ISSN: 2539-0015 (en línea)

TRIARIUS

Volumen 4 - N° 76

1 de Agosto de 2020

HONDURAS

2539-0015

Boletín de Prevención y Seguridad ante el

Terrorismo y las Nuevas Amenazas

ISSN: **2539-0015** (en línea)
Medellín - Colombia
Volumen **4** - Número **76**
1 de agosto de **2020**

Editor
Douglas Hernández

Analistas Triarius
Julian Urrego, Marianna Crudi, Alberto Carracedo, Micaela Abril, Agostina Taverna, Rodrigo Cárdenas, Guadi Calvo, Douglas Hernández.

Este boletín es una publicación del **Observatorio Internacional sobre el Terrorismo y las Nuevas Amenazas**. Se produce de manera quincenal, en formato pdf, y su distribución es gratuita.

Información de Contacto:

Douglas Hernández
Medellín, Colombia
Móvil: (+57) 321-6435103
director@fuerzasmilitares.org
hernandez.douglas@hotmail.com

EDITORIAL

En medio de la crisis generada por la pandemia del COVID-19, hemos visto cómo el personal del sector salud ha asumido el reto de defender a la sociedad de semejante amenaza, aun a riesgo de su propia seguridad. Desde TRIARIUS les decimos ¡GRACIAS!

Abrimos esta edición con un interesante artículo del analista colombiano Juan David Urrego, donde aborda el tema del vandalismo en Colombia. Conoceremos a través de esta lectura el marco legal fundamental para comprender el fenómeno y las responsabilidades de los distintos actores en un contexto de derechos y deberes.

Pasamos luego a revisar el tema de los apátridas, la situación terrible por la que atraviesan, y el peligro latente de que estas personas puedan transitar a la criminalidad y la violencia arrastrados por su necesidad de soluciones a sus penurias. Agradecemos a los analistas argentinos Crudi y Carracedo por este valioso aporte.

Después de leer el artículo de la analista argentina Micaela Abril Álvarez, seguramente usted se sentirá muy preocupado y vulnerable, y querrá supervisar los videojuegos que sus hijos suelen usar.

A paso seguido, los analistas argentinos Taverna y Cárdenas, nos ilustran sobre el tema de la protección de infraestructura crítica, y aunque se enfocan en la República Argentina, el componente teórico de su artículo, así como lo esencial de su propuesta, es extrapolable a cualquiera de nuestros países. Podemos aprender mucho de su trabajo.

En otro aporte importante, Julian Urrego, abogado colombiano, nos explica detalladamente la legislación que rige el tema de la tenencia y el porte de armas traumáticas en Colombia.

Viajamos luego al Cáucaso de la mano de Guadi Calvo, nuestro analista senior, para enterarnos de las últimas novedades del conflicto entre Armenia y Azerbaiyán, y sus implicaciones en la geopolítica regional y mundial. Cerrando esta edición con una nota sobre los UAV Scan Eagle y Night Eagle, que operan en las Fuerzas Militares de Colombia.

Gracias por leernos.

¡Conocer para vencer!

Douglas Hernández

Editor

Este boletín tiene versión en inglés.

TRIARIUS 076

Contenido:

TRIARIUS

La situación con la actual pandemia tiene múltiples aristas, que obligan a múltiples análisis. Son necesarias diversas aproximaciones al fenómeno para intentar comprender lo que pasó, y es necesario también hacer prospectiva sobre los escenarios futuros relacionados con nuevas pandemias -espontáneas o provocadas-. Debido a las restricciones científicas, técnicas, tecnológicas y además legales, desarrollar un arma nuclear es un reto casi que insuperable para la mayoría de los países del mundo, no así desarrollar un virus mortal y usarlo como arma de destrucción masiva. Hoy, todos hemos apreciado el poder desestabilizador de uno de estos microorganismos, y su alcance global. Es perfectamente factible que algunos gobiernos díscolos, y grupos terroristas de cualquier etiología, estén evaluando la posibilidad de hacerse con virus mortales y usarlos como arma. Es un plan viable para un grupo terrorista, liberar un virus del calibre del actual, en las principales ciudades del enemigo, mientras que sus seguidores y sus familias se aíslan en una región remota, impidiendo el acceso a viajeros que podrían estar contagiados. Causarían caos y destrucción masiva, mientras que ellos se preservan…

En portada, ***Soldado hondureño de Fuerzas Especiales.***
Ver más información al final de la revista.

Agradecimiento muy especial a los analistas internacionales que de manera gratuita nos han enviado sus artículos para este número.

Vandalismo y Orden Público en Colombia

Por Julián David Urrego Atehortua (Colombia)

Grupo de manifestantes violentos en la ciudad de Bogotá.

En el presente escrito me he propuesto analizar, jurídicamente pero también, de manera no tan técnica y sencilla, comprensible para todos, este asunto de las protestas en escenarios públicos además de los derechos que tenemos frente a ellas, contrarrestándolos con el vandalismo y, los deberes y obligaciones de alcaldes como autoridades de policía.

Sea importante señalar que los colombianos tenemos unas normas que nos regulan y nos permiten, en primer lugar, tener un norte como sociedad, es decir, responden a la pregunta ¿Hacia dónde vamos como nación? Y en segundo lugar unas normas de convivencia que nos permiten interactuar entre nosotros de una manera civilizada en el marco del respeto hacia los derechos del otro.

Dentro de este contexto podemos decir que el norte de nuestra sociedad, es un orden político, económico y social justo, que podemos encontrar en el preámbulo constitucional, que al tenor predica:

"*El pueblo de Colombia,*

en ejercicio de su poder soberano, representado por sus delegatarios a la Asamblea Nacional Constituyente, invocando la protección de Dios, y con el fin de fortalecer la unidad de la Nación y asegurar a sus integrantes la vida, la convivencia, el trabajo, la justicia, la igualdad, el conocimiento, la libertad y la paz, dentro de un marco jurídico, democrático y participativo que garantice un ***orden político, económico y social justo****, y comprometido a impulsar la integración de la comunidad latinoamericana, decreta sanciona y promulga la siguiente constitución política."*

-subrayado y negrilla fuera de texto original-

En Colombia entonces, las leyes están jerarquizadas, encontrando en la cima, como norma de normas a nuestra Constitución Política, debajo de ella, las leyes que hace el Congreso de la República y para efectos de tratar el orden público tenemos, debajo de las leyes, los decretos municipales que expiden los alcaldes.

De este modo, nos adentramos en la presente exposición, así:

De los derechos de quienes se expresan en el espacio público.

En primer lugar, remitiéndonos a nuestra norma máxima, la constitución política, encontramos:

"**Artículo 37:** *Toda parte del pueblo puede reunirse y manifestarse pública y pacíficamente. Sólo la ley podrá establecer de manera expresa los casos en los cuales se podrá limitar el ejercicio de este derecho".*

Y el **artículo 38**, que nos dice:

"Se garantiza el derecho de libre asociación para el desarrollo de las distintas actividades que las personas realizan en sociedad".

Teniendo claro nuestro derecho de reunión y a **expresar pública y pacíficamente** nuestras ideas, veamos entonces cómo la ley 1801 de 2016, regula este ejercicio, conforme se señala en el artículo 37 de la constitución política ya citado:

Artículo 53 *"Toda persona puede reunirse y manifestarse en sitio público con el fin de exponer ideas e intereses colectivos de carácter cultural, político, económico, religioso, social o de cualquier otro fin legítimo.*

Con tales fines debe darse aviso por escrito presentado ante la primera autoridad administrativa del lugar o mediante correo electrónico. Tal comunicación o correo debe ser suscrito por lo menos por tres personas.

Tal aviso deberá expresar día, hora y sitio de la proyectada reunión y se presentará con 48 horas de anticipación indicando el recorrido prospectado.

Toda reunión y manifestación que cause alteraciones a la convivencia podrá ser disuelta. (…)"

-**Subrayas fuera de texto original-**

En este orden de ideas, tenemos claro que como ciudadanos podemos expresar nuestras ideas políticas en el espacio público, pero dentro del marco de la normatividad vigente, es decir de manera pacífica y avisando a la autoridad administrativa de policía - alcalde - cuál será la ruta prevista en la marcha o si será una actividad estática pero desarrollada en el espacio público.

De los derechos de quienes no participan en manifestaciones públicas:

Lo anterior tiene una razón; Y es que, en una sociedad, existen deberes y derechos, en especial frente al tema que venimos abordando y, si bien los ciudadanos tienen un derecho a manifestarse pública y pacíficamente, la administración o alcaldía también tiene una obligación de garantizar la libre movilidad de quienes también como ciudadanos deciden no participar en marchas, paros o huelgas, veamos los derechos de estos:

"Articulo 24 C.N: *Todo colombiano, con las limitaciones que establezca la ley, tiene derecho a circular libremente por el territorio nacional, a entrar y salir de él, y a permanecer y residenciarse en Colombia".*

"Articulo 25 CN*: El trabajo es un derecho y una obligación social y goza, en todas sus modalidades, de la especial protección del Estado (…)"*

De esta manera nos queda claro que si bien una parte de la ciudadanía tiene derecho a manifestarse pública y pacíficamente frente a una posición política que se tenga, otra parte de la ciudadanía tiene todo el derecho a que se regule y garantice su movilidad en la ciudad y en especial cuando se trata de desplazamientos hacia o desde un lugar de trabajo.

De las obligaciones de Alcaldías frente a unos y otros ciudadanos.

Teniendo en cuenta todo este contexto de derechos, es importante observar las obligaciones de las autoridades municipales o distritales de Policía -alcaldes-, las cuales encontramos en la ley 1801 de 2016, así:

"Artículo 54: *Los alcaldes distritales o municipales, salvo circunstancias excepcionales o de fuerza mayor, deberán autorizar el uso temporal de vías dentro de su jurisdicción para actos o eventos de ejercicio del derecho de reunión o manifestación pública y pacífica en el espacio público. En el caso de las vías arterias principales o corredores de transporte público colectivo deberán establecer un plan efectivo de desvíos para la movilización de los ciudadanos que no participan del acto o evento, como medida de protección de los derechos de los demás ciudadanos".*

-subrayas fuera de contexto original-

Quedando con lo anterior, muy claro que con esta obligación de las autoridades de policía se protegen los derechos tanto de ciudadanos que se manifiestan en el espacio público como de los que se movilizan en el mismo.

Ahora bien, pasamos a una parte importante y es la del vandalismo y la de los asuntos sometidos a la legislación penal, para lo cual en primer lugar veremos el significado de las palabras vándalo y vandalismo que, según el diccionario de la real academia española, significan:

"Vándalo: Dicho de una persona: Que comete acciones propias de gente salvaje y destructiva (…)"

"Vandalismo: Espíritu de destrucción que no respeta cosa alguna, sagrada ni profana (…)"

En este orden de ideas catalogaremos como vándalo a aquel ciudadano que:

Primero: existiendo una ruta y unos permisos por parte de la alcaldía distrital o municipal para la utilización del espacio público en las manifestaciones, decide tomarse por medio de la fuerza o violencia las vías que no están autorizadas.

Segundo: existiendo diferentes medios alternativos de comunicación y redes sociales decide violentar el espacio público de todos, con el fin de comunicar a través de grafitis, rayones y escritos insultantes mensajes propios de su entender individual y particular de la situación política del país.

Así pues, esta definición de vándalo y vandalismo la podríamos dejar ahí, solo en la definición, pero es importante que el lector dentro de un ejercicio académico comprenda que, en nuestra legislación penal, existen los siguientes delitos:

LEY 599 DE 2000 CÓDIGO PENAL COLOMBIANO.

ARTICULO 173. APODERAMIENTO DE AERONAVES, NAVES, O MEDIOS DE TRANSPORTE COLECTIVO. *El que mediante violencia, amenazas o maniobras engañosas, se apodere de nave, aeronave, o de cualquier otro medio de transporte colectivo, o altere su itinerario, o ejerza su control, incurrirá, por esa sola conducta, en prisión de ciento sesenta (160) a doscientos setenta (270) meses y multa de mil trescientos treinta y tres punto treinta y tres (1333.33) a cuatro mil quinientos (4.500) salarios mínimos legales mensuales vigentes.*

ARTICULO 182. CONSTREÑIMIENTO ILEGAL. *El que, fuera de los casos especialmente previstos como delito, constriña a otro a hacer, tolerar u omitir alguna cosa, incurrirá en prisión de dieciséis (16) a treinta y seis (36) meses.*

ARTICULO 265. DAÑO EN BIEN AJENO: *El que destruya, inutilice, haga desaparecer o de cualquier otro modo dañe bien ajeno, mueble o inmueble incurrirá en prisión de dieciséis (16) a noventa (90) meses y multa de seis punto sesenta y seis (6.66) a treinta y siete punto cinco (37.5) salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya delito sancionado con pena mayor.*

La pena será de dieciséis (16) a treinta y seis (36) meses de prisión y multa hasta de quince (15) salarios mínimos legales mensuales vigentes, cuando el monto del daño no exceda de diez (10) salarios mínimos legales mensuales vigentes.

Si se resarciere el daño ocasionado al ofendido o perjudicado antes de proferirse sentencia de primera o única instancia, habrá lugar al proferimiento de resolución inhibitoria, preclusión de la investigación o cesación de procedimiento.

ARTICULO 266. CIRCUNSTANCIAS DE AGRAVACION PUNITIVA. *La pena se aumentará hasta en una tercera parte, si la conducta descrita en el artículo anterior se cometiere: (…)*

4. Sobre objetos de interés científico, histórico, asistencial, educativo, cultural, artístico, sobre bien de uso público, de utilidad social, o sobre bienes que conforman el patrimonio cultural de la Nación.

-Negrillas fuera de contexto original-

ARTICULO 429. VIOLENCIA CONTRA SERVIDOR PÚBLICO. *El que ejerza violencia contra servidor público, por razón de sus funciones o para obligarlo a ejecutar u omitir algún acto propio de su cargo o a realizar uno contrario a sus deberes oficiales, incurrirá en prisión de cuatro (4) a ocho (8) años.*

Concluyendo finalmente que un acto de vandalismo dentro del marco de una toma del espacio público que no está autorizada por la alcaldía puede ser tipificado como delito y originar, además, a la luz del artículo 94 de nuestra legislación penal, la obligación de resarcir el daño.

ARTICULO 94. REPARACION DEL DAÑO. *La conducta punible origina obligación de reparar los daños materiales y morales causados con ocasión de aquella.*

Corresponderá pues y para concluir el presente escrito, a la alcaldía distrital o municipal garantizar los derechos de todos sus asociados a través del ejercicio de sus derechos y en especial de su deber de protección de la convivencia en sus categorías de seguridad y tranquilidad, que rezan:

Categoría seguridad: garantizar la protección de los derechos y libertades constitucionales y legales de las personas en el territorio nacional.

Categoría tranquilidad: Lograr que las personas ejerzan sus derechos y libertades, sin abusar de los mismos y con plena observancia de los derechos ajenos.

Fuente de la Imagen:
https://www.alertapaisa.com/noticias/nacional/por-que-los-vandalos-quedan-libres-en-pocas-horas-en-colombia

Referencias

Constitución Política de Colombia. Gaceta Constitucional No. 116 de 20 de julio de 1991

Ley 1801 de 2016. Por la cual se expide el Código Nacional de Seguridad y Convivencia Ciudadana. Diario Oficial No. 49.949 de 29 de julio de 2016.

LEY 599 DE 2000. Por la cual se expide el Código Penal. Diario Oficial No. 44.097 de 24 de julio del 2000

Real Academia Española. Diccionario de la lengua española. www.rae.es

Julián David Urrego Atehortua
(Colombia) Abogado.

Apátridas: los fantasmas del sistema internacional

Por Marianna Crudi y Alberto Carracedo (Argentina)

La manifestación más pura de una amenaza a la seguridad humana es aquella invisible, la que se padece en la soledad del destino nómade y sin retorno posible. Con el desinterés de los demás, sean simples ciudadanos que ignoran la presencia del recién llegado o gobiernos que lo capturan en intrigas locales para las que hace falta encontrar responsables. Después de todo, qué mejor que observar con recelo a quién no tiene Patria para resguardar la propia.

Así, la apatridia, la falta del reconocimiento de la nacionalidad de una persona, se convierte en el punto de partida de una vida llena de desafíos, de padecimientos silenciosos, de pasos sin dirección cierta. Probablemente la mayoría de los individuos no sea realmente consciente de los privilegios que cobijan y protegen bajo el amparo de la nacionalidad, de la aparentemente insignificante pertenencia a un pasado común y compartido en una ciudadanía, una amalgama de historias, desafíos y esfuerzos que se heredan con la tierra que caminamos desde niños.

La nacionalidad se convierte, entonces, en la puerta de entrada a una vida que parecería ideal, aquella en la cual todas las personas son libres, dignas e iguales, que gozan de los mismos derechos sociales, civiles y políticos; y en la que existen autoridades que velan por su seguridad.

Sin embargo, la irrealidad de este idealismo de la vida soñada se enfrenta a una versión desfigurada en la vida real en la que conviven afortunados y desafortunados, nacionales y apátridas.

De más está decir que esta historia no es nueva y las razones que la explican encuentran su raíz en el sistema político, legal, religioso y social. Es su multiplicidad de causas las que complejizan la resolución del conflicto, las que profundizan las grietas en una sociedad que, a fin de cuentas, habitan todos, los privilegiados y los que no lo son.

En este contexto, el concepto de seguridad humana irrumpe a finales del Siglo XX revolucionando la teorización tradicional.

Las percepciones previas, cuyos objetos han sido los Estados y el único fin el de defender la soberanía nacional materializada en el territorio manteniendo la supervivencia misma de la unidad ante un contexto internacional anárquico; se entienden al considerar la historia mundial como un relato de vivencias colmado de enfrentamientos bélicos en la cual la protección de los recursos propios y las capacidades militares se tornaban las principales premisas.

En este nuevo enfoque -de seguridad humana- se asocia la seguridad con el bienestar de la población. Donde el bienestar de una persona se origina en su integridad, se multiplica con su libertad y se realiza en su totalidad con la oportunidad de satisfacer las necesidades básicas.

No tener nacionalidad podría entenderse erróneamente como una condición de libertad eterna; pero no basta con esta idea de ser libre, si la libertad no le permite al individuo ser feliz. Ninguna persona podría ser feliz ni gozar de la libertad aparente si padece hambre que no puede calmar, problemas de salud que no pueden ser atendidos, y si vive rodeado de condiciones que atentan contra su integridad y la de su familia.

Y, aunque una vida de este estilo, sin el goce de las oportunidades para crecer parecería inconcebible, al menos en el extremo amenazante en el que se consolida la apatridia, la única verdad es que existen millones de personas bajo esta condición. Desamparados de protección estatal y muchas veces expulsados del sistema social. Su desvinculación de la comunidad se rodea de desesperanza y de necesidad, generando en ocasiones elementos de rencor.

La anomia social que caracteriza el estado de los apátridas se convierte en una oportunidad para que aquellos con los fines más terroríficos comparezcan como salvadores. De este destino nadie se salva cuando la necesidad se antepone a la moralidad. Niños, jóvenes y adultos, individualmente o familias completas, sin importar su raza ni religión, son vistos como piezas de un sistema ilegal cuyo único fin es la generación de riqueza a expensas de sus servidores y a través de su explotación.

Así, el crimen organizado internacional, las redes de tráfico ilícito de estupefacientes y precursores químicos, la trata de personas con fines de explotación sexual y laboral, el trabajo forzado, la esclavitud y el terrorismo, pasan a concebirse como los horizontes más cercanos de los excluidos de las sociedades, de los negados de la nación. De quienes no tienen opción ante semejantes aberraciones y ceden sus vidas con la esperanza de poder salir en el futuro de tales infiernos.

Según el Alto Comisionado de las Naciones Unidas para los Refugiados (ACNUR), para finales del año 2019 había en el mundo 4,2 millones de personas apátridas (1) y, aunque la mayor parte de estas personas se encuentran en países de Asia como Myanmar, Kuwait, Tailandia e Irak, sería ingenuo pensar que es una problemática ajena a nuestra realidad. Tanto por la cantidad como por la capacidad de cooptación y traslado de las organizaciones criminales mencionadas, resulta un potencial caldo de cultivo para el daño y el terror.

Una amenaza latente a la integridad de las personas de quienes utilizan a nuestra región como factoría, como tránsito y como destino. Una desgracia, entre tantas, que condena a los Latinoamericanos a vivir en el continente más violento del mundo (2).

Los apátridas son una exposición palpable de la humillación a las personas, con potencial proyección sobre el mundo todo. Desamparo y desprotección a disposición de quién ofrezca tan solo una esperanza. Verdaderos fantasmas del sistema internacional.

Los apátridas viven en un mundo donde el hogar no les significa nada, y en donde pareciera que, como anticipaba Hannah Arendt, existe el derecho a tener derechos. Y así, la privación de tener un lugar reconocido en el concierto de naciones es la manifestación básica de la violación de los derechos humanos de una persona.

Ya la filósofa alemana -que vivió en carne propia los avances desgarradores del nazismo- señalaba que las personas sin derechos “se hallan privados, no del derecho a la libertad, sino del derecho a la acción; no del derecho a pensar lo que les plazca, sino del derecho a la opinión” y, lo que es peor “los privilegios (...), injusticias en su mayoría, los acontecimientos favorables y desfavorables, les sobrevienen como accidentes y sin ninguna relación con lo que hagan, hicieron o puedan hacer” (Arendt,1951: 247) (3).

Salvando las distancias que nos separan del momento histórico en el cual Arendt escribió la cita anterior, y teniendo las precauciones necesarias para permitir tal analogía, es posible afirmar que el mundo de hoy posee características muy similares a las de las peores décadas del siglo pasado.

El sistema internacional debe comprometerse para que los apátridas dejen de ser fantasmas y se corporicen en nuevas vidas, dignas y autosuficientes. Pero ello, no sólo será un deber de las cúpulas gubernamentales sino de la sociedad toda.

El incipiente siglo requiere un nuevo contrato social que ponga en jaque toda aquella manifestación que atente contra los derechos humanos de las personas, derechos humanos ciertos y no una andanada de declaraciones livianas o ideológicamente sesgadas.

No vaya a ser cosa que la necesidad conduzca a los sin Patria a mutar en demonios a manos del mismísimo diablo.

Referencias

(1) https://www.acnur.org/datos-basicos.html
(2) https://www.unodc.org/documents/data-and-analysis/gsh/Booklet2.pdf#page=18
(3) Arendt, H. (1951). Los orígenes del totalitarismo.

Fuente de la Imagen:
https://sites.google.com/site/derechoshumanosgregcaro777/-cuales-son-los-derechos-humanos

Marianna Anabel Crudi
(Argentina) Licenciada en Gobierno y Relaciones Internacionales (UADE), Diplomada en Negocios y Relaciones Internacionales (WYA), Ha cursado la Maestría en Inteligencia Estratégica Nacional de la Universidad Nacional de La Plata (UNLP). Directora del Instituto de Asuntos Transnacionales en la Fundación Pro Humanae Vitae. Investigadora en el Centro de Estudios de Medio Oriente Contemporáneo (CEMOC-CARI).

Alberto Carracedo
(Argentina) Ex Oficial de Infantería del Ejército Argentino (CMN), Licenciado en Administración (UNPA), Magister en Administración de Empresas (UB). Ha cursado la Maestría en Inteligencia Estratégica Nacional de la Universidad Nacional de La Plata (UNLP). Docente universitario de grado y posgrado, y analista de aspectos que hacen a la seguridad y defensa desde las ciencias económicas. Miembro de la Comunidad de inteligencia y Seguridad Global (CISEG).

LISA Institute
Security Education

Fórmate Online con Expertos.
Cuando quieras. Donde quieras.

+20% DESCUENTO

Código: *TRIARIUS20*

(Descuento disponible hasta fin de existencias)

CURSOS CON INSCRIPCIONES ABIERTAS

INTELIGENCIA

- Curso de Experto en Análisis de Inteligencia
- Curso de Analista de Inteligencia Especializado en Redacción de Informes de Inteligencia
- Curso de Analista de Inteligencia Especializado en Sesgos Cognitivos y Esquemas Mentales

TERRORISMO

- Curso de Gestión de Objetos Sospechosos y Explosivos
- Curso de Asistencia y Tratamiento a Víctimas del Terrorismo
- Curso de Análisis Interno de Procesos de Radicalización en Terroristas Yihadistas
- Curso sobre Drones como Tecnología Dual: Seguridad y Defensa vs Terrorismo y Crimen Organizado

RELACIONES INTERNACIONALES

- Curso-Certificado de Analista Internacional
- Curso de Experto en la Unión Europea

100%
ONLINE
INTERACTIVO
FLEXIBLE

www.LISAINSTITUTE.com

Radicalización islámica en videojuegos: “Una guerra sin fronteras”

Por Micaela Abril Álvarez (Argentina)

Radicalización en Redes

En el presente trabajo, frente a la ausencia de definiciones oficiales de las palabras “terrorismo” y “radicalización” definiremos esta última como “el proceso en el que un individuo se adhiere a opiniones, puntos de vista e ideas radicales, tendientes a la promoción del conflicto y uso de violencia, que puede llevar a los individuos reclutados a cometer actos terroristas (1).”

Del Califato al Cibercalifato

El proceso de globalización abrió sus puertas a un continuo avance tecnológico y un mundo interconectado. Sin entrar en detalles, estableceremos un punto medio sobre las perspectivas positivas y negativas (2) de la globalización, donde muchos de sus beneficios pueden ser utilizados para transgredir el orden y bienestar social.

Durante los últimos años, el terrorismo se destacó por la utilización de herramientas informáticas o “Propaganda Islámica”, no sólo para difundir su mensaje, sino para el reclutamiento y radicalización a través redes sociales. El relativo anonimato de los usuarios en línea y la capacidad de conexión global instantánea del Siglo XXI ofrece una larga lista de ventajas para quienes desean realizar sus crímenes sin ser descubiertos.

La Organización terrorista Daish (3), logró adaptarse a estas nuevas modalidades, y migró hacia un “califato virtual” luego de perder los territorios ocupados en Siria e Irak.

Captación en redes

La proliferación de las plataformas de redes sociales utilizadas por terroristas y radicalizados fue alternando a lo largo de los años; Desde Twitter, donde Abu Mohammad Al-Julani (4) motivó a sus seguidores a participar activamente, “hacer de su computadora una bomba y no quedarse en la comodidad de Telegram”, hasta Diáspora, Friendica, Quitter, Justpaste, Ask.fm, Soundcloud, TikTok, Sarahah17 y Mixlr luego de que sus cuentas fueran bloqueadas.

Utilizan ciertos sitios web, estaciones de radio, videos promocionales de Clanging of the Swords 5IV y su revista Dabiq para difundir su ideología y navegan infiltrados por la red sin dejar rastro mediante la utilización de Tor y sus propios Software de encriptación. Además, es usual ver el empleo de la esteganografía para evitar el ciberespionaje. Esta técnica permite ocultar archivos de datos en fotografías haciéndola lucir como cualquier otra.

Para comunicarse también utilizan servicios móviles con encriptación como Viber, Surespot, Wickr, FaceTime, Kik, Skype, WhatsApp y Telegram.

Mediante el modelo Swarmcast (6), los simpatizantes difunden y viralizan material terrorista a través de las redes sociales.

A pesar de que diversas redes sociales están invirtiendo en programas basados en inteligencia artificial para controlar la difusión de propaganda terrorista, los extremistas continúan encontrando formas alternativas de difundir sus mensajes. Las leyes y la política internacional no han sido suficientes para evitar que los extremistas usen la World Wide Web como un activo estratégico.

Difusión de propaganda

Daish utiliza la propaganda y desinformación al difundir su ideología a la mayor cantidad de personas posible en varios idiomas. En febrero de 2015 el ex presidente Obama argumentó: "Los videos de alta calidad, las revistas en línea, el uso de las redes sociales, las cuentas terroristas de Twitter, todo está diseñado para atacar a los jóvenes de hoy en línea, en el ciberespacio". En su plataforma de Twitter, comparte videos, textos, memes, infografías, enlaces a sus revistas y otros medios. Sus seguidores suben diariamente videos infundiendo el terror, transmitidos en vivo desde el campo de batalla, mensajes que representan una vida utópica bajo el califato islámico.

Videojuegos

El Daish no sólo se limitó a las redes sociales, sino que recurrió a los videojuegos para atraer a los jóvenes, apelando a juegos online FPS en inglés (disparos en primera persona) como Call of Duty, Grand Theft Auto, Counter Strike, ARMA III, Battlefield, entre otros.

Según el Global Terrorism Index 2019 (7) esto “Le permite al Daish aprovechar aproximadamente el 57% de los dos mil millones que juegan juegos de disparos en primera persona, la mayoría de los cuales representan su objetivo demográfico: jóvenes, en su mayoría varones y expertos tecnológicamente.”

La fuerte correlación entre las experiencias personales de los individuos y la psiquis de los jóvenes genera que existan personas vulnerables, con una mayor tendencia a la radicalización. Factores de riesgo como la anomia, la islamofobia, la injusticia (real o percibida), la exclusión, el extremismo religioso, el no sentirse aceptados en la sociedad, la discriminación percibida y las carencias identitarias pueden estar contribuyendo a la radicalización de los musulmanes en suelo europeo. También se enfatiza el papel que pueden desempeñar Internet y ciertas redes sociales según la Comisión Europea (2005). Estas variables generan que la manipulación sea trabajo fácil para explotar los sentimientos canalizados de odio, frustración y venganza. Aquí, es donde las adaptaciones de los videojuegos originales juegan un rol fundamental para consolidar una subcultura de la violencia, desencadenando el odio sistemático contra los infieles y apóstatas, alcanzando la deshumanización de sus blancos.

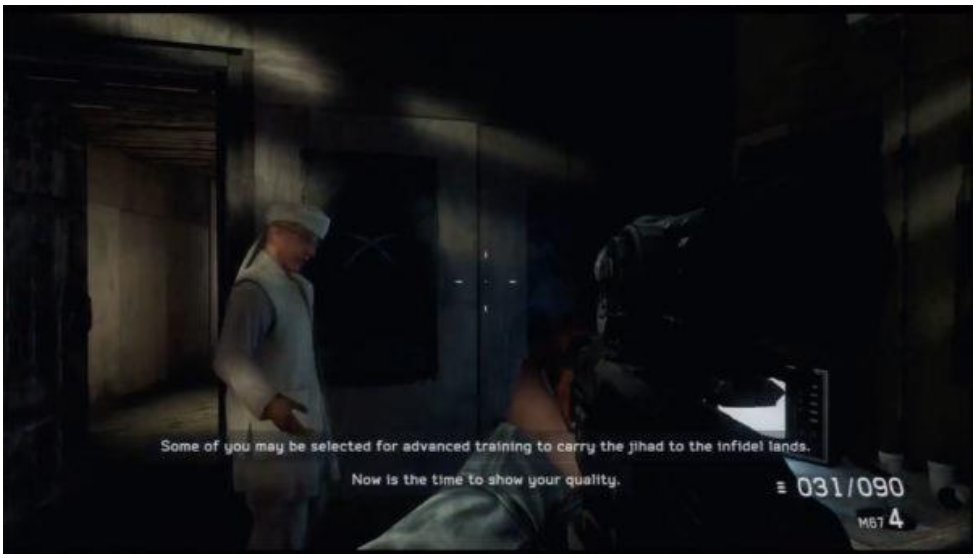


Imagen 1 Entrenamiento simulado yihadista (Fuente: Aim Down Sights. 2018)

Absortos en un mundo paralelo donde es posible ser quiénes deseemos, nos enfrentamos a un escenario que permite realizar actos terroristas sin consecuencias, que nos ofrece jugadores completamente comprometidos a elegir el bando de los terroristas, interactuando y compartiendo sus ideales con otros jugadores.

Imagen 2 GTA (Fuente: Rayal Al-lawheed)

En términos de su desarrollo, no es difícil realizar cambios en el juego original de GTA personalizando los skins de sus personajes, descargándolos a través de la Deep Web o desempeñando roles opuestos similares a los del Ejército de Estados Unidos y Modern Warfare 2. El juego alcanzó su popularidad en septiembre del 2014, basado en una búsqueda de Google en árabe usando el término "Descargar el juego de Salil al-Sawarem". (8)

Se llama "Salil al-Sawarim" en árabe (The Clanging of the Swords), que es un juego de disparos en primera persona (FPS). En su portada se lee: “Lo que realizas en el juego nosotros lo hacemos en el campo de batalla”.

En otras palabras, los tipos de confrontaciones armadas reales con las que Daish se involucra son similares a las guerras virtuales producidas en los videojuegos occidentales.

Los juegos se caracterizan por mantener una estética idéntica al original. En el caso del tráiler del GTA publicado por Daish muestra imágenes de explosiones, ataques con rifles de francotirador y tiroteos. Su calidad y parecido con el juego original confundiría a muchos si se pasaran por alto las nasheeds (canciones religiosas), el estandarte del Daish en la parte superior de la pantalla y los subtítulos en árabe llaman a la lucha contra las fuerzas estadounidenses y al "Ejército Safavid", referencia a las fuerzas iraníes o pro-iraníes.

Imagen 3 Grand Theft Auto (https://theintercept.com/2014/09/17/grand-theft-auto-isis/)

Se desconoce el autor de la adaptación debido a que no es producido por el Ministerio de Información centralizado del Daish, como Al-Hayat, Al-Furqan y Al-Ethar, especialmente porque el grupo se opone a las actividades de entretenimiento como escuchar música o los juegos que pueden “desviar la atención de la oración y la fe”.

Tampoco está claro si el juego fue realmente producido o no; ya que los enlaces que llevan al videojuego conducen a sitios web de torrents que no funcionan o a archivos con un peso impensable para un juego con estos gráficos. Por lo tanto, se cree que el juego fue desarrollado por algunos simpatizantes de Daish, probablemente fuera de la región de Medio Oriente.

Imagen 4 y 5 GTA. Se pueden observar estandartes del Daish

Imagen 6 GTA referencia al atentado 9/11, observándose rascacielos a punto de ser destruidos con claridad.

Es importante reforzar que la violencia empírica del terrorismo está fuera de nuestro alcance si los gobiernos no toman las medidas correspondientes. Lo que está en juego es el poder simbólico del terror sobre nosotros a través de nuestro consumo y reproducción de su imagen en los videojuegos.

Se tiende a demonizar este tipo de juegos por considerarlos violentos para niños cuando en sus portadas figura el requisito PEGI +18, siendo sólo aptos para adultos. Sin embargo, no sólo encontramos material extremista en juegos de disparos en primera persona, como normalmente se cree. Se han realizado modificaciones de “Los Sims”, donde un terrorista mata a musulmanes dentro de una mezquita y Minecraft, donde el jugador dispara a civiles con un rifle semi-automático.

El proceso de radicalización mediante videojuegos compone cuatro escalones:
1. Captación por chat
2. Invitación mediante Tor o Twitter
3. Divulgación por medio de la Deep Web.
4. Comunicación a través de Telegram u otros servicios móviles.

De esta manera, vemos que el terrorismo implica toda una realidad de símbolos, de geopolítica, de narrativas sociales históricas y de políticas del mundo real que se desarrollan en el presente. Esto lo diferencia de cualquier otro juego violento. Ya no se puede hablar de la violencia que otorga un juego como entretenimiento. No se debe pasar por alto un juego que permite elegir como arma un chaleco bomba. Sin embargo, citando al agente del FBI Ali Soufan: “La verdadera batalla reside en la batalla contra las ideas y métodos que utilizan los terroristas para reclutar, si no somos capaces de accionar frente a estas ideas, ésta guerra nunca terminará”. Es decir, nunca podremos combatir realmente al terrorismo si continuamos viéndolo como una sustancia determinada y no como lo que realmente es, una metodología.

Provoca una abducción de la personalidad de los jóvenes radicalizados, quienes dejan atrás la vida que alguna vez tuvieron, entregándose completamente a una causa externa, presos de una ideología que no sólo volvieron propia, sino que sacrificarían miles de vidas por ella.

Como conclusión, frente a la existente posibilidad de radicalizarnos desde cualquier punto del planeta y la comodidad de nuestra casa, es responsabilidad de cada Nación establecer un Plan de Protección de Infraestructuras Críticas, como de estrategias nacionales e internacionales de cooperación en ciberseguridad, con el fin de protegernos, prevenir y combatir el terrorismo de una manera viable.

Notas

(1) Entendido como el acto de infundir terror o miedo en la población, con fines políticos, religiosos o económicos.

(2) Referencia la perspectiva negativa marxista y El Capital Financiero de Hilferding como predominio del capital, el imperialismo y el poder hegemónico de una minoría sobre las mayorías, y a la perspectiva optimista, comúnmente encontrada en corrientes
neoliberales, la cual ve los procesos de globalización como el surgimiento de una nueva era de oportunidades, libre mercado y crecimiento económico para nuevos actores.

(3) O erróneamente denominado por algunos medios de comunicación como Estado Islamico

(4) “Es un terrorista yihadista sirio, comandante en jefe de Tahrir Al-Sham, filial siria de al- Qaeda. Además, fue emir de su organización predecesora Jabhat al-Nusra, al igual que esta, adherida al-Qaeda.”

(5) Película documental realizada por Daish como material propagandístico. En él se las
destacan ejecuciones y torturas a sus prisioneros.

(6) Este modelo sugiere que los simpatizantes se reúnen como un enjambre de abejas o pájaros que siempre se reorganizan ellos mismos y están listos para atacar y atacar en cualquier momento dado.

(7) Institute for Economics & Peace. Global Terrorism Index 2019: Measuring the Impact of Terrorism, Sydney, November 2019. Available from: http://visionofhumanity.org/reports (accessed 29/11/2019)

(8) "Salil al-Sawarem" es también el nombre dado por Daish a su canto religioso, que debe distinguirse del videojuego.

Referencias

Ahmed Al-Rawi (2018). Video games, terrorism, and ISIS’s Jihad 3.0, Terrorism and Political Violence, 30:4, 740-760, DOI: 10.1080/09546553.2016.1207633

Cori E. Dauber, Mark D. Robinson, Jovan J. Baslious and Austin G. Blair. Call of Duty: Jihad – How the Video Game Motif Has Migrated Downstream from Islamic State Propaganda Videos. Perspectives on Terrorism
Vol. 13, No. 3 (June 2019), pp. 17-31 (15 pages)

Ahmad M, Shehabat. Beyond Twitter Revolutions: The Impact of Digital Media Logistics on Terror Networks of Communication in Iraq and Syria from 2014 on Terror Networks of Communication in Iraq and Syria from 2014 to 2016.

Amid Telegram Crackdown, Jihadists Seek Alternate Platforms While Some Hold Steadfast

Fuente de la Imagen:
https://fundacionaprenderamirar.wordpress.com/2017/11/29/pasos-para-evitar-la-adiccion-a-los-videojuegos/

Micaela Abril Álvarez
(Argentina) Universidad Tecnológica Nacional. Facultad Regional Buenos Aires. Especialización Profesional en Terrorismo y Ciberseguridad.

Sistema de Protección de Infraestructuras Críticas de la República Argentina: Ciberinteligencia para la toma de decisiones

Por Agostina Taverna y Rodrigo Cárdenas Holik (Argentina)

Resumen - Considerando el auge de las ciberamenazas y los ciberataques ocurridos contra infraestructuras críticas en el mundo, es claro que la Argentina debe estar preparada para anticipar, prevenir, proteger y defender aquellas infraestructuras que brindan servicios esenciales. Es el Estado quien tiene la responsabilidad de garantizar el normal y continuo funcionamiento de dichos servicios, mediante la elaboración de normas nacionales por parte del Poder Legislativo y su cumplimiento por parte del Poder Ejecutivo, con el fin de evitar cualquier impacto en la vida humana, la economía, el ejercicio de los derechos humanos y la libertad individual así como en la soberanía nacional.

Frente a ello, el objetivo del presente trabajo es plantear la necesidad de crear un sistema nacional e institucional, especializado en la temática, que, por medio de un esquema innovador y multisectorial, con articulación interagencial, trabaje simbióticamente con otros de su estilo y existentes, a favor de organizar a la Administración Pública. Con este propósito, se presentan conceptos como inteligencia, ciberinteligencia, ciberamenazas, ciberataques, ciberseguridad y ciberdefensa en torno a la protección de las infraestructuras críticas, con el fin último de decidir qué camino deberá tomar la Argentina en virtud de escenarios futuros y prospectiva, potenciando la posibilidad de tomar decisiones estratégicas para nuestro país.

Palabras claves - ciberseguridad - inteligencia - ciberinteligencia - sistema de protección nacional de infraestructuras críticas - ciberamenazas - prevención.

INTRODUCCIÓN

Argentina tiene una serie de organismos, a nivel nacional, con distintas funciones y alcances, cuyo fin último es proteger al país frente a amenazas, sin distinción del origen, los actores involucrados o la forma en la que se llevan a cabo esas acciones. Frente a una guerra o un delito, el Estado posee elementos vigentes establecidos por ley cuya actuación de manera coordinada, conjunta y cooperativa permitiría la toma de decisiones y medidas para garantizar la soberanía, resguardar los derechos y garantías de la sociedad en su conjunto y su patrimonio, así como el sistema representativo, republicano y federal establecido por la Constitución Nacional. Por otra parte, parte de la estabilidad y perdurabilidad de la sociedad democrática se basa en la confianza de la población

para con el Estado. Para ello, los autores consideran que es imprescindible que sea la Administración Pública Nacional quien garantice el normal y continuo funcionamiento de los servicios esenciales - soportados en infraestructuras consideradas críticas - cuya responsabilidad recae sobre organismos públicos y entidades privadas con órganos de control estatal. La interrupción parcial o total de alguno de estos servicios, podría generar caos, confusión, alteración del orden público, pánico, afectación a la salud y la vida humana, daños al desarrollo económico y a la integridad territorial, así como incertidumbre sobre la perpetuidad de un gobierno constitucional.

Con el objetivo de evitar esto y considerando los sistemas nacionales, institucionales y gubernamentales existentes en la actualidad, será necesario articular todos aquellos actores que se relacionan con la protección de dichas infraestructuras críticas a favor de resguardar la república y los valores que representa, además de establecer las responsabilidades de cada uno para construir la base que permitiría preservar el ciberespacio y los servicios considerados como esenciales en la Argentina. Para ello, será imprescindible que la vinculación interagencial y multinivel pondere, mediante una visión estratégica, a la ciberseguridad y a la ciberdefensa (a través de herramientas decisionales como la ciberinteligencia) como pilares de protección de la información que hacen de vapor a una maquinaria que brinda prestaciones sustanciales para la sociedad.

ESTADO DEL ARTE

Sistemas institucionales y nacionales en Argentina

La Real Academia Española asevera que el término sistema proviene del latín tardío systēma, y este del griego σύστημα sýstēma y presenta diversas definiciones donde se destaca “conjunto de cosas que relacionadas entre sí contribuyen a determinado objeto” [1]. A pesar de ser una definición general, es posible extrapolar la misma al concepto de que un sistema institucional integra y reúne un conjunto de elementos que relacionados entre sí ordenadamente contribuyen al cumplimiento de un objeto o función determinado. Además, “un sistema integrado es un vínculo para conformarse a modelos de valores compartidos, en el interés de los sujetos” [2] donde las instituciones o elementos deben realizar esfuerzos voluntarios, dirigidos y coordinados para el cumplimiento de su misión.

En Argentina, considerando la temática a desarrollar en el presente trabajo, es posible hallar diferentes sistemas institucionales nacionales que reúnen exclusivamente elementos gubernamentales, como es el caso del Sistema de Inteligencia Nacional (SIN), el Sistema de Seguridad Interior (SSI) y el Sistema de Defensa Nacional (SDN) cuyos lineamientos son definidos por el Presidente de la Nación. En términos generales, estos sistemas se caracterizan por agrupar distintos organismos o instituciones del ámbito público que mantienen sus funciones y objetivos principales, pero se reúnen en un sistema integrador en pos de garantizar la soberanía, resguardar los derechos y garantías de la sociedad en su conjunto y su patrimonio, así como el sistema representativo, republicano y federal establecido por la Constitución Nacional.

Específicamente, el SIN agrupa a la Agencia Federal de Inteligencia (AFI), a la Dirección Nacional de Inteligencia Criminal (DINICRI) y a la Dirección Nacional de Inteligencia Estratégica Militar (DINIEM), y es definido como el “conjunto de relaciones funcionales de los organismos de inteligencia del Estado Nacional, dirigido por la Secretaría de Inteligencia a los efectos de contribuir a la toma de decisiones en materia de seguridad exterior e interior de la Nación” [3]. Por otra parte, el Sistema de Seguridad Interior está conformado por el Presidente de la Nación, los gobernadores de la provincia adheridos a la ley N° 24.059, el Congreso Nacional, los ministros del Interior, de Defensa y de Justicia, la Policía de Seguridad Aeroportuaria y las policías provinciales de aquellas provincias que adhieran a la norma así como Gendarmería Nacional y Prefectura Naval, y “tiene como finalidad determinar las políticas de seguridad así como planificar, coordinar, dirigir, controlar y apoyar el esfuerzo nacional de policía dirigido al cumplimiento de esas políticas” [4]. Por otra parte, el Sistema de Defensa Nacional “estará orientado a determinar la política de defensa nacional que mejor se ajuste a las necesidades del país, así como a su permanente actualización” [5] y compuesto por el Presidente de la Nación; el Consejo de Defensa Nacional; el Congreso de la Nación; el Ministro de Defensa; el Estado Mayor Conjunto de las Fuerzas Armadas; el Ejército, la Armada y la Fuerza Aérea de la República Argentina; Gendarmería Nacional y Prefectura Naval Argentina en los términos que prescribe la presente Ley; el Pueblo de la Nación mediante su participación activa en las cuestiones esenciales de la Defensa, tanto en la paz como en la guerra de acuerdo a las normas que rijan la movilización, el Servicio Militar, el Servicio Civil y la Defensa Civil.

Inteligencia

En la actualidad, la Argentina cuenta con la Ley de Inteligencia Nacional (Ley N° 27.126 del año 2015) la cual establece las bases jurídicas, orgánicas y funcionales del SIN. De forma complementaria, la Nueva Doctrina de Inteligencia Nacional aprobó la estructura orgánica y funcional de la AFI y explicita que "la inteligencia nacional es una actividad que se inscribe dentro del marco del estado constitucional social y democrático de derecho orientada fundamentalmente a producir conocimientos acerca de las problemáticas – riesgos, conflictos – inscritas en la defensa nacional y la seguridad interior, siempre en función de la protección y promoción de los intereses políticos, institucionales, sociales, económicos y culturales del pueblo argentino" [6]. Los autores consideran que estas problemáticas – en especial el terrorismo, la criminalidad organizada y las acciones que atenten contra la ciberseguridad - deben ser abordadas a los fines de su prevención y/o conjuración, con el objetivo de resguardar, proteger y estabilizar el sistema democrático. Es nuestra opinión que, además, el Plan de Inteligencia Nacional debería contener el conjunto de acciones tendientes a cubrir la necesidad y demanda de información para la toma de decisiones e implementar políticas que garanticen el estado democrático de nuestra nación.

La producción de inteligencia nacional comprende una serie de actividades conocidas como: inteligencia nacional estratégica, contrainteligencia, inteligencia criminal e inteligencia estratégica militar. La primera, contempla la producción de inteligencia desde el análisis integral del conjunto de problemáticas que afectan la defensa nacional y la seguridad interior. Este producto superior es desarrollado por el personal profesionalizado perteneciente al organismo rector del SIN, la AFI. La contrainteligencia comprende el conocimiento del despliegue y actividades de inteligencia llevadas a cabo por individuos, grupos u organismos nacionales o extranjeros, que pueden afectar la defensa nacional y la seguridad interior. Es decir que la contrainteligencia debe ser generada por todos los miembros pertenecientes al SIN. Por otra parte, la inteligencia criminal se refiere a las problemáticas delictivas complejas y de relevancia federal relativas al terrorismo, a los atentados contra el orden constitucional y la vida democrática, a la criminalidad organizada y los atentados contra la ciberseguridad. Esto es facultad de la DINICRI. Por otra parte, la inteligencia estratégica militar se relaciona con los eventuales riesgos y/o conflictos generados por agresiones de origen externo perpetradas por fuerzas armadas pertenecientes a otros Estados en contra de la soberanía, la integridad territorial o la independencia política de nuestro país. Por lo expuesto, esta inteligencia corresponde a la cartera de la DINIEM.

En cualquiera de sus dimensiones, el producto de inteligencia se basa en un proceso circular conocido como el ciclo de inteligencia [7], el cual se compone de una serie de etapas cuya iteración debe darse de acuerdo al fenómeno bajo análisis. Las etapas que componen el ciclo son: dirección, obtención, elaboración y difusión.

Fig. 1. Ciclo de inteligencia: modelo "ideal".

En el trabajo "El Ciclo de Inteligencia Complejo: una ágil herramienta para operar en red" [8] se evalúa, desde una perspectiva crítica, el ciclo clásico compuesto por estas cuatro fases. Sin embargo, otros países tienen subfases o añaden otras etapas [9] como, por ejemplo, el proceso español el cual considera que la etapa de elaboración posee subfases como valoración, análisis, integración e interpretación. En términos generales, desconcierta observar que, pese a ser un ciclo y suponer una constante retroalimentación, se afirma que la etapa final del ciclo de inteligencia es la difusión.

En la misma línea de ideas, Javier Jordán efectúa una revisión del ciclo de inteligencia [10] y aclara que acorde al modelo ideal, el proceso de inteligencia sigue las mismas cuatros fases donde:

(1) Durante la etapa de dirección, se presentan las demandas y necesidades de las autoridades gubernamentales y políticas. Estas son transformadas en requerimientos específicos, lo cual inicia la asignación de tareas y recursos.
(2) En la etapa de obtención, se busca y recopila información la cual es enviada a los analistas una vez procesada. Existen varios medios y técnicas de obtención de información, como la inteligencia geográfica y de imágenes, la inteligencia humana, la inteligencia de señales, la inteligencia de medidas y firmas, la inteligencia web, la inteligencia de fuentes abiertas y la inteligencia tecnológica, entre otras [11].
(3) Durante la etapa de elaboración, los analistas reciben la información la cual es evaluada, analizada, integrada e interpretada. El resultado se refleja en un documento o informe destinado al decisor.
(4) Por último, en la etapa de difusión se hace entrega del producto resultante conocido como "inteligencia". En caso de que se requiera una mayor claridad o haya nuevas necesidades, el ciclo podría ser reactivado.

En el marco de la problemática de la ciberseguridad en Argentina, el tercer anexo del Decreto N° 1311/2015 muestra que la AFI tiene en su estructura funcional la Dirección Operacional de Inteligencia sobre Ciberseguridad compuesta por la Dirección de Inteligencia Informática y la Dirección de Inteligencia sobre Delitos Informáticos. La Dirección de Inteligencia Informática produce inteligencia relacionada con "[…] los riesgos y conflictos vinculados o derivados del uso de las tecnologías de información y la comunicación que afecten la defensa nacional o la seguridad interior" [12]. Por otra parte, la Dirección de Inteligencia sobre Delitos Informáticos produce "[…] inteligencia orientada al conocimiento de las actividades que pudieran configurar delitos informáticos en cualquiera de sus formas y modalidades" [13] a través de oficiales y analistas de inteligencia especializados en ciberseguridad. Dicha estructura y organigrama permite deducir que se produce inteligencia sobre ciberseguridad. Sin embargo, ¿podemos considerar esto como ciberinteligencia?

Ciberinteligencia

En este último tiempo, los ciberataques se han transformado y son considerados como sofisticados y dinámicos [14] pudiendo superar, en gran parte, las medidas de ciberdefensa y ciberseguridad desplegadas. Frente a ello, se requieren soluciones innovadoras - desde estrategias hasta la utilización de herramientas preventivas y/o defensivas - que se adapten a la naturaleza compleja de las nuevas ciberamenazas y ciberataques. Una de estas herramientas podría ser la llamada inteligencia de ciberamenazas o ciberinteligencia.

A partir de lo analizado hasta ahora, podríamos inferir que todo evento y/o incidente de ciberseguridad (obtenible mediante sensores y dispositivos de manera activa o pasiva) puede concebirse como la información a emplear dentro del ciclo de inteligencia para el análisis de ciberamenazas y la prevención de ciberataques. En efecto y debido a que la fuente es un componente de las tecnologías de la información y las comunicaciones (TIC), podríamos decir que, a través del ciclo de inteligencia, el producto final sería ciberinteligencia.

En resumidas cuentas, en el presente artículo consideraremos a la ciberinteligencia como aquel producto que se obtiene, procesa, analiza y difunde cuando la información adquirida se relaciona con eventos y/o incidentes de ciberseguridad. La ciberinteligencia, tiene como fin la toma de decisiones y contramedidas necesarias para minimizar el riesgo de ocurrencia de un ciberataque o las capacidades de un actor ya sea criminal o estatal [15]. En caso de que se materialice el riesgo, la ciberinteligencia debería presentar un escenario donde el impacto sea lo suficientemente leve como para garantizar la resiliencia y la continuidad [16] de, por ejemplo, las infraestructuras críticas de la información nacionales.

Ciberamenazas y sus efectos globales: las infraestructuras críticas argentinas

Es preciso afirmar que cualquier interrupción - parcial o total - en la prestación de un servicio esencial podría resultar en consecuencias catastróficas entre las cuales se destacan el impacto en la vida humana, la destrucción de instituciones del Estado y efectos económicos ajenos. En efecto, la estabilidad del país y la confianza del ciudadano en el Estado se verían comprometidas si ocurriera un ataque masivo y coordinado a alguno (o varios) de los sectores definidos como infraestructura crítica (IICC). Algunas fuentes de amenazas

para dichas infraestructuras son los Estados extranjeros, el crimen organizado, las organizaciones terroristas y los hacktivistas; las cuales pueden tener como objetivo el espionaje industrial, el robo de datos, el sabotaje, la indisponibilidad del servicio, la explotación de código malicioso, la divulgación ilícita de contenido y los conflictos entre naciones, entre otros.

Una amenaza es aquello de lo que una organización se defiende [17], es decir, ante la ocurrencia de un evento debe estar preparada para responder frente a la misma. Por eso, las organizaciones efectúan un análisis de riesgo (el segundo anexo de la Resolución N° 1523/2019 lo define como "un proceso que comprende la identificación de activos de información, sus vulnerabilidades y las amenazas a los que se encuentran expuestos, así como la probabilidad de ocurrencia y el impacto de las mismas, a fin de determinar los controles adecuados para tratar el riesgo") lo cual permite comprender la naturaleza del riesgo y determinar su nivel. Son las debilidades (en forma de vulnerabilidades) y las amenazas (en forma de riesgos) lo que se debe ponderar para garantizar la continuidad de cualquier organización, sabiendo que el ciberespacio es un vector que conecta de forma directa o indirecta a las IICC con el mundo.

En lo que respecta a ciberamenaza, la Resolución N° 1523/2019 la define como una "amenaza a los sistemas y servicios presentes en el ciberespacio o alcanzables a través de éste" y deben ser detectadas lo antes posible dado que el tiempo de respuesta es esencial. Para ello, es posible obtener capacidad de anticipación al conocer a los actores, sus métodos, sus capacidades y sus éxitos en escenarios similares. Un estudio [18] estipula que el tiempo medio de detección de un incidente de ciberseguridad es de 206 días y que se tarda un promedio de setenta y tres (73) días para contenerlo, a esto se le denomina "ciclo de vida de una brecha". Para reducir ese tiempo, se aplican conceptos de caza de amenazas o threat hunting, actividad asimilable a la detección de amenazas [19], donde se proponen hipótesis de ataque como iniciativa proactiva, la captura de información por medio de la telemetría y la utilización de ataques dirigidos, entre otras. En efecto, la información que se genera en los componentes de una red de elementos interconectados sobre eventos o incidentes de ciberseguridad puede ser capturado y analizado con el fin de prevenir la expansión de la incidencia y contener el efecto [20], manteniendo la resiliencia de las organizaciones consideradas como infraestructuras críticas desde la vista táctica de un sensor a nivel de endpoint que tiene un valor estratégico en el conjunto de las IICC.

A nivel global, existen antecedentes de ciberataques que han afectado infraestructuras críticas como por ejemplo el sucedido en Estonia en mayo del 2007 – considerado como el primer acto de ciberguerra. Allí, a partir de un conflicto por la reubicación de la estatua de un héroe ruso de la Segunda Guerra Mundial, Estonia sufrió varios ciberataques coordinados que afectaron los servicios financieros, policiales, de emergencia, al parlamento, ministerios y servicios de noticias [21]. Por otra parte, en el año 2010 la planta de Natanz (Irán) sufrió la afectación del sistema de centrifugadoras de enriquecimiento de uranio a raíz de una infección por parte del código malicioso conocido como stuxnet [22]. Es posible encontrar otro ejemplo de ciberataque sucedido en el año 2012, donde la empresa de oleoductos y gasoductos Saudi Aramco se vio afectada por otro código malicioso que perjudicó 30.000 puestos de trabajo. Un lustro después, en Ucrania otro código malicioso impactó en la distribución de energía eléctrica en diciembre del año 2015, lo que ocasionó que una localidad de alrededor de 1,5 millones de habitantes quedara sin luz [23]. En el año 2017 hubo una oleada de diversos códigos maliciosos del tipo ransomware cuyo fin era extorsionar a individuos y organizaciones por una suma de dinero en formato de criptodivisa para desencriptar la información residente en los discos rígidos de las víctimas [24]. Más cercano en el tiempo y durante la pandemia de covid-19, Australia sufrió una serie de ciberataques sofisticados y bajo supuesto patrocinio de un estado soberano en el mes de junio del año 2020. Acorde a lo expresado por el primer ministro de dicho país, Scott Morrison, esto afectó al gobierno, las industrias, las organizaciones políticas, la educación, la salud, los proveedores de servicios esenciales y los operadores de otras infraestructuras críticas [25].

En términos generales, estos ciberataques se caracterizan por ser sofisticados, volumétricos, de diversos orígenes (inclusive con posible apoyo y financiamiento gubernamental), con campañas que pueden durar desde días hasta años, y con un alto nivel de impacto en el funcionamiento de las IICC, que no debe eludir el ojo de las autoridades nacionales. Luis María Mozzoni afirma que la "Argentina es uno de los países con la tasa de penetración de internet más alta de la región, considerando la cantidad de recursos naturales estratégicos como petróleo, gas, agua dulce, biodiversidad o minerales estratégicos que tenemos en nuestra extensión geográfica" [26], no sería descabellado reparar en la idea de que los ciberataques podrían impactar pronto en nuestro país.

En Argentina, las IICC fueron definidas de forma genérica como "aquellas que resultan indispensables para el adecuado funcionamiento de los servicios esenciales de la sociedad, la salud, la seguridad, la defensa, el

bienestar social, la economía y el funcionamiento efectivo del Estado, cuya destrucción o perturbación, total o parcial, los afecte y/o impacte significativamente" [27] mientras que las infraestructuras críticas de información "son las tecnologías de información, operación y comunicación, así como la información asociada, que resultan vitales para el funcionamiento o la seguridad de las Infraestructuras Críticas" [28]. En ambos casos y mediante esta misma resolución, se establecieron ocho criterios de identificación de dichas infraestructuras y once sectores tales como energía, TIC, transportes, hídrico, salud, alimentación, finanzas, nuclear, químico, espacio y Estado. Entre los sectores a considerar se podrían hallar infraestructuras consideradas como críticas cuya responsabilidad sea tanto de organismos públicos como empresas privadas.

En adhesión, en julio del año 2017 se creó - a través del Decreto N° 577 - el Comité de Ciberseguridad integrado por los Ministerios de Modernización, de Defensa y de Seguridad. Dos años más tarde, a través del Decreto N° 480/2019, se amplió la composición del mismo con representantes de la Secretaría de Asuntos Estratégicos, del Ministerio de Relaciones Exteriores y Culto y del Ministerio de Justicia y Derechos a raíz del alcance global y abordaje internacional de las amenazas. La creación del Comité se basa en la necesidad de obtener la "capacidad para responder a incidentes de seguridad de gran escala, legislación en la materia, la protección de infraestructuras críticas, capacidad para colaborar con otros países, así como la cultura de seguridad desarrollada por los ciudadanos" [29]. Como principal objetivo, el Comité debía elaborar la Estrategia Nacional de Ciberseguridad y el plan de acción que permitiera su implementación en coordinación con las áreas competentes de la Administración Pública Nacional además de "fijar los lineamientos y criterios para la definición, identificación y protección de las infraestructuras críticas nacionales" [30].

La estrategia, aprobada y publicada en mayo del año 2019, es considerada como un documento fundacional y vivo, cuya actualización acompañaría la evolución de las tecnologías. Allí se definen los principios esenciales y ocho objetivos centrales del país en lo que respecta a la protección del ciberespacio sobre las cuales se espera el despliegue de acciones concretas. El octavo objetivo, hace referencia a la protección de las infraestructuras críticas nacionales de la información e incluye la promoción de la definición, identificación y protección de dichas infraestructuras, así como la articulación del sector público-privado para la construcción de capacidades de detección, resguardo y respuesta ante amenazas de ataque, el fortalecimiento de la cooperación para el intercambio de información o conocimiento que permita desarrollar una cultura común en lo que hace a la protección de las IICC y que se construya sobre la base de una confianza mutua.

PROPUESTA

En el presente artículo, se plantea la necesidad de crear el Sistema de Protección de Infraestructuras Críticas de la República Argentina (SIPICRA) integrado por todos los actores - tanto públicos como privados - que se relacionen con las infraestructuras críticas declaradas como tal y su protección. Además, se plantea la importancia de articular este Sistema con el SIN con el objetivo de incrementar la prevención y resiliencia de las infraestructuras críticas argentinas mediante la producción de ciberinteligencia.

ARGUMENTACIÓN

A favor del cumplimiento del octavo objetivo de la estrategia, los autores consideran indispensable que la Argentina identifique las infraestructuras que brindan servicios esenciales y se determine la criticidad sobre la base de un diagnóstico que permita reconocer aquellos activos de información, sistemas y redes que sean en verdad críticos. A partir de esto, se debería realizar un análisis de riesgos, diseñar una estrategia adecuada para su gestión, en conjunto con un Plan Nacional de Protección de las Infraestructuras Críticas que contenga medidas eficaces de prevención y protección contra posibles amenazas tanto en el plano de la seguridad física como en el de las TIC.

Por otra parte, con la identificación, determinación y declaración de las IICC nacionales en Argentina será necesario establecer los derechos y obligaciones de cada una de las infraestructuras - ya sea agrupada por sector, generalizada o específica - con el fin de efectuar el seguimiento y control que se requiere para la protección y defensa de las mismas. Asimismo, con base en la criticidad de cada infraestructura, se deberán desarrollar planes y programas estratégicos sectoriales y de seguridad para los operadores y capital humano que contemplen la reducción de riesgos y el incremento de la resiliencia de las mismas.

Sin duda, la amplitud del concepto de IICC y la multiplicidad de sectores afectados requiere afrontar su protección de forma integral y multidisciplinaria. Inclusive, raramente las infraestructuras críticas funcionan de forma aislada, sino que, por el contrario, suelen agruparse a raíz de su dependencia o interdependencia donde converge información y tecnología de las comunicaciones. Frente a esto, se requiere un trabajo en conjunto con

todos aquellos sectores y agentes que se relacionan para lo cual los autores consideran se debería crear, mediante un esquema multipropósito y transversal, el Sistema de Protección de Infraestructuras Críticas de la República Argentina.

Bajo este nuevo paradigma de mejora de las instituciones para cumplir con los objetivos más primordiales para una Nación, sus instituciones y su gente, los autores consideran que el SIPICRA reuniría tales instituciones y elementos del ámbito público y privado, y se debería caracterizar este esfuerzo por ser intersectorial, multinivel y creado por ley.

En principio, el Sistema de Protección de Infraestructuras Críticas de la República Argentina debiera estar integrado por los usuarios, recursos humanos, operadores, propietarios, fabricantes, instituciones de investigación, desarrollo e innovación, autoridades reguladoras de los sectores, así como órganos del ámbito público y del sector privado que tengan responsabilidades y relación con el correcto funcionamiento de los servicios esenciales que brindan dichas infraestructuras. Además, debería estar encabezado por un organismo cuya responsabilidad primaria sea supervisar el cumplimiento de las regulaciones, normas, políticas y planes de la temática; la articulación y coordinación de los integrantes de los Sistemas de Defensa Nacional, Seguridad Interior e Inteligencia Nacional (teniendo en cuenta las funciones que se relacionan con la protección de las IICC) y aquellos operadores críticos que provengan del sector público y/o privado.

A partir de la creación o determinación del organismo responsable del SIPICRA, será necesario incluir en el mismo una dirección dependiente cuya función principal sea la efectiva identificación de las infraestructuras consideradas como críticas con base en una metodología objetiva y razonable que pondere de forma cuantitativa los criterios de identificación establecidos en el marco normativo que debiera desarrollarse. Asimismo, esta dirección debería ser responsable de determinar las infraestructuras consideradas como críticas, así como gestionar y mantener actualizado de forma periódica el inventario con clasificación de seguridad “confidencial” que contenga información completa como la descripción de las infraestructuras, la forma de contactar con el personal de la misma, datos geográficos, riesgos evaluados, entre otros. Es preciso acompañar la idea de que “es esencial exponer [en el inventario] la vinculación entre servicios y activos y detallar las instalaciones y sistemas (software, hardware, comunicaciones, etc.) que los proporcionan, así como las personas involucradas en los distintos procesos” [31] para su debida protección.

Es nuestro parecer que la responsabilidad de desarrollar y coordinar el Sistema de Protección de Infraestructuras Críticas de la República Argentina recae en el gobierno nacional, debido a la importancia y relación directa con la seguridad nacional. Inclusive, la sociedad pretende que el Estado sea el responsable de velar por la seguridad y las garantías de continuidad de los servicios vitales, aun cuando las IICC se encuentren en manos de operadores y empresas privadas. Frente a esto, los autores consideran que el enfoque regulado es un puntapié positivo para implementar políticas obligatorias de protección de las infraestructuras críticas mediante legislación clara y transparente, cuya funcionalidad sea la de un instrumento que permita impulsar la cooperación de todos los sectores y articulación de los agentes que formen parte del Sistema.

Además de la identificación, determinación y los derechos y obligaciones que deriven de la declaración como infraestructura crítica, los autores consideran que el SIPICRA deberá contemplar la necesidad de coordinar el monitoreo y alerta de aquellas infraestructuras a proteger. La importancia de esto se relaciona con la posibilidad de tomar medidas destinadas a prevenir y/o anticipar emergencias mediante alertas tempranas. Inclusive, el monitoreo permanente permite la generación de información clave para el desarrollo de estrategias de prevención y protocolos de acciones frente a vulnerabilidades, ataques y amenazas cibernéticas que pudieran afectar los servicios esenciales para la sociedad. Esta información puede obtenerse de fuentes internas (como por ejemplo de un firewall, registros de router y señuelos -honeypots y honeynets- de las infraestructuras críticas) o externas (por ejemplo, bases de datos de vulnerabilidades, foros, redes sociales o información de la dark web entre otros). Teniendo en cuenta el contexto argentino, los autores consideran que el Estado debería incorporar al Sistema a aquellos organismos existentes que acceden en la actualidad a esta información (como los equipos de respuesta a incidentes y centros de operaciones de seguridad), con el fin de orquestar y vincular la información que se genera, así como impulsar el incremento de sistemas de monitoreo a nivel nacional e internacional.

En paralelo a esto, a razón de que “la colección de información no se traduce automáticamente en mejores resultados en el proceso de toma de decisiones” [32] y a favor de la articulación entre sistemas, esa información podría ser compartida con el Sistema de Inteligencia Nacional. con el objetivo de, en el marco del cumplimiento del ciclo de inteligencia, elevar ciberinteligencia oportuna y pertinente como producto final y producir una herramienta decisional para anticipar y prevenir cualquier afectación parcial o total de las infraestructuras que

brindan servicios esenciales. Como dice Nikolaos Tsouroulas, "....conocer y comprender a nuestros adversarios es crucial si queremos anticipar y detectar nuevos ataques que se escapan de nuestras soluciones defensivas. En este punto entra en juego la inteligencia de amenazas que nos proporciona la información necesaria …"[33].

Es innegable que, en pos de la prevención y protección de las IICC, la recolección, análisis, integración y evaluación de la información suministrada por los organismos del sector público y privado, así como las fuerzas de seguridad y policiales, y las fuerzas armadas (además de aquellos sectores considerados como estratégicos) podría ser una ventaja considerable frente a cualquier ciberamenaza o ciberataque. A partir de ello, todos los organismos pertenecientes al Sistema de Inteligencia Nacional - dado el *expertise* de los recursos humanos, la experiencia y procesos internos - debieran en estrecha colaboración efectuar la evaluación de amenazas y el análisis de los riesgos sobre las infraestructuras críticas. Esto permitiría diseñar y presentar la información (ya considerada como inteligencia), mediante el empleo de los mecanismos de comunicaciones adecuados y seguros, al responsable del Sistema de Protección de Infraestructuras Críticas de la República Argentina con el objetivo de proporcionar una alerta temprana y disminuir (o evitar) la probabilidad de ocurrencia de una catástrofe.

Existen diversas metodologías de análisis de riesgos (para la gestión de riesgos) y modelado de amenazas (para el desarrollo seguro de software seguro) que se basan en la inteligencia de amenazas para proponer posibles escenarios, actores, actividades y modalidades (formas de explotación de vulnerabilidades), lo que puede ser parte del proceso de producción de ciberinteligencia destinado al organismo responsable del SIPICRA.

En efecto, los autores consideran que el intercambio de información es uno de los elementos de mayor importancia en lo que hace a la protección de las infraestructuras críticas, lo cual no escapa a la necesidad de generar confianza entre los sistemas que integrarían el Sistema de Protección de las Infraestructuras Críticas de la República Argentina, como el SIN. Este intercambio proporciona una mejor comprensión de las ciberamenazas, los riesgos, las dependencias y los efectos previsibles, para lo cual es primordial que sea ágil y bidireccional, con el fin de incrementar la probabilidad de diseñar e implementar las contramedidas apropiadas y prevenir ataques que pudieran afectar parcial o totalmente las IICC. Algunos de los beneficios de dicho intercambio son: crea conciencia sobre la necesidad de proteger a las IICC (en especial relacionado con la gestión de la continuidad del negocio y la gestión de riesgos); mejora el nivel de educación, formación y capacitación, y conocimiento sobre el tema; a medida que se comparte información, se incrementan las habilidades de los operadores e integrantes del sistema e, inclusive, el organismo responsable puede dirigirse a toda o parte del Sistema con información específica con una adecuada clasificación de seguridad que permite prevenir cualquier perturbación de las IICC. La inteligencia a compartir podrá ser considerada de carácter estratégico, operativo y/o táctico, y se podría dar en el marco de vulnerabilidades y amenazas permitiendo la promoción de los esfuerzos coordinados dentro de las redes industriales a favor del fortalecimiento y resguardo de los servicios críticos y productivos.

CONCLUSIONES

La existencia de diversas ciberamenazas, sumado a los antecedentes internacionales de ciberataques contra las infraestructuras críticas, demuestra que las organizaciones y organismos en el mundo no han podido coordinar sus mecanismos de ciberdefensa y ciberseguridad a favor de la protección de las mismas y de la sociedad en general. Lamentablemente, la República Argentina no es la excepción.

Nuestro país cuenta con una serie de sistemas, entendidos como el conjunto de organismos públicos que trabajan de manera coordinada y cooperativa con el fin de resguardar los valores de la república, la soberanía, los derechos y garantías, y el sistema democrático establecido por la Constitución Nacional, a la par de resguardar a la sociedad en su conjunto. Sin embargo, todos los sistemas actuales que poseen algún nivel de incidencia sobre las infraestructuras críticas u objetivos estratégicos nacionales dentro de sus alcances y objetivos, no se encuentran coordinados en pos de su protección.

Frente a esta organización existente, los autores consideran que crear el Sistema de Protección de Infraestructuras Críticas de la República Argentina permitirá coordinar todos los sistemas ya existentes en pos de la protección de la sociedad y los servicios que son esenciales mediante el empleo de un esquema innovador y multisectorial, cuya articulación requerirá de esfuerzos conjuntos para garantizar un entendimiento común y un objetivo claro, con efecto excipiente. Asimismo, podrá considerar a la ciberseguridad y la ciberdefensa como pilares de la protección de las IICC y los servicios esenciales, así como a la ciberinteligencia como herramienta imprescindible para decidir qué camino deberá tomar la Argentina en virtud de escenarios futuros y prospectiva.

En efecto, el SIPICRA - mediante un trabajo mancomunado con el Sistema de Inteligencia Nacional - no solo significa más capacidades para la identificación, detección y mitigación de ciberamenazas y ciberataques mediante la producción de ciberinteligencia, sino también que todos los actores tengan un lenguaje común para entender el fenómeno y aplicar las técnicas necesarias con el fin de gestionar las contramedidas que garanticen la resiliencia de las infraestructuras críticas de la Nación y en última instancia, los valores democráticos de la sociedad.

Referencias

[1] Real Academia Española: Diccionario de la lengua española, 23ª edición. España, 2019. Recuperado de: https://dle.rae.es/sistema

[2] M. Herrera Gómez, A. M. J. Castillo, "Generación y transformación de las instituciones sociales: los procesos morfoestáticos y los procesos morfogenéticos". España, 2004. Revista Española de Investigaciones Sociológicas (REIS), n° 107, pág. 49-88.

[3] Infoleg, Ley n° 25.520, artículo 2°, inciso 5°. República Argentina, 2001. Recuperado de: http://servicios.infoleg.gob.ar/infolegInternet/anexos/70000-74999/70496/norma.htm

[4] Infoleg, Ley n° 24.059, artículo 6°. República Argentina, 1992. Recuperado de: http://servicios.infoleg.gob.ar/infolegInternet/anexos/0-4999/458/texact.htm

[5] Infoleg, Ley n° 23.554, artículo 7°. República Argentina, 1988. Recuperado de: http://servicios.infoleg.gob.ar/infolegInternet/anexos/20000-24999/20988/texact.htm

[6] Infoleg, Decreto N° 1311, Anexo 1, Folio 12. República Argentina, 2015. Recuperado de: http://servicios.infoleg.gob.ar/infolegInternet/anexos/245000-249999/248914/norma.htm

[7] Centro Nacional de Inteligencia, "El Ciclo de Inteligencia". Recuperado de https://www.cni.es/es/queescni/ciclo/

[8] L. Martinez Viqueira, "El Ciclo de Inteligencia Complejo: una ágil herramienta para operar en red", Instituto Español de Estudios Estratégicos. España, 2016. Recuperado de http://www.ieee.es/Galerias/fichero/docs_opinion/2016/DIEEEO50-2016_CicloInteligComplejo_MartinezViqueira.pdf

[9] J. M. Díaz, C. Greciano, "ANÁLISIS CRÍTICO DEL CICLO DE INTELIGENCIA" en Inteligencia y Liderazgo - Liderando inteligencia. 2017. Recuperado de https://inteligenciayliderazgo.com/wp-content/uploads/2017/11/analisis-ciclo-inteligencia.pdf

[10] J. Jordan, "Una revisión del ciclo de inteligencia", Defensa.com. España, 2016. Recuperado de https://www.defensa.com/analisis-gesi/revision-ciclo-inteligencia

[11] M. Kamiński, "Intelligence Sources in the Process of Collection of Information by the U.S. Intelligence Community". 2019. Recuperado de https://www.researchgate.net/publication/340647256_Intelligence_Sources_in_the_Process_of_Collection_of_Information_by_the_US_Intelligence_Community

[12] Infoleg, Decreto N° 1311, Anexo 1, Folio 66. República Argentina, 2015. Recuperado de: http://servicios.infoleg.gob.ar/infolegInternet/anexos/245000-249999/248914/norma.htm

[13] Infoleg, Decreto N° 1311, Anexo 1, Folio 67. República Argentina, 2015. Recuperado de: http://servicios.infoleg.gob.ar/infolegInternet/anexos/245000-249999/248914/norma.htm

[14] W. Tounsi, H. Rais, "A survey on technical threat intelligence in the age of sophisticated cyber attacks", Elsevier. Francia, 2017. Recuperado de https://www.researchgate.net/profile/Wiem_Tounsi/publication/320027747_A_survey_on_technical_threat_intelligence_in_the_age_of_sophisticated_cyber_attacks/links/59fc7cb70f7e9b9968bd9e02/A-survey-on-technical-threat-intelligence-in-the-age-of-sophisticated-cyber-attacks.pdf

[15] Ernst & Young, "Cyber threat intelligence − how to get ahead of cybercrime". 2014. Recuperado de https://www.ey.com/Publication/vwLUAssets/EY-cyber-threat-intelligence-how-to-get-ahead-of-cybercrime/$FILE/EY-cyber-threat-intelligence-how-to-get-ahead-of-cybercrime.pdf

[16] Bank of England, "CBEST Intelligence-Led Testing. Understanding Cyber Threat Intelligence Operations. Version 2.0". Inglaterra, 2016. Recuperado de https://www.bankofengland.co.uk/-/media/boe/files/financial-stability/financial-sector-continuity/understanding-cyber-threat-intelligence-operations.pdf

[17] Threat Modeler, "Differences Explained: Threat vs. Vulnerability vs. Risk". 2019. Recuperado de https://threatmodeler.com/differences-explained-threat-vs-vulnerability-vs-risk/

[18] IBM Security, "Cost of a Data Breach Report". 2019. Recuperado de https://www.all-about-security.de/fileadmin/micropages/Fachartikel_28/2019_Cost_of_a_Data_Breach_Report_final.pdf

[19] Tarlogic, "Threat Hunting, Mejora la eficiencia de detección y respuesta ante ciber amenazas". Recuperado de https://www.tarlogic.com/blackarrow-servicios-seguridad-ofensiva/threat-hunting/

[20] N. Tsouroulas, "Detección y respuesta basadas en Ciberinteligencia. Parte 1: los pilares básicos", Telefónica. 2018. Recuperado de https://empresas.blogthinkbig.com/deteccion-respuesta-ciberinteligencia/

[21] R. Ottis, “Analysis of the 2007 Cyber Attacks Against Estonia from the Information Warfare Perspective”, Cooperative Cyber Defence Centre of Excellence. Estonia, 2008. Recuperado de https://ccdcoe.org/uploads/2018/10/Ottis2008_AnalysisOf2007FromTheInformationWarfarePerspective.pdf
[22] G. Romero Sanchez, “STUXNET: La primera ciberarma de la historia”, Cronicaseguridad.com. 2018. Recuperado de https://cronicaseguridad.com/2018/05/16/stuxnet-primera-ciberarma-historia/
[23] INCIBE-CERT, “BlackEnergy y los sistemas críticos”. España, 2016. Recuperado de https://www.incibe-cert.es/blog/blackenergy-sistemas-criticos
[24] Redes Zone, “Estos han sido los 5 ataques de ransomware más importantes de 2017”. Recuperado de https://www.redeszone.net/2017/12/16/estos-los-5-ataques-ransomware-mas-importantes-2017/
[25] BBC News, “Australia cyber attacks: PM Morrison warns of 'sophisticated' state hack”. 2020. Recuperado de https://www.bbc.com/news/world-australia-46096768
[26] L.M. Mozzoni. “Ciberguerra, el ataque a infraestructuras críticas como política internacional y porque Argentina tiene que trabajar en este aspecto”. Universidad Blas Pascal, 2019. Recuperado de: http://www.vectus.com.ar/wp-content/uploads/2019/06/Trabajo-Final-API-UBP-Luis-Maria-Mozzoni.pdf
[27] Boletín Oficial, Resolución N° 1523/2019, anexo I. República Argentina, 2019. Recuperado de: https://www.boletinoficial.gob.ar/detalleAviso/primera/216860/20190918
[28] Boletín Oficial, Resolución N° 1523/2019, Anexo I. República Argentina, 2019. Recuperado de: https://www.boletinoficial.gob.ar/detalleAviso/primera/216860/20190918
[29] Infoleg, Decreto N° 577. República Argentina, 2017. Recuperado de: http://servicios.infoleg.gob.ar/infolegInternet/anexos/275000-279999/277518/norma.htm].
[30] Infoleg, Decreto N° 577, Art. 2°, inc. e. República Argentina, 2017. Recuperado de: http://servicios.infoleg.gob.ar/infolegInternet/anexos/275000-279999/277518/norma.htm
[31] M. Calvo Matalobos, “Ad-HOC Incibe - Protección de Infraestructuras Críticas”. España, 2018. Recuperado de: http://openaccess.uoc.edu/webapps/o2/bitstream/10609/81225/6/mcmTFM0618memoria.pdf
[32] C. Gomes de Assis, “La nueva era de la información como poder y el campo de la ciberinteligencia”, URVIO – Revista Latinoamericana de Estudios de Seguridad Numéro 19. Ecuador, 2016. Pg- 94-109.
[33] N. Tsouroulas, “Detección y respuesta basadas en Ciberinteligencia. Parte 1: los pilares básicos”, Telefónica. 2018. Recuperado de https://empresas.blogthinkbig.com/deteccion-respuesta-ciberinteligencia/

Fuente de la Imagen:
http://elite-formacion.blogspot.com/2018/07/el-sistema-nacional-de-proteccion-de.html

Agostina Taverna
(Argentina) Universidad Tecnológica Nacional. Facultad Regional Buenos Aires. Especialización Profesional en Terrorismo y Ciberseguridad.

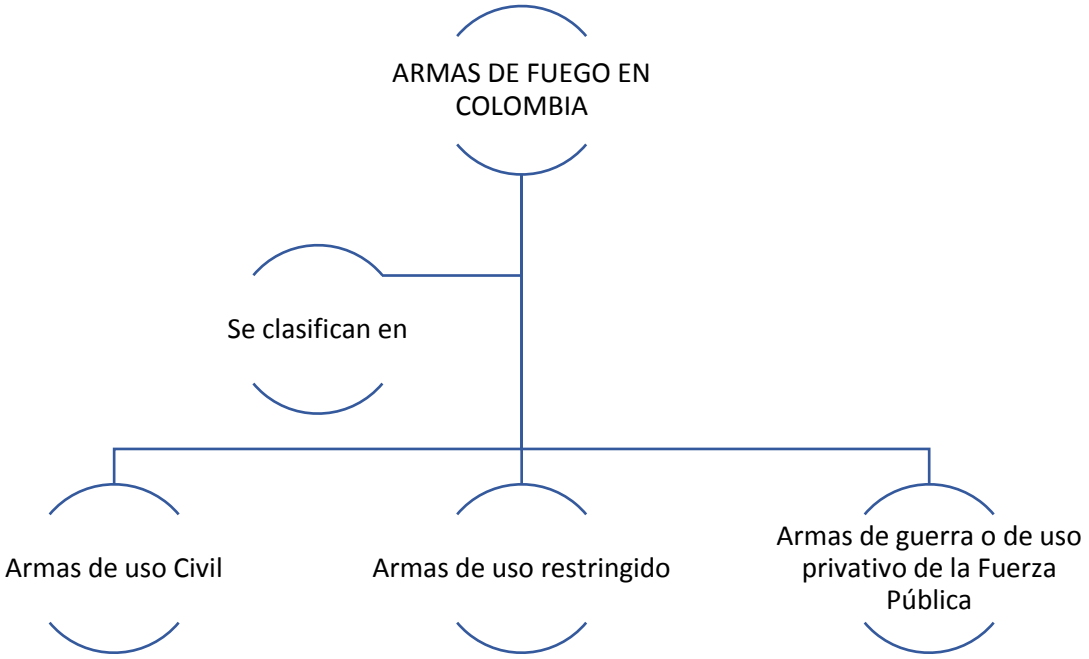
Rodrigo Cárdenas Holik
(Argentina) Universidad Tecnológica Nacional. Facultad Regional Buenos Aires. Especialización Profesional en Terrorismo y Ciberseguridad.

Porte o tenencia de réplicas de armas frente a la legislación colombiana

Por Julián David Urrego Atehortua (Colombia)

Lo primero que debemos tener claro en el momento de abordar este tema, es que en Colombia existe un monopolio frente a la fabricación y comercialización de las armas de fuego que se encuentran en nuestro territorio nacional, por lo cual solo será el estado quién autorice su porte y tenencia.

Ahora bien, conforme al Decreto 2535 de 1993, de la Presidencia de la República, en su artículo sexto y siguientes, las armas se clasifican en:



Teniendo en cuenta lo anterior, analizaremos solo lo correspondiente a las armas de uso civil, encontrando que las mismas conforme al decreto anteriormente citado se clasifican en:

Todas las anteriores requieren autorización por parte del Gobierno Colombiano para su tenencia y porte.

En este artículo nos concentraremos en las armas para **uso deportivo**, las cuales son definidas en el artículo 12 del decreto anteriormente citado, así:

Artículo 12º.- *Armas deportivas. Son las armas de fuego que cumplen con las especificaciones necesarias para practicar las modalidades de tiro aceptadas por la Federación Internacional de Tiro y las usuales para la práctica del deporte de la cacería.*

Y sobre las cuales, el decreto 2535/93 es enfático al señalar:

Artículo 16 *(…) Las armas deportivas solamente serán utilizadas en actividades de tiro y caza, con las limitaciones establecidas en la Ley y el reglamento, en particular las normas de protección y conservación de los recursos naturales.*

Así pues; en primera instancia, será importante concluir que para la tenencia y porte de un arma deportiva será estrictamente necesaria nuestra afiliación a un club deportivo reconocido por la federación colombiana de tiro y caza, así como el respectivo permiso gubernamental para su porte y tenencia.

DE LAS ARMAS -RÉPLICAS-

Veamos algunas excepciones:

Decreto 2535/93

Artículo 25º.- *Excepciones. No requieran permiso para porte o para tenencia, las armas neumáticas, de gas y las armas largas de pólvora negra, incluso las escopetas de fisto.*

En este orden de ideas, la comercialización, compra, porte y tenencia de esta última clase de armas es legal, pero su porte tiene unas restricciones que podemos encontrar en la ley 1801 de 2016, articulo 27, numerales 6 y 7, que consagran la prohibición del mismo en determinados escenarios, por entenderlo como un comportamiento que pone en riesgo la vida e integridad de las personas y como tal, dejando claro que es una conducta contraria a la convivencia, veamos:

Código Nacional de Policía.

6. Portar armas, elementos cortantes, punzantes o semejantes, o sustancias peligrosas en áreas comunes o lugares abiertos al público. Se exceptúa a quién demuestre que tales elementos o sustancias constituyen una herramienta de su actividad deportiva, oficio, profesión o estudio.

7. Portar armas neumáticas, de aire, de fogueo, de letalidad reducida o sprays, rociadores, aspersores o aerosoles de pimienta o cualquier elemento que se asimile a armas de fuego, en lugares abiertos al público donde se desarrollen aglomeraciones de personas o en aquellos donde se consuman bebidas embriagantes, o se advierta su utilización irregular, o se incurra en un comportamiento contrario a la convivencia.

De esta manera el porte de armas o réplicas, en los espacios anteriormente mencionados, daría motivo para que la Policía Nacional incautara la misma y procediera con la imposición de una multa general tipo 2, que para este año 2020 es de DOSCIENTOS TREINTA Y CUATRO MIL PESOS CON OCHENTA CENTAVOS M/L ($234.080) aparte de que se prohibiría el ingreso a actividad que involucre aglomeraciones de público complejas o no complejas y finalmente se destruiría el bien.

Precisamente esta última parte, la destrucción del bien, es la que interesa a tantos portadores de réplicas de armas, pues como ya hemos visto, en el artículo 6 ya mencionado, existe una excepción frente al porte, que señala: ***Se exceptúa a quién demuestre que tales elementos o sustancias constituyen una herramienta de su actividad deportiva, oficio, profesión o estudio.***

Situación que tendrá que demostrarse con elementos probatorios orientados a la exoneración, en la Inspección de Policía correspondiente al municipio de incautación del arma, dentro de los tres días siguientes a la imposición del comparendo e incautación del arma, conforme el parágrafo 1 del artículo 222 de la ley 1801 de 2016 que consagra el Proceso Verbal inmediato de los comparendos de Policía.

A este respecto me resulta importante nuevamente señalar, como ya lo habíamos concluido, que el uso de armas -réplicas- para actividades deportivas no será válido tal y como lo manifiesta expresamente FEDETIRO:

Informamos que las actividades deportivas que se desarrollan bajo supervision de la Federacion Colombiana de Tiro y Caza Deportiva,no incluyen ninguna modalidad en las que se utilicen armas traumaticas, armas de fogueo o armas de airsoft. si requiere informacion de nuestras actividades, puede comunicarse con nosotros.

ARMAS TRAUMÁTICAS

Actualmente existe un vacío legal frente a las armas traumáticas, pues estas aún no han sido reconocidas en la clasificación de deportivas por parte del Estado Colombiano y tampoco, debido a sus mecanismos internos, las podemos catalogar como neumáticas, de gas o pólvora negra; razón por la cual no entrarían en las excepciones de permiso del decreto que venimos desarrollando:

Decreto 2535 de 1993

Art. 25 Excepciones. No requieran permiso para porte o para tenencia, las armas neumáticas, de gas y las armas largas de pólvora negra, incluso las escopetas de fisto.

En este orden de ideas, no existe legislación en Colombia que regule la comercialización (hasta ahora legal) el porte y la tenencia de estas armas.

Sin embargo, con el fin de aportar al debate frente al tema, es importante señalar que, si analizamos el arma traumática, por el impacto y daño que sus proyectiles pueden tener en el ser humano, estamos claros que nos encontramos frente a un arma de letalidad reducida, tanto así que, en algunos países, estas son utilizadas como de defensa personal y en otros, su uso es prohibido.

DOS PUNTOS DE VISTA FRENTE A LAS ARMAS TRAUMÁTICAS

PERSPECTIVA DE LA AUTORIDAD POLICIAL

El análisis entonces, que una autoridad policial puede realizar frente a la incautación de estas armas, tendría un piso jurídico, que sería justamente el artículo 27, numeral 7 de la ley 1801 de 2016 cuando señala: las armas de letalidad reducida.

PERSPECTIVA DEL CIUDADANO PROPIETARIO DEL ARMA

Por otro parte, el ciudadano podría hacer uso de la máxima del derecho que señala: todo aquello que no esté prohibido está permitido, ya que al no existir una clasificación del arma traumática a la luz del decreto 2535 de 1993, no sería claro el marco jurídico aplicable a su destrucción, razón por la cual su fundamento de defensa en instancia de la Inspección de Policía, sería la solicitud de exoneración con el fin de solicitar la devolución de la misma.

De no tenerse clara esta defensa, el arma podría ser destruida, conforme al marco legal de la ley 1801 de 2016, ya citado.

Estas dos perspectivas nos permiten hacer una segunda conclusión de que el arma traumática podrá ser incautada, más no se podrá destruir la misma por parte de las inspecciones cuando se adelante la defensa jurídica ya señalada.

¿ES RECOMENDABLE MODIFICAR EL CAÑÓN DE UN ARMA DE FOGUEO PARA VOLVERLA TRAUMÁTICA?

Una práctica común de algunos propietarios de armas de fogueo es la modificación del cañón para que puedan ser utilizadas con los proyectiles de las traumáticas, esta acción altera las características de fábrica del arma de fogueo, convirtiéndola en un arma hechiza, que está totalmente prohibida, salvo las escopetas de fisto.

Es decir, que su porte y tenencia no solo estaría prohibido, sino que podría ser objeto de sanción penal, conforme al Art 365 del código penal colombiano.

ARTÍCULO 365. FABRICACIÓN, TRÁFICO, PORTE O TENENCIA DE ARMAS DE FUEGO, ACCESORIOS, PARTES O MUNICIONES. El que sin permiso de autoridad competente importe, trafique, fabrique, transporte, almacene, distribuya, venda, suministre, repare, porte o tenga en un lugar armas de fuego de defensa personal, sus partes esenciales, accesorios esenciales o municiones, incurrirá en prisión de nueve (9) a doce (12) años.

En la misma pena incurrirá cuando se trate de armas de fuego de fabricación hechiza o artesanal, salvo las escopetas de fisto en zonas rurales.

-Negrilla y subraya fuera de contexto original-.

DEL TRANSPORTE DE ARMAS RÉPLICAS

Como recomendación final, es importante que el porte y transporte de armas réplicas se dé en las cajas originales en las que son vendidas, no en fundas o chapuzas, ni en la pretina, pues de hacerlo bajo estas últimas modalidades citadas, será muy factible que sean objeto de incautación por parte de la Policía Nacional, bajo el entendido de que es un comportamiento que pone en riesgo la vida y la integridad de las personas y, en caso de ser vencido en el proceso administrativo ante una inspección de policía, la misma podrá ser objeto de destrucción.

OTRAS CONCLUSIONES

Damos por terminado el presente escrito, resaltando que hasta el momento hemos citado dos conclusiones importantes, pero del texto necesariamente se desprenderán, además, las siguientes:

- La comercialización, porte y tenencia de armas traumáticas es legal.
- Un arma traumática puede ser catalogada como de letalidad reducida, por lo cual le aplica el procedimiento de incautación del articulo 27 numeral 7 de la ley 1801 de 2016.
- El porte o tenencia de armas deportivas solo será válido si se acredita afiliación a un club de tiro y caza que a su vez esté afiliado a la federación colombiana de tiro y caza.

- La tenencia de armas -réplicas- ya sean neumáticas, de aire, de fogueo o de letalidad reducida, aplica para el ámbito de la propiedad privada y no para el espacio público.
- En el porte o transporte de las armas -réplicas- ya sean neumáticas, de aire, de fogueo o de letalidad reducida, no será válida la argumentación de que la misma se da con fines deportivos.
- El carnet que viene con las armas réplicas y que en su descripción solo transcribe la legislación colombiana de la ley 1801 de 2016 y del decreto 2535 de 1993 no tiene ninguna validez como elemento de prueba.
- El carnet de miembro de un club deportivo, solo será válido como elemento probatorio si dicho club está avalado por la Federación Colombiana de Tiro.

Referencias

http://www.cortesuprema.gov.co/corte/index.php/2020/04/30/corte-suprema-fija-limites-sobre-armas-de-fuego/
http://www.cortesuprema.gov.co/corte/wp-content/uploads/2020/04/SP911-2020.pdf
https://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=1540
http://www.fedetirocol.com/index.php/noticias/53-informacion-importante
https://www.youtube.com/watch?v=8usf9KelDXg&t=539s
https://www.youtube.com/watch?v=4_hMbrmwziE

Julián David Urrego Atehortua
(Colombia) Abogado.

Otra vez el Cáucaso

Por Guadi Calvo (Argentina)

Una vez más la candente frontera entre Armenia y Azerbaiyán ha vuelto a ser noticia, y pone en tensión al mundo, por la cantidad de interés y naciones involucradas de un lado y otro de la línea divisoria, lo que podría arrastrar a toda la región a una guerra de proporciones históricas.

Entre el 12 y el 16 de julio último, se produjeron acciones militares que han dejado según datos oficiales 17 muertos, cinco efectivos armenios y 12 azeríes, en el sector de Tavush -Tovuz, próxima a Karabaj, donde desde 1991 a 1994 se libró una guerra que dejó cerca de 30 mil muertos y un millón de desplazados. Los hechos se han producido a unos trecientos kilómetros de Nagorno-Karabakh, el campo de batalla habitual de estos enfrentamientos, que hoy se encuentra bajo el nombre de la República de Artsaj, un estado sin reconocimiento internacional.

Durante los choques de julio, que se habrían iniciado por la intromisión de efectivos azerbaiyanos en territorio armenio, según informó su Ministerio de Defensa, los azeríes habrían perdido una gran cantidad de insumos, entre ellos drones que habrían sido derribados durante las operaciones, los que fueron exhibidos en Ereván.

Para agregar más dramatismo a la crítica situación, Ankara, disparó una declaración en la que dice: “Turquía apoyará cualquier decisión que tome el fraternal pueblo azerbaiyano en su justa lucha”. Al tiempo que el ministro de defensa turco, Hulusi Akar, declaró que: “Turquía y su ejército están listos para apoyar completamente a Azerbaiyán”. Lo que fue considerado como una amenaza directa por parte de Armenia.

Cuando la situación parecía volver a la “tensa normalidad” que impera en la frontera desde los acuerdos de paz de 1994, firmados en Biskek, la capital de Kirguistán, con los auspicios rusos, el pasado 27 de julio a primeras horas de la madrugada el militar armenio Ashot Mikaelián, murió producto del disparo de un francotirador azerí, lo que incremento la tensión todavía más y podría echar por tierra los esfuerzos de estructuras regionales como la *Organización del Tratado de Seguridad Colectiva* o CSTO, compuesto por Armenia, Bielorrusia, Kazajstán, Kirguistán, Rusia y Tayikistán, por alcanzar un punto de estabilidad.

Estos choques fronterizos, no son los primeros en producirse desde 1994, en ese mismo sector durante 2014 y 2015, se produjeron enfrentamientos importantes, pero en 2016 estalló lo que se conoció como “la guerra de los cuatro días”, quizás los choques de mayor gravedad, en la que murieron unos 300 militares de ambos bandos y otros tantos resultaron heridos.

Este foco de inestabilidad pone a ese pequeño sector geográfico en la centralidad de la atención internacional, ya que jugadores de peso mundial tienen intereses económicos, políticos, militares y religiosos en las dos naciones en conflicto. Como es el caso de

Turquía, que articula con Azerbaiyán su presencia en las costas del Mar Caspio y donde cuenta con una base militar.

La nación azerí, la única en el mundo que comparte fronteras con la Federación de Rusia y la República Islámica de Irán, es de mayoría *musulmana*, con casi el 96 por ciento de los 10 millones de habitantes, y aunque de esa mayoría, un 85 por ciento es de creencia *chií*, lo que coloca a Teherán en esa contienda ya que la vasta comunidad *chiita*, tiene muy buena sintonía con sus vecinos del sur, la dirigencia política ha construido una fuerte alianza con Turquía, que más allá de las razones históricas, étnicas y religiosas, los une la siempre espinosa relación con Armenia, de mayoría cristiana, que nunca ha olvidado los padecimientos que ha sufrido a mano de los *otomanos*, cuya máxima expresión se tradujo en el genocidio que se extendió desde 1915 a 1917, en que más de un millón y medio de armenios fueron asesinados por las tropas turcas, hecho que hasta la actualidad Ankara se niega a reconocer como tal.

Por su parte Azerbaiyán, tiene un pleito de siglos con Armenia, por Nagorno Karabaj (o Alto Karabaj o Karabaj Montañoso), un territorio de mayoría armenia, que ambas naciones reclamaban para sí y que a pesar que durante la era soviética ese conflicto estuvo invernado, apenas ambas naciones se proclamaron repúblicas independientes en 1991, tras la desaparición de la Unión Soviética, emergió con más fuerza lo que arrastró a las dos naciones del Cáucaso sur a constantes enfrentamientos diplomáticos y bélicos.

Más allá de la conformación *musulmana* de Azerbaiyán, importante productor de petróleo y gas, tiene substanciales relaciones con los Estados Unidos e Israel, al tiempo que su dirigencia, si bien nunca se ha acercado a Irán, mantiene una relación equilibrada con Teherán, lo que no le impidió convertirse en un enclave *sionista*. En 2016, el presidente, Ilham Aliyev, compró insumos militares a Israel por unos 5 mil millones de dólares, incluidos drones, misiles y barcos. Azerbaiyán se convirtió en el tercer mercado más importante para las exportaciones militares *judías*, mientras que Tel-Aviv es el segundo cliente para el petróleo azerí. En octubre de 2018, su Ministro de Defensa visitó Tel-Aviv, para fortalecer los “lazos militares”, lo que se tradujo en la construcción de instalaciones militares entre ellas un centro subterráneo de comando y control para la inteligencia azerí, en la capital azerbaiyana. Además de que Israel, utiliza es territorio para espiar las instalaciones nucleares iraníes utilizando drones que despegan desde bases locales.

El cada vez más difícil equilibrio que mantiene Bakú, en su relación con Ankara, Washington, Tel-Aviv y Teherán, podría desbaratarse a medida que la tensión aumenta entre estos países, lo que podría dejar a Azerbaiyán en medio de un conflicto que sobrepasaría, en mucho, sus propios intereses.

Por otra parte, Armenia, aliada con Irán y Rusia, es clave para Moscú, ya que, desde Azerbaiyán, los Estados Unidos pretenden, comercializar hacia Europa utilizando el oleoducto Bakú-Tbilisi-Ceyhan, el petróleo azerí, con el fin de que los países de la *Unión Europea* dejen de proveerse de petróleo ruso.

Un vecindario convulso

El Cáucaso sur, se ha convertido en una de las regiones más tensas del mundo, en este momento tanto o más que la frontera Pakistán-India en Cachemira. Ya que juegan demasiados elementos que pueden agravar la situación de un momento a otro. Dado los acuerdos militares entre Azerbaiyán e Israel, si estos últimos decidieran atacar Irán, sus aviones podrían repostar en territorio azerí, en lugar de tener hacerlo en el aire y regresar a Israel. Según se conoció en notas reveladas por el *Departamento de Estado* de los Estados Unidos, el presidente Aliyev respecto a sus relaciones con Israel, las comparó con un iceberg: “nueve décimas partes están debajo de la superficie”.

Además de que si Azerbaiyán, fuera atacado por alguna otra potencia, Turquía se vería obligada a participar en su defensa, ya que es un punto estratégico de la política expansionista hacia el interior del *islam*, planteada por el presidente Recep Tayyip Erdogan, quien en esa misma dirección acaba de engarzar una de sus más exquisitas perlas la *Hagia Sophia*, de Estambul, a quien después de más de ochenta años ha vuelto a reconvertirla en *mezquita*. (Ver: Turquía: El sultán en la catedral). La cuestión del Cáucaso sur también agrega un nuevo foco de controversia entre Ankara y Moscú, quienes ya se miran fijo a la cara en Siria y Libia.

Por su parte las relaciones Teherán-Bakú, están empapadas de desconfianza ya que Irán, durante la última década del siglo XX, no solo reclamó con fuerza algunas cuestiones fronterizas, sino que alentó a la mayoría *chiita*, que derroquen al gobierno civil, para adoptar un modelo político similar al suyo. Pasados veinte años de aquello, las heridas en la casta política azerí siguen abiertas.

En los últimos dos años, Estados Unidos, ha otorgado a Bakú ayuda militar para aumentar sus defensas marítimas. En “coincidencia “con las importantes inversiones que el actual presidente norteamericano en su rol de empresario viene haciendo desde hace más de diez años en ese país.

Por su parte Rusia al igual que en Siria, también cuenta una base militar en Armenia, país netamente hostil a Turquía, con quien no cuentan con relaciones oficiales a partir del genocidio, por lo que Ereván, tiene explícitos vínculos con el *Partido de los Trabajadores del Kurdistán* (PKK), que viene llevando una larga y sangrienta guerra contra Turquía desde 1978, en procura de la instauración de un estado kurdo.

Turquía, en el marco de las maniobras militares con Azerbaiyán, que comenzaron el pasado miércoles 29, envió aviones de combate *F-16* de fabricación estadounidense al país del Caspio, en el que también participaron helicópteros, estás maniobras

están programadas para que se repitan durante el mes de agosto. Ya que como lo declaró Erdogan. "Turquía no mostrará vacilaciones para oponerse a cualquier ataque hacia Azerbaiyán".

La cuestión en la región vuelve a ser imprevisible poniendo otra vez al Cáucaso en pie de guerra.

Fuente de la Imagen:
https://www.elpais.cr/2020/07/14/azerbaiyan-afirma-haber-destruido-una-instalacion-militar-y-maquinaria-belica-de-armenia/
Modificada por TRIARIUS

Guadi Calvo
(Argentina) escritor y periodista argentino. Analista Internacional especializado en África, Medio Oriente y Asia Central.

Aeronaves Remotamente Tripuladas Scan Eagle / Nigh Eagle en las Fuerzas Militares de Colombia

Por Douglas Hernández (Colombia)

Aeronave Remotamente Tripulada Night Eagle en F-Air Colombia 2019. Foto de www.fuerzasmilitares.org

Fue en el año 2006, cuando la Fuerza Aérea Colombiana recibió los primeros Scan Eagle, a través de la empresa estadounidense INSITU. Este programa se realizó en coordinación con el US Southern Command, que facilitó el entrenamiento de los primeros operadores de la FAC. La aeronave mide un metro de largo por tres metros de envergadura, y tiene un peso de 19 kilos. Este tamaño compacto y bajo peso, facilita su transporte en toda clase de vehículo o aeronave, y su manipulación por un pequeño grupo de hombres. Su costo se justifica plenamente con los beneficios obtenidos con su operación. Con ellos hay una importante economía de combustible, pueden volar hasta 18 horas continuas, alcanzar grandes alturas, y tomar fotografías y video de muy alta calidad.

Un equipo ART Scan Eagle de la FAC está integrado por un Comandante de Misión, un Operador, un Analista de Imágenes, y dos Técnicos de Mantenimiento.

Actualmente la Fuerza Aérea Colombiana cuenta con más de 50 ART de los modelos Scan Eagle y Night Eagle, así como con un simulador desarrollado nacionalmente por la Corporación de Alta Tecnología, CODALTEC, al que se denomina SIMART, siglas de SIMulador de ART.

Vistos los buenos resultados obtenidos por la Fuerza Aérea con el empleo de estas aeronaves, y con la intención de estandarizar los equipos, la Armada Nacional de Colombia también adquirió un lote de Scan Eagle, que operan desde las Fragatas Ligeras FS-1500 y desde los patrulleros tipo OPV-80, pero también se emplean en operaciones costeras o tierra adentro, en apoyo a la Infantería de Marina.

Los Scan Eagle de la Armada Nacional fueron mostrados por primera vez al público en la Feria Aeronáutica Internacional F-Air 2017, conociéndose que estaban operativos desde el año anterior en operaciones de reconocimiento marítimo antinarcóticos. Valga anotar que en el Informe de Gestión

de la Armada Nacional 2015-2018, se señala que el modelo adquirido es el Scan Eagle, y que a estos equipos se les denomina Sistema de Plataforma Aeronaval de Vigilancia Marítima - PAVMA. Se destaca que con ellas se han desarrollado operaciones de inteligencia, vigilancia y reconocimiento, con las que se ha logrado ubicar lanchas tipo Go Fast para su posterior interceptación en alta mar, también ha permitido a la Armada Nacional detectar embarcaciones que realizan pesca ilegal en aguas territoriales colombianas. Y en operaciones de apoyo a la Infantería de Marina, han facilitado la detección de cultivos ilícitos y laboratorios del narcotráfico, así como zonas de minería ilegal y operaciones de contrabando de combustible por vía fluvial. Por supuesto, todo lo anterior ha impactado negativamente las finanzas de los grupos narcotraficantes y terroristas que operan en Colombia.

En particular se destaca del empleo de los ART de la Armada Nacional, su bajo costo en el consumo de combustibles y lubricantes.

La Armada Nacional ha contado con el apoyo de la Escuela Básica de Aeronave Remotamente Tripuladas (EBART) de la Fuerza Aérea Colombiana, para el entrenamiento de sus tripulaciones. En la revista Semana (2016), se exaltan las bondades de los ART de la Fuerza Aérea Colombiana. Se señala que una aeronave tripulada puede tener unas 8 horas de autonomía de vuelo, mientras que las ART llegan a 20 horas con capacidad diurna y nocturna. Señalan además que para ese año un helicóptero Black Hawk podría llegar a costar entre 16 y 24 millones de dólares, pero el ART más costoso de la Fuerza Aérea Colombiana apenas cuesta 9 millones de dólares (probablemente se refieran al Hermes 900). Señalan además que "las ART están en capacidad de ascender hasta 19.000 pies, permiten comunicación en tiempo real y su costo operacional puede ser un 40 por ciento menor que el de una aeronave tripulada."

Según la misma fuente, para el año 2016, la Fuerza Aérea Colombiana contaba con más de 200 hombres y mujeres operando sistemas ART a nivel nacional. Ratificando que cada equipo está formado por cinco personas, entre ellos "un comandante de misión, encargado de la interacción con otras aeronaves y la comunicación con el servicio de tránsito aéreo; un operador, quien lleva el control de la aeronave desde tierra; un analista de imágenes y dos técnicos de mantenimiento."

En diciembre del año 2018 la Escuela Básica de Aeronaves Remotamente Tripuladas (EBART) de la Fuerza Aérea Colombiana, fue certificada por la empresa INSITU fabricante de los ART Scan Eagle y Night Eagle en uso por la FAC, avalando los procesos de formación que allí se llevan a cabo.

La EBART opera desde el año 2014 en el Comando Aéreo de Combate No. 3, CACOM 3, en Malambo, departamento del Atlántico, en la costa caribe colombiana. Hasta allí se desplazó el Director de la Escuela de Entrenamiento de INSITU, para hacer la respectiva certificación. Valga anotar que esto convierte a la EBART en la primera escuela de estos ART certificada en Latinoamérica.

La Escuela Básica de Aeronave Remotamente Tripuladas de la Fuerza Aérea Colombiana se dedica a la formación y entrenamiento de pilotos de Scan Eagle / Nigh Eagle, técnicos, instructores de vuelo, y analistas de video. Al momento de obtener la certificación, se habían formado en sus instalaciones más de 900 alumnos de las Fuerzas Militares de Colombia y de la Policía Nacional, y también miembros de las Fuerzas Armadas de otros países de América Latina, estrechando lazos de cooperación, y fortaleciendo sus capacidades para el mantenimiento del orden público y la lucha contra el narcotráfico, el terrorismo, y las nuevas amenazas. Además, estos ART pueden emplearse para la vigilancia de oleoductos, la prevención de desastres naturales, la detección y vigilancia de incendios forestales, para la prevención de la deforestación, la vigilancia vulcanológica, entre otras aplicaciones importantes.

Referencias:

Semana (2016). Los drones se unen a las filas de la Fuerza Aérea. Recurso en línea, disponible en: https://www.semana.com/nacion/articulo/militares-comienzan-a-usar-drones-en-operaciones/464063

Douglas Hernández
(Colombia) Fundador y director del website www.fuerzasmilitares.org, ejerce como periodista especializado en seguridad y defensa. Es colaborador de la *Air and Space Power Journal* -revista institucional de la USAF, ahora llamada *Revista Profesional Fuerza Aérea de EUA, Continente Americano*-, y de la revista brasilera *Segurança & Defesa*. Es Sociólogo y Magister en Educación de la Universidad de Antioquia (Medellín, Colombia), estudiante de Doctorado. Posee un Diplomado en Relaciones Internacionales.

Honduras

TESON

Las Tropas Especializadas en Selvas y Operaciones Nocturnas (TESON), son un cuerpo elite de las Fuerzas Armadas de Honduras. Fue creado con apoyo de instructores de las Fuerzas Especiales y Rangers estadounidenses para actuar en todo tipo de condiciones extremas e inclemencias climáticas.
El aprendiz TESON necesita completar un programa de entrenamiento similar a las que da el U.S. Army a los Army Rangers. Se hace énfasis en la capacidad de continuar operando bajo extremo estrés físico y mental. La formación de los primeros TESON se realizó en la base de paracaidistas de Támara, con la presencia de Ranges del US Army llegados de Fort Benning. El entrenamiento avanzado se realizó cerca de la frontera de Nicaragua en la selva de La Mosquitia. Las operaciones de guerra y noche selva fueron los principales focos de instrucción.
Luego de ese primer grupo, el Curso TESON se institucionalizó, habiéndose graduado múltiples promociones. Actualmente goza de reconocimiento nacional e internacional, como uno de los cursos para Fuerzas Especiales más exigentes en la región.
Durante el adiestramiento se busca una resistencia física y psicológica superior al soldado regular, para soportar todo tipo de privaciones, incomodidades e inclemencias en la zona de combate, aunado a ello, una fortaleza espiritual y moral inquebrantable, durante 54 días, entrenándose por la noche y madrugada.

Reseña Histórica del curso de TESON en Honduras

La historia de los hombres que conforman la hermandad de las Tropas Especializadas en Selvas y Operaciones Nocturnas (TESON) soldados comando de Honduras es una leyenda empapada de coraje, osadía, valor, resistencia, y un gran don de mando sobresaliente. Es una historia de hombres la cual su destreza en el arte del combate ha sido rara vez superada, soldados que integran una unidad de operaciones especiales que esta entrenada para realizar operaciones tras las líneas enemigas. Los TESONES están adiestrados de una forma específica para situaciones de alta seguridad y como tropas paracaidistas aerotransportadas y especialistas en operaciones anfibias. Son soldados ágiles y versátiles entrenados y formados para llevar a cabo una serie de tareas específicas que van desde operaciones convencionales hasta operaciones no convencionales, se adaptan para operar como fuerzas asimétricas y capaces de operar de una forma independiente, en apoyo directo de cualquiera de las fuerzas militares convencionales o de otros elementos gubernamentales.

El Centro De Adiestramiento de Tropas Especializadas en Selvas y Operaciones Nocturnas (TESON), fue creado a iniciativa del señor jefe de las fuerzas armadas, General de división Don Policarpo Paz García; es así como en el mes de mayo del año 1976 se selecciona el Segundo Batallón de Infantería Aerotransportado Táctico (II BIAT) como sede de adiestramiento de los Comandos Hondureños.
En las décadas de los 70´s, 80´s y mediados de los 90´s en la mal recordada guerra fría cuando además de los problemas de sub-desarrollo, Honduras también tenía que enfrentar las invasiones abiertas y clandestinas a su territorio por parte de grupos insurgentes armados de izquierda y derecha, con ello su soberanía e integridad territorial estuvo amenazada por esos conflictos vecinales. El alto mando militar de ese entonces para cubrir esas áreas fronterizas decidió conducir operaciones de vigilancia y patrullajes intensivos y para ello fue necesario crear unidades especiales decidiendo así en el año de 1976 iniciar la capacitación necesaria para re potenciar y crear unidades élites como las fuerzas especiales inaugurando en el agrupamiento táctico especial el 21 de mayo de ese año, el primer curso de tropas especializadas en selvas y operaciones nocturnas (TESON), culminando el entrenamiento 27 nuevos TESONES, 14 oficiales, 12 clases y 1 soldado que posteriormente se convirtieron en instructores de lo que hoy es el centro de adiestramiento TESON, y en sus unidades de origen expandieron la intención del mando creando cursos similares para las tropas y mejorar el apresto operacional

de cada una de ellas, con ello nacieron una variedad de cursos como: ATECI, COMANDOS, PUMAS, CAZADORES, DRAGONES, MONTAÑESES, etc.

El curso tiene una duración de 58 días dentro de los cuales está dividida en tres fases con un adiestramiento que implica pruebas de sobre vivencia en condiciones altamente extremas simulando un combate regular, durante el adiestramiento se busca una resistencia física y psicológica superior al soldado regular para soportar todo tipo de privaciones, incomodidades e inclemencias en la zona de combate sumado a ello una fortaleza espiritual y moral inquebrantable durante 58 días entrenándose por la noche y madrugada.

- **Primera fase o fase básica:** La primera fase tiene una duración de 18 días en la cual se realizan actividades de mucha exigencia física como cruce de pista de obstáculos, clases de defensa personal, y clases básicas de un soldado profesional.
- **Segunda fase o fase de montaña:** La segunda fase tiene una duración de 20 días en dicha fase se llevan al terreno todas las clases impartidas y vistas en los salones de clase del centro de adiestramiento y a la vez se llevan a cabo tareas en ambientes urbanos y acuáticos.
- **Tercera fase o fase selva:** La tercera y última fase tiene una duración de 20 días la cual se realiza en su totalidad en la zona norte del país dado que es ese sector es donde se encuentra el terreno más propicio para la práctica de las clases de supervivencia en selvas.

El curso de TESON comienza su adiestramiento en el Segundo Batallón de Infantería Aerotransportado, pero utiliza diferentes escenarios del territorio nacional que brinden un ambiente adverso.

Como ganadores de Fuerzas Comando

Al finalizar el curso se trasladan vía aérea conduciendo una operación de inserción, mediante salto de paracaidismo, haciendo uso de la zona de lanzamiento en Támara y tomando control de un terreno clave dominado por grupos de asociación ilícita o tráfico de drogas.
Con este último ejercicio culminará la nueva promoción de tesones, dejando claro el alto apresto operacional del Ejército a través de su unidad élite de TESONES, capaces de desarrollar operaciones y alcanzar el éxito deseado con una unidad consiente, comprometida y confiable de esta fuerza bajo la Secretaria de Defensa Nacional. Van más de 30 promociones graduadas bajo el lema “Después de TESON nada”.

Fuentes:
https://sedena.gob.hn/2017/07/03/adiestramiento-extremo-reciben-en-curso-teson/
https://histriadeteson.blogspot.com/2018/

TRIARIUS

Por un mundo más seguro, estable y en paz