STRATOP

Policy Brief

Estrategia Conjunta de Ciberdefensa SEDENA-SEMAR

STRATOP RISK CONSULTING

MTRO. RAÚL A. ÁLVAREZ PANIAGUA

Policy Brief mayo, 2023
Stratop Risk Consulting®

La delgada línea entre la actividad académica y la de inteligencia. ¿Cómo alinear esfuerzos en este sentido?

Muchos de los versados académicos, saben que por inteligencia se conceptúa al conocimiento obtenido a partir de la recolección, procesamiento, diseminación y explotación de información, para la toma de decisiones en materia de seguridad nacional y por contrainteligencia se entienden las medidas de protección de las instancias en contra de actos lesivos, así como las acciones orientadas a disuadir o contrarrestar su comisión.

En este sentido, se advierte que son amenazas a la seguridad nacional, los actos que impidan a las autoridades actuar contra la delincuencia organizada y los actos tendientes a obstaculizar o bloquear actividades de inteligencia o contrainteligencia.

Por lo que, en los Lineamientos Generales en materia de clasificación y desclasificación de la información[1], así como para la elaboración de versiones públicas, se considera información reservada, aquella que de difundirse actualice o potencialice un riesgo o amenaza a la seguridad nacional, cuando se obstaculicen o bloqueen las actividades de inteligencia o contrainteligencia y cuando se revelen normas, procedimientos, métodos, fuentes, especificaciones técnicas, tecnología o equipo que sean útiles para la generación de inteligencia para la seguridad nacional.

ANÁLISIS

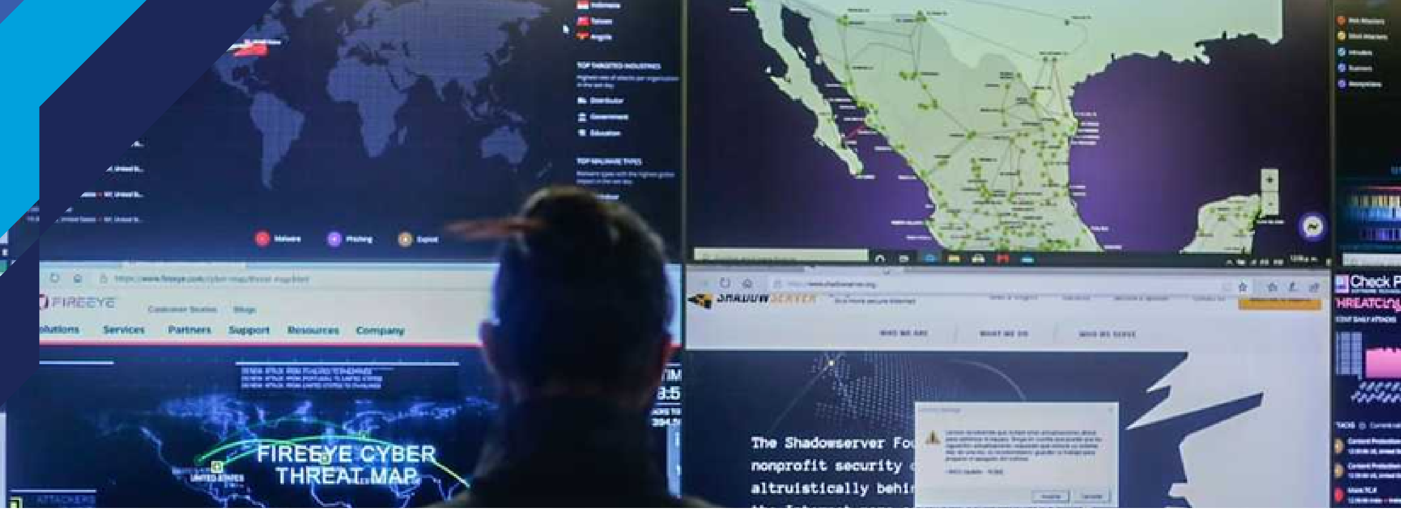
Al respecto, en la interpretación de la causal de reserva relativa a la seguridad nacional, debe decirse que ésta figura alude a las acciones destinadas, de manera inmediata y directa a mantener la integridad, estabilidad y permanencia del Estado, la cual se rige, entre otros, por los principios de legalidad, responsabilidad y respeto a los derechos fundamentales.

De ahí que, el artículo 28 de Constitución Política de los Estados Unidos Mexicanos[2] prevé que el Estado contará con los organismos que requiera para el eficaz manejo de las áreas estratégicas a su cargo y en las actividades de carácter prioritario donde, de acuerdo con las leyes, participe por sí o con los sectores social y privado.

Por su parte, el artículo 146 de la Ley General del Sistema Nacional de Seguridad Pública[3] establece que se consideran instalaciones estratégicas: los espacios, inmuebles, construcciones, muebles, equipo y demás bienes, destinados al funcionamiento, mantenimiento y operación de las actividades consideradas como estratégicas por la Constitución Política de los Estados Unidos Mexicanos, así como de aquellas que tiendan a mantener la integridad, estabilidad y permanencia del Estado Mexicano, en términos de la Ley de Seguridad Nacional[4].

Además, de conformidad con lo dispuesto por el artículo 51, fracciones I y II de la Ley de Seguridad Nacional, es información reservada por motivos de seguridad nacional, aquella cuya aplicación implique la revelación de normas, procedimientos, métodos, fuentes, especificaciones, técnicas, tecnologías o equipo útiles a la generación de inteligencia para la seguridad nacional, sin importar la naturaleza o el origen de los documentos que la consignen y, aquella cuya revelación pueda ser utilizada para actualizar o potenciar una amenaza.

[1] Disponible para su consulta en: https://www.dof.gob.mx/nota_detalle.php?codigo=5433280&fecha=15/04/2016#gsc.tab=0 , recuperado el 2 de abril de 2023.
[2] Disponible para su consulta en: https://www.diputados.gob.mx/LeyesBiblio/pdf/CPEUM.pdf , recuperado el 2 de abril de 2023.
[3] Disponible para su consulta en: https://www.diputados.gob.mx/LeyesBiblio/pdf/LGSNSP.pdf , recuperado el 2 de abril de 2023.
[4] Disponible para su consulta en: https://www.diputados.gob.mx/LeyesBiblio/pdf/LSN.pdf , recuperado el 2 de abril de 2023.



Por lo anterior, y sin menoscabar la importante labor académica como elemento generador de cultura de seguridad nacional, sea este sector el que exponga motivos en algunas plataformas digitales para sentirse insatisfechos con la versión pública en la que únicamente se revela el texto de la Introducción y su Marco Jurídico Nacional del documento estratégico en materia de ciberdefensa elaborado entre las Secretarías de la Defensa Nacional y Marina.

Derivado de la clasificación como “Reservada” del documento estratégico en comento, diversos académicos y expertos en seguridad nacional han argumentado que contrario a mermar la seguridad nacional o interferir con las acciones de las fuerzas armadas, y tener presente las estrategias que emanan de sus deberes y responsabilidades, se coadyuva a fortalecer acciones específicas y se permite mejor coordinación para con la academia, y la industria, y las distintas dependencias que tienen incidencias en el ciberespacio. Así como que resulta natural el deseo de tener conocimientos de cuáles son los marcos rectores que guían a grandes rasgos las capacidades en el "quinto dominio", a forma de fomentar, una cultura de defensa nacional, y además defender la soberanía e integridad territorial de la nación con acciones en este ámbito.

Al respecto, es importante precisar que la Ley Federal de Transparencia y Acceso a la Información Pública[5] establece que toda la información generada, obtenida, adquirida, transformada o en posesión de los sujetos obligados en el ámbito federal, es pública y sólo podrá ser clasificada excepcionalmente como reservada de forma temporal por razones de interés público y seguridad nacional o bien, como confidencial.

Recordemos algo importante, militarmente y desde el enfoque de la comunidad de inteligencia al ciberespacio se le conoce en la mayoría de los países como el “quinto dominio de la guerra” como se indicó anteriormente, aunado a los dominios de tierra, mar, aire, y espacio exterior; por lo que existe la necesidad de proteger el ciberespacio de acciones ilícitas y potencialmente dañinas en el ciberespacio, dominio en el que incluso se pueden realizar actividades en contra de Estados nación, por ejemplo, actos como ciberespionaje, ciberterrorismo y ciberguerra.

[5] Disponible para su consulta en: https://www.diputados.gob.mx/LeyesBiblio/pdf/LFTAIP_200521.pdf , recuperado el 2 de abril de 2023.

CONCLUSIÓN

Es por esto que a manera de conclusión en un ejercicio de pensamiento asertivo y prospectivo, respetando el ámbito de la academia y de la comunidad de inteligencia para alinear sus esfuerzos en un frente común en el análisis de este documento estratégico, debe ser prioridad contar con andamiaje técnico-jurídico en el que México contemple promover e impulsar una Ley de Inteligencia que funcione de encuadramiento estratégico a las actividades de ciberseguridad y ciberdefensa, con la finalidad de servir de peso y contrapeso en el marco de las funciones de evaluación, supervisión y de mejora continua de la Comisiones Bicamerales de Seguridad Nacional y la de Evaluación y Seguimiento de la Fuerza Armada Permanente en tareas de seguridad pública; con la finalidad de que al contar con una Ley de Inteligencia sea garantice el respeto a la privacidad, datos personales y derechos fundamentales de los ciudadanos en el marco de la actuación de las fuerzas armadas en el “quinto dominio”.

México ya cuenta con una estrategia que incluye los esfuerzos de dos instituciones nacionales especializadas en ciberdefensa, las cuales entre sus filas están los elementos necesarios para garantizar la capacidad del Estado mexicano de interactuar respetando las fronteras en las que estrechamente se encuentran vinculadas la política, las políticas y la seguridad nacional propia y la de otros Estados en el ciberespacio, solventando tensiones legales de gobernanza para evaluar, decidir y actuar en este dominio.

STRATOP®

RISK CONSULTING

Este documento documento se distribuye de forma gratuita sin fines de lucro y ha sido elaborado por el personal de:
Stratop Risk Consulting®
Para más información, otros materiales, consultas, productos o posibles ideas de análisis de factores de riesgo asociados, por favor contáctenos en:

stratoprisk.com

contact@stratoprisk.com

@StratopRisk

StratopRisk

STRATOP RISK CONSULTING