad de la Información, Identificación Electrónica y el Centro de Respuesta a Incidentes de Seguridad Informática. Cada una de estas divisiones tiene cometidos específicos que en su conjunto coadyuvan a obtener un nivel de seguridad adecuado, y es AGESIC quien establece las directivas asociadas y promueve su cumplimiento por parte de todas las dependencias gubernamentales.

[12]AGESIC (2016) Disponible en https://www.agesic.gub.uy/innovaportal/v/685/1/agesic/decreto-n%C2%BA-205_2006-del-26-de-junio-de-2006.html

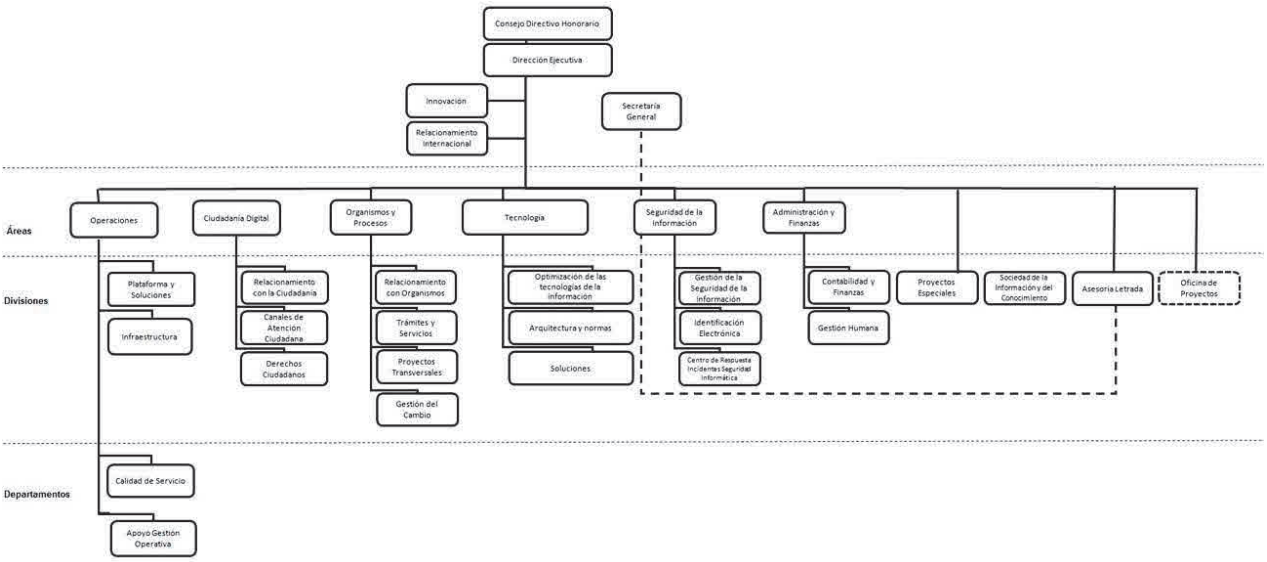

Figura 1. Organigrama de AGESIC. Página web de AGESIC[13]

Poco después de su creación, en el año 2007 AGESIC recibió la función de "impulsar el avance de la Sociedad de la Información y del Conocimiento, promoviendo que las personas, las empresas y el Gobierno realicen el mejor uso de las tecnologías de la información y las comunicaciones"[14]. Este cometido lo ha cumplido a través del desarrollo de una Agenda Digital que periódicamente[15] se desarrolla basada en un consenso entre diferentes actores, y que constituye en los hechos la política digital del país para el período considerado.

El Centro Nacional de Respuesta a Incidentes de Seguridad Informática (CERTuy)

Como se expuso anteriormente, este centro depende de AGESIC. El mismo fue creado en el año 2008 por la Ley 18.362, la cual establece que su cometido será "difundir las mejores prácticas en el tema, centralizar, coordinar la respuesta a incidentes informáticos y realizar las tareas preventivas que correspondan"[16]. Más adelante, en el año 2009 al procederse a la reglamentación de la mencionada norma, a través del Decreto No. 451[17] se establece que el CERTuy "protegerá los sistemas informáticos que soporten activos de información críticos del Estado, así como los sistemas circundantes a éstos".

[13]AGESIC (2016). Disponible en http://agesic.gub.uy/innovaportal/v/92/1/agesic/organigrama.html
[14]PODER LEGISLATIVO (2007) Art.118.
[15]En general asociada a los períodos de gobierno.
[16]PODER LEGISLATIVO (2008) Art. 73.
[17]PODER EJECUTIVO (2009) Capítulo I - Disposiciones Generales Artículo 1º.- Ámbito Objetivo.

El decreto mencionado profundiza además los cometidos derivados del definido originalmente en la ley. Los mismos son:[18]

> a) Asistir en la respuesta a incidentes de seguridad informática a los organismos estatales afectados.
>
> b) Coordinar con los responsables de la seguridad de la información de los organismos estatales para la prevención, detección, manejo y recopilación de información sobre incidentes de seguridad informática.
>
> c) Colaborar y proponer normas destinadas a incrementar los esfuerzos con la finalidad de aumentar los niveles de seguridad en los recursos y sistemas relacionados con las Tecnologías de la Información y la Comunicación (TIC) en el Estado.
>
> d) Asesorar y difundir información para incrementar los niveles de seguridad de las TIC, desarrollar herramientas, técnicas de protección y defensa de los organismos.
>
> e) Alertar ante amenazas y vulnerabilidades de seguridad en sistemas informáticos delos organismos.
>
> f) Realizar las tareas preventivas que correspondan.
>
> g) Coordinar planes de recuperación de desastres y realizar un análisis forense del incidente de seguridad informática reportado.
>
> h) Centralizar los reportes y llevar un registro de toda la información sobre incidentes de seguridad informática ocurridos en sistemas informáticos del Estado y reportados al CERTuy.
>
> i) Fomentar el desarrollo de capacidades y buenas prácticas, así como la creación de equipos de respuesta ante incidentes de seguridad informática (CSIRT) para mejorar el trabajo colaborativo.
>
> j) Interactuar como único interlocutor nacional en las comunicaciones con organismos nacionales e internacionales de similar naturaleza.

Basado en sus cometidos, el CERTuy en caso de incidentes de seguridad informática en el país coordina con el CSIRT-ANTEL[19], con otros CSIRT regionales y organizaciones internacionales. El Centro es quien lleva la estadística sobre ataques cibernéticos y es el encargado de emitir alertas sobre riesgos emergentes. La Figura 2 presenta la gráfica correspondiente a los ataques cibernéticos registrados en el País en 2015.

[18]Ibíd. Capítulo I - Disposiciones Generales Artículo 4º.- Cometidos.

[19]Administración Nacional de Telecomunicaciones. Empresa estatal, es la principal empresa de telecomunicaciones nacional que brinda servicios de telefonía fija, móvil, de banda ancha y de datos. La misma cuenta con la mayor porción del mercado en las áreas mencionadas.

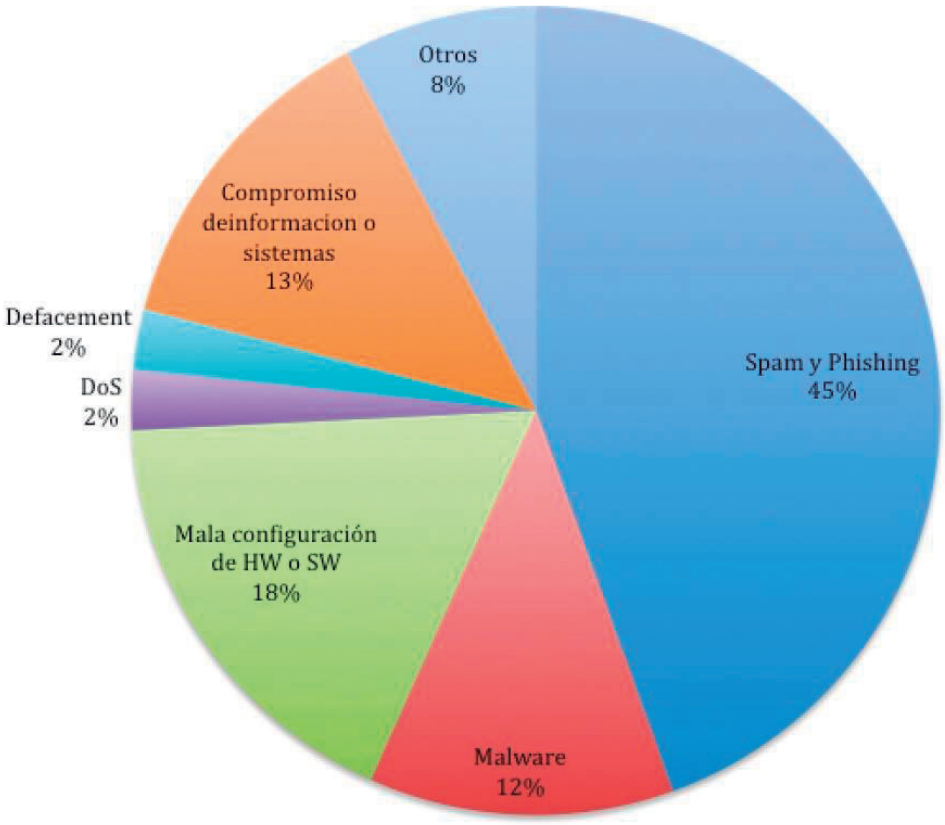

Figura 2. Estadística de Incidentes 2015. Página web de CERTuy[20]

La gráfica presentada se elaboró en base a los 577 ataques registrados[21] durante el año. Ese número corresponde a un 20 % más de los ataques registrados por el Centro durante el año anterior.

Centro de Respuesta a Incidentes de Seguridad Cibernéticos de Defensa (DCSIRT)

En abril del año 2015 se creó en el ámbito del Ministerio de Defensa Nacional en Centro de Respuesta a Incidentes de Seguridad Cibernéticos de Defensa (DCSIRT).

Su creación representa la primera organización en el ámbito específico de la Defensa Nacional encargada de atender los asuntos de ciberdefensa. La comunidad objetivo a la que

[20]CERTUY (2016).

[21]Es importante destacar que muchos de los incidentes que ocurren no se registran ya que no son reportados, ya sea porque la persona o entidad atacada le resta importancia a hacerlo, o por razones de reserva prefiere no hacerlo.

dirige su acción son las organizaciones dependientes del propio Ministerio, entre las que se encuentran las Fuerzas Armadas. El Centro además de atender los incidentes comunes a cualquier organismo se especializará en los incidentes específicos en materia de Defensa que ocurrieran.

Además de las eventuales acciones correctivas una vez que se materialice un ataque, el Centro se fija como objetivo medidas preventivas para minimizar su impacto. Entre ellas se puede mencionar la concientización en Gestión de Seguridad de la Información y la implementación de la Política de Gestión en Seguridad de la Información en el propio Ministerio entre otras. En este sentido, desde el año 2014 en el ámbito del Centro de Estudios Nacionales (C.AL.E.N.)[22], se realizan cursos sobre ciberseguridad dirigidos a profesionales provenientes del propio Ministerio, de otros organismos del Estado e incluso del ámbito privado vinculados o simplemente interesados en la materia.

El DCSIRT a partir de su creación pasa a formar parte de la estructura nacional de respuesta a incidentes, y trabaja a nivel nacional en estrecha coordinación con el ya mencionado CERTuy. El Ministerio integra además el Consejo Asesor Honorario de Seguridad de la Información (CAHSI) junto a otras instituciones nacionales[23].

Fuera de fronteras el DCSIRT para cumplir con su cometido integra igualmente con múltiples redes y equipos de respuesta como ser "el Comité Interamericano Contra el Terrorismo (CICTE) de la Organización de los Estados Americanos (OEA) y la de Ministerios de Defensa en el marco de la Unión de Naciones Suramericanas (UNASUR)"[24].

Estrategia de ciberseguridad

Como se ha expresado anteriormente, el país se encuentra en fase de desarrollo de su estrategia nacional de ciberseguridad, no contando actualmente con la misma. Sin embargo, los marcos legales aprobados, junto con las estructuras de alerta y de respuesta ya creadas han demostrado que se avanza en la dirección correcta para ese desarrollo.

El pasado mes de marzo, fue publicado un informe sobre ciberseguridad en América Latina y el Caribe[25] realizado por la Organización de Estados Americanos y el Banco Interamericano de Desarrollo. El extenso estudio realizado por múltiples expertos desarrolló un Modelo de Madurez de Capacidad de Seguridad Cibernética para evaluar cada uno de los países. Este modelo mide cuarenta y nueve indicadores agrupados en las siguientes cinco áreas: 1) Política y estrategia nacional de seguridad cibernética; 2) Cultura cibernética y sociedad; 3) Educación, formación y competencias en seguridad cibernética; 4) Marco jurídico y reglamentario; y 5) Normas, organizaciones y tecnologías.

[22]El Centro de Altos Estudios Nacionales constituye el Colegio de Defensa del Uruguay. El mismo depende del Ministerio de Defensa Nacional.

[23]El Consejo Asesor Honorario de Seguridad de la Información (CAHSI) está integrado por representantes de la Pro Secretaría de la Presidencia de la República, del Ministerio de Defensa Nacional del Ministerio del Interior, de ANTEL y de la Universidad de la República.

[24]MINISTERIO DE DEFENSA NACIONAL (2016).

[25]ORGANIZACIÓN DE ESTADOS AMERICANOS, BANCO INTERAMERICANO DE DESARROLLO (2016).

Cada uno de los indicadores, fue evaluado individualmente para todos los países de América Latina y el Caribe, estableciéndose cinco niveles de madurez. Los mismos se definieron como: Inicial, Formativo, Establecido, Estratégico y Dinámico, correspondiendo a cada uno un valor de uno a cinco respectivamente. Como es posible observar en la Figura 3, el país recibe en cuatro de los seis indicadores del área de política y estrategia una evaluación de estado Establecido o Estratégico, siendo los dos indicadores restantes evaluados como en estado Formativo.

Figura 3. Valoración para Uruguay de Indicadores correspondientes al Área Política y Estrategia. Ciberseguridad ¿Estamos preparados en América Latina y el Caribe?[26]

El informe basa su evaluación en las siguientes consideraciones:

> La Agencia para el Desarrollo del Gobierno de Gestión Electrónica y la Sociedad de la Información y del Conocimiento (AGESIC) incluyó el tema de seguridad cibernética en su Agenda Digital quinquenal para 2011-2015, y enfatizará aún más la seguridad cibernética en el próximo plan a 5 años. Por otra parte, la Política de Defensa Nacional de Uruguay incorpora medidas de defensa cibernética. El mecanismo nacional de respuesta a incidentes de seguridad informática del país, el CERTuy establecido en 2008, coordina regularmente con otros CSIRT regionales y organizaciones internacionales.
>
> Además de respuesta a incidentes, el CERTuy suministra registros estadísticos sobre ataques cibernéticos y emite alertas sobre riesgos emergentes. Uruguay también se basa en el análisis y la respuesta de incidentes del CSIRT-ANTEL

[26]Ibid. Pág.109.

de la Administración Nacional de Telecomunicaciones, que fue fundada en 2005 para abordar cuestiones relacionadas con los datos y servicios de telefonía celular. Por otra parte, la Política de Defensa Nacional de Uruguay incorpora medidas de defensa cibernética[27].

Sin lugar a dudas queda un largo camino por recorrer para llegar a tener una completa estrategia de ciberdefensa y ciberseguridad, así como las estructuras conjuntas e integradas para enfrentar un eventual ataque. Sin embargo es posible delinear algunas características que muy probablemente tendrán las mismas.

En cuanto a la creación de una estrategia de empleo de medios en el ciberespacio, sin dudas la misma se ajustará a los preceptos que establece nuestra legislación en lo referido al ejercicio del derecho de legítima defensa consagrada en la Carta de las Naciones Unidas y se reserva el uso de la fuerza para los casos de agresión militar[28]. En este sentido, un ataque cibernético por parte del estado se daría únicamente ante una agresión externa en ese ámbito.

La creación de estructuras de ciberdefensa militares, seguramente estarán encuadradas en el ámbito del Estado Mayor de la Defensa que depende del Ministerio de Defensa Nacional y le compete tanto la elaboración doctrinaria, como la planificación y el mando de las operaciones conjuntas de las fuerzas armadas.

Conclusiones

La disponibilidad creciente de las nuevas tecnologías de la información y de las comunicaciones ha dado lugar a la creación de un nuevo ámbito de interacción entre los seres humanos. En este lugar virtual se ofrecen y brindan múltiples servicios de gran utilidad, pero ha dado lugar a la realización de actividades ilícitas de diferentes características.

La realización de actividades que afecten la seguridad de los diferentes países por parte de otras naciones, organizaciones o individuos es posible, y puede causar efectos devastadores. Por esto, los estados deben adaptar su legislación y crear nuevas estructuras para combatir las nuevas amenazas que surgen. El Uruguay, al igual que los restantes países del orbe ha modernizado su marco legal y ha incluido a las amenazas provenientes del ciberespacio entre las que pueden afectar el bienestar de su población, pasando estas a ser objeto de la Defensa Nacional.

En virtud de lo anterior, se han estructurado políticas y creado al más alto nivel organizaciones para enfrentar las nuevas amenazas. El país ha identificado como primordial fomentar el gobierno electrónico y a la vez estructurar a nivel nacional redes que permitan brindar seguridad cibernética y garantizar el libre uso de los recursos reales y virtuales. Estas redes tienen como base la concientización de la población en lo referente a seguridad de la información y su capacitación para utilizar de la mejor forma los servicios.

A pesar de que el País carece de una estrategia de ciberseguridad, ha sido evaluado positivamente en un reciente informe conjunto del Banco Interamericano de Desarrollo y la Organización de Estados Americanos.

---

[27] Ibid. Pág. 108.

28 PODER LEGISLATIVO (2010) Art. 4º.

De igual forma se carece actualmente de una organización conjunta a nivel Fuerzas Armadas que tenga como cometido específico repeler ataques cibernéticos que afecten la seguridad nacional o eventualmente realizarlos como respuesta a un ataque anterior.

Referencias

AGESIC. Página Web. [en línea] 2016. Disponible en <http://agesic.gub.uy> Fecha de consulta 20mar.2016.

BANCO MUNDIAL. Internet users (per 100 people). [en línea] 2016. Disponible en:<http://data.worldbank.org/indicator/IT.NET.USER.P2> Fecha de consulta 15 mar.2016.

CERTUY. Página Web. [en línea] 2016.
Disponible en:
<https://www.cert.uy/inicio/novedades/amenazas_y_alertas/
estadistica_de_incidentes_certuy_2015> Fecha de consulta 20 mar.2016.

CONSEJO ARGENTINO DE RELACIONES INTERNACIONALES. Ciberdefensa-Ciberseguridad Riesgos y Amenazas. [en línea] 2013.
Disponible en:<http://www.cari.org.ar/pdf/ciberdefensa_riesgos _amenazas.pdf.> Fecha de consulta 15 mar.2016.

MINISTERIO DE DEFENSA NACIONAL. Página Web. [en línea] 2016. Disponible en <http:// www.mdn.gub.uy/?q=node/3994> Fecha de consulta 25 mar.2016.

ORGANIZACIÓN DE ESTADOS AMERICANOS, BANCO INTERAMERICANO DE DESARROLLO. Ciberseguridad ¿Estamos Preparados en América Latina y el Caribe? [en línea] 2016.
Disponible en < https://publications.iadb.org/bitstream/handle/11319/7449/Ciberseguridad-Estamos-preparados-en-America-Latina-y-el-Caribe.pdf?sequence=2> Fecha de consulta 25 mar.2016.

PODER EJECUTIVO. Decreto 451/009 [en línea] 2009.
Disponible en <https://www.cert.uy/ wps/wcm/connect/certuy/8f327272-c58e-4a63-8bb7-b6d37db4ec22/Decreto+451-009.pdf?MOD=
AJPERES&CONVERT_TO=url&CACHEID=8f327272-c58e-4a63-8bb7-b6d37db4ec22>
Fecha de consulta 20 ene.2016.

PODER EJECUTIVO. Decreto 105/014 [en línea] 2009. Disponible en <http://www.calen.edu.uy/noticias/2014/05_mayo/pdf/Politica-de-Defensa-Nacional-CODENA-Uruguay-2014.pdf> Fecha de consulta 10 ene.2016.

PODER LEGISLATIVO. Ley Nº 18.172 [en línea] 2007.Disponible en
<https://parlamento.gub.uy/documentosyleyes/leyes/ley/18172?width=800&height=600&hl=en_US1&iframe=true&rel=nof ollow> Fecha de consulta 10 ene.2016.

PODER LEGISLATIVO. Ley Nº 18.362 [en línea] 2008. Disponible en <https://parlamento.gub.uy/documentosyleyes/leyes/ley/18362?width=800&height=600&hl=en_US1&iframe=true&rel=nof ollow> Fecha de consulta 10 ene.2016.

PODER LEGISLATIVO. Ley Nº 18.650 [en línea] 2010 Disponible en <https://parlamento.gub.uy/documentosyleyes/leyes/ley/18650?width=800&height=600&hl=en_US1&iframe=true&rel=nof ollow> Fecha de consulta 10 ene.2016.

THE ECONOMIST. Ciberwar. 2010. Volumen 396, número 8689, 3-9 Julio.

LA POLÍTICA ANGLO-PORTUGUESA y LA PATRIA VIEJA

Daniel Torena[1]

RESUMEN

El Río de la Plata a comienzos del S XIX, era profundamente disputado por su importancia estratégica y geopolítica, al igual que por sus ricas tierras, por las Grandes Potencias Coloniales de la Gran Bretaña y Portugal, que se lo querían quitar al viejo y decadente Imperio Español; en medio de la lucha por la Libertad y de un Ideario Republicano–Democrático y Federal del Artiguismo, para los Pueblos de la Cuenca del Plata.

Palabras clave: Política, Geopolítica, Anglo Portuguesa, Río de la Plata, Imperios coloniales.

Introducción

A comienzos del S XIX, el Virreinato del Río de la Plata estaba en una profunda crisis, ante la incapacidad de la Corona española, de defender su Imperio Colonial siendo la Región del Plata, la que durante siglos despertaba el mayor interés geopolítico y estratégico, en las Américas de los Imperios británico y portugués. El Virreinato del Plata, con sus 5.OOO.OOO de kilómetros cuadrados, se había convertido en la colonia más rica y trascendente para ambos imperios aliados en Europa y América por las enormes posibilidades de expansión económica y vital para los intereses británicos en el Atlántico Sur, como para la antigua política colonial imperial lusitana en el Plata.

Para el Reino Unido de la Gran Bretaña e Irlanda del Norte, el territorio de la Cuenca del Río de la Plata, era la más valiosa que todas las otras antiguas Colonias españolas; no solo por sus minas del Alto Perú, sino por la enorme riqueza de las tierras de la Pampa, las mejores de América Latina y su gran producción ganadera y de grandes posibilidades agrícolas; como también por la ubicación estratégica en el Atlántico Sur y sus conexiones con el Pacífico por el Cabo de Hornos.

Era todo un conjunto de intereses económicos por un lado y navales para la Royal Navy por el otro. El historiador y académico argentino Scalabrini, especialista en la Política británica en el Río de la Plata, en sus trabajos magistrales detalla con documentación de la

1 Profesor Titulado de Historia, Magister en Historia Americana y Brasileña, Magister en Historia y Museología Militar. Profesor de Tesis Universitaria, Asesor Histórico y Consultor de Patrimonio Diplomático y Judicial. Director del Museo del Primer Gobierno Patrio de la Nación (Canelones). Docente de la FAU. Realizó publicaciones académicas en Uruguay, Brasil y España.

Cancillería Inglesa, el "Foreing Office" las intenciones de los distintos Gobiernos Británicos "Tories" de los Reyes Jorge lll y Jorge IV, con cartas firmadas por el Duque de Wellington Lord Liverpool y Sir. George Canning. Además, los historiadores de la Marina de Brasil, el académico Porto de Albuquerque y el Almirante Guedes, explican en la Historia de la Marina de Brasil, la estrategia y la política de Portugal, aliado de Inglaterra, en territorios de la Cuenca del Rio de la Plata.

Los ingleses aprendieron de los errores estratégicos y tácticos de las operaciones militares durante "Las Invasiones Inglesas" al Río de la Plata de 1806 y 1807, se retiraron aparentemente pero no en forma real, cambiando a una estrategia mucho más efectiva y duradera para sus intereses imperiales con mucha sutilidad diplomática y apoyada por la mayor fuerza naval del mundo ya en esos tiempos.

La Invasión Napoleónica y sus consecuencias

Cuando Napoleón invade a fines de 1807 a Portugal, aliado histórico de los británicos quedó demostrado con extrema dureza para Portugal, cómo era su alianza con Inglaterra. El historiador brasileño Joao Ribeiro que fue un académico del Instituto Histórico y Geográfico Brasileño y Correspondiente de Instituciones Históricas de Portugal, describe con precisión cómo aprovecharon la debilidad portuguesa los ingleses en su beneficio:

> Cuando Napoleón decretó el bloqueo continental contra Inglaterra, Portugal se alió a Inglaterra. En marcha forzada a través de España, las tropas francesas penetraron en Portugal. El Rey (el Príncipe Regente Don Juan de Braganza, en ese momento, futuro Rey Juan VI) llorando en secreto, aceptó el consejo del ministro inglés Lord Strangford y decidió huir al Brasil con su corte (...) Tradiciones que indirectamente remiten a Tomás Antonio de Vila Nova refieren que la noche del 28 de noviembre de 1807, Lord Strangford fue a bordo de la nave Medusa y entró a proponer condiciones interesadas e insoportables en base a las cuales, únicamente, el comandante inglés del bloqueo, Sidney Smith, consentiría la salida de la corte portuguesa para el Brasil. Una de esas condiciones era la apertura de los puertos del Brasil a la concurrencia libre y reservada de Inglaterra marcándole, desde luego, una tarifa de derechos insignificante y además, que uno de los puertos del Brasil, fuese entregado a Inglaterra (Scalabrini, 1981, p. 57).

Don Juan como Príncipe Regente, a cargo del Reino por enfermedad de su madre la Reina María, tuvo que aceptar por la fuerza de los hechos las condiciones muy duras impuestas por los ingleses, a su aliado caído en desgracia. La diplomacia inglesa utilizará en el futuro mediato y a lo largo del S XIX, el instrumento del soborno tanto económico, como militar-naval para sus intereses en América y en especial en el Río de la Plata, que era fundamental para su estrategia.

A principios de 1808 la Corte Real de Portugal se establece en Río de Janeiro, con la protección de la poderosísima Royal Navy, el Príncipe Regente y su Corte organizan el gobierno portugués en Brasil y continúa la guerra contra Napoleón en Europa junto a Inglaterra, a la que luego se sumará España al caer los Borbones reinantes Carlos IV y su hijo luego Fernando VII, prisioneros de Napoleón, al abdicar en Bayona. Inglaterra tendrá una

doble actuación con referencia a España, la apoyará en Europa contra Napoleón y al mismo tiempo muy hábilmente estimulará y apoyará a los nuevos Gobiernos Americanos contra su antigua metrópolis España, sin aparecer demasiado, para no ofender los derechos dinásticos de la Corona Española y Fernando VII, que reclamaba sus dominios americanos.

Antes de mayo de 1810, los ingleses por intermedio de Lord Strangford ahora Ministro Británico en la Corte de Río de Janeiro, como embajador con plenos poderes, apoyan la misión portuguesa a Buenos Aires del Brigadier Francisco Xavier Curado, a proponerle a Liniers como aliado, "que la margen oriental del Río de la Plata, se pusiera bajo la protección del Príncipe Regente de Portugal Don Juan de Braganza". Liniers como Virrey no accedió a la propuesta de los ahora aliados portugueses contra Napoleón.

A todas estas gestiones diplomáticas, hay que sumar las aspiraciones políticas de la Princesa Carlota Joaquina de Borbón, hermana del Rey Fernando VII de España y esposa del Príncipe-Regente Don Juan VI de Portugal. Carlota Joaquina era una mujer de fuerte temperamento a diferencia del amable y pacífico Don Juan, ella tenía grandes ambiciones políticas y tenía el plan determinado de ser coronada como Reina del Río de la Plata. Realizó varias acciones secretas con esos fines, se consideraba legítima heredera por ser hija de Carlos IV y hermana de Fernando VII. Sus planes eran separados a los de los portugueses para la región, quería ser una Soberana Independiente de Portugal, pero también de España a la que supuestamente defendía.

Luego de la Revolución de Mayo de 1810, los ingleses astutamente a nivel diplomático y en secreto apoyaron a la Junta de Gobierno de Buenos Aires y sus planes emancipadores. Simultáneamente apoyando en secreto los planes del Gobierno Real de Portugal en Brasil, que acudió en auxilio del Virrey Elío, enviando los portugueses un Ejército de la Capitanía General de San Pedro de Río Grande desde su base en Porto Alegre, al mando del experimentado Teniente General Diego de Souza. Por no tener los medios militares y materiales para enfrentar a los portugueses, el Gobierno de Buenos Aires aceptó los términos del "Armisticio de Octubre de 1811" con Elío. Por lo que Artigas y el Pueblo Oriental se vieron obligados a retirarse a fines de 1811 de la Banda Oriental, en lo que fue la gran efeméride del "Éxodo del Pueblo Oriental", dejando toda la campaña a merced de los portugueses. Al firmarse el Tratado Herrera-Rademarker, el Ejército de Portugal debió retirarse del territorio de la Banda Oriental, pero no lo realizó completamente estableciendo, el Teniente General de Souza, puestos y bastiones en lugares estratégicos muy cerca de Melo y dominando las Misiones Orientales.

El Teniente General Diego de Souza, será premiado después con los Títulos de Barón y Conde, por la Corona de Portugal y alcanzará el grado de Mariscal de Campo y Jefe de la Casa Real Militar, por el Rey Juan VI.

El Almirante Sidney Smith, Comandante en Jefe de la Flota Británica en el Atlántico y América del Sur, desde Río de Janeiro apoyó las operaciones terrestres portuguesas. Lord Stranford en Río de Janeiro realiza una muy hábil operación diplomática con el Agente Oficial del Gobierno de Buenos Aires, Manuel de Sarratea, quien quería destruir toda influencia de Artigas en la Banda Oriental y era partidario de una Monarquía para el Río de la Plata, con la protección de Inglaterra.

En ese contexto es que Artigas deberá enfrentar a la "Segunda Invasión Portuguesa", contra un enemigo mucho más poderoso que los "Ejércitos de la Patria Vieja"[2], como decía el historiador Prof. Juan Pivel Devoto, creador de su gran obra académica el " Archivo Artigas".

La Segunda Invasión Portuguesa y sus consecuencias diplomáticas

En 1816 los ingleses darán el visto bueno a la Segunda Invasión Portuguesa de la ahora Provincia Oriental, donde se contaba con el apoyo diplomático secreto del Gobierno de Buenos Aires contra Artigas, al cual querían derrotar completamente. Los ingleses harán acuerdos comerciales reservados con Artigas, sin informar a sus aliados los portugueses, preocupados por la presencia norteamericana y los acuerdos comerciales de "libertad de Puertos y Comercio" firmado entre Artigas y el Cónsul de los EE.UU. A su vez era preocupante para los ingleses y los portugueses, las actividades de los "Corsarios de Artigas", que eran navíos mercantes armados en puertos del sur de los EE.UU, la gran mayoría bergantines artillados, que no eran específicamente barcos de guerra con ese fin, otros armados en la Banda Oriental, eran fluviales los cuales realizaban la "Guerra de Corso" contra naves españolas y portuguesas, afectando su comercio marítimo. Los "Corsarios" oceánicos llegaron a atacar puertos de Portugal, incluida Lisboa.

Lord Liverpool informaba al Duque de Wellington:

> El mayor y favorito objeto de la política británica durante un plazo quizá mayor de cuatro siglos debe ser la de crear y estimular bases seguras para nuestra navegación, tener aliados seguros para nuestras flotas y puertos en los nuevos Estados de la antigua América Española, evitando siempre la competencia de otras potencias europeas o de los Estados Unidos (Scalabrini, 1981, p. 58).

También Canning escribía: "los nuevos estados americanos son altamente favorables a Inglaterra (…) Si nosotros sacamos ventaja de nuestra posición por la diplomacia, tendremos una influencia eficiente como contrapeso a los poderes combinados de los Estados Unidos de América y Francia" (Scalabrini, 1981, p. 59).

Sir Charles Webster[3] muestra con claridad las intenciones británicas de una política de apoyo a los Gobiernos de Portugal y luego de Brasil y de las Provincias Unidas del Río de

---

[2] Patria Vieja, término empleado por el Historiador Pivel Devoto, para el Período Artiguista.

[3] Sir Charles Wesbter es considerado como uno de los principales académicos británicos especializados en temas diplomáticos e históricos del S XIX del Imperio Británico y de las Guerras Napoleónicas. Formado en el prestigioso King College of Cambrige, del cual era Académico de Honor y Profesor de las Universidades de Oxford y Harvard; fue embajador y diplomático de la Gran Bretaña en la ONU.

la Plata, buscando equilibrios estratégicos potenciales, convenientes a su política económica y geopolítica regional y universal a nivel naval.

Los ingleses querían claramente que en la región del Río de la Plata, se garantizara la libertad de navegación en los ríos Paraná y Uruguay; como al mismo tiempo, tener puertos aliados para sus negocios de ultramar y para su poderosa Royal Navy, la mayor flota de guerra y comercial del mundo en ese momento.

Por esa razón no podía permitir que otras potencias emergentes como los Estados Unidos de América o el Reino de Francia, potencia militar y económica poderosa, le disputaran su liderazgo en América del Sur y el Río de la Plata; en especial donde Inglaterra será el mayor poder inversor de capital de las Repúblicas del Plata a lo largo del S XIX.

Los proyectos Imperiales Coloniales de los portugueses en el Plata, eran apoyados por los británicos hasta cierto punto, pese a que Portugal era un aliado importante. Los ingleses ya tenían información muy precisa del enorme potencial económico de la región del Río de la Plata y por supuesto no querían que Portugal y luego Brasil fueran absolutamente dominantes.

Los planes de los porteños de tener una Monarquía Constitucional en las Provincias Unidas del Río de la Plata, era algo bien visto por los ingleses, porque sería un gobierno tutelado por Inglaterra, como querían Carlos María de Alvear "Gran Maestre de la Logia Lautaro" y su mayor aliado político porteño Nicolás de Sarratea. Un gobierno que asegurara las inversiones de capitales ingleses y a su vez tener el control del comercio, de la navegación y de los ríos interiores, de la región del Plata. Los ingleses además querían tener puertos amigos o propios para su gran marina, dentro de un plan estratégico naval global con colonias y puertos en todos los continentes.

La muy hábil diplomacia británica tendrá como elementos fundamentales de sus operaciones el apoyo económico-financiero para incluso comprar muchas veces políticos y gobiernos, por intermedio de la "City de Londres", ya el mayor centro financiero del mundo, en el primer cuarto del S XIX, como la presencia de su incomparable poder naval dominante.

América del Sur tendrá en el primer cuarto del S XIX, dos grandes diplomáticos y políticos inteligentes como Lord Stranford primero y luego su sucesor Lord Ponsomby. Ambos se desempeñaron como Embajadores de "Su Graciosa Majestad Británica" en Río de Janeiro y además de cultos aristócratas, fueron ricos empresarios en tierras y en el mundo de las finanzas, en Inglaterra y con intereses personales, en el Río de la Plata, la región clave para el Gobierno Británico.

La situación diplomática era muy compleja, porque luego de derrotado Napoleón, el Rey Fernando VII de España pide apoyo al Congreso de Viena donde las Monarquías Europeas más poderosas, establecieron el principio del regreso al "legitimismo" y de los "Derechos Sagrados de los Soberanos". Con el apoyo de las grandes potencias con monarcas legitimistas o de tendencia absolutista, como los Imperios de Rusia y de Austria y el Reino de Prusia, más la colaboración de la Francia de Luis XVIII, Fernando VII esperaba recuperar sus colonias americanas. Inglaterra hará un doble juego muy sutil, evitando un choque con España y menos si era apoyada por Rusia que era la mayor potencia militar terrestre de Europa y por las otras grandes potencias como Prusia, Austria y Francia la que tenía la segunda flota de guerra más importante de Europa. Pero apoyando a los movimientos revolucionarios en Hispanoamérica

y en especial al Gobierno de las Provincias Unidas del Río de la Plata, su mayor interés comercial y estratégico.

España nombra, como embajador en la Corte de Río de Janeiro, al Conde de Casa-Flores, noble de origen porteño y con fuertes amistades en el Gobierno de Buenos Aires, siendo amigo personal del Brigadier General Carlos María de Alvear. Su misión era la de reconciliar a las Provincias Unidas del Río de la Plata y que aceptaran a Fernando VII como a su Rey legítimo o a un miembro de la Familia Real Borbón por él elegido como quería Alvear y su Logia. Pero los planes fracasaron al caer políticamente Alvear en Buenos Aires y por la política extrema de Fernando VII de aspirar ser un monarca absoluto o de no querer controles constitucionales a su poder regio.

Inglaterra no aceptaba de ninguna manera los propósitos de Fernando VII de recuperar las Colonias Americanas. Con mucha habilidad diplomática logró que Rusia no interviniera como lo había prometido el Zar Alejandro I, ni otras potencias y se fueron abandonando los planes de apoyo militar al morir el Zar poco tiempo después.

Si España hubiese logrado el apoyo militar de las grandes potencias continentales de Europa como Rusia y Austria, más Prusia y Francia, el impacto en nuestro continente hubiera sido muy grande. Posiblemente ante la abrumadora superioridad militar, los procesos independentistas se habrían atrasado o una larga guerra se hubiese desatado entre los nuevos estados americanos apoyados por la flota británica, que hubiera intentado evitar el transporte de grandes ejércitos. Pero ello hubiera significado una guerra en Europa casi sola contra la "Santa Alianza" de las Grandes Potencias Imperiales Continentales, que la habrían debilitado muchísimo. Por lo tanto, el muy hábil juego diplomático de los británicos fue dejando sola a España en sus intenciones de reconquista y sin chocar con esta y sus planes, lograron su objetivo principal de su influencia en la América del Sur y en especial en el Plata.

La expedición militar destinada a América por Fernando VII al mando del Mariscal de Campo Pablo Morillo en abril de 1815, fue a Venezuela y no al Río de la Plata. España además de actuar sola, pese al gran esfuerzo bélico de 15.000 efectivos y 60 naves de guerra y de transporte, careció del apoyo logístico y de una fuerza superior a la enviada necesarios para su éxito. Con otras potencias como Francia que estuvo a punto de apoyar a España, es muy posible que se hubiera logrado un triunfo militar mayor pero temporal, porque Francia tenía sus serios problemas internos con los grupos bonapartistas, contrarios a los Borbones.

La estrategia diplomática británica amparada en el mundo de las finanzas y de la Royal Navy, como dice el historiador militar británico Mayor General John H. Fuller, en el tomo II de "Las Grandes Batallas del Mundo Occidental", logrará a largo plazo lo que se llamó en el S XIX, "La Pax Británica", como anteriormente la "Pax Romana". Logra alcanzar sus objetivos estratégicos en América del Sur y en especial en el Río de la Plata, sin tener que llegar a un conflicto armado con España y sus aliados de la "Santa Alianza Europea" y al mismo tiempo apoyar a sus aliados portugueses en la región, sin descuidar su relación privilegiada con Buenos Aires, que tantos beneficios le dará en el futuro. Simultáneamente los ingleses compartían con los lusitanos, la opinión de la importancia estratégica del territorio de la Banda y luego Provincia Oriental, por su geografía, ríos y puertos, en particular el de Montevideo, para el control de la navegación del Río de la Plata y por extensión a los ríos interiores Uruguay y Paraná, vitales para la expansión del comercio británico. También los

ingleses querían de todas las formas posibles con garantías diplomáticas, lograr que el puerto de Montevideo fuera un puerto aliado y seguro para la flota británica y para su comercio de ultramar, así como un lugar clave de comunicación con las Islas Malvinas y todo el Atlántico Sur.

Portugal que era una potencia regional importante y con un vasto Imperio Colonial, era un aliado clave para los ingleses en América del Sur y un contrapeso confiable frente a los intereses de los Estados Unidos de América y de Francia en la región, preocupación permanente del "Foering Office" y de los Primeros Ministros de la época, Lord Liverpool y Sir George Cannig.

También los ingleses querían tener de aliados a los distintos Gobiernos de las Provincias Unidas del Río de la Plata, las cuales se independizaron de España definitivamente el 9 de Julio de 1816, para beneplácito de Inglaterra.

La figura de Artigas y sus ideas democráticas y federales eran de gran preocupación y de un profundo rechazo de las élites porteñas que manejaban los Gobiernos de Buenos Aires y por su intermedio el de las Provincias Unidas y de los grupos monárquicos y aristocráticos de Montevideo, que añoraban volver a la Corona Española y pactar con Portugal como finalmente ocurrió.

Al igual que para los portugueses Artigas representaba una amenaza revolucionaria republicana en la región. Inglaterra no quería de ninguna forma la presencia estadounidense, en particular en el Río de la Plata y desconfiaba de las intenciones expansionistas de Washington en el continente. El Libertador Simón Bolívar pensaba lo mismo que los ingleses, con quienes tenía relaciones, con referencia a los planes de los Estados Unidos de América. Inglaterra por lo tanto no era enemiga políticamente del Gobierno Artiguista, solo le interesaba que la dejaran actuar de acuerdo con sus intereses comerciales y de navegación. Los que sí estaban absolutamente en contra de Artigas eran los portugueses y las grandes élites de corte aristocrático, del patriciado criollo de Buenos Aires y Montevideo.

Los portugueses en Río de Janeiro, establecieron no solo la Corte Real del Reino Unido de Portugal, Brasil y Algarve; sino las academias, instituciones culturales, la administración del Estado y una gran cantidad de obras públicas como museos, teatros, un jardín botánico, al igual que mejoras en las instalaciones portuarias y avenidas. Al estilo de las importantes capitales de Europa, transformaron a la ciudad en la mayor de América del Sur y de las más grandes de las Américas.

Entre 1808 y1810 se crean las Academias Militares del Ejército y de la Marina, organización posterior a la Escuela Náutica que ya existía desde 1782, además del Banco do Brasil, la Junta de Comercio, Escuelas y Facultades de Medicina y Derecho, y demás. Todo esto fue posible por la muy eficaz e inteligente política del Príncipe Regente Don Juan, quien se enamoró de Brasil y será un gobernante modernizador del país, apoyado por una aristocracia lusitana y criolla que la Corte le dio poder, nacionalista y formada en Academias de Alta Administración Estatal y Diplomática y de las Fuerzas Armadas como no había en otras partes de la América Latina.

En 1816 asume Don Juan VI como Rey del Reino Unido de Portugal, Brasil y Algarve, al fallecer su madre la Reina María. La Corte y los miembros más importantes del

Consejo Real, asesoraron al Rey a tomar medidas en lo inmediato en el Plata y en la codiciada Provincia Oriental. El fin era conquistar todo lo posible al sur y llegar al Río Uruguay y si era viable al Paraná, que era la vieja estrategia lusitana desde el S XVIII impulsada por el entonces Virrey en Brasil, el Conde de Bobadela.

Portugal tenía el mayor ejército del continente y la más grande marina de guerra, ambos comandados por oficiales profesionales, muchos de ellos con experiencia de haber combatido en las Guerras Napoleónicas en Europa.

Según la documentación dejada por el Conde de Viana en su obra "La Campaña Cisplatina" del Archivo Histórico de Itamaraty:

> Artigas incomodaba a Buenos Aires y Río de Janeiro. Pretendía la formación de una Gran República Oriental, que englobaría territorios de Paraguay, Corrientes, con el territorio de las Misiones, Rio Grande, Entre Ríos y la Banda Oriental (...) Hacía mucho tiempo que la Invasión a la Banda Oriental, estaba siendo organizada. Ello se comprueba con la llegada de la División Real Portuguesa, a Río de Janeiro, que venía de luchar contra el Emperador de Francia, Napoleón I en Europa.

Según lo expresado por José Mariluz (1958) en su obra "Los proyectos Españoles, para reconquistar el Río de la Plata":

> Existieron gestiones de entendimiento con la Corte Real en Río de Janeiro por personajes rioplatenses como el Dr. Nicolás Herrera, en una reunión de alto nivel, realizada el 30 de enero de 1816 (...) Allí se acordó la ocupación por Portugal de la Banda Oriental. Decidida la ejecución del proyecto de ocupación de la Banda Oriental del Paraná, como plan primario. Se conviene ocupar la Plaza de Montevideo, como al mismo tiempo que el Ejército empiece sus operaciones, de ocupar la campaña de la Banda (Mariluz, 1958, p. 41).

En los Informes Diplomáticos e Historia de la Campaña Cisplatina, obra del Conde de Viana-Archivo Histórico de Itamaraty se dice:

> El Dr. Nicolás Herrera informó al Consejo Real, que era digno de observarse, que al principio de la Revolución, el espíritu de resistencia al dominio extranjero era general, en aquellos habitantes al día de hoy cansados de los Caudillos de la anarquía y temerosos de la venganza de los Españoles, desean la pacificación y el orden por cualquiera de los medios, que les presente la fortuna.
> Muchas familias de distinción de Montevideo, verán con agrado a los oficiales y al Ejército Real de su Majestad Fidelísima Don Juan VI, para poner orden y fin a los desmanes de los Caudillos.

Artigas no estaba desprevenido de los planes portugueses a quienes conocía bien del pasado y como General en Jefe dio la orden siguiente: "No hay que vivir descuidados, cuando los portugueses no se duerme (...) Sus movimientos son muy sospechosos y nunca debemos esperar que no sorprendan. Julio- agosto de 1816. Cuartel General. Purificación" (Archivo Artigas T.17, copia fiel). Artigas dio órdenes expresas a los Coroneles Andresito Artigas y Fernando de Otorgués de "extremar el cuidado de la frontera y vigilar los movimientos de los portugueses" (Archivo Artigas.T.17).

El plan estratégico portugués de acuerdo con lo planeado por el Teniente General Federico Lecor Barón de la Laguna y el Marqués de Alegrete Capitán General de Río Grande, fue una operación de triple avance con el apoyo de la marina de guerra para controlar y tomar todos los puertos y dominar el Río de la Plata hasta el Uruguay. Se emplearon 6.000 hombres del Ejército Real por el noreste y 3.000 de Milicias de Río Grande al mando de Alegrete con la gran ayuda del Teniente General Curado y 10.000 hombres por el sur al mando de Lecor, apoyados con artillería pesada y de campaña completas. Además, se contó con tropas de fusileros navales y artillería pesada, embarcadas en Río de Janeiro, en naves de guerra y transporte, de la Marina Real (Porto de Albuquerque y Guedes, 1985, Tomo I A I).

El Ejército Oriental y sus Milicias de apoyo de los Pueblos de la Campaña, eran la mitad de las fuerzas lusitanas, además contaban con escasa artillería, no poseían obuses pesados, solo pocos cañones de menor calibre, así como, escasas municiones. Los cañones de campaña Orientales eran de 4 pulgadas y los de los portugueses eran de 6 pulgadas. Las Milicias de los Departamentos tenían muy pocas armas de fuego y estaban armadas básicamente a lanza.

La Marina Real de Portugal, poseía dos grandes navíos de línea, el "Vasco da Gama" y el "Conde Don Enrique", de 80 y 74 cañones respectivamente, en su poderosa flota. Ninguna marina de guerra en esa época en América tenía tales embarcaciones, ni siquiera la de los Estados Unidos de América, que estaba equipada con mayor cantidad de fragatas, pero ningún navío de línea, como Portugal. Solo las más importantes armadas de Europa como Inglaterra, Francia, España y Portugal tenían esas naves, que por su tonelaje superior de 2.500 toneladas hasta 4.000 de promedio, eran los mayores buques, llevaban cañones pesados de 24 libras de hasta 2.000 metros de alcance, verdaderas fortalezas flotantes para principios del S XIX.

Fue una guerra que duró cuatro años de resistencia heroica de los patriotas, en especial de los Pueblos de la Campaña de la Provincia Oriental. Montevideo y su Cabildo, tuvo una política de colaboración y alianza con los portugueses, traicionando a Artigas y al Pueblo Oriental, con tratados firmados el 30 de enero de 1819. Muchos integrantes del Patriciado Montevideano, se relacionaron socialmente con lusitanos, a cambio de favores económicos, políticos y de títulos nobiliarios, tal el caso de Lecor que se casó con la hija del Dr. Nicolás Herrera, premiado como Caballero-Gentil Hombre del Rey de Portugal y Caballero del Cristo de Portugal, Joanicó como Vizconde del Miguelete, García de Zúñiga como Barón de la Calera, y otros.

En las últimas patriadas con las memorables Batallas de Paso Cuello y poco después del Combate del Pintado en 1817, Queguay Chico en 1818, al igual que las acciones en las Misiones, se luchó a muerte contra un poderos invasor muy superior en el plano militar, tanto en armamento como numéricamente.

Era bien claro que los portugueses además de conquistar la Provincia Oriental, querían derrotar definitivamente al Ejército Oriental y al General Artigas y sus ideas republicanas y democráticas.

El Teniente General Joaquín Xavier Curado, quién fue el Comandante en Jefe del Ejército Portugués en el norte en las Misiones Orientales y al norte de los ríos Arapey y parte del Negro y que culmina derrotando al Ejército Patriota, expresaba:

> Se deben tomar todas las providencias, por orden del Consejo Real de Su Majestad Fidelísima y por orden del Señor Ministro Consejero Marqués de Aguiar, para derrotar a Artigas y sus seguidores que tantas calamidades han provocado sus ideas republicanas en la región del Plata. Su derrota será de felicidad para la paz de nuestro reino y de la Augusta Majestad del Rey Don Juan VI.

Curado será premiado en el futuro con el grado de Mariscal de Campo, Consejero Militar del Consejo Real, Caballero del Reino, y los títulos nobiliarios de Barón y Conde.

Conclusiones

Los Imperios Coloniales de Portugal y su aliado Inglaterra querían tener el primero el dominio territorial de nuestra Provincia y los segundos el control de los mares, puertos y ríos de la región. Las ideas Artiguistas republicanas, federales y democráticas iban en contra de los planes imperiales de Portugal, que tenía como aliados a las élites del Patriciado de Montevideo y Buenos Aires, que eran claramente aristocráticas y mayoritariamente monárquicas.

El Artiguismo y sus ideas fueron defendidos en una lucha desigual, por los pueblos y habitantes de la Campaña Oriental, que gracias a su sacrificio durante cuatro años de guerra, lograron evitar los planes lusitanos de conquistar las actuales Provincias Argentinas de Entre Ríos y Misiones. Allí la figura del Coronel "Andresito" Artigas (indio misionero hijo adoptivo de Artigas) fue descollante y hoy es reconocido oficialmente, por las autoridades de la Provincia y del Gobierno Nacional Argentino, como el héroe que salvó a Misiones de Portugal.

Sin el esfuerzo simultáneo del prócer y sus grandes jefes militares y caudillos de nuestra campaña, en ese entonces; tales como los Coroneles Andresito o Andrés Artigas, Fernando de Otorgués, Fructuoso Rivera, Manuel Francisco Artigas (hermano del General), el Teniente Coronel José de la Santísima Trinidad Llupes, al igual que el valeroso Capitán Juan Antonio Lavalleja, los portugueses habrían conquistado todo el litoral actual argentino hasta el Río Paraná y amenazado la independencia de Paraguay.

Lamentablemente el Cabildo de Montevideo, aceptó completamente la incorporación de la Provincia Oriental, al Reino Unido de Portugal, Brasil y Algarve, como Provincia Cisplatina; traicionando así los principios soberanos y republicanos, del "General en Jefe Don José Artigas" y su valeroso Ejército y a la "Patria Oriental".

Referencias

Abilleira, J., Borra, L., López F., Nóbile O., Pocecco A., Torena D. y Vidal J. (2017). *Canelones, Historias de Resistencia Artiguista*. Canelones, Uruguay: Edición Oficial del Gobierno de Canelones.

Archivo Artigas del Archivo General de la Nación. Montevideo, Uruguay: Ministerio de Educación y Cultura.

Archivo del Conde de Viana y del Vizconde de Porto Seguro del Archivo Histórico de Itamaraty y del Archivo Nacional de Río de Janeiro, Brasil: Edición Oficial del Ministerio de Relaciones Exteriores de Brasil.

Archivo del Instituto Histórico y Geográfico Brasileño. (1927). Río de Janeiro, Brasil: Secretaría de Educación del Estado de Río de Janeiro.

Archivo General de la Nación. Archivo NAV Gral. Administrativo. Montevideo, Uruguay: Ministerio de Educación y Cultura.

Archivo Histórico de Itamaraty. Río de Janeiro, Brasil: Edición Oficial del Ministerio de Relaciones Exteriores de Brasil.

Frega, A. (2011). *Historia Regional e Independencia del Uruguay: Proceso histórico y revisión crítica de sus relatos*. Montevideo, Uruguay: Banda oriental.

Fuller, J.F.C. (Edición Española 1961). *Batallas decisivas del Mundo Occidental y su influencia en la Historia*. Tomo II. Barcelona, España: Talleres Gráficos Duplex.

Historia Naval Brasileira. Tomo I A y II A. (1985). Rio de Janeiro, Brasil: Departamento de Documentación de la Marina de Brasil.

Instituto Geográfico e Histórico do Brasil. (1980). *De la Colonia al Imperio*. V Tomos. Rio de Janeiro, Brasil: Secretaría de Educación del Estado de Río de Janeiro.

Mariluz Urquijo, J. M. (1958). *Los proyectos Españoles, para reconquistar el Río de la Plata*. Buenos Aires, Argentina: Talleres Gráficos Dorrego.

O´Donnell, P. (1998). *El Grito Sagrado: La Historia argentina que nos contaron*. Buenos Aires, Argentina: Editorial Planeta.

Porto de Albuquerque, L. (1985). *Historia do Brasil*. Rio de Janeiro, Brasil: Departamento de Documentación de la Marina de Brasil.

Reyes Abadie, W., Bruschera O., y Melogno T. (1971) *El ciclo artiguista*. Montevideo, Uruguay: Banda Oriental.

Scalabrini Ortiz, R. (1981). *Política Británica en el Río de la Plata*. Buenos Aires, Argentina: Editorial Plus Ultra.

Wesbter, C. (1921 y Nueva edición 1960). *British Diplomacy 1813-1815*. Londres, Reino Unido de Gran Bretaña e Irlanda del Norte: Editorial Plus Ultra.

Wesbter, C. (1925 y Nueva edición 1961). *The foreign Policy of Lord Castleragh*. Londres, Reino Unido de Gran Bretaña e Irlanda del Norte: Editorial Plus Ultra.

ASPECTOS GEOPOLÍTICOS DEL PROYECTO ARTIGUISTA

Mario Abella[1]

RESUMEN

Desde el año 1811 hasta 1820, el General José Artigas junto al Pueblo Oriental es protagonista de un período histórico de inexorable valor geopolítico en la región, mojón fundamental para la conformación de nuestro Estado-Nación, la República Oriental del Uruguay.

Palabras clave: Factores geopolíticos, Proyecto Federal, Espacio, Puertos, Estructuras.

Introducción

Entre los más antiguos sentimientos del hombre en su existencia es la veneración al lugar en el cual nació; donde vivió su infancia, estableció la convivencia con su familia, creó usos y costumbres; en el que disfrutó del paisaje, el clima y la satisfacción de sus necesidades. Es una escala de valores cargados de recuerdos y emociones, que fortalecen la actitud y el espíritu de amar el espacio territorial que le da lo necesario para nacer, crecer y desarrollarse; es el fundamento de los sentimientos patrióticos.

Lo expresado es la génesis de cómo el hombre debió organizarse en su territorio, con la unión cultural como Pueblo-Nación y como Estado-Nación, con el entorno que lo rodea. Para comprender esto, apelamos al conocimiento que nos aporta la Geopolítica como ciencia del Estado, insertada como una ciencia social y moderna como tal. A ésta le interesa el espacio en el cual se desarrolla la política en su plenitud integral, ya se trate de las jurisdicciones territoriales de los Estados o el escenario geográfico donde tienen lugar los hechos sociales, políticos y económicos que lo involucran.

La Geopolítica está guiada por distintos factores, que son parte de la geografía en general y pueden ser estables o variables según la dimensión y efecto que tengan en el tiempo. En esa apreciación podemos extraer y considerar aquéllos como extensión, posición, configuración, estructuras físicas que compartimentan las regiones, clima, recursos, población y las estructuras sociales, políticas y económicas que organizan al Estado-Nación (Celérier, 1961, p. 39 y Marini, 1985, p.74).

1 Coronel de Caballería en situación de retiro egresado de la Escuela Militar en el año 1978. Diplomado en Estado Mayor. Realizó cursos de Altos Estudios Nacionales en el Centro de Altos Estudios Nacionales (CALEN), de Planificación Estratégica en la Escuela Superior de Guerra (ESG) de Brasil, Geopolítica en el Centro Superior de Estudios de la Defensa Nacional (CESEDEN) de España. Es Docente de Geopolítica en el CALEN y en el Instituto Militar de Estudios Superiores (IMES).

Por lo tanto el conocimiento geopolítico es integrador que contempla diversos aspectos del escenario geográfico en su evolución histórica e implica asuntos de orden multidimensional con atención multidisciplinaria, al momento de analizar esa relación del hombre con el espacio en que habita y se desenvuelve.

La Ciencia Geopolítica puede adoptar visiones desde distintas ópticas. Una de ellas es la que pone énfasis en la incidencia determinante de la geografía en la conducta del hombre; concepto que se circunscribe en el llamado determinismo geográfico, por lo que el medio físico moldea la economía y la idiosincrasia de los pueblos, dictándole los cursos históricos. En cambio, otra apreciación impulsada por el pensamiento posibilista nos hace percibir que el ser humano es un actor geográfico, que es capaz de ejercer mediante sus acciones las modificaciones de la naturaleza para adaptarla a sus intereses y necesidades (Marini, 1985, p. 58).

Todos los acontecimientos históricos están atados al hombre en sus mutuas relaciones con el espacio. De la relación de los Estados han surgido diversas luchas entre ellos, en el marco natural de la defensa de sus intereses, se han manifestado en diferentes grados, desde las más violentas como las guerras y conflictos armados, pero también las pacíficas, en estas últimas priman las vías de las relaciones diplomáticas. En todos ellos hay un denominador común, que va más allá de todo lo heroico y sublime en el ejercicio del Poder, que son los asuntos de carácter económico y el espacio geográfico en donde se circunscriben las causas y efectos de las acciones.

Existe una particular relación de la Ciencia Geopolítica con muchas ciencias. Es fundamental destacar la que tiene con la Historia y sus hechos, con su génesis, vida y efectos ulteriores. En ese sentido, entendemos necesario, el análisis de los aspectos geopolíticos del escenario donde se desarrolló la gesta de nuestro héroe nacional, el General José Gervasio Artigas y su Proyecto Federal.

El Virreinato del Río de la Plata y su crisis

El proceso poblacional de Hispanoamérica se fue realizando junto a los sucesivos descubrimientos. Inicialmente éstos ocurrieron en los territorios que comprende México y luego Perú, así fue que se constituyeron los principales núcleos poblacionales que dieron origen a los Virreinatos de Nueva España con capital en México, el de Nueva Granada con capital en Santa Fe de Bogotá y el del Perú con capital en Lima.

Todos estos núcleos quedaron muy aislados con el resto del continente, en especial con la Cuenca del Plata. Esta región platense se fue modificando una vez descubierta y es así que sobrevinieron las fundaciones de Asunción en 1537 y la refundación de Buenos Aires en 1580. Al comenzar sus incursiones, los portugueses fundaron la Colonia de Sacramento en 1680 como baluarte de expansión comercial, ya que geográficamente el estuario del Río de la Plata se constituía en la ruta de ingreso al "heartland"[2]sudamericano. Eso preocupó a la Corona española, que debió fundar un bastión en la Bahía de Montevideo en 1726 y de esta manera

[2]"Heartalnd" es la Tierra Corazón o sea el centro del Continente sudamericano, que comprende fundamentalmente Bolivia, donde se encontraban las minas de Plata del Potosí.

contrarrestar la presencia lusitana en la Banda Oriental (Reyes Abadie, 1998, T1, p. 383).

Ya el mundo se circunscribía en las luchas por el mar, donde los ingleses querían arrebatarle a la Corona española ese dominio. Inglaterra había comprendido que para introducir su comercio no bastaba con atacar a la flota española o conquistar alguna isla estratégica, debía ir al "heartland", al corazón de la tierra americana. En esa estrategia naval intentaron inicialmente hacerlo por el norte del continente, incursionando en la región del Istmo de Panamá, particularmente en el puerto de Portobelo.

La Corona española comprendió el problema al considerar que el abandono del Río de la Plata desde el punto militar perjudicaría sus intereses en el Reino de Indias. Para los ingleses, España estaba muy debilitaba, no solo en su poder naval, cuyo comercio proteccionista era vulnerable. Es así que salieron decididamente a apoderarse de las posesiones hispánicas y conquistaron las Islas Malvinas, posteriormente reforzaron política y militarmente a los portugueses, como sus aliados. Contribuyendo a ello, en 1763 fue creado el Virreinato del Brasil unificando los territorios de Portugal en Sudamérica, luego trasladando la capital de Bahía a Río de Janeiro.

Estos acontecimientos condujeron a la Corona española la encomendación de Pedro de Cevallos en calidad de Jefe de una expedición, para fundar el Virreinato del Plata con capital en Buenos Aires. Su creación fue en el marco de una visión geopolítica, de manera de servirle al Virreinato del Perú a modo de antemural frente al avance lusitano con plenos intereses expansionistas con el apoyo inglés. Se lograba el establecimiento de una jurisdicción política y militar, para articular la defensa y las comunicaciones en los frentes marítimos del Pacífico y el Atlántico. A partir de ahí, Buenos Aires sería la puerta del territorio, Montevideo como Apostadero Naval del Atlántico sur y llave estratégica de la Cuenca del Plata (Reyes Abadie, 1998,T1,p. 385).

Europa, y por sobre todo España, estaba sufriendo los efectos de las campañas napoleónicas. En ese especial escenario internacional, los ingleses aprovecharon las circunstancias a través del dominio de los mares, para generar un nuevo orden económico a impulso de su Revolución Industrial.

Con esa voluntad los ingleses invadieron el Río de la Plata en 1806 y 1807, golpeando los "núcleos vitales"[3]del Virreinato, a Buenos Aires y a Montevideo. Más allá de la resistencia y posterior derrota, lograron erosionar al comercio español, con duras críticas al sistema de aduanas muy conservador y proteccionista, introduciendo sus propias mercaderías y alentando las ventajas del libre comercio (Williman y Panizza, 2006, pp. 133-141).

El escenario no solo involucraba lo económico, también se fueron introduciendo nuevas ideas políticas, despertando la voluntad de los criollos. Aquellos ciudadanos hijos de españoles, algunos de ellos habían logrado grandes fortunas como comerciantes y el desarrollo de algunas industrias, otros eran intelectuales, pero estuvieron siempre relegados de los cargos políticos. Frente a los hechos, estos criollos tanto en Buenos Aires como en Montevideo,

[3] Es el área donde se ubican los poderes directivos del Estado, donde se concentra la mayor capacidad cultural, económica, política y militar.

desarrollo de algunas industrias, otros eran intelectuales, pero estuvieron siempre relegados de los cargos políticos. Frente a los hechos, estos criollos tanto en Buenos Aires como en Montevideo, comenzaron a visualizar y encender esas nuevas ideas, las de modificar las estructuras políticas y económicas, comenzando así el declive de las existentes creadas por los españoles. En ese proceso de emancipación afloraron conflictos y además los hombres, sus nuevos líderes, entre quienes se encontraba nuestro principal protagonista el General José Artigas.

La geografía regional que correspondía al Virreinato del Río de la Plata, tuvo para aquella jurisprudencia características muy particulares, que fueron determinantes en la organización económica y política, ya que comprendía tres regiones bastantes dispares por sus peculiaridades geográficas, de las que podemos distinguir las siguientes:

El Litoral que se caracterizaba por la llanura, propicia para la cría de ganado, el desarrollo de la agricultura con la utilización de herramientas agrícolas. Sus productos tenían una fácil salida al mar, conectada con una red de ríos navegables, abundantes lluvias con un clima favorable a ese desenvolvimiento agrícola. Ese espacio comprendía a las Provincias de Santa Fe, Corrientes, Entre Ríos, Buenos Aires y la Provincia Oriental. Con las condiciones esenciales por sus praderas para el crecimiento ganadero, el establecimiento de las estancias y la industria saladeril, impulsando el comercios de dicha producción (Barrán y Nahum, 2010, p.12).

Otra región era la Central o mediterránea, una zona de transición entre las tierras de fácil producción agrícola ganadera y otras más limitadas que requerían de otros elementos. Su clima más seco y el suelo más quebrado e improductivo que el territorio antes mencionado, la salida al mar era más restringida por la lejanía a los puertos naturales. Ahí se encontraban las Provincias de Córdoba, San Luis, San Juan, Mendoza, Tucumán, Jujuy y La Rioja, con terrenos menos fértiles que las hacía económicamente más débiles (Barrán y Nahum, 2010, p. 13).

Por último la región Serrana, correspondía a la parte occidental del territorio virreinal, que abarcaba en su totalidad lo que es la Cordillera de los Andes. Su clima muy seco, con algunas cuencas fluviales, naturalmente no apropiada para el desarrollo agrícola-ganadero, por lo que sus principales recursos estaban en la minería, fundamentalmente la plata. Su posición orientada a la salida hacia el Pacífico, opuesto al Atlántico, comprendía a las Provincias de Potosí, Chuquisaca, Cochabamba y La Paz, en el Alto Perú. Regiones, que como ya se expresó, eran muy limitadas en su producción natural, estando enfocadas a la extracción minera. No se considera la zona patagónica, ya que, en aquella época estaba casi despoblada y no era significativa dentro de la jurisdicción virreinal (Bárran y Nahum, 2010, p.13).

Las diferencias de las estructuras físicas, el clima, el suelo y la posición con respeto al mar de estas regiones, determinaron tres grandes zonas con características económicas muy dispares, que comenzaron a contraponerse a medida que se acercaban todos los hechos que generaron el proceso de emancipación.

Además se deben agregar las especiales características de la población, que fue el resultado del determinismo geográfico, que incidió en la conformación de la sociedad

colonial. En los aspectos sociales y económicos, se puede diferenciar que los habitantes del interior fueron estables y sedentarios, con algunos cultivos y artesanías, en cambio los del litoral eran más nómades o semi-nómades, de grandes agricultores y recolectores.

Artigas adopta un idealismo y con él su Proyecto Federal, siguiendo el camino y la idiosincrasia de los pueblos establecidos, particularmente los del litoral. Estos eran habitantes de la misma cuna y lengua, de acendrada cultura hispánica. Su pensamiento central era la soberanía de dichos pobladores, frente a una realidad virreinal que se encontraba en difícil situación, insegura, pobre, además de todas las dificultades de comunicaciones y los transportes existentes.

El rol geopolítico de la Provincia Oriental

Si bien, la Banda o Provincia Oriental se insertaba con la región del litoral, ésta por sus características tiende a separarse como la cuarta zona geográfica. Su posición frente al mar, poseedora de grandes praderas, una red fluvial muy abundante, donde la producción de ganado y la industria saladeril involucraban todas las actividades de la población, son peculiaridades que la hacían diferente al resto de las Provincias. Agreguemos además, que el área cuya cabeza estaba en Montevideo, un centro poblado instalado sobre el Plata, bastión de seguridad contra los portugueses y puerto de salida del comercio provincial, hizo que esta se constituyera en un jugador geopolítico significativo en la región.

Una vez que la Corona española decidió establecer un asentamiento poblacional en la Bahía de Montevideo, este se transformó en la Ciudad-Puerto, un puerto natural con posibilidades de comunicación con el mercado y el comercio mundial. Ese emplazamiento se constituyó en un "núcleo vital", que empezó a ejercer el Poder en el espacio de la comarca fronteriza de la Marca del Plata, constituida por Maldonado, Santa Teresa, San Miguel y Santa Tecla (Prada, 2010, p.15). Estas características fronterizas fueron el fruto de la acción humana, que en sus avatares definieron las líneas de demarcación entre españoles y portugueses, determinando una "zona de marca" en medio de esos grandes imperios, conformando así el "hinterland espacial" de la Banda Oriental inicialmente, para transformarse más tarde en la Provincia Oriental.

La Ciudad-Puerto de Montevideo, con su posición a la entrada de los extensos territorios del Atlántico del Sur, tenía una vecindad especial con las posesiones portuguesas. Las características naturales de su puerto, lo hacían un punto de recalada en la navegación al Perú, dándole a Montevideo la peculiaridad de convertirse en una plaza comercial, con considerables operaciones de importación y exportación de productos. En cambio, el acceso al puerto de Buenos Aires era muy difícil al estar limitado para el ingreso de grandes embarcaciones por lo que el embarque y desembarque de mercadería no se podía ejecutar con regularidad, marcando el diferencial que generó la competencia entre ambos puertos.

Esos aspectos le dieron a la Provincia Oriental y a su territorio, la triple condición de una pradera, puerto y frontera. La pradera y el puerto son condiciones inevitables del determinismo geográfico, es decir que ese campo y sus recursos en la producción de alimentos y la salida por una puerta natural, compone una cabeza natural en el frente

marítimo constituido por el Río de la Plata y sus afluentes, que lo conectaban al "hinterland sudamericano".

En 1787 se concedió a Montevideo el derecho de ser la única plaza en el Virreinato de introducción de esclavos, con la oposición de Buenos Aires, pero eso le dio la posibilidad del vínculo con embarcaciones inglesas. Éstas traían sus mercaderías de contrabando junto a los cautivos y retornaban con los cueros y otros productos del país. De esta manera es que se generó ese contacto irregular, con ese particular comercio ejercido por Inglaterra y Portugal (Barrán y Nahum, 2010, p. 52). Una relación directa de Montevideo y su Provincia Oriental con los grandes mercados compradores, de los más amplios del mundo, incrementó notablemente la cría de ganado, la industria saladeril y el comercio de los frutos.

La Corona española había adoptado una política que le concedía privilegios y facilidades al puerto de Montevideo. Obviamente que esto provocó un gran encono por parte de la capital del Virreinato, ya que asumía el rol de ser la metrópoli comercial. Es así que Montevideo comenzó a disputar el monopolio en las relaciones comerciales con Europa, por lo tanto la hegemonía de la capital porteña sobre las tierras del interior y litoral del Virreinato empezó a debilitarse (Williman y Panizza, 2011, pp. 19-25).

La Provincia Oriental con el puerto natural de Montevideo incrementó su privilegio al ser designado como Apostadero Naval, sede de registros de buques, con responsabilidad para dar seguridad al frente marítimo sobre el Atlántico. Su posición privilegiada en el escenario del Plata lo configuró y estructuró como la llave estratégica del mismo estuario, junto a la hidrovía de los ríos Uruguay, Paraná y Paraguay que se unían al "hinterland sudamericano".

Barrán y Nahum en el libro "Bases económicas de la revolución artiguista" extraen un concepto expresado por Zorrilla de San Martín en su "Epopeya de Artigas", al referirse a la Provincia Oriental, que dice así:

> Forma una unidad geográfica perfectamente definida; constituye una unidad étnica y sociológica imposible de confundir. Para fijaros más esa idea, os quiero hacer advertir desde ahora una circunstancia fundamental, que más tarde examinaremos más. Todos los dominios españoles que conformaron el Virreinato del Plata, el mundo andino, dependían de un solo puerto de salida al que convergía toda la región: Buenos Aires. Pero ese pedazo ultraplatense u oriental del Plata era independiente de Buenos Aires en ese sentido; independiente por naturaleza. Solo él tenía salida propia, comunicación amplia y libre con el mundo, puertos en el Plata y en el Atlántico, incomparablemente superiores al de la capital del Virreinato: la Colonia, Montevideo, Maldonado, Coronilla, toda la profundísima costa atlántica, la más cercana a Europa, la más accesible, la verdadera puerta de entrada, y de salida, para toda la región subtropical del continente (Barrán y Nahum, 2010, p. 67).

Esa independencia geográfica es determinante para la independencia económica, de hecho puso a la Provincia Oriental a la cabeza de todas las demás Provincias, pues era ella la que tenía la única salida al mar, ofreciendo sus puertos para toda la producción del litoral e interior del territorio de las Provincias Unidas. Esa salida de la Provincia Oriental fue también la salida para la independencia política, al cambio de sus estructuras, en la que el

Pueblo Oriental con sus características sociales asume ese rol geopolítico con el liderazgo de Artigas, sus ideas y su Proyecto Federal.

Sistema de los Pueblos Libres y la Liga Federal

Buenos Aires trataba de controlar y limitar el tráfico comercial que ejercía Montevideo, para ello, el Consulado de Comercio de la capital virreinal estableció un impuesto a las mercaderías que entrasen o saliesen por mar y tierra, afectando a los comerciantes de Montevideo y Buenos Aires. Esa medida provocó una dura reacción de los comerciantes montevideanos, quiénes se reunieron y expresaron a través de un documento, que el comercio de Buenos Aires era totalmente independiente a la Plaza de Montevideo, negándose a toda determinación o subordinación por parte de cualquier partido o Provincia del Río de la Plata. En una palabra, para el comercio montevideano la dependencia administrativa de Buenos Aires era una carga muy pesada, dando lugar a la creación de un Consulado de comercio propio (Barrán y Nahum, 2010, pp. 55 y63).

Artigas era un criollo que nació en una familia fundacional de Montevideo, pasando sus primeros años en esa ciudad. Si bien no tuvo una elevada formación académica, tuvo sus primeras letras en la Escuela de los Padres Franciscanos y también supo imbuirse de las nuevas ideas políticas que venían desde Europa. Más tarde, siendo muy joven se fue para los establecimientos rurales que poseían sus familiares a las afueras de los límites de Montevideo, donde se desarrolló como un ciudadano muy avezado en el conocimiento y dominio de las tareas del campo, recorriendo toda la campaña oriental y gran parte de lo que hoy es Río Grande del Sur. Eso prueba que fue un hijo de su tiempo, como un morador de la pradera, participando en distintas faenas, recogida de ganado, vaquerías, haciendo corambre y en el comercio de contrabando junto a los gauchos, morenos y algunos indios (Reyes Abadie, 1974).

Más tarde, junto a quienes habían sido sus compañeros de aventuras, se enroló como Soldado en el Cuerpo de Blandengues de la Frontera de Montevideo. A los pocos meses fue comisionado para contener las incursiones de portugueses, changadores y contrabandistas y algunos malones indígenas, con el fin de poner orden en la campaña; esto le permitió conocer aún mejor el territorio y su gente. Además, formó su personalidad, típica de ese criollo aferrado a su propio terruño, con una voluntad poderosa y de hierro.

Siendo Oficial de las Milicias de Caballería participa en las campañas militares contra las invasiones inglesas, luego forma parte de la Revolución de Mayo de 1810, adhiriéndose a la Junta de Buenos Aires. En ese contexto histórico es que nace el Proyecto Artiguista, insertado en el proceso de emancipación, pero tiene su génesis geopolítica en la competencia de los puertos de Buenos Aires y Montevideo, la Ciudad-Puerto junto a la Provincia Oriental que se constituían a modo de actor geopolítico en el escenario de la cuenca platense, originándose la dicotomía “centralismo – autonomismo” (Reyes Abadie, 1974, pp. 71-76).

La geografía en su aspecto determinante estaba presente, ya que el conflicto radicaba en que los dos puertos poseían un “hinterland” similar, pero el encono se daba más en la región del litoral. Montevideo llegaba a esa zona con mucho más énfasis, en donde Artigas

constituido como Caudillo de su Pueblo Oriental influyó políticamente, al mismo tiempo que desde Montevideo se influía en los aspectos mercantiles por las ventajas poseídas.

El año1811 fue de inflexión para la gesta del criollo General José Artigas, quien se puso a la cabeza de las campañas militares con su primer triunfo en Las Piedras, al servicio de la Junta de Buenos Aires. A partir de mayo las milicias artiguistas inician el Sitio de Montevideo, Artigas intima al Virrey Elío a la rendición de la Plaza y se dirige al Cabildo; Elío no se rindió y trató de eliminar a todo adherente a la causa revolucionaria y el Cabildo no contestó. A pedido de Elío en el mes de julio el territorio de la Provincia Oriental comienza a ser invadido por las fuerzas portuguesas que vienen en su auxilio, con el propósito de cercar a los revolucionarios orientales por Misiones, a través del Río Uruguay por Paysandú y Montevideo, no obstante las tropas sitiadoras habían recibido el apoyo del General Rondeau.

Comienza ahí el disgusto y la indignación para los orientales, en agosto de 1811 se iniciaron tratativas entre la Junta de Buenos Aires y el Virrey Elío a los efectos de llegar a un arreglo, con lo cual se arriba al Armisticio de Octubre, muy desfavorable y perjudicial para los intereses y la causa revolucionaria del Pueblo Oriental, ya que no se le dio participación en las negociaciones de paz (Reyes Abadie, 1974).

A partir de entonces era la primera vez que el Pueblo Oriental ejerció el "uso de su soberanía", con los Congresos Orientales, primero en la Panadería de Vidal y luego en la Quinta de la Paraguaya, en este último Artigas fue designado Jefe de los Orientales. Acontecimientos estos muy significativos para el devenir de ese Pueblo, además Artigas ya era un actor político y militar reconocido, pues había sido nombrado por el Triunvirato porteño Teniente Gobernador del Departamento del Yapeyú en las Misiones. En ese escenario geopolítico se configura el llamado Éxodo del Pueblo Oriental, el cual es el inicio de una identidad de Pueblo-Nación, que se dirige al norte con una visión del espacio, que lo conectaba con ese "hinterland" que completaban las Provincias del interior. Al mismo tiempo Artigas ya visualizaba el nexo territorial con el Paraguay y necesitaba instalar su "núcleo vital" lejos de Montevideo. A fin de coordinar el ejercicio del poder político y militar en conexión con el litoral, lo que él llamaba la fuente de sus recursos, el prócer instaló sus Cuarteles Generales en el Ayuí, y más tarde, en Purificación.

El hombre como agente geográfico y desde la óptica del factor geopolítico población, vemos que Artigas y los pueblos de la campaña oriental abrazaron con entusiasmo la causa de la Revolución. Eran situaciones muy difíciles las que vivían los diversos "pagos" de la Provincia y en ese sentido se unieron como un Ejército, "el Pueblo Oriental armado", por voluntad propia y espontánea. Es el "pueblo soberano" como una entidad sociológica, dándose la oportunidad de un gobierno inmediato, es decir, crear sus propias estructuras sociales, políticas y económicas (Reyes Abadie, 1999, T3, pp. 111-115).

Los pueblos del interior del ex Virreinato habían abrazado la causa de Mayo, con las expectativas de cambiar las estructuras políticas, que basadas en el régimen de Intendencias, les era restrictivo para sus administraciones y el desarrollo económico. Se esperaba y ansiaba poder regir sus jurisdicciones a fin de ejercer una mayor libertad de comercio y obviar la dependencia del puerto de Buenos Aires.

El gobierno de Buenos Aires quería gravitar acorde a sus intereses en el proceso revolucionario. Incrementó sus acciones defensivas al tomar conocimiento que el Jefe de los Orientales mantenía correspondencia y relaciones con el gobierno paraguayo, además de la evidencia de que el mismo adoptaba algunos planes de orden político con un nuevo esquema institucional, alentando las autonomías provinciales. Esto determinó un verdadero enfrentamiento entre el centralismo porteño y la emergente figura de Artigas y su Proyecto Federal.

El escenario estaba planteado y el año 1813 fue clave para Artigas, cuando intenta impulsar doctrinariamente su proyecto a través de las Instrucciones del Año XIII, la concepción federal, la independencia y autonomías de las provincias y la base de organización política de los pueblos del interior. En su texto también establecía algunos asuntos muy peculiares desde el punto de vista geopolítico:

> Art. 12. Que el puerto de Maldonado sea libre para todos los buques que concurran a la introducción de efectos y exportación de frutos, poniéndose la correspondiente aduana en aquel pueblo; pidiendo al efecto se oficie al Comandante de las fuerzas de S. M. B. sobre la apertura de aquel puerto para que proteja la navegación, o comercio, de su nación.
>
> Art. 13.Que el puerto de Colonia sea igualmente habilitado en los términos prescritos en el artículo anterior. (Reyes Abadie, 1974, p. 319).

Quedaba así instalado el sistema de puertos y aduanas, con ello el artiguismo contemplaba las aspiraciones de las provincias del interior, que buscaban emanciparse a través de los puertos sucedáneos al círculo mercantil que regía Montevideo como puerto de ultramar.

Las primeras Provincias en incorporase al sistema federal fueron Entre Ríos, Corrientes y Misiones; luego se sumaron Santa Fe y Córdoba, conformando una superficie con una extensión en el orden de 700 mil kilómetros cuadrados. Su estructura física correspondía a las vías fluviales de la hidrovía Paraná, Uruguay y Paraguay con el encauce en el Río de la Plata, sumado a una llanura con pradera apropiada a la producción ganadera y sus derivados. Se configuraba con esto un espacio geográfico integrador en la visión geopolítica del Proyecto de Artigas, que buscaba con ello la unidad de los intereses económicos de las Provincias. Cabe agregar también su conexión a los mercados mundiales, donde el puerto de Montevideo con su privilegiada posición era el resorte principal del sistema.

En el marco de esa vertebración dada por la hidrovía y la integración provincial, Misiones, por su situación geográfica, era un espacio sensible que se constituía en el pivote geopolítico[4](Brzezinski, 2008, p. 49). Artigas la consideraba el nexo interregional, en donde se ganaba a un actor geopolítico significativo como el Paraguay, librándolo de la dependencia del puerto bonaerense y brindándole la posibilidad de sacar todos sus recursos por los puertos de Montevideo, Maldonado y Colonia (Reyes Abadie, 1974).

[4]Los pivotes geopolíticos son los Estados cuya importancia se deriva no de su poder y de sus motivaciones sino más bien de su situación geográfica sensible y de las consecuencias que su condición de potencial vulnerabilidad provoca en el compartimiento de los jugadores geoestratégicos.

A través de Misiones, Corrientes y Entre Ríos se coordinaba el espacio mesopotámico que unía a la Provincia Oriental con esos puertos, pero también Santa Fe conformaba un enlace comercial con Tucumán y el Alto Perú. De esa manera todos los recursos propios, la producción de la región basada en la yerba mate, tasajo, cueros, maderas, tabaco, artesanías, mineral y caña podían circular en el ámbito regional. Al mismo tiempo como consumidores de las manufacturas importadas se trataba de que las mismas les llegaran en la medida de lo necesario y que no compitiera con la productividad propia, es decir, una conexión directa al mundo sin la interferencia forzosa de los porteños.

El Proyecto Federal de Artigas desde el punto de vista militar no se limitaba solo a ejercer el control en el espacio terrestre. Como ya lo hemos expresado, el mar fue determinante en todo el proceso histórico y el estamento mercantil montevideano. Montevideo tenía al mar como su objetivo fundamental, como puerto de ultramar y de cabotaje para el tránsito de mercaderías por el Río Uruguay al litoral oeste de la Provincia Oriental y por el Paraná y el Paraguay a los puertos del litoral argentino y paraguayo.

El puerto de Montevideo desde el punto de vista militar ya había tenido su primordial participación como Apostadero Naval. Eso fortaleció esa especial relación de la pradera con el mar y la hidrovía, en la que Artigas debió contemplar asuntos de seguridad y defensa marítima, debiendo componer una marina propia y su consecuente estrategia naval. Organizó la llamada “Guerra de Corso”, particularmente en la defensa de la soberanía frente a la potente flota naval portuguesa.

El espacio fluvial y marítimo era vital para la Liga Federal, por ello Artigas adopta una estrategia naval propia de un estado continental, con muy escasos recursos, pero bajo el accionar de Pedro Campell, primer Comandante General de la Marina. Estableció la lucha convencional en el mar, a fin de negarles el libre uso a sus adversarios, así como, interrumpir y estrangular las líneas de comunicaciones y de aprovisionamiento.

Los permisos de corso inicialmente fueron expedidos desde el Cuartel General en Purificación, pero Artigas buscó ampliar la flota corsaria, celebrando acuerdos con los Estados Unidos de América, a través de su agente consular en las Provincias, Thomas Halsey. Este muy entusiasmado por las políticas artiguistas en la región colaboró, lo que permitió que el Poder Naval oriental partiera desde distintos puertos norteamericanos y operara en el Océano Atlántico (Laborde, 1995, pp. 33-48).

Conclusión y resumen final

Como conclusión y resumen final de este trabajo, nos queda expresar que la Geopolítica existió siempre, si bien como ciencia es muy moderna, en todos los acontecimientos de la Humanidad hubo Geopolítica. De ello no escapa a lo que fue nuestro propio devenir histórico, donde la Gesta de Artigas con el Pueblo Oriental marcaron un mojón significativo en el proceso que culminó con la conformación de nuestro Estado-Nación, la República Oriental del Uruguay.

Artigas y su Proyecto inexorablemente estuvieron marcados por los siguientes aspectos: hubo una configuración de espacio con sus recursos, sus estructuras físicas, una privilegiada

posición con frente marítimo, la competencia de puertos, la lucha por esos espacios y la expansión del comercio, un clima apropiado para un tipo de producción atrayente a los mercados mundiales del momento, puja de comercio entre grandes potencias, la crisis española, un nuevo orden económico y comercial y la afloración de nuevas ideas políticas adaptadas a las nuevas estructuras de comercio. Si bien el tema desarrollado es histórico, nos trasladamos a nuestros tiempos y concluimos que la Geopolítica está presente en el devenir del contexto mundial de las naciones actuales.

Figura 1. Mapa económico de la Liga Federal. Muestra la integración de la producción de las distintas regiones de la Liga Federal. Blog revolucionartiguista.blospot.com /2011/la revolución artiguista 1811-1820.

Referencias

Barrán J.P., y Nahum B. (2010).*Bases económicas de la Revolución artiguista.* Montevideo, Uruguay: Banda Oriental.

Brzezinski Z. (2008). *El gran tablero mundial.* Barcelona, España: Paidós Ibérica SA.

Celérier P. (1961). *Geopolítica y Geoestratégia*. Buenos Aires, Argentina: Círculo Militar Argentino.

Prada U. (2010). La Marca del Plata. *Revista El Soldado, 179*(1), 13 – 25.

Laborde A. (1995). Artigas y la Guerra de Corso.*Revista Naval, 21 (1)*,33 – 47.

Marini J.F. (1985). *El Conocimiento Geopolítico*. Buenos Aires, Argentina: Círculo Militar Argentino.

Reyes AbadieW. (1974).*Artigas y el Federalismo en el Rio de la Plata*. Tomo 2.Montevideo, Uruguay: Banda Oriental.

Reyes Abadie W y Vázquez Romero A. (1998).*Crónicas Generales del Uruguay*. Tomos 1,2 y 3.Montevideo, Uruguay: Banda Oriental.

Williman J.C. yPanizzaC. (2006).*La Banda Oriental en la lucha de los Imperios*. Tomo 1.Montevideo, Uruguay: Banda Oriental.

Williman J.C. y Panizza C. (2011). *La Banda Oriental en la lucha de los Imperios*. Tomo 2.Montevideo, Uruguay: Banda Oriental.

Esta Obra se terminó de imprimir en
la División Publicaciones de la O.R.T. yA.
del Comando General del Ejército
en el mes de abril de 2019.

Tiraje: 250 ejemplares.

Depósito Legal N° 375.503

ISSN 0797-4604