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, cuyo daño puede aparejar consecuencias negativas sobre la seguridad de las personas y la seguridad

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.

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 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

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"

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.

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

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.

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 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

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

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 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.

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

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

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-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,

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

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.

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/c06cac0047612e998806cb6dc6329423/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.