INSTITUTO DE INVESTIGACIONES
ESTRATÉGICAS DE LA ARMADA DE MÉXICO

TI 02/16

02/02/2016

Doctor
Emilio Vizarretea Rosales

NUEVA INTELIGENCIA Y CIBERSEGURIDAD

Dr. Emilio Vizarretea Rosales[1]

Resumen:

El ensayo propone (a) Re-Pensar la idea de Seguridad Nacional de México, con el fin de articular una (b) Nueva Visión de la Inteligencia Estratégica, considerando los (c) Riesgos y amenazas para la CiberSeguridad mexicana, proponiendo elementos de (d) CiberInteligencia para la Seguridad Nacional. Termina con algunas sugerencias y conclusiones, así como una breve bibliografía.

Abstract:

The essay proposes Strategic Intelligence and Cibersecurity, in order to rethink Mexico´s National Security, based on risks and threats for Ciberdefence.

Conceptos clave: Seguridad nacional, Inteligencia Estratégica, Ciberseguridad, Ciberinteligencia, Ciberdefensa.

Keywords: National Security, Strategic Intelligence, Cybersecurity, Cyberintelligence, Cyberdefence.

[1] El Dr. Emilio Vizarretea Rosales, colabora como profesor e investigador en el CESNAV y en el Instituto de Investigaciones Estratégicas de la Armada de México. El texto recupera ideas expresadas en la conferencia impartida con motivo del XXIV Intercambio Académico 2015, entre el Colegio de Defensa Nacional (SEDENA) y el Centro de Estudios Superiores Navales (SEMAR-Armada de México) realizado en la Escuela Superior de Guerra-SEDENA, abril 14, 2015.

I. Repensar e Incidir en la Seguridad Nacional mexicana

Donde no hay visión los pueblos sucumben.

Proverbios

En las disciplinas sociales, toda **definición** conceptual es un **punto de partida**, jamás de llegada, que propicia el despliegue del proceso de reflexión y, en su devenir, permite la incorporación de múltiples determinaciones. Esta tarea, aplicada a la seguridad nacional en México conlleva las siguientes consideraciones:

En una **perspectiva crítica**, tanto el proceso como el resultado son parte de la articulación teórico-práctica, de estructuras en un tiempo y espacio determinados, que demandan el ejercicio de abstracción, intelectual y mental, sobre las prácticas y propuestas generadas, con el fin de generar la comprensión y la explicación de un hecho o fenómeno dado.

Así, en un enfoque global, con referencia local, amplio y profundo, es pertinente considerar a la Seguridad Nacional, en el contexto mexicano, en una triple perspectiva: como política pública gubernamental, como política de Estado y, por otra parte, como un instrumento de análisis de una situación determinada.

Como ***política de gobierno***, la política de seguridad nacional atiende la instrumentación institucional, práctica y concreta, en su formulación, aplicación y conducción, bajo la responsabilidad del gobierno y, en particular, del titular del Ejecutivo federal, por lo que la ley en la materia rige su orientación. Es una consideración táctica u operativa.

Como ***política de Estado***, la Seguridad Nacional considera la doctrina y los principios de la nación –su evolución histórica y constitucional-, como una normatividad condicional del desarrollo, en forma equilibrada y sustentable para mantener la independencia, soberanía y defensa nacionales, estableciendo la competencia de cada actor estatal. Es una consideración estratégica.

Como ***instrumento de análisis***, y en una ampliación de la noción jurídica[2], con el fin de recuperar una dimensión política actualizada, proponemos la siguiente aproximación: **La**

[2] Conforme al artículo 3 de la Ley de Seguridad Nacional: "Para efectos de esta ley, por seguridad nacional se entienden las acciones destinadas de manera inmediata y directa a mantener la integridad, estabilidad y permanencia del estado mexicano, que conlleven a:

i. La protección de la nación mexicana frente a las amenazas y riesgos que enfrente nuestro país; ii. La preservación de la soberanía e independencia nacionales y la defensa del territorio; iii. El mantenimiento del orden constitucional y el fortalecimiento de las instituciones democráticas de gobierno; iv. El mantenimiento de la unidad de las partes integrantes de la federación señaladas en el artículo 43 de la Constitución Política de los

seguridad nacional es la condición de un Estado, que estratégica y armónicamente articula y desarrolla sus elementos fundamentales, de acuerdo al equilibrio de sus fines y medios, para sustentar la permanencia de su poder nacional soberano, con relación a su interés y objetivos nacionales. Es una noción que considera lo multidimensional en sus diversas expresiones, que articulan una visión analítica, descriptiva, comprensiva y explicativa.[3]

Esta última *definición analítica* de seguridad nacional, que proponemos como punto de partida, presupone *elementos y relaciones* que describen y vislumbran el despliegue reflexivo, para una mayor comprensión y explicación del fenómeno de la seguridad nacional. De tal forma que:

- La seguridad (nacional) es considerada como una condición para el desarrollo (nacional).
- Otorga a lo estratégico, como vital, fundamental y crucial, un peso fundamental para el desarrollo de los elementos estatales (tales como el territorio, pueblo, gobierno y los valores nacionales).
- Atiende el equilibrio de los fines y los medios disponibles en el Estado. Determinando los objetivos y metas de acuerdo a los recursos existentes y potenciales, propiciando la prevención y la prospectiva.
- Considera y Defiende su poder nacional, para sustentar la soberanía nacional, el interés nacional y sus objetivos nacionales (Por lo que considera su posición y situación en un mundo globalizado, a la vez que presupone la competencia de otros Estados, naciones, actores, poderes, soberanías, intereses y objetivos).

En suma, esta aproximación conceptual permite la ponderación comparativa de la situación que guarda el Estado en sí y en su relación con otras entidades, propiciando la intervención para desarrollar sus fortalezas y disminuir sus debilidades y amenazas, en un claro momento de oportunidad.

Repensar la CiberSeguridad Nacional en México

Este esfuerzo reconceptualizador de la seguridad nacional mexicana, conlleva la posibilidad de disminuir los errores tradicionales en la teoría, que tienen costos altos en la práctica, por su desfase de atender problemas en el funcionamiento de la gobernabilidad y en la demanda para resolver necesidades, intereses y deseos de la sociedad.

Estados Unidos Mexicanos; v. La defensa legítima del estado mexicano respecto de otros estados o sujetos de derecho internacional, y vi. La preservación de la democracia, fundada en el desarrollo económico social y político del país y sus habitantes."

[3] Vid la amplia discusión del tema en el libro del autor: **Poder y Seguridad Nacional**, CESNAV-17-Instituto de Estudios Críticos-Fundación para la Democracia y el Desarrollo, México, 2014, 582 pp.

Las dificultades de dichas situaciones, provienen de una concepción de la seguridad nacional limitada –ya sea en acciones, modelos externos o visión parcial- que se refleja en las operaciones de sus diversos campos y en las respectivas políticas púbicas, así como en la carencia de soluciones por falta de atención o simple crecimiento de problemas nacionales.

La definición jurídica mexicana actual, registrada en la Ley de Seguridad Nacional vigente y otros documentos jurídicos rectores en la materia, obliga a **repensar**, desde su origen conceptual, jurídico y político, un nuevo alcance y sentido de Seguridad Nacional. Que **incida** en una Política de Estado. Que impulse el desarrollo potencial existente.

En la mirada geopolítica ocurre la necesidad de actualizar la CiberGeoPolítica mexicana, acorde al desarrollo global y tecnológico, para prever riesgos y amenazas.

II. Nueva visión de la Inteligencia Estratégica

Los límites de mi lenguaje son los límites de mi mundo.

Ludwig Wittgenstein

Recordemos que la información en sí no es poder, con su tratamiento genera conocimiento para sí y tiende a lograr un Poder, que se articula bajo diversas mediaciones en el Poder Nacional. Es un camino que muestra una ruta inteligente que va de la multitud de Hechos, a los Hechos Relevantes y a la determinación y provocación de Acontecimientos, que devienen en Datos, Registros y Fenómenos Políticos. Los cuales deben hilvanarse con una concepción constructivista de Políticas de Estado.

Un papel fundamental, juega la inteligencia en todas sus dimensiones, que implica análisis e investigación de conocimiento objetivo, para cursos de acción y toma de decisiones.

Establecer y promover **lo estratégico** es una determinación de todo Estado que desea competir e insertarse en lo global, con un claro proceso de racionalidad entre fines-medios, actores-factores, información-operación, prevención-prospectiva y global-nacional-local; estos binomios proveen de los recursos que el tomador de decisiones debe considerar para instrumentar una política de Estado.

Ponderemos la relación **Información e Inteligencia:**

Es común escuchar la idea de que ***la Información es…poder.*** En efecto, la información genera cierto poder…pero, ni toda información, ni el mismo tipo de poder. Así, **la información no genera poder**, sino más bien la información puede conducir a cierto tipo de conocimiento que, con **uso adecuado** y en determinadas circunstancias, **puede lograr poder**.

El papel del analista de inteligencia, es vital, estratégico, pues no sólo **analiza** la política, el Estado o el poder, el individuo y la sociedad, las circunstancias que les rodean, las fuentes de información; realiza estimación de un dato, hecho, fenómeno, enunciado, afirmación o

hipótesis y el discurso que emite un actor relevante, sino que hace sus reflexiones, análisis e interpretaciones y propone ciertos cursos de acción posible, para el logro de fines determinados. El análisis institucional se asocia a la toma de decisiones, surgen aquí amplias posibilidades de retroalimentación.

Este proceso analítico requiere de **Elementos y Relaciones** en la ruta de la Información. La forma en que se determina, al ubicarse en el tiempo y el espacio. Los distintos cruces establecen una matriz que configura el proceso del que surge todo objeto –estructura y resultado de información; el campo de relaciones que establece en su devenir y la construcción de hechos, datos o fenómenos, que tienden hacia un horizonte, con la dimensión tecnológica global. La **CiberInformación** despliega el mismo camino, utilizando infraestructura y saber informático.

Inteligencia

La voz ***Inteligencia***, posee polisemia significativa que obliga a determinar su sentido. El discurso lo permite. Proviene del latín *intelligentia*, como una facultad de comprender, de conocer, que se relaciona con la posibilidad de comprensión, conocimiento, habilidad y destreza.

Posee también una vinculación con las ideas de correspondencia (relación) secreta (del latín *secretus*), de algo que se mantiene oculto, que debe guardarse, o permanecer en reserva, que forma parte del arcano, que es una cifra, a la que rodea cierto misterio, que se muestra silencioso, que no es visible de inmediato, que tampoco no es aparente, sino más bien disimulado.

Esta característica, origen y destino en la inteligencia, da perspectiva de duplicidad, una re-formulación binómica, que le acercará a sus adjetivos como inteligencia militar, civil, estratégica, financiera, comercial o diplomática.

Detenta varios alcances que configuran su sentido con cierta tensión, oposición, negación, diálogo, otredad, disyuntiva, dilema. Que la muestra como es. Que le establece un espíritu agonal olímpico. Una inteligencia que siempre demanda más, ser mejor, más veloz, más fuerte, más resistente, más efectiva.

Una idea que le acerca al Dios Jano, especie de santo patrono de la inteligencia. Por su doble rostro que contrasta con el tiempo. Una mirada al pasado y al futuro, a la historia y al porvenir, desde un presente instantáneo.

Bajo esta dicotomía de utilidad entre la información y la inteligencia, muchas veces la primera sirvió para ocultar a la segunda y, la segunda cobijó un quehacer de indagación informativa.

En los inicios de esta relación, desde los tiempos bíblicos hasta los momentos de conquista y de guerra, la información era escasa, limitada, corta y muchas veces

inventada, que no necesariamente deducida. Era un juego de espejos en donde triunfaba el más informado.

Hoy día existe demasiada información, requerimos de sistemas de análisis que permitan una mayor y mejor explotación. La CiberInformación como apoyo para el análisis. Asistimos a una **Nueva Visión de lo real físico y presencial, a lo imaginario virtual, lo simbólico,** que repercute en el sujeto y el objeto de conocimiento, de acción política.

Lo Tecnológico está inscrito en los procesos que corren, de un medio ha devenido fin. Los tiempos actuales, preñados de tecnología, varían en términos diacrónicos y sincrónicos, en su cercanía en el tiempo y en el espacio, en la forma que la globalidad ha permeado de instantaneidad los fenómenos de la información. La manera en que transforma la vida de los individuos y las instituciones, la forma de convivir, el nuevo poder.

Una situación estratégica en que las redes de comunicación, privadas, gubernamentales o sociales nos muestran que, en la actualidad globalizada y de impulso a una sociedad informatizada, el problema no es la información, sino la capacidad para su interpretación e integración en un sistema que genere resultados definidos.

Hay una mayor cantidad de datos, de flujos informativos, por diversos dispositivos, que implica más dispersión de objetivos. Evaluarlos es complejo, casi imposible. Demanda reflexión racional. Se contrapone a lo urgente, al era para ayer. Lo cual demerita la actividad de análisis de la información, al margen de las particulares burocratizaciones o áreas de control de la información.

Las complejas magnitudes, obligan a restructurar el saber y a una clasificación constante, por ejemplo, EU generó en la primera Administración Obama, un promedio de 50 mil informes por año, con 1.7 millones de comunicaciones interagencias, relacionadas con información para la inteligencia y la seguridad nacional. La relación del trabajo de análisis con los usuarios-consumidores de estos productos, requiere un claro esquema estratégico de prioridades para mantener vigente su rol preventivo y su actuación en la dinámica mundial.

Los informes denominados vitales, en y para una organización política, que no generan estimaciones de inteligencia, esto es, cursos de acción viables, poseen fallas del sistema de información y en su propia inteligencia. Generan desgaste institucional y costos al presupuesto público, que ante la necesidad de resultados inmediatos, chocan con el proceso de toma de decisiones.

Información para la Inteligencia

Partimos de una Idea básica: el análisis de información nutre la inteligencia estratégica. Sin información clara, precisa, distinta, completa y oportuna, la inteligencia es afectada, disminuida en su acción.

Dicho análisis de información para la inteligencia matiza, ubica y reconstruye acontecimientos, datos, hechos, fenómenos; los expone espacial y temporalmente, establece secuencias lógicas encadenadas de futuros e inmediatos procesos de acción; racionaliza la información con relación a sus fines y medios, busca apoyar la toma de decisiones, de manera objetiva, realista y factible. En una economía favorable del costo-beneficio.

Con la información no se cancelan errores posibles, pero se busca evitar que se cometan por ignorancia, inexperiencia e incompetencia. Es la utilidad del proceso y el resultado, de la relación entre lo estratégico y lo táctico-operativo.

Predomina en el medio de seguridad, que la Inteligencia estratégica es un conocimiento para salvaguardar el bienestar nacional. Es la idea inicial que Sherman Kent planteara en su libro clásico sobre la inteligencia estratégica norteamericana. Ahí está descrito el paradigma original de la inteligencia, en el ámbito occidental y con la plena hegemonía estadounidense, después de la II Guerra Mundial y del fin de la guerra fría. Es claro que los intereses tampoco desaparecen.

La Inteligencia estratégica puede ser comprendida como actividad (proceso), fenómeno (producto), u organización (estructura). Estos componentes poseen diversas variables, acciones y mecanismos que movilizan el análisis de la información y su aplicación en tareas de inteligencia. Acontecimientos relevantes que han colocado este proceso como prioritario, fueron la caída del Muro de Berlín, la desintegración de la ex URSS, el ataque terrorista del 11 de septiembre en Nueva York, en pleno territorio de EU, la competencia por productos energéticos estratégicos y el posicionamiento de China en el nuevo tablero mundial; desde luego, las manifestaciones en contra de las políticas neoliberales y de afectaciones a derechos gremiales y humanos entran también.

Reflexión sobre Inteligencia Estratégica

En el proceso de determinación de **lo estratégico**[4], está inscrita la visión de racionalidad que un Estado posee, los elementos de información que guían sus procesos de política, le permite considerar los elementos a su disposición, para que su poder nacional sea repensado conforme a los elementos mediadores que intervienen: fines-medios; actores-factores; prevención-prospectiva; información-operación; global-nacional; nacional-local. Ello establece las aproximaciones significativas a la tarea informativa y de operación de inteligencia. A la oportunidad estratégica de medir el alcance y limitación de su poder nacional.

[4] *Vid* del autor el ensayo "Sobre el discurso estratégico", primera parte, **en Revista del Centro de Estudios Superiores Navales**, julio-septiembre 2013, Vol 34, Número 3, pp. 6-21 y la segunda parte en el número siguiente.

Las acciones reagrupadas en las constelaciones del *Decir, hacer o pensar* son fórmulas aglutinadoras de lo que los actores actúan en observación de cada au(c)tor, estructura, proceso o resultado realizan.

De acuerdo a diversos acontecimientos globales y nacionales, ya mencionados con anterioridad, la determinación de objetivos de seguridad y desarrollo ha variado. Los métodos también. La versión clásica del interés científico del objeto y el método son cobertura ideal para expresar y mantener los intereses estratégicos y nacionales.

El interés por hurgar en la vida privada de ciertos personajes ha entrado a la farándula del espectáculo informativo, hoy nos atañe más aún, las relaciones que establece, las decisiones que toma o puede tomar, la valoración de estas decisiones. Una información relacional basada en la concepción de lo estratégico.

Así, se atienden pormenorizadamente, los sujetos que inciden o pueden afectar la seguridad nacional. Los delincuentes de todo tipo. Los sujetos que están más cercanos a los denominados riesgos de seguridad. La vigilancia cotidiana del enemigo, en todo tiempo y lugar. Y desde luego, quienes toman las decisiones, de gobierno, de empresas.

El registro sistemático de un hecho significativo: se ha pasado de una fórmula metodológica persecutoria, amenazante, interventora y de complicidades, a un nuevo estilo, cercano al investigador especializado, más higiénico. Con ventajas y desventajas y sin que se haya eliminado la primera. Hemos entrado a un proceso virtual en el que se despliegan la Información, la Inteligencia y la Ciberseguridad. Esta última, concebida como la nueva Quinta Dimensión, después de los espacios estratégicos de tierra, agua, aire, radioeléctrico. Cobra fuerza en la dimensión del poder internacional.

La triple relación entre información, inteligencia y ciberseguridad, responde a la Geopolítica contemporánea, está determinada por los avances globalizadores y el constante desarrollo tecnológico. No hay forma de soslayarla.

En la situación actual: dominan el escenario los actores de la Globalidad, impersonalizados que deben determinarse, siguiendo el guión de la competencia, en una acción de instantaneidad, con propuestas *kleenex*, de úsese y tírese, sean sujetos, cosas, propuestas, proyectos o políticas.

En este contexto generalizado, la información y la inteligencia son relevantes, fundamentales, indispensables, necesarias y únicas. El *Plus* es ***Io Ciber***, de ahí la continuidad en el espacio-dimensión de la Ciberinteligencia. Lo ciber es el reencuentro con un mundo nuevo.

La evolución de la información y de las áreas de inteligencia, han creado una tipología de inteligencia; de la humana a la tecnológica, una inteligencia virtual para conquistar el ciberespacio. Los dispositivos han cambiado pero las formas y los contenidos permanecen.

Esta dinámica del cambio innovador confronta la usual permanencia de la doctrina de inteligencia. En donde concurren los nuevos paradigmas y problemas que buscan modificar de tajo la doctrina de inteligencia y contrainteligencia vigentes, resguardada por todos. Una reformulación conforme a las necesidades de las potencias, del *hegemón* norteamericano o de la alianza chino-rusa, no necesariamente acorde con los cambios requeridos en cada país o gobierno. A una confrontación entre militares y civiles o dentro de ambos, incluso ahí entre los conservadores y los renovadores, los desarrollistas y los securitólogos. Es un proceso político reflexivo, de carácter teórico de gran impacto práctico. La *praxis* de la inteligencia.

CiberSeguridad en Lucha Doctrinal

Estos aspectos conllevan a una situación de conflicto doctrinal. Donde mantener la protección del conocimiento y la actividad sensible, sin perder la flexibilidad de la adquisición de lo nuevo y actual, provoca una apertura desafiante de lo virtual.

De una visión en donde el secreto tradicional, la confidencialidad y la reserva requieren renovarse ante el desarrollo tecnológico, que rompe barreras de control concreto y obligan a desarrollar un nuevo tratamiento sobre asuntos confidenciales o de la visión secreta, sobre los asuntos estratégicos de Estado.

Publicitar el uso de Estado, gubernamental o político-partidario-privado de la información, es una vertiente que se vincula con la rendición de cuentas, la lucha contra la corrupción y la impunidad; la democratización de lo público nos conduce a la necesaria readaptación a la ciberseguridad, de toda la legislación y de la ac ción gubernamental primero, y en seguida en la sociedad en su conjunto. Sobre todo ante un mayor uso de tecnología satelital, digital, inteligente.

Por lo que es menester impulsar un proceso de actualización a los tres poderes públicos, a los tres niveles de gobierno, a toda la sociedad para crear y utilizar redes de información más amplias, asegurando y evitando riesgos en la información misma. Una situación que rememora la evolución de los teléfonos móviles (del tamaño ladrillo a lo manual), del fogón a la estufa, de la píldora y el condón a los cambios de sexo, de los libros a los *e-books*. Con acciones y vehículos no tripulados por humanos, para obtener resultados más efectivos, en todo tipo de operaciones, en tiempo y forma.

Con la construcción y uso compartido de plataformas de datos y tecnología, de medios de comunicación y redes sociales, que proporcionan información o **inteligencia en tiempo real**, que afecta las respuestas (gobierno-empresa-academia), accedemos a una inteligencia artificial de uso cotidiano. Con la respectiva prevención, pues no necesariamente la información que se transmite en medios y redes sociales es verdadera. Al respecto ha mencionado recientemente Umberto Eco, al referirse al cuidado e impacto de la sociedad de información y comunicación, que fluye en las redes sociales, y donde se intercambian opiniones de un premio nobel como de un ocurrente cualquiera.

Doctrina de Inteligencia/CiberInteligencia

La discusión doctrinal informal que se ha iniciado en determinados grupos académicos y gubernamentales, en las fuerzas armadas y las áreas de seguridad, sobre conceptos, procesos, procedimientos y políticas considera que:

- La determinación de los objetivos de inteligencia es una decisión política.
- Responsabiliza a quien dirige la seguridad nacional y a quienes la operan y hacen posible, en la teoría y en la práctica.
- En México corresponde al Presidente de la República y a su gabinete de seguridad nacional, al gabinete legal y ampliado, al Consejo de Seguridad Nacional, que responden a las directrices del Ejecutivo federal.
- Pueden ser convocados los representantes o miembros de los otros poderes públicos (legislativo y judicial) y de los otros niveles de gobierno, estatal o municipal; así como personajes de la sociedad civil, organizada o no, nacional o internacional.
- Dependiendo del **caso y de la situación** misma en términos de su **gravedad o urgencia**; o de su antagonismo, como amenaza o riesgo para la seguridad nacional.
- Bajo estas características, la **relación doctrinal Inteligencia/CiberInteligencia,** está inscrita en diversos campos del poder nacional. Se reconoce que en el análisis cibernético, la prevención y la prospectiva son elementos que acompañan, nutren y corrigen, a la información y la inteligencia estratégicas.
- Los diagnósticos, estrategias, políticas, planes y programas, gozan de los productos de inteligencia, de las estimaciones que surgen de los sistemas de información e inteligencia y, cuando no los tienen, no sólo sufren los actores, sino los autores, participantes y observadores.
- Surgen, de manera irreparable, las pérdidas, derrotas, deterioros o desajustes, en políticas públicas, en las carreras políticas de personajes encumbrados, en tomas de decisiones tardías, que provocan un menor desarrollo nacional para la sociedad, en déficit público, caída de la inversión, en cierres de empresas, en conflictos sociales, en alejamientos de aliados políticos, en la falta de involucramiento de los propios aliados, en suma en la afectación al desarrollo y la seguridad de la nación.
- En este contexto, la discusión doctrinal no es un ejercicio terapéutico o de ocio académico-burocrático, es la oportunidad estratégica de analizar alcances y límites de la relación inteligencia-ciberinteligencia.

Tempo Real, Espacio Virtual

Por lo anterior, se debe impulsar una reflexión a fondo, amplia y sistemática, de que nuestras viejas categorías espacio-temporales han cambiado con el desarrollo tecnológico, revalorar las posibles sustituciones, el impacto desde lo global y en lo local. Han quedado atrás las tradiciones de inteligencia humana, de espionaje personalizado, que se han sustituido por técnicos de la informática, *hackers*, diseñadores de sistemas y analistas de lo complejo.

Los **Modelos Románticos,** del agente de campo separado de quienes trabajan en gabinete han superado el consumo popular, de gran impacto e iniciativa en aprendices de brujo de la inteligencia. Rodeados del misterio, distracción y legitimidad de acciones maquiavélicas. Que aparecen en alternancias gubernamentales, cambios sexenales o relevos institucionales, en las instancias de seguridad nacional y áreas de información e inteligencia; y que sucumben, al fin personajes nuevos e inexpertos, al ficticio canto de sirenas. Resonancia en obras, autores y personajes de ciencia ficción cobran realidad, como los expuestos por:

- David Cornwell conocido como John Le Carré (y sus héroes Alec Leamas y George Smiley, **El espía que surgió del frío**).
- Robert Ludlum (con el ameritado **Jason Bourne**).
- Graham Green (con los personajes **del Tren de Estambul o el Expreso de Oriente, Nuestro hombre en La Habana**, el profesor **de El agente secreto; El Americano Impasible; Scobie y el sacerdote de El poder y la gloria**).
- Ian Fleming (con el famoso archiespía con licencia para matar, el **007**, Bond, James Bond).
- Los Agentes de Cipol, Solo y Kuriaki o el clásico de Misión Imposible.
- Los de desarrollo analítico y mental como **La carta robada** de Edgar Allan Poe;
- El detective belga Hércules Poirot de Agatha Cristie. Irónico y trágico.
- El inspector Jacques Clouseau, que expone el mito divertido y crítico de **La pantera rosa**.
- El gran analista, de la vía deductiva, el amigo del médico John Watson, el elementalista **Sherlock Holmes**, personajes de Sir Arthur Conan Doyle.

Estos modelos configuran personajes y situaciones que se han actualizado en la vida del espectáculo, de los medios y se vuelven velos que nublan la verdadera visión, pueden ser considerados como metáforas del quehacer inteligente o como creadores de ciencia ficción para la futura realidad**.** Una especie de Matrix re-evolucionada.

Inteligencia Humana, Antigua y Contemporánea

Los nuevos prototipos de la inteligencia, son ahora, expertos en el manejo de sistemas de información, redes sociales, sistemas complejos y tienen gran impacto en los medios de comunicación y en la población, con los temas relacionados al *espionaje:*

La actual difusión pública de acciones de investigación y espionaje, nos ha mostrado no sólo situaciones-límite en el mundo virtual, sino también las situaciones de realidad y demanda en un mundo en competencia, que requiere de mayor y mejor información, de organizarla en un eficaz sistema de inteligencia, de adjetivarla como estratégica, para acuñar la relevancia que poseen. Incluso se puede observar en tiempo real, los ataques o supuestos ataques cibernéticos.

Estos actos, han expuesto la debilidad del imperio en las tareas de información e inteligencia, los descuidos en la seguridad de la información y la contrainteligencia, la

presentación de personajes que son vistos, por algunos, como traidores y por otros, con una gran capacidad de intervención que califican de heroísmo, desde los miembros *hackeadores* de Anonymous, hasta las entregas del militar norteamericano Bradley Manning y el creador de *wikileaks*, Julian Assange, hasta las revelaciones del espionaje de amigos y aliados por la Agencia de Seguridad Nacional, hechas por Edward Snowden. Y sus correspondientes señalamientos y acciones en los gobiernos, en las organizaciones y agencias de inteligencia y seguridad.

Ellos han mostrado la importancia del ciberespacio, de las oportunidades y fallas del sistema de inteligencia. De la nueva guerra por conquistar el mundo virtual.

En los hechos, las anteriores situaciones críticas de manejo y difusión de información, dados a conocer al público, **muestran una Inteligencia penca.** Que en la teoría y la práctica, necesitan ser atendidos de inmediato, cubriendo los **requerimientos para lograr fines o medios necesarios para su éxito.**

La actual situación Cibergeopolítica internacional, ha mostrado la existencia en México de una limitada visión Cibergeoestratégica, producto entre otras cuestiones de *una Inteligencia estratégica penca debido a que*:

- La información estratégica debe contribuir a una inteligencia estratégica y esta se encuentra alejada de quienes deben tomar las decisiones fundamentales del Estado.
- Se nutre de investigación, análisis, discusión, elaboración de documentos, participaciones y debates públicos, proyectos de estudios, formación y profesionalización de cuadros, creación y fortalecimiento de centros estratégicos, nacionales e internacionales, de infraestructura informativa e informática que apoya la recolección y la difusión de los productos de inteligencia. Todo lo cual ha sufrido mermas presupuestales para un pleno desarrollo.
- No se ha fortalecido conforme a la necesidad que la globalidad impone, obteniendo resultados menores en la inserción internacional.
- Sin recurso humano, sin inteligencia humana, la inteligencia estratégica está penca, tunca, chimuela, tuerta, coja, débil e incompleta y, las más de las veces, disfuncional de los fines, objetivos y metas de seguridad nacional.
- Bastaría señalar el nivel de la modesta comunidad que labora en estas áreas, los instrumentos de apoyo con que cuenta, la limitada capacitación y el balance en general, sobre todo si se compara no con los países desarrollados, sino con aquéllos que tienen un desarrollo similar. De tal forma que, sin conexión adecuada a la red, a la internet, no hay posibilidad de crear cibercomandos o una ciberseguridad que de certeza.
- Sin inteligencia tecnológica, no hay CiberInteligencia, la inteligencia estratégica está disminuida, no amplía su radio de acción, el alcance de los sentidos pierde su fortaleza, se pierde la complejidad evolutiva e innovadora del todo, desaparecen oportunidades, se vuelve menos competitiva.

- Los recursos económicos, públicos o privados, para invertir en tareas de inteligencia y seguridad no debieran escatimarse. Es la incomprensión del sentido de lo estratégico.

Navegando en la **nueva inteligencia,** producto de una **nueva realidad sociotecnológica.** Observamos que la **Nueva Inteligencia como CiberInteligencia** para la **Ciberseguridad de la Nación** está constituida por un esfuerzo de Sísifo, por tejer la tela de Penélope que las une en lo nacional al considerar:

- La asunción de que un sistema de información y de inteligencia consta de procesos funcionales de recolección, análisis, contrainteligencia y acciones encubiertas que se relacionan con las políticas de seguridad nacional.
- La afectación o modificación de uno de estos elementos altera indiscutiblemente a los otros. Es un círculo virtuoso que cuando se desconoce o se transforma, sin fines específicos, se vuelve en un círculo vicioso.
- Hay necesidad urgente de recursos humanos especializados, de tecnología de punta para favorecer los procesos de análisis y las operaciones, de realizar inteligencia en tiempo real con el respaldo tecnológico y cobertura satelital. De actualizar mecanismos, procesos y dispositivos de ciberinteligencia.

CIBERSEGURIDAD

Cabe destacar que una nueva realidad propicia una **Nueva Jerga Lingüística, que nos obliga a actuar de forma distintiva.**

Desplegando en las palabras los usos de mayor y mejor alcance, de explicación y comprensión, en donde está la Evolución y Desarrollo del Lenguaje, como preludio del cambio societal.

Ciber es un prefijo de gran impacto, como **neo**, neorrealistas, neoliberales o **wiki**, como wikipedia, wikicomunicación, wikileaks o como **pseudo**, pseudoestudiantes, pseudomaestros, pseudolíderes, pseudopadres.

Lo **ciber/cyber**: expresa el ámbito asociado y dependiente, relacionado con, o que involucre computadoras (y otros dispositivos) o redes informáticas (internet). En 1991, se difunde el primer uso de la palabra. A la fecha ha originado una Nueva Familia de palabras:

- Cibernético, ciberespacio, ciberdimensión, ciberfuerzas, ciberataque, ciberhostilidades, ciberconflicto, ciberguerra, cibercomando (EU contaba en 2014, con 6,200 personas en 133 equipos de trabajo; China contempla entre sus usuarios y huéspedes, 20 veces más, y analizar lo que está en la ***dark web***), ciberinteligencia, cibermisión, ciberactivismo, hacktivismo (hackear y activismo), ciberacoso, ciberespionaje, ciberterrorismo, ciberbulling, ciberpolítica, ciberseguridad (de la nación), ciberdefensa, ciberestrategia, ciberterreno, cibercomponentes, ciberResilience, entre otras muchas más palabras.

Cada día avanzamos del **mundo y realidad actual**, presencial, (con espacio fisico, con tiempo pasado-presente futuro) al **cibermundo**, virtual, aespacial y atemporal.

Dando origen a la **Quinta Dimensión, al ciberespacio,** que asimila y articula las dimensiones de Tierra, mar, aire, espectro radioeléctrico y, desde luego el CiberEspacio, con sus respectivos **Elementos y Relaciones.**

En términos generales, se agrupan **al CiberEspacio, tres familias de palabras: *CIBERESPACIO**: CIBERNÉTICA, CIBERSEGURIDAD, CIBERPOLÍTICA.*

	CIBERESPACIO	
CIBERNÉTICA	**CIBERSEGURIDA**	**CIBERPOLÍTICA**
Lo digital-Virtual, ciberDimensión, CiberInfraEstructura, CiberComponentes, CiberTerreno, CiberNaturaleza, InteligenciaArtificial, Redes sociales, computadoras, teléfonos inteligentes, Web, e-mail, facebook, tweeter, instagram	**CIBERDEFENSA:** CiberInteligencia, CiberEstrategia, CiberComando, CiberFuerzas, CiberMisión, CiberGuerra, CiberAtaques, CiberHostilidad, CiberConflicto, CiberTerrorismo.	CiberActivismo, CiberAcoso, CiberBulling, CiberEmpresas, Ciborg, Nueva CiberLegislación, CiberCultura, Ciber-Resilience
Y las que surjan hoy		

CiberSeguridad de la Nación

Para actuar con cierta libertad y autonomía en el mundo global actual, requerimos CiberInteligencia y Ciberestrategia con posibilidad de una CiberGeopolítica para avanzar en una CiberSeguridad funcional y efectiva.

Desde la historia de cada país, surge la idea-propuesta que otea el horizonte, un futuro que ya es presente, vincula ***lo geopolítico con lo geoestratégico***, de luchas y alianzas, de desarrollos y seguridades, que reconoce la relevancia de ***la información y de la inteligencia, para alcanzar la propia CiberGeoPolítica.***

La ciberinteligencia concebida como un trabajo profesional, como una tarea que debe ser realizada por profesionales. Con una ruta de control sistematizada y confiable. Con programas de desarrollo que atiendan lo urgente, lo relevante, lo formativo.

A nivel gubernamental y estatal, la información e inteligencia y la Ciberinteligencia con una Ciberestrategia, son necesidades que deben ser cubiertas para lograr metas y objetivos, dentro y fuera del país, para evitar sorpresas o ser atropellado por la competencia globalizada o los intereses de otros AuCtores, estados o países.

CiberSeguridad de la Nación, como una política de Estado, para tomar las mejores decisiones en el momento y lugar oportunos, manteniendo ventajas estratégicas y disminuyendo posibles costos. Para lograr el desarrollo y bienestar nacional.

Conforme al modelo jurídico mexicano, partimos de los principios de legalidad y legitimidad, se requiere de una reforma constitucional que propicie una **Nueva Legislación en Ciberseguridad y Ciberdefensa.**

Que atienda en el ámbito **internacional,** tanto el actual Convenio sobre Ciberdelincuencia de Budapest como los constantes Seminarios y Reuniones de actualización y formación legal, técnico y en todas las diversas materias relacionadas con lo ciber.

En el aspecto **regional,** debe considerarse el Convenio Iberoamericano de Cooperación sobre Investigación, Aseguramiento y Obtención de Pruebas en Materia de Ciberdelincuencia

Y en lo **nacional,** la actualización en los aspectos constitucionales y los documentos rectores como el Plan Nacional de Desarrollo 2013-2018, el Programa para la Seguridad Nacional 2014-2018 y los Programas Sectoriales de la SeGob, SEMAR, SEDENA, SRE, SCT, PGR, entre otros[5].

Condiciones de posibilidad de una CiberEstrategia de México.

La oportunidad, que la necesidad establece en la dimensión de la ciberseguridad permite contribuir a la articulación y conducción política del Estado, considerando las consecuencias posibles y probables de una dirección ciberpolítica en un ambiente determinado.

Como política de Estado, una ciberestrategia puede mantener o modificar *la dirección y la velocidad*, del desarrollo y la seguridad nacional, aunque ella no es responsable del uso, alcance y sentido de éstas. Pues tiene un carácter instrumental. La observación desde la CiberGeopolítica sugiere claridad extrema en el análisis, pues aunque conserva el estilo propio de la Política, lo hace en y sobre una estructura CiberEspacial y suma a todas las políticas aplicadas en el espacio y tiempo físicos.

[5] Vid del autor, "Consideraciones al Programa para la Seguridad Nacional 2014-2018", **Examen**, No. 230, año XXIII, mayo 2014, pp. 29-39

México debe re-evaluar la mirada y condicionamiento de una Ciberpolítica fundamental y, desde luego, generar una concepción Cibergeopolítica, Cibergeoestratégica y Cibergeoeconómica.

El saber cibernético (con dispositivos e infraestructura estratégica) es su fuerza, como en su momento lo fueron el ferrocarril o el buque.

¿Cómo se logra la CiberSeguridad?

Con mayor y mejor CiberInformación. Con CiberInteligencia estratégica. Con conocimiento de Geopolítica, Geoestrategia y Geoeconomía aplicadas a *lo ciber*:

- Con una toma de decisiones correcta –individual, social e institucional- en tiempo y forma. Para el beneficio e interés nacional.
- Con una organización social basada en el bienestar colectivo, popular o nacional.
- Con instituciones políticas que respondan al interés de las mayorías sociales.
- Con grupos de emprendedores que promuevan la generación y distribución de la riqueza social y no sólo sus intereses particulares o de grupo y que genere fábrica de pobres.
- Con planeación, aprovechamiento y desarrollo productivo y sustentable de nuestros recursos humanos y naturales.
- Con la aplicación, respeto y cumplimiento de las responsabilidades sociales, institucionales y constitucionales.
- Con la aplicación de sanciones y penalidades para quienes no cumplan con las responsabilidades que les corresponden.
- Con énfasis de una cultura de la responsabilidad, que premie el esfuerzo colectivo y castigue la corrupción, el abuso, el fraude y la impunidad.

Para lograr este nuevo estadio requerimos una **información social comprometida** con:

- Una Nación, con claridad de fines y conocimiento de los medios para alcanzarlos, en lo económico, político, social, militar, diplomático y tecnológico.
- Un Estado que haga del gobierno un instrumento de desarrollo.
- Un liderazgo político y económico responsable, con conocimiento de causa, que conduzca al logro de objetivos comunes, nacionales y regionales.
- Una participación ciudadana abierta, con oportunidades para todos aquellos que posean habilidades, conocimientos y actitudes, para sumar esfuerzos productivos nacionales.
- Una fórmula de generación educativa de cuadros en todos los niveles, para impulsar el desarrollo regional y nacional.
- Una estrategia de desarrollo democrático, participativo, incluyente, responsable, equilibrado y armónico.
- Hacer funcionar los mecanismos de consulta y acuerdo, que eviten ser tendenciosos o parciales y faciliten las decisiones de interés nacional.
- Mostrar y remover los obstáculos que pudieran afectar el desarrollo seguro de la estrategia nacional.

De lo contrario, sólo nutriremos **La visión Ciber-Negativa** de nuestra propia realidad social, favoreciendo la intervención de aquéllos que no desean la buena marcha de los asuntos públicos y sociales.

III. Riesgos y amenazas para la CiberSeguridad Nacional Mexicana

La vida es breve, el arte largo, la ocasión fugaz,

el intento arriesgado y el juicio difícil.

Aforismo hipocrático

Considerando la situación global, nacional y local, la seguridad en toda su multidimensionalidad actual, es el reto fundamental de los Estados-gobiernos-países. De impacto en sus sociedades.

Los riesgos y amenazas que han surgido, tanto como las oportunidades y desafíos, son amplios, diversos, complejos y en varios campos y frentes.

Cabe destacar, que el impacto en una sociedad informatizada y del conocimiento, provoca necesariamente un nuevo modelo gubernamental, de seguridad y justicia para el desarrollo –con inteligencia y operación- de coordinación, transversalidad y eficacia para lograr resultados que demanda la sociedad. Establecer las Políticas de Estado, como fórmulas y mecanismos de articulación política y social, para atender con decisiones estratégicas, tácticas y operativas; con oferta eficaz, eficiente y efectiva, la demanda urgente de la acción social. Es resolver antiguos y nuevos problemas con una visión de Estado, en un mundo globalizado.

Las condiciones actuales del mundo globalizado:

En política, se actúa para adquirir o mantener poder y, las actuales *realidades cibernéticas*, dan por supuesto la existencia real, verdadera e inobjetable, de la influencia de la tecnología, en el hombre y su comportamiento.

Las comunicaciones, en un sentido amplio, son actores y factores fundamentales para toda sociedad y, desde luego, determinantes en todo pensar geopolítico.

La Cibernética ha creado con su desarrollo el CiberEspacio, como la ***Quinta Dimensión***, cuyo significado y sentido está en integrarle un cierto y determinado valor, cuantitativo y cualitativo, que supera en tiempo, comunicación y difusión, la actividad humana real, presencial.

Entender el CiberEspacio significa una toma de conciencia de las posibilidades históricas y políticas de un lugar sin lugar, en tiempo real, no sólo como potencialidad-continente de bienes tecnológicos, materiales, espirituales o mentales.

Genera un cambio de valores, identidad, unidad y proyecto nacionales. De qué, cómo y para qué.

Tradicionalmente el mundo ha considerado lo espacial-temporal como los hechos histórico-políticos trascendentes. Desde el origen de las civilizaciones hasta la oportunidad de la sobrevivencia y del desarrollo. El conflicto no ha perdido su presencia. Hoy estamos en una etapa de cambio en el tiempo y el espacio. Lo cibertemporal y ciberespacial nos envuelve.

Entender la política de los estados como una política de posiciones (estables) es partir de una actividad racional, fin-medio o medio-fin, que posibilita todos los posibles planes por hacer, la construcción de un proyecto realista, que le permite una trascendencia autónoma, tanto en lo político, económico y militar.

Es reposicionar la geopolítica, la geoeconomía y la geoestrategia en un entorno global mundial fundamental. Una nueva mirada *ciber*. Que requieren todos los A(u)ctores.

Un punto en un territorio estatal con sus coordenadas de longitud y latitud, tiene diferentes significados según el enfoque, por lo que el concepto *posición* es relacionalmente estratégico, *posición o situación con respecto a qué…*Ello obliga a una mirada política relacional. Del individuo, la sociedad y el Estado.

Eso, que es estratégico, está cambiando, si no es que ya cambió, con el CiberEspacio. Afectando con nuevas CiberEstrategias.

En alcance globalizador y tecnológico propicia una mirada cibergeoestratégica de los riesgos y amenazas, desde México, del impacto Cibergeopolítico de algunos eventos actuales como:

- La **Crisis en Ucrania**. Su posible impacto en los flujos de energéticos hacia Europa, en su producción y distribución y, desde luego, el impacto en los precios del petróleo que afectarían los ingresos nacionales y pondría en una situación de crisis a la economía mexicana. La situación interventora de Rusia para mantener su salida al mar Báltico y controlar su Área de Defensa Estratégica ha movilizado fuerzas militares que generan reacciones en los países fronterizos y su aliado norteamericano
- El **Conflicto-crisis del Estado Islámico** en Siria e Irak, que provoca la reacción beligerante de los países afectados por la muerte de ciudadanos, sobre todo los inscritos en la órbita de la OTAN. Más allá de un conflicto de ideologías, los recursos estratégicos en juego y las posiciones internacionales en la zona, deben sopesar la relevancia de la industria bélica y el impacto en nuestro país, por nuestra posición fronteriza con EU, de la que irracionalmente el gobernador de Texas, en su aspiración presidencialista, ha convocado a la Guardia Nacional en su estado, para evitar supuestas filtraciones de miembros del Estado Islámico por nuestro país, impactando la política migratoria.

- El **conflicto en la Franja de Gaza**, con las dificultades propias y tradicionales entre los actores locales (Gobierno de Israel y grupo Hamás) y la posible intervención de las potencias dominantes y cercanas a cada uno de ellos, que podría propiciar una escala mayor en la zona y que pondría en crisis las relaciones mundiales por los aliados en juego.
- **Pandemia Ébola** en África y para el mundo; el problema de salud, de enfermedades y virus nos muestra la fragilidad y la limitación para su atención en muchas partes del mundo, aún cuando las autoridades mexicanas de salud han señalado que no hay posibilidad de que nos alcance, y que hay previsiones al respecto, no parece que sea una situación confortable cuando se valora la irradiación de los enfermos contaminados con dicho virus, hacia España o Estados Unidos y por qué no a México como país de paso hacia una mejor atención en Norteamérica.
- Conformación económica de **los BRICS**, el activismo desarrollado por China y Rusia en Latinoamérica, con la creación de un fondo económico para el desarrollo, ha colocado en una perspectiva de alerta a Estados Unidos, con la posibilidad de una política de endurecimiento que seguiría al abandono en que se han mantenido las relaciones. El cambio con Cuba y el Acuerdo Transpacífico, muestran un giro internacional que impulsa una mirada latinoamericana. El impacto geopolítico para México está en su limitada participación en este grupo de los BRICS que contrasta con el impulso de la Alianza del Pacífico, en donde China está en primer lugar. Las presiones a enfrentar no son menores y tienen que calcularse sobre el verdadero interés nacional.
- **Dificultades económicas en países europeos**: España, Grecia y Francia, la situación geoeconómica internacional muestra los vaivenes de las políticas neoliberales y el estrangulamiento de algunas economías nacionales europeas, situación que debe retomar el adagio “cuando veas las barbas de tu vecino recortar pon las tuyas a remojar”, pues el aspecto económico en México, a pesar de las amplias potencialidades de crecimiento y desarrollo, no logra cuajar aún.
- **Inseguridad en la información**, aquí resuenan los nombres de Assange, Snowden, este tema tiene un gran alcance Geopolítico, Geoestratégico y Geoeconómico, por el impacto en el ciberespacio y el espionaje industrial y político, que ha afectado las relaciones entre los aliados, colocando a EU en una situación de frágil colaboracionismo por algunos gobiernos como Brasil, Alemania, Gran Bretaña y México, que han expresado inconformidad diplomática y que no han obtenido respuestas satisfactorias.
- **Delincuencia Organizada Transnacional**, un actor y factor de poder real y de facto en muchas naciones latinoamericanas, en particular en México, sin embargo, la posible corresponsabilidad de los países consumidores de drogas como EU no ha estado a la altura de la circunstancia de riesgo y conflicto que el tema tiene. Los tráficos de droga, dinero, armas, personas, siguen en la ruta, con conflictos latentes en todo momento. La relación de México con EU sobre este tema ha tenido encuentros delicados como ocurrió con el exFiscal norteamericano y la otrora

operación “rápido y furioso”, que decidieron guardar información que vinculaba a las autoridades estadounidenses en la complicidad delincuencial, bajo el ropaje de una acción encubierta, situación similar ocurre con algunos elementos de la Guardia Nacional o de Inmigración y Aduanas.

Este registro de algunas situaciones internacionales actuales, ameritan una lectura Cibergeopolítica, Cibergeoestratégica y Cibergeoeconómica de México, muestran la necesidad de conocer con Ciberinteligencia y capacidad, preventiva y prospectiva, y apoyar así la toma de decisiones.

CiberAnálisis

Desde luego que **el desarrollo tecnológico nacional es fundamental en la CiberSeguridad,** que en su proceso debemos mantener una caracterización jánica hacia el exterior sin descuidar el interior nacional.

La mirada vigilante e inteligente de México debe enfocar una **regionalización geoestratégica, geopolítica y las áreas funcionales** en su Agenda Nacional de Riesgos o de Seguridad, con prioridades claras, distintas, específicas y comprensibles para todos, que contemple los actores y factores, entre los cuales debieran ser considerados como tópicos relevantes de una agenda mínima los siguientes:

- Estados Unidos.
- Frontera Sur-Sureste con Centroamérica y el Caribe.
- Bloques geoeconómicos del Pacífico asiático y europeo.
- Regiones y países de gran inestabilidad política y social.
- La situación nacional interna.
- El desarrollo nacional
- El desarrollo tecnológico.

En este esquema la atención se concentra en lo nacional, desde aquí se observan los elementos que caracterizan la situación en que se ubican las diversas relaciones de México. Dado el carácter dinámico, los a(u)ctores mantienen una política relacional que los ubica y determina, que los posiciona y reposiciona constantemente.

- **Estados Unidos**. Es la potencia estratégica más fuerte, nuestro vecino al norte, con la frontera física y los cruces de personas y de mercancías más importantes.

  La economía política de nuestro país está vinculada asimétrica y estrechamente al desarrollo y seguridad estadounidense, la influencia social que existe, abarca diversas manifestaciones a favor y algunas en contra del modelo norteamericano, que tienen que ver con la ubicación en la escala socioeconómica nacional y en la participación política e ideológica. Los diversos y necesarios tráficos de ambos lados (armas, drogas, dineros, personas, mercancías, saberes) fomentan el comercio, provocan competencia y alejan la confianza recíproca. El ciberanálisis de los Estados Unidos nos brinda la oportunidad de considerar el grado de desarrollo

en todo lo concerniente a lo *ciber* y al potencial necesario que debe impulsarse para el conocimiento y desarrollo.

El **diálogo estratégico**, EU-México, es un mecanismo que debe trascender lo bilateral y enmarcarlo en una perspectiva multilateral, para negociar, coordinar y establecer acciones, mecanismos y políticas comunes, que contribuyan a nuestro desarrollo y seguridad, conlleva implícitamente la búsqueda de elementos que permitan disuadir o evitar acciones y políticas que disminuyan nuestro potencial nacional y generen un dominio abierto por su parte, en los diversos campos de nuestra economía, la política, los aspectos sociales y militares, la tecnología y los esfuerzos internacionales.

El equilibrio es la meta de las acciones estratégicas gubernamentales, con todos los medios a nuestro alcance, incluidos los considerados imposibles.

- **2. La frontera sur-sureste con Centroamérica y El Caribe**. Propicia una situación de paso por nuestro país, implica tanto a los migrantes provenientes de los diversos países centroamericanos y del Caribe, como de mercancías ilícitas que fomentan la delincuencia, el narcotráfico, la trata de personas, la prostitución y los mercados negros de tabaco y alcohol, afectando la trama social, la seguridad y las relaciones entre los países de origen de estas actividades. La porosidad que prevalece en la región, es una oportunidad en donde el ciberanálsis tendría un gran impacto para la seguridad y el desarrollo fronterizo.
- **3. Los bloques geoeconómicos del Pacífico-asiático** (China y Japón básicamente y medio oriente**) y Europeo**. Que fungen como equilibradores del poderío norteamericano, vía competencia comercial y de producción de mercancías estratégicas, como el petróleo, armas y tecnología y los servicios de alto nivel en materia de seguridad, salud y proyectos productivos, con modalidades educativas alternas y de mayor rendimiento. Con posibilidad de inversiones favorables a nuestras reformas estructurales. Estos bloques son fundamentales en y para el ciberdesarrollo mexicano.
- 4. Como un espejo o rebote funcional**, las regiones y países de gran inestabilidad política y social** y las que promueven acciones violentas y terroristas, en contra del capitalismo y los Estados Unidos. Ubicadas en Medio Oriente, África del Sur, Asia y Latinoamérica. Es claro que en la situación globalizada, no importa dónde ocurran los eventos, finalmente tardan en alcanzar a los usuarios, lo que dura la redacción de un *tuit*. El ciberespacio y la ciberdefensa están en la dimensión regional de los conflictos posibles que deben ser analizados cotidianamente para ponderar los impactos nacionales.
- 5. **La situación nacional interna**. Las reformas estructurales y políticas públicas de mayor competencia globalizadora y productiva, alteran las relaciones tradicionales, en una segunda alternancia, con los grupos de presión más relevantes: empresarios, maestros disidentes, grupos delincuenciales y de acciones violentas (narcotráfico, delincuentes organizados, violencia y prostitución, derechos de piso, homicidios, secuestros y extorsiones, conatos de guerrilla) entre otros. El uso de los medios que el ciberanálisis y la ciberseguridad proporcionan es relevante en este

contexto nacional-local. Riesgo mayor es la posible sinergia entre los eventos y demandas con los diversos grupos, por ejemplo la secuencia de los hechos trágicos de Iguala, Guerrero, el abuso de la autoridad local en complicidad con la delincuencia, y los representantes opositores surgidos del reciente proceso electoral. La ruptura de las pautas de buen gobierno con un cómplice silencio de corrupción e impunidad, alteran la confianza y la unidad nacional. Las aplicaciones de la ciberpolítica son relevantes en la situación mexicana actual.

- 6. Los **elementos y aspectos del desarrollo nacional** ligados a los campos de la seguridad nacional, son el impulso a lo estratégico, más allá del discurso, con recursos expresos. Una ciberestrategia propicia la actualización para fortalecer los recursos humanos, la tecnología y los proyectos de prevención y prospectiva en los temas críticos, ya sean de tecnología, de producción de básicos, climáticos o ambientales, de salud y alimentación, de conocimientos universitarios en todas las disciplinas para fortalecer el capital humano y evitar la fuga de cerebros, del activo fundamental que constituye la inteligencia humana y estratégica. Uso intensivo de ciberinteligencia estratégica para el desarrollo nacional.
- 7. La atención a los **problemas del desarrollo tecnológico**, con las ventajas y afectaciones para la estabilidad y el desarrollo social y económico. Una ciberestrategia nacional que considere los problemas globales que están asociados al terrorismo internacional, al crimen cibernético, al crecimiento de mercados globales, al incremento de organizaciones delictivas nacionales y transnacionales, al desarrollo de armas químicas, biológicas y de destrucción masiva, a la degradación del medio ambiente, al descontrol del cambio climático, al narcotráfico, la piratería, la biopiratería, el espionaje económico e industrial y a la tecnología de uso delincuencial. Todo ello implica nuevas estrategias en la dimensión *ciber*, mayor presupuesto, personal, preparación preventiva y prospectiva, evaluación y la eficaz capacidad de respuesta.

Estos siete elementos geoestratégicos y funcionales son esenciales a un modelo de organización y de trabajo, de inteligencia estratégica para la seguridad nacional. Ni la totalidad ni los únicos elementos, sí los prioritarios. La ciberseguridad debe responder a las circunstancias del país, estableciendo la oportunidad de trabajar en las agendas de riesgo, de desarrollo y de seguridad nacionales. Es el reto del momento cibergeopolítico mexicano.

Programa para la Seguridad Nacional 2014-2018

En el contexto de la planeación democrática nacional y a partir del Art. 3º. de la *Ley de Seguridad Nacional* se desprenden las proposiciones siguientes:

La población, el territorio nacional, el orden constitucional, las instituciones de gobierno y la soberanía e independencia nacionales son elementos indispensables para la existencia del Estado mexicano, por lo que constituyen **intereses nacionales permanentes o esenciales**.

Atender los aspectos relativos a lo Nacional **como una función** de índole superior que **dirige, integra y coordina las acciones** de las autoridades e instituciones que están vinculadas con los sectores de la seguridad, la defensa y el desarrollo **a fin de prever, prevenir, disuadir, contener o desactivar aquellas vulnerabilidades, riesgos y amenazas** que pueden comprometer nuestro proyecto de nación.

De tal forma que los Riesgos y amenazas que considera el Programa para la Seguridad Nacional 2014-2018, son estratégicos y sus consideraciones atienden las políticas públicas vigentes en lo que concierne a las tradicionales y nuevas amenazas, destacando:

1. Desastres naturales y pandemias

2. Delincuencia Organizada Transnacional

3. Ciberseguridad

4. Fronteras, mares y flujos migratorios irregulares

5. Terrorismo y armas de destrucción masiva

Atendemos en esta reflexión el punto 3, sobre la **Ciberseguridad.**

El diagnóstico que establece el Programa para la Seguridad Nacional 2014-2018, considera el incremento de las **amenazas** en el **ciberespacio,** con **ataques** en contra de la infraestructura crítica, los intereses económicos, las redes de información y las capacidades de defensa de ciertas naciones, desarrollado por gobiernos, grupos criminales y organizaciones terroristas que explotan el ciberespacio con propósitos hostiles. México posee una pionera e incipiente cultura de seguridad de la información, que representa una vulnerabilidad actualmente, por lo que debe desarrollar una política de Estado en materia de ciberseguridad y ciberdefensa. Debe generar una ciberestrategia que desarrolle y asegure capacidades nacionales de comunicación y de los sistemas de información estratégicos existentes. El propósito central de la estrategia debe ser el fortalecimiento de la ***dimensión ciber*****,** en las operaciones de seguridad: la **ciberseguridad y la ciberdefensa**. La capacitación y formación de cuadros especializados en ciberseguridad y ciberdefensa va en paralelo, junto con el desarrollo y actualización del marco jurídico en materia de seguridad de la información y ciberdefensa, así como en la prevención, investigación y sanción de delitos cibernéticos. También atender los acuerdos de cooperación bilateral en materia tecnológica, de inteligencia y ciberseguridad.

Retos actuales de ciberseguridad

El ***desafío*** del ciberespacio está ***manifiesto en el actual momento mexicano*** en una serie de activos y retos:

- La seguridad y la CiberSeguridad son los **retos fundamentales** que tienen que enfrentar la sociedad y el gobierno de manera coordinada.
- Establecer un nuevo modelo de **coordinación, transversalidad** y **eficacia** para lograr los resultados que espera la sociedad.
- Considerar una profunda y clara ciberestrategia, pues donde no existe una **visión** adecuada los resultados serán distintos a lo esperado.
- De aquí que **claridad y precisión** se encuentran vigentes para una toma de **decisiones estratégicas, tácticas y operativas**.
- El gobierno, como motor, articulador y generador de la acción social, posee **normatividad e instituciones** que le favorecen en el logro de sus objetivos y metas,
- Y en los **resultados** comprometidos y observados por la sociedad en materia de ciberseguridad y procuración de justicia.

IV. CiberInteligencia para la Seguridad Nacional

El amo prevee, el esclavo provee.

Aristóteles

La relación estratégica en Inteligencia/CiberInteligencia tiene dificultades que devienen retos y oportunidades en la ***Inteligencia mexicana***, que tienen que ver con algunos elementos clásicos y relacionados con:

- El Ciclo de inteligencia
- La Inteligencia y las operaciones
- La Fusión de inteligencia
- La Contrainteligencia
- La necesaria Coordinación y Diagnóstico

Ciclo de Inteligencia (Basado en el modelo de Defensa)

El ciclo de inteligencia es similar en la Ciberinteligencia, de manera sencilla, las funciones, tareas, recursos y elementos relacionales son muy cercanos, el uso de dispositivos informáticos, de redes de comunicación, simples o complejas, determina mucho del resultado o producto, en tiempo y forma. Como se puede observar en el siguiente gráfico:

En el ciclo de inteligencia tradicional, basado en el modelo de la defensa, observamos que, mucho más de lo que se supone y desearía un analista, y que vale para la inteligencia, su estudio y aplicación, lo vale para la ciberinteligencia.

Requiere recursos humanos, tecnológicos y financieros en cada una de las etapas, en quien toma las decisiones, que define los fines, los objetivos y las metas.

En el personal inteligente que recaba la información, en las fuentes abiertas o las encubiertas, en quienes manejan los datos recolectados, en quienes hacen estimaciones y evalúan las probabilidades de certidumbre, para establecer cursos de acción, operaciones, escenarios, con la suficiente prospectiva.

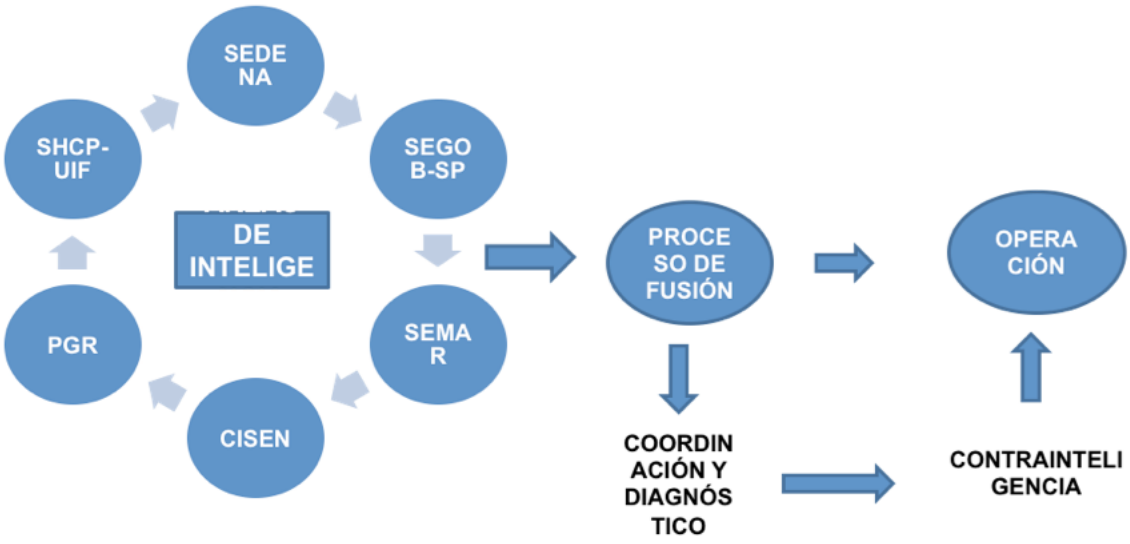
Los objetivos son la guía para la elaboración de los productos de inteligencia. Puede haber subproductos, pero no perder de vista, el objetivo original, para evitar la *serindipia*, el atínele al objetivo, y realizar un cálculo de inteligencia, que aproveche los medios disponibles. Ese cálculo maquiaveliano necesario de siempre.

Los productos alimentan y retroalimentan el objetivo original, corroboran o modifican los planes y establecen una ruta con mayor certidumbre.

En cada fase o etapa, se requieren sujetos distintos, multidisciplinarios, con visión multidimensional, con las características propias de quien realiza el análisis de información, de inteligencia, de operación, cada uno con una visión que se complementa en el todo.

En los aspectos relativos a la ciberinteligencia, el saber de *lo ciber*, en su teoría y práctica, y todos los aspectos vinculados con el desarrollo y la seguridad nacionales tienen un valor incrementado, un *plus* de información, de acceso, de relacionalidad y de respuesta que debe ser considerado en su uso.

Fusión de Inteligencia / OPERACIÓN



Como se observa en el cuadro anterior, en la ***fusión de inteligencia/operación, la coordinación y diagnóstico***, que provienen desde el momento inicial del ciclo de inteligencia, que pasan por el proceso de fusión, de operación y de la contrainteligencia, vuelven más compleja la actividad del análisis de información, del trabajo de articulación de la inteligencia y de las acciones de operación. El ciberanálisis es el sustento para la ciberseguridad.

No sólo es un tema de análisis en sí mismo, es el tema que tiene que ver con la política de seguridad nacional. Que coloca en discusión la articulación del trabajo que realizan todas las instancias de seguridad nacional.

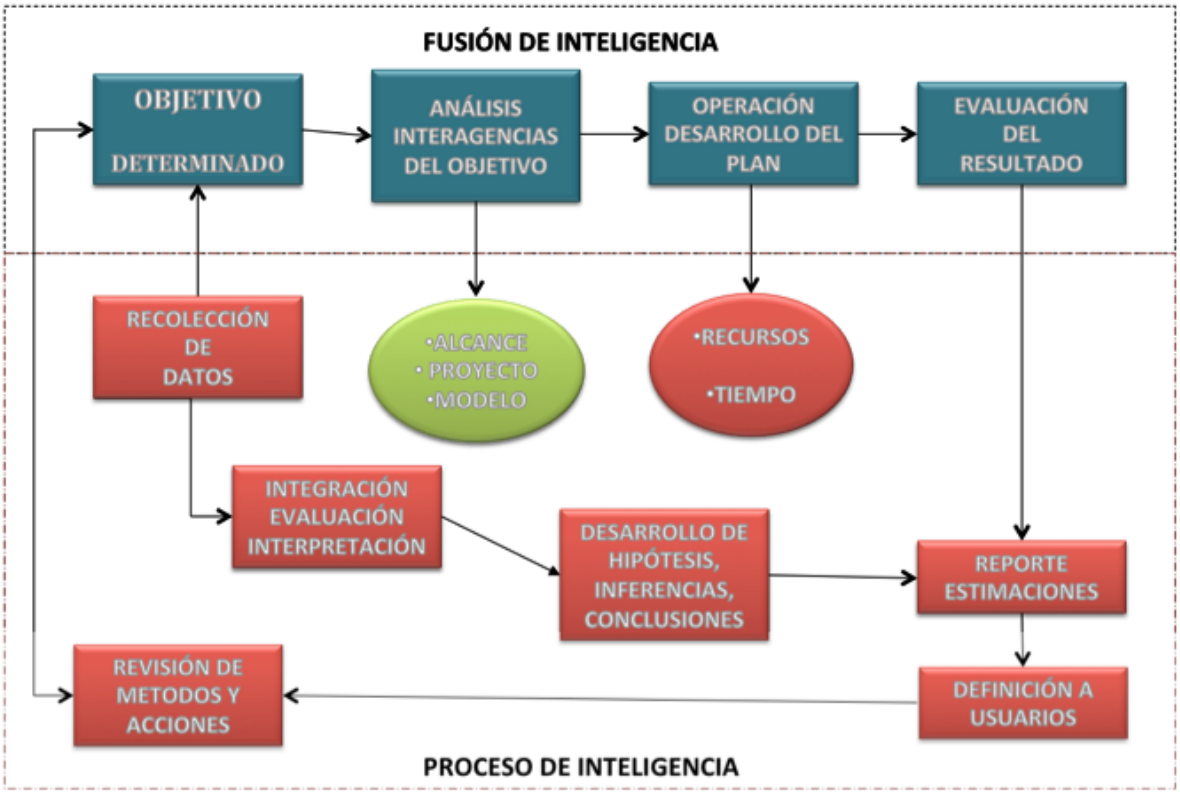
Que obligan a reflexionar sobre los alcances y límites, sobre los resultados esperados y, desde luego, sobre las responsabilidades de las autoridades, de los diseñadores y tomadores de decisión, y con sus respectivos costos sociales, que en términos de los

resultados obtenidos, no pueden constituir certeza al manejo de los datos estadísticos que las autoridades responsables generan.

La confusión, la manipulación y la no intervención estratégica en los temas de seguridad, acarrea el desbarrancamiento de quienes caminan, por el propio alcance de los tópicos, en el filo de la navaja de la seguridad nacional. Podría ser la curva del deterioro de un gobierno en su conjunto. Por ello la ciberdefensa está en la orden del día de toda la Agenda Nacional de Riesgos o de Seguridad.

Inteligencia/CiberInteligencia

Es importante recalcar, conforme al cuadro anterior y el siguiente, las grandes similitudes de inteligencia y ciberinteligencia, que la distinción fundamental está en los dispositivos informáticos, las redes de comunicación, los objetivos reales o virtuales. Que se aplican en todas las etapas, con funciones específicas.



En la amplitud de responsabilidades de las agencias de inteligencia de un país, con sus respectivas áreas, es pertinente incorporar en el proceso de inteligencia la posibilidad la fusión de inteligencia, con el fin de articular los esfuerzos y recursos, en la búsqueda de efectividad contra objetivos que atentan contra la seguridad de la nación y, en específico contra la delincuencia organizada. Esfuerzo estratégico en que se ha comprometido el

gobierno y que en ocasiones no logra mantener el ritmo de continuidad necesaria. La CiberInteligencia o CiberSeguridad apoyarían este importante proceso.

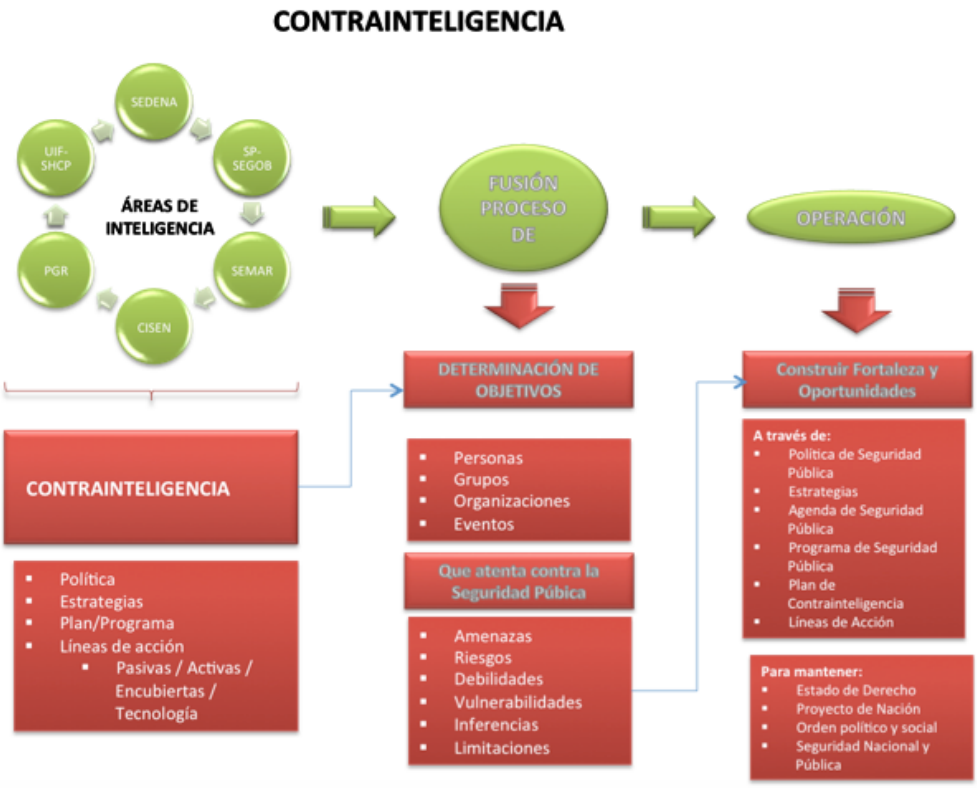
En esta etapa de la sociedad de la información y del conocimiento de acciones en el ciberespacio. La necesidad de profesionales en la materia, que aporten sus mejores conocimientos y experiencias es una demanda creciente y, en ocasiones, la oferta es limitada; a veces obnubilados por particulares prejuicios e inseguridades, por incapacidad de saber conducir una convocatoria que los integre. Situación que mina un esfuerzo institucional que requiere sensibilidad, prudencia, paciencia, persistencia y compromiso con los intereses de la nación.

En las tareas concurrentes al proceso de fusión, el ciclo de inteligencia considerado previamente, se sostiene, generando modificaciones que podrían alterarlo, en el entendido de que el personal que realiza las tareas específicas institucionales, debe no sólo conocer, sino respetar la línea de mando re-estructurada también. La ciberinteligencia conlleva implícita la necesidad de articulación de información, por ello es la estrategia natural de la fusión misma.

En el ciberespacio, las variables que intervienen, así como los tiempos comprometidos, no permiten equivocaciones, ni simplificaciones, ni desperdicios, sin embargo, el tiempo de prueba casi se ha agotado, los recursos necesarios no están del todo disponibles. Lo prioritario, lo estratégico y lo mediático, están en competencia, lo que muestra confusión en las áreas que deben tomar las decisiones fundamentales. La ciberinteligencia limitada obstruye la posibilidad de la ciberseguridad.

CiberContraInteligencia

La idea predominante que se sustenta en el cuadro siguiente, es que la contrainteligencia tradicional, puede incorporar un plus de alto nivel en el tratamiento de los datos y en la persecución de los objetivos previamente determinados, si agregamos el proceso de CiberContraInteligencia que, reiteramos, se integraría en todas las áreas, las funciones y tareas y en la aplicación de objetivos y fines.



El aspecto de *Contrainteligencia*, inscrito en el proceso de inteligencia y en la misma etapa de fusión, debe configurar el todo. La necesidad de cibercontrainteligencia es una necesidad. No es una posición optativa.

Sin CiberContraInteligencia no hay CiberSeguridad.

Es una cuestión estratégica y de doble dificultad, pues debe continuar atendiendo las tareas tradicionales que le competen, en el ámbito de la inteligencia, pero también debe participar de los nuevos elementos que genera el propio proceso de fusión y, más aún, debe estar atento y vigilante ante las propuestas de operación, para disuadir o atacar a los objetivos señalados. Por ello es relevante considerar la posibilidad de integrar la CiberInteligencia en una Agencia de CiberSeguridad Nacional.

La siguiente propuesta, de fusión de inteligencia y de creación de una nueva **Agencia de CiberSeguridad** que articule la información gubernamental, que le de sentido y dirección a

la actividad de inteligencia y que coadyuve en las decisiones que tienen que ver con las Ciberoperaciones, permite mirar una posibilidad que puede ser realizada.

No sólo el diseño de cursos de acción posible, de establecimiento y orientación de objetivos relevantes, sino de retroalimentación en la operación cotidiana, serían los renovados nutrientes de la inteligencia.

Una Agencia de Ciberseguridad Nacional que integre la ciberinteligencia, implica recuperar de manera armónica y equilibrada los diversos productos y, algunos procesos, realizados por las diversas instancias de inteligencia, articulados en un todo, con posibilidad de establecer en determinados momentos las partes de un conflicto, situación, personaje o cualquier otro objeto de análisis.

La creación de una **Agencia de CiberSeguridad Nacional,** facilitaría el desarrollo de **la Ciberinteligencia,** de una **CiberEstrategia de CiberSeguridad y CiberDefensa.**

De esta forma, habría la posibilidad de dar respuesta a las Cuatro Tendencias que predominan actualmente en torno al CiberConflicto/Riesgo/Amenaza:

- Gobiernos autocráticos que observan un internet abierto como algo letal para el régimen (ciberdemocracia, ciberpolítica). Lucha por controlar el ciberespacio.
- Actores disruptivos o antisistémicos (propios, manipulados o contratados) para afectar servicios o actividades, interrumpiendo el tráfico de información o destruyendo infraestructura estratégica. Todos los ciberriesgos posibles.
- Estados que desarrollan capacidades y dan acceso a sistemas para hostilidades potenciales, con la idea de derrocar o establecer cabezas de playa para futuros cibersabotajes. Escenario de complicidades interesadas.
- Campañas que afectan la propiedad intelectual (lo público y lo privado), o la actividad y prestigio de ciertos actores; plena ciberpolítica.

Ante la situación de frágil ciberseguridad, ¿Qué Hacer?

El político es quien hace de sus deseos actos.

Aristóteles

Otorgar el lugar que corresponde a lo *ciber*, una nueva dimensión de **lo estratégico prioritario,** considerando que:

- En el diseño de la Ciberseguridad requerimos de políticas públicas de Estado.
- CiberEstrategias para recolección, análisis y contrainteligencia de la información, para instrumentar operaciones, abiertas o encubiertas, acordes a las políticas de seguridad nacional.
- Actuar estratégicamente para incidir en el mundo actual, demanda el desarrollo de conocimientos y recursos estratégicos. Con iniciativas de alcance nacional y de impacto mundial.
- Tomar decisiones de Estado relevantes y trascendentes, por quiénes posean conciencia y conocimiento de la importancia de su desarrollo. Con los recursos necesarios y suficientes generar CiberInteligencia para construir la CiberSeguridad.
- Promover y Urgir al estadista, al gobernante, al político y al militar, que es necesario un pleno conocimiento de Estado, que son cuestiones vitales para la nación, de historia y tradición, de vigencia de proyecto y de futuro. Revalorar la quinta dimensión.
- La intervención en ciberseguridad no es cuestión de la fortuna, azar o providencia, es un cálculo racional de actores y factores en la escena nacional e internacional.
- Fortalecer una cultura que considere que el concepto real de Patria está sustentado en un sentimiento tradicional, que debe ser renovado en el Ciberespacio, que anuda e integra el patrimonio nacional común.

- La limitada atención a la mentalidad Cibergeopolítica ha generado pérdidas lamentables al país. Recuperar una nueva visión espacio-temporal a partir de lo *ciber*.
- La posición estratégica de México está vinculada y condicionada por la relación con Estados Unidos, no obstante, México debe desarrollar políticas de desarrollo y seguridad autárquicas, como Japón o Alemania en su momento de derrota y actuar de manera racional y estratégica en la realidad mundial. Atender sus comunicaciones, por ejemplo, aun cuando sea en 20, 30 ó 50 años, es prioritario.
- Fomentar visiones estratégicas y regionales y así enfrentar la idea de que Latinoamérica no sabe qué quiere y cómo lograrlo, que no se halla aún. Mirar el horizonte como futuro promisorio. No voluntarista, sino realistamente.
- En el caso mexicano existen valores históricos fundamentales que no han logrado integrarse del todo. Predomina una mentalidad política, de altiplano, que vuelve ajeno o desconocido lo que el mar es y representa para nuestro desarrollo nacional. Imaginemos las dificultades de concebir el CiberEspacio. Por ello, la formación de cuadros en instituciones estratégicas es un paso fundamental para revalorar la situación y posición mexicana
- La cercanía fronteriza con Norteamérica y la actividad comercial (80% aproximadamente) y de diversos intercambios, muestra un *complejo estratégico natural*, como se observó con el TLCAN, sin embargo debe enfatizarse la perspectiva de una amistad conveniente, de una alianza productiva que genere la autarquía nuestra. El intercambio tecnológico es fundamental.
- Las políticas interior y exterior son dos rostros del interés nacional mexicano, las relaciones interestatales son impersonales y frías, marcadas por cierta indiferencia ética, por lo que debe prevalecer una consistencia, no contradictoria, en la política nacional mexicana, sin utopías ni chauvinismos insensatos o nacionalismos mal entendidos. Las relaciones en la ciberpolítica son una opción real.
- Afianzar una política exterior que sin estar subordinada ni enajenada en contenido y futuro a los EU, se complemente fortaleciendo nuestros objetivos estratégicos, con nuestros intereses vitales mutuos, de común Defensa Estratégica en todos los campos de la producción humana. Así, con la ciberestrategia atendemos de lo local a lo global.
- La cercanía norteamericana nos coloca en posición privilegiada que puede ser motivo de riesgos y amenazas por intereses adversos al nacional.
- Hay un Área de Defensa Estratégica de EU que se relaciona con México, tanto por la situación actual de Cuba, como por los acercamientos de los BRICS, Brasil, Rusia y China a Venezuela y Nicaragua, hay un estado vigilante. La diplomacia digital favorece la ciberseguridad global, regional y nacional.
- Dadas las características relevantes de nuestras instalaciones estratégicas, en la cuenca mexicana del Golfo de México y en los centros de telecomunicaciones, es importante considerar un Centro de Gravedad CiberEstratégico. La ciberdefensa en plenitud.

- Asistimos a la competencia por mercados, batalla anticipada de futuras guerras comerciales, antesala a conflictos bélicos. Cibercompetencia geoestratégica.
- La dependencia de un solo producto, sobre todo si es no renovable, establece una economía suicida, afectando el desarrollo social y toda posible política nacional. *Mutatis mutandis* la dependencia tecnológica con una sola empresa, producto, país o gobierno.
- La carencia de política comercial basada en mercados diversificados, se muestra en la relación de las importaciones, concentrada en pocos países, en alimentos o insumos para la industria, de una economía petrolizada, que desequilibra cualesquier desarrollo armónico nacional, y propicia una dependencia forzada y difícil de modificar. El tema *ciber* es prioritario.
- La lucha por los energéticos en Medio Oriente, corresponde a un posible control de los países pérsicos por Rusia. Si bien es un factor fundamental no es el único, de ahí la *Guerra de Posiciones* que observamos en Ucrania, en Gaza y en África, incluso con el uso y manejo de la pandemia del Ébola. Incluso en la negativa a la independencia de una parte del Reino Unido, que muestra el dilema de la seguridad y la libertad. Esos aspectos, en el ciberespacio, reposicionan los intereses nacionales en el mundo global.
- No sólo los recursos que se tienen, sino también de lo que se carece, debe estar en una visión Geoestratégica, para dar impulso a una posición Geopolítica. La ciberdefensa y la ciberseguridad alcanzan estos campos.
- Como elementos condicionantes de negociación y coacción, de conflictos latentes y manifiestos en el mundo. El petróleo y el gas siguen siendo elementos de inobjetable valor estratégico, determinantes en el desarrollo industrial y la geopolítica mundial, seguidos de los productos agrícolas y el agua. Sin embargo, cada segundo, el dominio de la tecnología, del conocimiento, va colocando la primacía en un saber basado en la idea, el diseño, la innovación, dejando la producción en otros países, con la consecuencia del costo en empleos de maquila e ingresos bajos, contaminación ambiental y limitación al desarrollo. Revalorar la ciberestrategia nacional.
- Toda decisión beneficia a unos y perjudica a otros. Hay riesgos probables o posibles, el primero es cuantificable, el segundo puede o no puede aparecer, aunque las circunstancias hacen que lo posible o latente se vuelva manifiesto y lo probable se acerca a lo necesario.
- De ahí la necesidad de *establecer un riesgo calculado* en toda acción decidida, que valore lo aceptable como costo o beneficio, en función del interés nacional. En los riesgos aceptados hay posibilidades, pero nada garantiza su éxito, son los factores que condicionan a los actores.
- Lo más escaso en el mundo actual es la certeza, de ahí que el trabajo estratégico sea una necesidad ineludible en el desarrollo y la seguridad nacional. En todas y cada una de las cinco dimensiones que constituyen el campo de batalla actual.

V. Conclusiones

- Colocar en el centro de la Cibergeopolítica a México y desarrollar una visión CiberGeoestratégica, que mapee con claridad y precisión las acciones estratégicas y los actores-factores relevantes. Implica repensar la idea de seguridad nacional mexicana.
- Diagnosticar a fondo y tomar decisiones para una CiberEstrategia de CiberSeguridad en las instituciones e instancias de seguridad y justicia, para el desarrollo nacional. Considerar la creación de una Agencia de Ciberseguridad Nacional.
- La Confusión en potencialidad, desarrollo y debilidad institucional no debe distraer los recursos estratégicos disponibles. Por ello, es prioritario atender la CiberSeguridad de la Nación. Replanteando alcances y límites de la nueva inteligencia estratégica.
- Conformar un sistema con Bancos de datos e información, muchas veces incompletos y desarticulados, podría subsanarse con la propuesta de fusión de inteligencia, que rompa el trabajo de campo limitado, con una CiberEstrategia para la ciberseguridad y una CiberInteligencia para la CiberDefensa.
- Romper la estrechez formal de una estrategia de combate a la delincuencia organizada parcial y limitada. Incluir corrupción e impunidad. Trascender el límite de la legislación actual. Revalorar el papel de la CiberDefensa, en aspectos de los delitos cibernéticos, digitales y o en redes sociales. Ponderar la doctrina existente al respecto.
- Impulsar el conocimiento pleno del ciberespacio, en las condiciones actuales del mundo globalizado, en las situaciones críticas existentes, bajo una estrategia mínima de riesgos o de seguridad. Ciberanálisis y cibercontrainteligencia.
- Disminuir la falta de coordinación política en los tres poderes y los tres niveles de gobierno. Buscar mayor interlocución con la sociedad. Una oportunidad está en la CiberPolítica. Información para la Inteligencia.
- Re-Impulsar la Cultura de seguridad y legalidad para con la sociedad y al interior del ámbito gubernamental. Fomentar la CiberCultura. La nueva inteligencia para la ciberseguridad de la nación.
- Siempre es ***el momento de México***, pero ***sin inteligencia, no habrá desarrollo ni seguridad*** que hagan viable nuestro futuro promisorio. Una CiberEstrategia contribuirá a la CiberSeguridad de la Nación.
- En suma, más y mejor información e inteligencia estratégica, con capacidad profesional y recursos suficientes, para fortalecer la seguridad y el desarrollo nacionales. Llegó la hora de la CiberInteligencia.

Bibliografía

Clausewitz, Carl von, **De la Guerra**, (est. Prel. Bernard Brodie, Trad. Celer Pawlowsky, Tecnos, España, 2010, 531 pp.

Thiago Cintra, José, **Seguridad nacional, poder nacional y desarrollo**, abril de 1991, s.p.i.

Morgenthau, Hans J., **Política entre las naciones;** l**a lucha por el poder y la paz**, GEL, Argentina, 718 pp.

Paret, Peter, **Creadores de la Estrategia Moderna; desde Maquiavelo a la Era Nuclear,** Ministerio de Defensa-España, Madrid, 1992, 969 pp.

Peón, Alvarez, Lorenzo del**, Pefil filosófico de la estrategia (teoría pura),** Edit. Herrero, México, 1987, 304 pp.

Taleb, Nassim Nicholas, **El cisne negro; el impacto de lo altamente improbable**, Paidós, México, 2013, 591 pp.

Santos Caamal, Mario**, La globalización de la seguridad nacional**, CESNAV-Secretaría de Marina, México, 2002, 301 pp.

Vizarretea Rosales, Emilio, **Poder y Seguridad Nacional**, CESNAV-17-Instituto de Estudios Críticos-Fundación para la Democracia y el Desarrollo, México, 2014, 582 pp.

-----, "Estabilidad y desarrollo regional para la seguridad mexicana" en **La Seguridad Nacional Integral de México; diagnósticos y propuestas**, CESNAV, 2013, 61-75.

-----, "La importancia de la información y la inteligencia en los modelos geopolíticos contemporáneos" en **Inteligencia Estratégica; retos y oportunidades para México**, CESNAV, 2014, pp. 215-239.

-----, "Sobre el discurso estratégico" (Primera Parte) en **Revista del Centro de Estudios Superiores Navales**, Julio-Septiembre 2013, Vol. 34, Número 3, pp. 6-21.

-----, "Sobre el discurso estratégico" (Segunda Parte) **en Revista del Centro de Estudios Superiores Navales**, Octubre-Diciembre 2013, Vol. 34, Número 4, pp. 6-25.

-----, "Maquiavelo y la razón de Estado" en **Examen**, Número 227, año XXIII, febrero 2014, pp. 72-88.

-----, "Consideraciones al Programa para la Seguridad Nacional 2014-2018", **Examen**, No. 230, año XXIII, mayo 2014, pp. 29-39

-----, "Análisis político-coyuntural, el Caso Guerrero" en **Examen**, Número 237, Año XXIII, Diciembre 2014, pp. 54-63.

-----, “La seguridad humana en México; democracia y políticas públicas para el desarrollo” en **La seguridad humana como pilar del desarrollo social en México**, Pedro Núñez (Coord.), Centro de Estudios Sociales y de Opinión Publica, Comisión de Desarrollo Social, México, 2015, LXII Legislatura, Cámara de Diputados, pp. 91-109.

-----, “Proceso electoral local, Veracruz 2013” en **Los estados en 2013; la nueva configuración político-electoral,** Gustavo López, Rosa María Mirón y Francisco Reveles (Coords.), IEDF, UNAM, ITESM, Fundación Friedrich Naumann, México, 2014, pp. 321-339.

-----, “Inteligencia y Seguridad Nacional en México; una visión estratégica”, en la **Conference Cyber Security and Cyber Defence**, Cancún, Q. Roo, 9 diciembre 2014.

-----, “La Nueva Inteligencia y la CiberSeguridad”, Conferencia en la Escuela Superior de Guerra en el **Intercambio Académico** de la SEDENA-Colegio de Defensa Nacional y SEMAR-Cesnav, Abril de 2015, 50 pp.

Amable lector para atender sus dudas, comentarios o sugerencias del presente texto siga

el siguiente link http://www.cesnav.edu.mx/ININVESTAM/contacto.html