PROYECTO DE LEY

EL SENADO Y LA HONORABLE CÁMARA DE DIPUTADOS DE LA NACIÓN SANCIONAN CON FUERZA DE

LEY

LEY DE CIBERPROTECCIÓN

Artículo 1°. Objeto. -La presente ley establece las bases jurídicas, orgánicas y funcionales del Sistema Nacional de Ciberprotección y cuyo fin es conservar y fortalecer la Seguridad Nacional y de los ciudadanos frente a incidentes, incidentes de seguridad, incidentes de defensa, eventos, amenazas, riesgos y ataques en el ciberespacio que afecten a personas, infraestructuras críticas y tecnológicas, activos de información, sistemas informáticos y recursos naturales.

Artículo 2°. Orden Público. -Las disposiciones pertinentes de la presente ley son de orden público y de aplicación en todo el territorio de la República.

Artículo 3°. Definiciones. - Para aplicar, concordar y relacionar la presente Ley se consideran las siguientes definiciones:

a. Activo de información: cualquier información o sistema relacionado con el tratamiento de la misma, que tenga valor para la organización. Pueden ser

procesos de negocio, datos, aplicaciones, equipos informáticos, personal, soportes de información, redes, equipamiento auxiliar o instalaciones.

b. Amenaza: circunstancia desfavorable que puede ocurrir y que cuando sucede tiene consecuencias negativas sobre los activos, provocando su indisponibilidad, funcionamiento incorrecto o pérdida de valor. Una amenaza puede tener causas naturales, ser accidental o intencionada.

c. Análisis de riesgos: 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. Permite comprender la naturaleza del riesgo y determinar el nivel de riesgo.

d. Ciberataque: acción producida en el ciberespacio que compromete la disponibilidad, integridad y confidencialidad de la información mediante el acceso no autorizado, la modificación, degradación o destrucción de los sistemas de información y telecomunicaciones o las infraestructuras que los soportan.

e. Ciberespacio: ambiente complejo, que resulta de la interacción de personas, software y servicios en internet, por medio de dispositivos y redes conectadas.

f. Ciberseguridad: preservación de la disponibilidad, integridad y confidencialidad de la información en el ciberespacio.

g. Disponibilidad: capacidad de un servicio, un sistema o una información de ser accesible y utilizable por los usuarios o procesos autorizados cuando éstos lo requieran.

h. Evento o suceso de seguridad de la información: ocurrencia o cambio detectado en el estado de un sistema, servicio o red, que indica una posible

violación de la política de seguridad de la información, un fallo de los controles, o una situación desconocida hasta el momento y que puede ser relevante para la seguridad.

i. Incidente: ocurrencia que real o potencialmente resulte en una consecuencia adversa o amenaza para un sistema de información, o la información que el sistema procesa, almacena o transmite y que puede requerir una acción de respuesta para mitigar las consecuencias.

j. Incidente de defensa: cualquier suceso que afecte a la confidencialidad, integridad o disponibilidad de los activos de información e infraestructura tecnológica de las Fuerzas Armadas Argentinas, menoscabe o impida el cumplimiento de sus misiones y funciones conforme la legislación vigente.

k. Incidente de seguridad: cualquier suceso que afecte a la confidencialidad, integridad o disponibilidad de los activos de información de la empresa u organismo.

l. Infraestructuras críticas: son 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.

m. Infraestructura tecnológica: conjunto de dispositivos de hardware, software y comunicaciones, utilizados por la organización para el cumplimiento de sus funciones, incluyendo el ámbito físico donde se encuentran ubicados.

n. Riesgo: potencial de que una amenaza específica explote las debilidades de un activo o grupo de activos para ocasionar pérdida y/o daño a los activos. Por

lo general, se mide por medio de una combinación del impacto y la probabilidad de ocurrencia.

o. Seguridad Nacional: es la acción del Estado dirigida a proteger la soberanía, integridad, estabilidad, permanencia y autodeterminación de la República, sus principios, valores y derechos constitucionales, su acervo, recursos, orden público, paz, bienestar y forma de vida de su pueblo.

p. Sistema informático: todo dispositivo aislado o conjunto de dispositivos interconectados o relacionados entre sí, cuya función, o la de alguno de sus elementos, sea el tratamiento automatizado de datos en ejecución de un programa.

Artículo 4°. Finalidades. - Conforme el objeto general, la presente ley tiene por misión:

1. Procurar la disponibilidad y uso seguro del ciberespacio.
2. Ampliar las capacidades de anticipación, prevención, respuesta y mitigación frente a incidentes, incidentes de seguridad, incidentes de defensa, eventos, amenazas y ataques en el ciberespacio que afecten a personas, infraestructuras críticas y tecnológicas, activos de información, sistemas informáticos y recursos naturales.
3. Crear un Consejo Nacional de Ciberprotección como organismo rector, de planificación, diseño, cooperación y contralor en la materia.
4. Crear un Centro Nacional de Ciberprotección como organismo ejecutor de las políticas, planes y acciones de prevención, anticipación, respuesta y mitigación en la materia.

5. Velar por el cumplimiento de las mandas específicas de la Estrategia de Seguridad Nacional y las particulares de la Estrategia Nacional de Ciberseguridad y la de Ciberdefensa.
6. Promover el cumplimiento de los fines establecidos en los artículos 14, 19, 20, 23, 29, 30, 35 y concordantes del Convenio sobre Cibercriminalidad o Convenio de Budapest, conforme la Ley Nacional 27.411.

Artículo 5°. Consejo Nacional de Ciberprotección. Dependencia Funcional e Integración.- El Consejo Nacional de **Ciberprotección**, así como el Centro Nacional de **Ciberprotección**, estarán bajo la dirección, competencia y aplicación de la Jefatura de Gabinete, absorbiendo y concentrando todo elemento o función que en materia de ciberseguridad y ciberdefensa operen en otros ministerios, áreas o entes del Estado Nacional.

El Consejo Nacional de Ciberprotección será conducido por un Director General propuesto por el Presidente de la Nación, tres Directores Adjuntos a propuestas del Jefe de Gabinete de Ministros, del Ministro de Defensa y del Ministro de Seguridad de la Nación respectivamente. El resto de su integración será plural debiendo estar representados al menos el Ministerio de Interior; el Ministerio de Relaciones Exteriores, Comercio Internacional y Culto; el Ministerio de Obras Públicas; el Ministerio de Economía; la Agencia Federal de Inteligencia; la Unidad de Información Financiera; y la Secretaria de Asuntos Estratégicos de Presidencia de la Nación o el órgano que en el futuro remplace sus funciones. La vía reglamentaria establecerá los roles y funciones.

Artículo 6°. Comité Federal de Expertos. - El Consejo Nacional de Ciberprotección contará, como órgano consultor, con un Comité Federal de Expertos integrado por un titular y un suplente, a proposición de cada provincia y la Ciudad Autónoma de Buenos Aires. El Comité será presidido por el Director General del Consejo Nacional de Ciberprotección, quien lo convocará periódicamente y coordinará la producción de sus informes y recomendaciones.

Artículo 7°. Misiones y funciones del Consejo Nacional de Ciberprotección.

1. Diseñar las políticas, planes y acciones necesarias para prevenir ciberataques y restablecer, resguardar, fortalecer y consolidar un entorno digital seguro.
2. Realizar análisis de riesgos y fortalecer la ciberseguridad y la ciberdefensa de la República.
3. Diseñar y supervisar políticas de innovación, formación, especialización, difusión, prevención, forenses, de investigación, de compatibilidad, asistencia y cooperación nacional e internacional en la materia y sus afines.
4. Definir técnicamente una escala de riesgo que permita caracterizar a las infraestructuras críticas en todos los niveles sean éstas públicas, privas o mixtas.
5. Elaborar y actualizar el inventario de infraestructuras críticas de acuerdo con el grado de riesgo de las mismas. La elaboración se hará con la información suministrada por los entes territoriales, los Ministerios y entidades que tengan a su cargo dichas estructuras, y de las organizaciones privadas que sean incluidas.
6. Preservar debidamente la información y datos sensibles o aquella que pueda afectar la seguridad nacional.

7. Interactuar con el sector privado, fijar controles, homologaciones, y solicitar medidas, planes, estándares y compromisos para mantener un entorno digital seguro, prevenir y responder a incidentes, incidentes de seguridad, incidentes de defensa, eventos, amenazas y ataques en el ciberespacio que afecten a personas, infraestructuras críticas y tecnológicas, activos de información, sistemas informáticos y recursos naturales.
8. Poner en funcionamiento el Centro Nacional de Ciberprotección, coordinar, supervisar y controlar el cumplimiento de sus misiones y funciones, así como garantizar su modernización, actualización y fortalecimiento continuo.
9. Conformar una Comisión Edilicia, que será la encargada de identificar la locación segura, de dirigir, coordinar y controlar la construcción y posterior actualización y fortalecimiento del Centro de Ciberprotección con la participación necesaria del Ministerio de Seguridad y del Ministerio de Defensa de la República Argentina. Esta comisión contemplará las construcciones, equipamientos y necesidades propias y separadas a la seguridad y la defensa, trabajará y exigirá los máximos criterios de seguridad y confidencialidad.
10. Receptar, considerar y supervisar el cumplimiento de las directivas y recomendaciones emergentes de la Estrategia de Seguridad Nacional.
11. Diseñar las estrategias de acción y asesorar en la implementación de medidas preventivas y operativas.
12. Generar planes, protocolos, normas, interacciones y cooperaciones para cumplir con sus fines y competencias.
13. Recibir las recomendaciones e informes del Comité Federal de Expertos y desarrollar todas las políticas de interacción necesarias a sus fines.

14. Desarrollar un sistema de gestión de seguridad de la información de la Administración Pública Nacional.

15. Instrumentar mecanismos de capacitación y especialización de los operadores del Sistema de Ciberprotección, así como promover las actividades de investigación y desarrollo.

16. Se priorizarán los principios de eficacia y concentración y todas las instrumentaciones que correspondan, se cursarán por ante en Centro Nacional de Ciberprotección o los efectores que este anexe o coopere.

Artículo 8°. Composición técnica, misiones y funciones del Centro Nacional de Ciberprotección. El Centro Nacional de Ciberprotección contará con un Director en Jefe, un Director Adjunto y una Mesa Operativa de 15 miembros. Los roles, sus alcances, misiones y funciones serán dados por un reglamento interno confeccionado por el Director General, con el asesoramiento de la mesa operativa.

Asimismo, para operar contará con técnicos, administrativos y personal propio y de las Fuerzas de Seguridad y Armadas.

Artículo 9°. De las misiones y funciones del Centro Nacional de Ciberprotección. Serán sus principales objetivos:

a. Aplicar las políticas, recomendaciones, directrices o encomiendas emergentes de la Estrategia de Seguridad Nacional, o la especial de Ciberseguridad y Ciberdefensa.

b. Aplicar las políticas, planes y acciones emergentes del Consejo Nacional de Ciberprotección.

c. Centralizar, coordinar, optimizar, ejecutar los procesos, medidas e intervenciones preventivas, anticipatorias, reactivas y de mitigación frente a incidentes, incidentes de seguridad, incidentes de defensa, eventos, amenazas y

ataques en el ciberespacio, que afecten a personas, infraestructuras críticas y tecnológicas, activos de información, sistemas informáticos y recursos naturales.

d. Realizar todas las interacciones, cooperaciones y procesos de homogeneización necesarios al cumplimiento de sus fines.

e. Aplicar el sistema de gestión de seguridad de la información de la administración pública nacional.

f. Podrá solicitar y contará con el acceso, disponibilidad y apoyo inmediato de todas las agencias, elementos y áreas del Estado para el cumplimiento de sus fines.

g. Deberá disponer lo necesario para el trabajo articulado y presente, con la Procuración de la Nación conforme lo dispuesto en el artículo siguiente.

h. Cuando se trate de incidencias de defensa, la conducción y gerenciamiento operacional de las mismas estará a cargo de personal especializado de las Fuerzas Armadas.

i. Cuando se trate de incidencias a la Seguridad Nacional, el Presidente será informado y ordenará el curso de acción correspondiente.

j. Instrumentar un mando de situación, gerenciamiento de eventos y emergencias.

k. Instrumentar un laboratorio de innovación, desarrollo y evaluación forense.

l. Anualmente elevará al Consejo Nacional de Ciberprotección un presupuesto de funcionamiento y fortalecimiento para que sea considerado al momento del diseño del Presupuesto General de la Nación.

m. Ejecutar las mejores prácticas de transparencia y rendición de cuentas. Se preservará debidamente la información y datos sensibles o aquella que pueda afectar la Seguridad Nacional.

Artículo 10. Interagencialidad. - Se invitará a la Procuración General de la Nación a tener un ámbito integrado dentro del Centro de Nacional de

Ciberprotección, para que sus efectores especializados puedan ejecutar la política de persecución penal y el ejercicio eficaz de la acción penal pública con inmediatez y oportunidad. La vía reglamentaria determinará lo necesario al funcionamiento coordinado.

También se contará con un ámbito reservado como despacho de la Justicia Federal competente, cuando se trate de incidencias de seguridad o defensa que requieran de su intervención *in situ.*

Artículo 11.- Los fondos y recursos para la construcción y ulterior funcionamiento, así como para el fortalecimiento continuo del Centro Nacional de Ciberprotección se imputarán al presupuesto asignado a la Jefatura de Gabinete de la Nación con su debida readecuación. El Poder Ejecutivo deberá afectar los recursos materiales y humanos en cantidad y calificación necesarias para el cumplimiento de la presente ley.

Artículo 12.- Se invita a las provincias y a la Ciudad Autónoma de Buenos Aires a readecuar su legislación y reglamentaciones pertinentes.

DISPOSICIÓN COMPLEMENTARIA. -

Artículo 13.- Créase en el ámbito del Honorable Congreso de la Nación, la Comisión Bicameral de Fiscalización y Seguimiento del Centro Nacional de Ciberprotección, la que tendrá como finalidad fiscalizar que su funcionamiento se ajuste estrictamente a las normas constitucionales, legales y reglamentarias

vigentes, verificando la observancia y respeto de las garantías individuales consagradas en la Constitución Nacional.

La Comisión Bicameral tendrá amplias facultades para controlar e investigar de oficio. A su requerimiento, el Centro Nacional de Ciberprotección, deberá suministrar la información o documentación que la Comisión solicite.

Artículo 14.- Comuníquese al Poder Ejecutivo.-

FUNDAMENTOS. -

Sr. Presidente:

Es necesario destacar que el presente proyecto es una reproducción del expediente 0393-D-2022.

Como punto de partida ha de notarse que el presente se trata de un cuerpo normativo para el aseguramiento y protección frente incidentes que operan y

transitan en el "ciberespacio". Este nuevo dominio es un ámbito virtual e intangible, pero generador de peligros y afectaciones absolutamente reales y por ende, un problema público que necesita ser legislado.

El término "ciberespacio" fue acuñado por el famoso novelista de ciencia ficción William Gibson en 1981, con lo cual queda claro que ninguna interpretación teleológica de las posteriores leyes 23.554 (Defensa Nacional) y 24.049 (Seguridad Interior), puede remontarnos o aplicar a esas virtualidades.

La modernidad ha puesto en una encrucijada al plexo reglamentario (Decretos, 727/06, 1691/06, 1714/09) y las doctrinas de respaldo. En este estado es muy acertado el análisis de Sergio G. Eissa y Ana Albarracín Keticoglu: "En un artículo previo (Eissa, et al, 2019) sosteníamos que la definición de ciberdefensa no era inocua por al menos tres (3) motivos. En primer lugar, el ciberespacio ponía en "jaque" la separación orgánica y funcional entre la defensa y la seguridad interior. En segundo lugar, la decisión sobre cómo se resolvía esa separación frente a la problemática que el ciberespacio representaba para la seguridad nacional de Argentina. Por último, las Fuerzas Armadas pujaron con el Estado Mayor Conjunto ya no por la definición, sino sobre a quién le correspondía operar en el ciberespacio y cómo". (Ver Publicación de la Universidad de la Defensa Nacional Revista Defensa Nacional - Nro 5 - Diciembre 2020).

Que tanto la Ley de Defensa Nacional 23554, como la Ley de Seguridad Interior 24.059, obedecieron a un contexto histórico nacional e internacional determinado. Ambos cuerpos legales, que han permitido transitar años de la vida nacional, hoy han quedado atrasados a los nuevos fenómenos a regular, anticipar y prevenir.

En relación al quinto dominio, la doctrina especializada ha dicho: "El espacio cibernético, junto con los tradicionales ambientes terrestre, marítimo, aéreo y espacial es objeto de análisis por parte de numerosas instituciones públicas y privadas, tanto nacionales como internacionales. Esto puede demostrarse si se observa a las instituciones universales y regionales de seguridad como la ONU, la OEA, la NATO y la OSCE que han incorporado en sus estructuras a organismos competentes sobre el tema, así como diversos países que han incluido la problemática del espacio cibernético a sus agendas de estrategia nacional de seguridad ya que los incidentes y los ataques cibernéticos se han convertido en una fuente de amenazas en el mundo globalizado, debido a su capacidad de acceso a sistemas de información diplomáticos, gubernamentales y militares". (General de División (RE) Evergisto de Vergara Contraalmirante
(RE) Gustavo Adolfo Trama, en "Operaciones Militares Cibernéticas,
Planeamiento y Ejecución en el Nivel Operacional", Escuela Superior Conjunta de las Fuerzas Armadas, pág. 13 y 14).

Que es necesario flexibilizar los esquemas rígidos y compartimentados, buscando miradas multidimensionales en ámbitos donde la complementariedad se transforme en valor agregado, dinamismo y fortaleza.

También el desarrollo de nuestra defensa se lentificaría por desinversión y falta de hipótesis de asistencia y colaboración en situaciones que demandan de su presencia y auxilio profesional. Seguir un camino pasivo no refleja el espíritu de nuestra Nación, ni el del constituyente que ordenó al legislador fijarlas "en tiempo de paz ...y dictar las normas para su organización y gobierno" (art. 75 inc. 27 de la Constitución Nacional) y tampoco se corresponde con el disponer para su

"organización y distribución" como competencia del Ejecutivo Nacional conforme el art. 99 inc. 14 de la Constitución Nacional.

En algunos momentos puntuales de nuestra historia reciente, el salto colaborativo pudo expresarse en los hechos. Prueba de ello es la fundamentación del Decreto 1091/11, que da lugar al operativo llamado "Escudo Norte", donde para luchar contra el narco criminalidad y el contrabando en nuestras fronteras establecen un operativo específico donde intervendrán las Fuerzas Armadas.

En particular, el artículo 5 del mencionado Decreto dispuso: "Instrúyase al Ministerio de Defensa para que en el ámbito de su competencia, adopte todas las medidas administrativas, operativas y logísticas necesarias para intensificar las tareas de vigilancia y control de los espacios de jurisdicción nacional por parte de las Fuerzas Armadas". (Sic).

En igual sentido la resolución 590/11 del Ministerio de Defensa donde se instruyó al Estado Mayor Conjunto para incrementar las capacidades de vigilancia y reconocimiento aeroespacial en la frontera norte. Este operativo se conoce como "Fortín II" y vuelve a colocar a las Fuerzas Armadas en tareas coordinadas.

Nuevas amenazas y riesgos vuelven permeables y obsoletas nuestras respuestas individuales. Hay campos, como el quinto dominio, necesariamente mixtos e incluso superpuestos, que requieren de la utilización de los recursos tanto de la seguridad como de la defensa e incluso de otras áreas del Estado en forma integrada.

A la indefinición por falta de previsión del legislador original ha de sumarse la súper población de efectores, la concurrencia de competencias y un desorden organizativo que en lugar de minimizar vulnerabilidades las acrecienta.

En este escenario fue importante circunscribir la definición de "incidencia de defensa". Entendemos, que con los límites que impone la misma se podrá operar sin inconvenientes, reservando el resto de las acciones militares según su estado y fines.

En cuanto a mandas relativas a la tipificación legal, a los institutos procesales y la cooperación internacional, la República Argentina por Ley N° 27.411, adhirió al Convenio sobre Ciberdelito del Consejo de Europa, adoptado en la Ciudad de Budapest, República de Hungría, el 23 de noviembre de 2001.

Que este ingreso a las protecciones y cooperaciones internacionales además es dinámico, pues de la norma madre se desprenden los protocolos que nuestro país también afirma y consolida.

Que la producción de derecho interno está en constante progreso, abarcando entre otras: la Ley 26.388 (Ley de delito informático); 25.326 (Ley de protección de datos personales); 25.506 (Ley de firma digital); 26.904 (Ley de Grooming); los Decretos reglamentarios 1558/2001, 2628/2002 (dictados por el Poder Ejecutivo Nacional); los Decretos 577/2017, 480/2019 (de creación del Comité de Ciberseguridad, dictados por el Poder Ejecutivo Nacional); las Decisiones Administrativas 641/2021, 6/2021 (de la Jefatura de Gabinete de Ministros); las Disposiciones 6/2021, 1/2021, 3/2013 (de la Administración Pública Nacional) y las Resoluciones 580/2011, 1523/2019, 829/2019 y 141/2019 (de la Jefatura de Gabinete de Ministros), con más sus antecedentes. Que la voluntad emergente de estas normas, de los órganos por ellas instrumentados, así como de la modernización de la ley penal, refiere el interés nacional permanente en mantener un "entorno digital seguro".

Que la velocidad, la mutación y el camuflaje son características esenciales de los ciberataques, es por ello que los Estados están cambiando sus marcos legales y

estrategias de acción. Nuevos dominios como el ciberespacio no sólo son puertas de acceso directas y poco detectables al menoscabo de los bienes jurídicos sujetos de protección, sino a la propia integridad, estabilidad y permanencia de los Estados, la paz y el bienestar de sus pueblos.

El Doctor en Seguridad Internacional Guillem Colom Piella en su trabajo "Guerras Híbridas. Cuando el contexto es todo", afirma: "El concepto de guerra híbrida se convirtió (junto con las noticias falsas, los trolls, los bots o la desinformación) en uno de los hypes informativos del pasado año, a pesar de las importantes controversias que genera entre los expertos. Mientras muchos consideran que no existen razones suficientes para acuñar nuevas denominaciones que solamente añaden confusión al análisis estratégico, otros sostienen que, el conflicto híbrido es el producto natural de la adaptación de la guerra irregular (a grandes rasgos, contraria a los usos y costumbres de la guerra) y asimétrica (encaminada a explotar las vulnerabilidades de las fuerzas regulares) al mundo actual".

El Presidente del Gobierno de España Mariano Rajoy Brey, en su mensaje de presentación de la Estrategia de Seguridad Nacional de 2013, ya advertía: "A los riesgos y amenazas tradicionales se suman, en efecto, otros nuevos de naturaleza generalmente transnacional, que se interconectan y potencian su peligrosidad, a la vez que aparecen nuevos espacios abiertos que facilitan su expansión e impacto. El ciberespacio es hoy el ejemplo más claro de un ámbito accesible, poco regulado y de difícil control, y en consonancia, la ciberseguridad es uno de los principales ámbitos de actuación de esta Estrategia".

En nuestros márgenes y con razón, afirma la Estrategia de Ciberseguridad de la República Argentina del año 2019: "El Ciberespacio, nombre por el que se designa al dominio global y dinámico compuesto por las infraestructuras de tecnología de la información, incluida Internet, las redes y los sistemas de

información y de telecomunicaciones, tiene entre otras, como características esenciales, su dimensión global y transfronteriza, su naturaleza dual, su masividad y su vertiginosa y constante evolución. Como toda construcción humana, esta revolución tecnológica no es perfecta, contiene errores y debilidades y conlleva vulnerabilidades que es necesario reconocer. Uno de los prerrequisitos esenciales para que el Ciberespacio se despliegue en toda su potencialidad en beneficio de la humanidad, es alcanzar niveles razonables de seguridad y confiabilidad".

Es importante recordar también que los objetivos 3, 4, 5 y 7 de la citada estrategia, instan al desarrollo del marco normativo, al fortalecimiento de capacidades de prevención, detección y respuesta, a la protección y recuperación de los sistemas de información del sector público y a la cooperación internacional. Cada una de estas previsiones y fines se reflejan en el articulado del presente proyecto de ley.

En un continuo la nueva estrategia del año 2023, dentro de sus principios rectores exhorta la construcción de capacidades de corte federal, previendo específicamente en el apartado tercero, la siguiente manda: "En materia de ciberseguridad el Estado Nacional debe promover políticas públicas basadas en riesgos, que tengan por objeto construir capacidades de detección, prevención, monitoreo, resiliencia, respuesta y recuperación a incidentes cibernéticos, de forma articulada entre el Sector Público Nacional y en coordinación con los estados provinciales, la Ciudad Autónoma de Buenos Aires, los municipios, el sector privado, el sector académico y la sociedad civil, con una adecuada articulación de las competencias y recursos involucrados". (SIC).

En la faz criminal, el ciberdelito es una variedad ilícita que se monta en la innovación y por lo tanto hay que construir, no sólo nuevas definiciones y tipicidades que recepten sus prácticas, sino la herramienta material donde las

capacidades humanas de nuestros expertos puedan desarrollar todo su potencial preventivo, forense y auxiliar.

Por otra parte, y dada la naturaleza híbrida de las agresiones hemos dado recepción legislativa a la "Seguridad Nacional" con una definición precisa y su consecuente instrumentalización emergente.

Las estrategias de Ciberseguridad y Ciberdefensa son herramientas esenciales al Estado moderno, pero no dejan de ser sólo parte integrante de la Estrategia de Seguridad Nacional, como compendio totalizador de riesgos y amenazas posibles al Estado, a los Derechos y el progreso de su gente.

Una estrategia de Seguridad Nacional puede ser un libro arrumbado en un cajón, un documento que sólo pueden entender unos pocos, o una herramienta útil a la "defensa común y el bienestar general".

Si tuviese que emplear un sólo término para expresar lo que significa para el Estado contar con una Estrategia de Seguridad Nacional y su entorno instrumental, sin dudas la definiría como un ACTIVO.

En este estado argumental, es necesario recalar en un mandato pocas veces divisado y considerado: "el Preámbulo de la Carta Magna".

El citado, ha contemplado un "mandato a ejecutar" cual fue la Constitución misma y por ende su ligazón al plexo oportunamente encomendado es de "carácter inescindible".

Conforme lo dicho, reza el preámbulo: Nos los representantes del pueblo de la Nación Argentina, reunidos en Congreso General Constituyente por voluntad y elección de las provincias que la componen, en cumplimiento de pactos preexistentes, con el objeto de constituir la unión nacional, afianzar la justicia, consolidar la paz interior, proveer a la defensa común, promover el bienestar general, y asegurar los beneficios de la libertad, para nosotros, para nuestra

posteridad, y para todos los hombres del mundo que quieran habitar en el suelo argentino: invocando la protección de Dios, fuente de toda razón y justicia: ordenamos, decretamos y establecemos esta Constitución, para la Nación Argentina.

La "defensa común y la prosperidad" para los habitantes del suelo argentino, deben ser consolidadas en acciones concretas como las emergentes de la ley en ciernes.

En base a las realidades antes descriptas, que ya no tocan nuestra puerta, sino que nos dañan en el interior de la casa, es necesario desarrollar un efector potente, especialmente diseñado a sus fines y que nos proteja en forma organizada, correctamente financiada y sostenida como política consensuada del Estado.

Por lo antes dicho, solicito a nuestros pares que nos acompañen con su voto.

Autor: Ramiro Gutiérrez