JORGE RETANA YARTO

NUEVAS TENDENCIAS EN INTELIGENCIA DE ESTADO: HACIA LA INTEGRACIÓN DE LOS SERVICIOS PÚBLICOS DE INFORMACIÓN SOBRE RIESGOS

ENSAYO

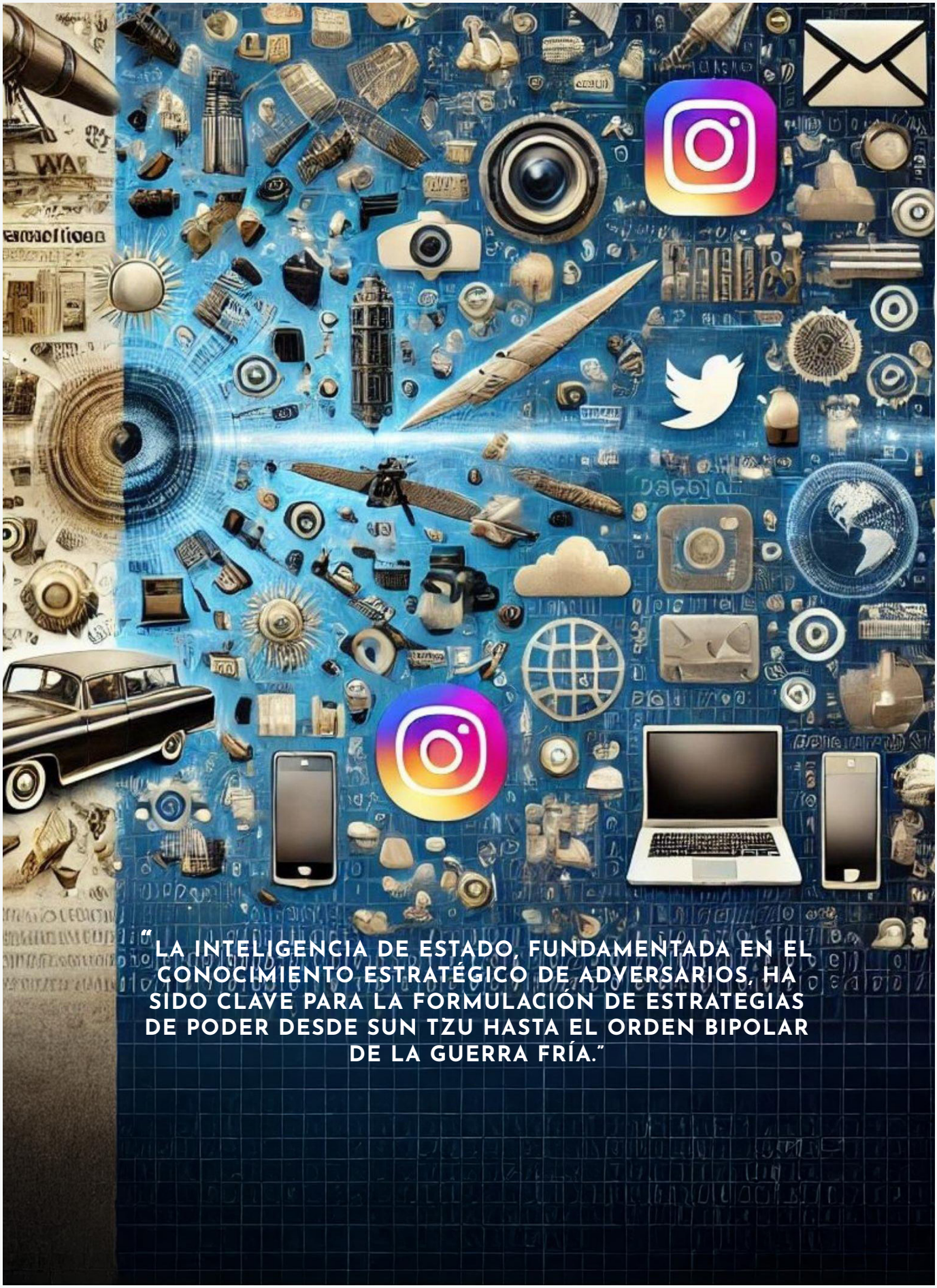
Antecedentes Históricos.

La Inteligencia de Estado (IE) puede rastrearse desde tiempos inmemoriales en versiones muy primarias, ya Sun Tzu establece algunos lineamientos básicos pero muy lúcidos sobre la importancia que el conocimiento sobre los adversarios y enemigos, fortalezas y vulnerabilidades, tiene en la formulación de estrategias para derrotarlos y ganar batallas importantes, conquistar o conservar el poder. De allí en adelante, encontramos distintos referentes en diversos pensadores que son muy útiles, pero la construcción de una ciencia convergente e interdisciplinaria orientada a la seguridad nacional, interior y pública, se desarrolla notablemente en los periodos posteriores al último tercio del siglo XIX, y principalmente, después de la segunda guerra mundial en el contexto del Orden Bipolar y de la paridad miliar nuclear estratégica entre los dos campos contendientes en la "guerra fría", lo que algunos teóricos de la bipolaridad denominaron "la destrucción mutua asegurada".

Irremediablemente la IE para la seguridad nacional, nació ligada a la doctrina del Realismo en materia de relaciones entre Estados, apoyada en el antecedente de las formulaciones de la Geopolítica de los autores alemanes de principios del siglo XX y especialmente del inglés Sir Halford John Mac Kinder y de los alemanes Rudolf Kjellén y Friedrich Ratzel, que inspiraron a otro alemán histórico: Adolf Hitler y su locura del Tercer Rich. Hitler tomó de Mac Kinder la teoría del "pivote estratégico" cuya piedra angular era la región euroasiática, "el heartland" para dominar el planeta Tierra, la región que era asiento del poder soviético de la URSS, en donde mandaba Josif Stalin y el ejército rojo, por lo tanto, había que lanzarse a la conquista de ella. Aún con 3.0 millones de soldados ultra equipados, Hitler fracasó en su empeño. De los geopolíticos alemanes, tomó el postulado central de que los Estados eran "organismos vivos" que debían crecer y expandirse más allá de sus fronteras naturales, una especie de "selección natural" darwiniana de perfil geopolítico.

El Orden Bipolar fue el escenario de otra gran batalla, la "guerra fría" con dos ejércitos multinacionales organizados, la OTAN y el Pacto de Varsovia, armados, dotados de pertrechos, tecnología y especialización militar para el combate a tope, y poseedores de una filosofía política y económica antagónica en cuanto al tipo de Orden Social que debía predominar en las sociedades nacionales.

Esa otra gran batalla a escala internacional por los cinco continentes, fue librada por los servicios de inteligencia de ambas grandes potencias nucleares que protagonizaban la "guerra fría", EUA y la URSS, al frente de sus respectivos bloques de países aliados



“LA INTELIGENCIA DE ESTADO, FUNDAMENTADA EN EL CONOCIMIENTO ESTRATÉGICO DE ADVERSARIOS, HA SIDO CLAVE PARA LA FORMULACIÓN DE ESTRATEGIAS DE PODER DESDE SUN TZU HASTA EL ORDEN BIPOLAR DE LA GUERRA FRÍA.”

llamados "países del mundo libre" frente a los países del "socialismo real", dos bloques contrapuestos y enfrentados.

La CIA y el KGB eran los otros protagonistas de esta "guerra de inteligencia" sin cuartel. Se hicieron famosas y hasta memorables algunas historias de "espionaje político y militar", de "agentes dobles", de traiciones, "secretos de Estado revelados", pero también de asesinatos y hasta experimentos con agentes de inteligencia mediante la psiquiatría como en la URSS, o con proyectos como el "MK Ultra" y el "Hombre de Manchuria" de la CIA, los Manuales de Asesinatos de enemigos, y hasta los ataques radiactivos para favorecer el desarrollo de tumores cancerígenos empleando "aceleradores y multiplicadores de células infectadas", y decenas de cosas más por increíbles que puedan parecer. La Ciencia de Investigación y la Experimental al servicio de la inteligencia y contrainteligencia de Estado, pero además una doctrina de inteligencia que conllevó dos axiomas que eran dos caras de una misma moneda: "hacer la guerra de inteligencia al enemigo en su propia casa" y "cuidar la retaguardia" desarrollando al máximo la contrainteligencia como actividad para la mayor protección, inteligencia interior y exterior para derrotar al enemigo.

Se trató durante la posguerra de crear un aparato de Estado lo mejor organizado posible, con estructuras sólidas que conformaban subsistemas del sistema integrado de la inteligencia, sin duda, una actividad inter y multidisciplinaria orientada a la preservación y/o conquista del poder, es decir, una actividad que utiliza distintas disciplinas científicas como el Derecho, la Ciencia Política, la Economía, las Relaciones Internacionales, la Sociología, la Antropología Social, la Biología, la Ciencia militar, la Ingeniería, y algunas otras. Para lo cual se conforman grupos de trabajo interdisciplinarios que abordan las tareas necesarias de manera colectiva y coordinada, bajo un mando centralizado de disciplina y normatividad para el control avanzado.

En enfoque predominante en la llamada "Inteligencia Clásica" (Lahneman, 2008) quien estableció un modelo de "inteligencia tradicional" o "clásica", que antes del 11 de septiembre de 2001, había predominado con las siguientes características: a) la centralidad del adversario o enemigo como eje de toda la actividad de inteligencia; b) la idea de que el enemigo opera de acuerdo a un modelo de conductas y acciones respecto al que está frente a ellos, lo cual posibilitaba la anticipación mediante la metodología y las técnicas de investigación y acción; c) era necesario descubrir toda la información oculta que tuviera el enemigo, "la investigación del misterio" dice el autor citado, que era la pieza central del trabajo a realizarse; d) para este tipo de inteligencia el enemigo era siempre "externo", la inteligencia de Estado se abocaba al enemigo exterior y la seguridad interior a los nacionales, en América Latina en la guerra fría, surgió el "enemigo interno que trabajaba para intereses externos", la doctrina de Seguridad Nacional de las dictaduras militares impulsadas con golpes de Estado desde el norte del continente, y se desarrollaron las doctrinas de la "anti subversión" de la escuela militar francesa, y las de "contrainsurgencia" de la escuela estadounidense de West Point; e) su origen era los riesgos y amenazas de origen militar; f) todo esto le otorgaba a este modelo de IE un carácter reactivo-preventivo, concentrada en riesgos y amenazas de origen humano y militar-humano.

Este tipo de IE revela secretos, información oculta, actividades subrepticias, ataques y sabotajes posibles, pero no desde el punto de vista epistemológico, de un conocimiento de lo real que lo explique y pueda prever su desarrollo ulterior. Apropiarse de información no es lo mismo que generar conocimiento de la realidad sobre las amenazas que ellas significan para los intereses nacionales, para la seguridad de una nación, de una sociedad o Estado, o república. Distingamos entonces entre información y conocimiento, lo uno puede llevar a lo otro, pero no son lo mismo. El conocimiento "confiere a la inteligencia un valor estratégico"; la información le da un valor táctico u operacional (lo cual no quiere decir que no pueda ser útil)".

La Crisis de los Modelos de Inteligencia Clásica y Anticipatoria.

El paradigma de una IE reactiva-preventiva evidencia su fracaso, con el ataque a las torres gemelas en Nueva York el 11 de septiembre de 2001. Porque este atentado que el mejor aparato de Inteligencia de Estado del mundo, el más grande y con mayores recursos, y de alta especialización, fue incapaz de detener, pone de manifiesto varias cuestiones inaprehensibles en el modelo anterior: i) el enemigo identificado sigue siendo el centro de gravedad de nuestra organización y operación, pero este tiene hoy múltiples cabezas, no es simétrico y tampoco plenamente identificado, puede ser externo, pero atacar desde dentro; ii) a consecuencia de este cambio, las amenazas se han diversificado y ofrecen una perspectiva distinta, por lo que los aparatos de IE deben ampliar su radio de acción y campo de trabajo frente a los nuevos riesgos y amenazas de orden transnacional, que operan bajo esa lógica; iii) las redes o la red -como se quiera- configuran un nuevo gran espacio de comunicación y coordinación, de interacción dinámica que ha modificado y ha incrementado las fortalezas de quienes desarrollan a escala regional-global una guerra asimétrica contra un enemigo poderoso que parecía imposible de atacar mediante un golpe de alto impacto; iv) la red devuelve la sensación de una realidad que envuelve a los enemigos diversos, en un entorno caótico, muy complejo de prever e identificar, sobre la cual es muy difícil planificar acciones tácticas defensivas efectivas.

Hay un cambio notable que complica en exceso el trabajo de los especialistas de la inteligencia; v) los riesgos y amenazas se vuelven -como dicen hoy los expertos- difusas, múltiples y diferenciadas en su naturaleza y contenidos, y los enemigos actúan como nodos articuladores dentro de un diseño de red adversaria y en la cual cada nodo puede replicar y ampliar el impacto y fortalezas de la red completa. Las redes de atacantes potenciales están en todas partes y en ninguno en concreto, a la vez; vi) los enemigos son como virus, se introducen dentro del cuerpo social o institucional de sus enemigos para mejor atacarlo. Frente a esta capacidad de los nodos, los "topos" o los "agentes dobles" o los que "traicionan" se quedan muy lejos en su efectividad, porque son sinérgicos y menos complejos de descubrir.

Así, el paradigma de la IE clásico exhibe graves limitaciones de carácter, no sólo predictivo (con apoyo en las técnicas de la prospectiva), sino principalmente anticipativo sobre el comportamiento futuro de los nuevos riesgos y amenazas, sobre su causalidad contradictoria, su falta de linealidad, y la complejidad en que se desarrollan las mismas, por lo que no van dos pasos adelante de la inteligencia predictiva, y ocultan su plena identificación, y la IE va tres pasos atrás por su carácter reactivo-preventivo. Pero, además, restringida por una normativa legal que le obliga a actuar ex post al evento.

De esta reflexividad, surgió en EUA la Inteligencia Anticipatoria, como expresión de un nuevo enfoque de inteligencia militar del ejército de EUA: las guerras de intervención estabilización y los ataques preventivos, o la guerra preventiva. El concepto de "Inteli-

gencia Anticipativa" fue acuñado por Jordi Serra, Joan Antón y Enric Miratvillas y fue presentado como "búsqueda de un nuevo paradigma en inteligencia estratégica" en un escrito conjunto en el año de 2010 (https://es.scribd.com/document/520159600/SERRA-) frente a lo que denominaron "el viejo paradigma" que es lo que nosotros llamamos "el modelo clásico de la IE", que ellos afirman que "sigue estando el vigente", al que contraponen el "nuevo enfoque proactivo en construcción", con lo que claramente afirman un proceso de aproximación, no concluido.

Así el concepto que empleamos sobre la crisis del "viejo paradigma reactivo-preventivo" significa que desfallece, pero no ha muerto, y el "nuevo paradigma anticipatorio y proactivo" no acaba de surgir. Su función teórica-práctica es adecuada -dicen- a "las amenazas a la libertad, la seguridad y el bienestar" de los ciudadanos, ante las "complejas sociedades del siglo XXI".

La doctrina de las guerras de intervención y estabilización y los ataques o guerras preventivas, configuraron la nueva doctrina militar estratégica después de los atentados a las torres gemelas, le dieron cobertura teórica a una política de mayor intervencionismo para desarrollar "la nueva guerra contra el terrorismo internacional", le daba legitimidad al sostener que un ataque preventivo era la única manera de evitar un daño mayor si los hechos catastróficos planeados llegaban a consumarse.

Esta teoría plantea críticas certeras a la IE clásica o tradicional, pero al surgir para acompañar y dar cobertura a una estrategia política militar, no pareció tener una larga vida asegurada porque había mucho de coyuntural o transitorio en dicho enfoque, tan es así, que el presidente Barak Obama modificó el mismo y echó mano de un conjunto de postulados que diferenciaron las herramientas teóricas y de análisis de los gobiernos anteriores al de George W. Bush, avanzando iniciativas doctrinarias de corte geoeconómico y geopolítico y estratégico diferenciadas.

Tuvo y tiene una enorme complejidad este paradigma en desarrollo cuyo eje gravitacional es la "postura anticipatoria", dado que se debe actuar sobre la base de eventos no acontecidos y que resulta muy complejo probar que van a suceder. Se trabaja entonces desde la IE al seno de un entrono altamente incierto, que resulta más complejo para los analistas de inteligencia que el del enfoque proyectivo o predictivo del modelo clásico en donde se trabaja con datos duros en sí mismos, no en la interpretación de ellos volcados al futuro.

Los autores del postulado, de un modelo de Inteligencia Anticipatoria sitúan como eje gravitacional las amenazas de orden transnacional que se generan, desarrollan y actúan bajo el ámbito de la lógica geopolítica, no sólo transfronteriza, debido a zonas de pertenencia geográfica y conflictos inherentes a dichas regiones o a la conexión de ellas entre sí, y en muchos casos, desde organizaciones no estatales generando beneficios para su propia causa, de cualquier orden, que actúa como sujeto nodal, porque las nuevas amenazas se originan en redes organizadas por nodos, la cual llega incluso a los espacios públicos o privados que se quieren atacar. En esa medida son transnacionales.

"los parámetros del viejo paradigma, que asignaba la lucha contra este fenómeno a los cuerpos de seguridad estatales, han sido uno de los principales factores de desarrollo del crimen organizado internacional, ya que es en la transaccionalidad donde han encontrado su ventana de oportunidad. Mimetizando el comportamiento de las multinacionales, pero llegando incluso más allá (al fin y al cabo, no están limitados por legislación de ningún tipo), el crimen organizado es argumentablemente el fenómeno que más y mejor ha entendido la lógica del capitalismo global."

Obviamente existen otros riesgos relevantes respecto del crimen transnacional organizado. Son los riesgos y amenazas que no se explican a no ser por las redes de comunicación, organización y actuación. Son un gran instrumento de la guerra asimétrica, incluso de la guerra híbrida.

Si consideramos todos estos factores juntos, entendemos que el modelo de la "inteligencia vieja" pueda ser inoperante en países de alto desarrollo , profundamente integrado a la globalidad de todo tipo de procesos, en donde la comunicación en red, los sistemas informáticos, la universalidad de los accesos al ciber espacio está altamente desarrollada, con relación a otros donde es compleja la adopción de un nuevo paradigma, complejo y muy gradual, porque, debemos pasar de lo reactivo-preventivo a lo anticipatorio y proactivo con todas las herramientas de análisis, las metodologías, técnicas, teorías, modelos organizativos, jerárquicos, etc. y con las políticas públicas puestas en praxis y que han generado determinadas experiencias nacionales.

Por ello un cambio de paradigma genera siempre mucha confusión y resistencia para adoptar una nueva racionalidad sobre una problemática en común o un fenómeno emergente. Más aún si los tiempos de la actividad, de la praxis, se modifican radicalmente, desde los tiempos ex post, a los tiempos ex ante, haciendo a un lado, o sin haber adaptado, la normatividad legal para el efecto, y evitar situarte en la anticonstitucionalidad, al trascender el modelo predictivo, anticipando el macro entorno frente a las amenazas en evolución.

Si nosotros tomamos en cuenta que este enfoque de la inteligencia militar traducida en actos de gobierno y medidas castrenses fuera del territorio nacional, produjo "invasiones estabilizadoras" en Irak, Afganistán y Libia, o "ataques preventivos" en Líbano por parte de Israel, cuesta trabajo aceptar un paradigma apoyado en este razonamiento que recula de cualquier norma constitucional restrictiva, por lo menos para quienes tenemos una concepción de la inteligencia de Estado, transparente, controlada y que rinda cuentas a quienes la financian. En su caso, si hay consenso, pasar a efectuar los ajustes jurídicos correspondientes con absoluta conciencia de sus implicaciones.

Pensemos en arrestos ciudadanos preventivos, represiones sociales preventivas, encarcelamientos preventivos. Imposible.

Podemos estar de acuerdo en el desgaste de las metodologías, técnicas y teorías, políticas públicas y liderazgos de la "vieja inteligencia", sobre todo, el carácter obscuro, impenetrable de la misma que dio origen a todo tipo de aparatos para la inteligencia criminalizada contra opositores internos que actúan dentro del marco constitucional, en un cuasi régimen de excepción legal en muchos episodios nacionales. Imposible aceptarlo. La necesidad de renovación es real y auténtica como necesidad nacional y científica. La inteligencia con cualquier adjetivación que se use, sin tener al centro el respeto irrestricto de los derechos humanos es incompatible con cualquier proyecto de democratización política completa.

Otros expertos se orientaron a buscar el cambio epistemológico hacia una Inteligencia Proactiva sin invalidar el marco constitucional restrictivo que protege a los ciudadanos, y empezaron a trabajar en una doble vertiente: i) el enfoque sistémico de las problemáticas a ser abordadas, y ii) la generación de un meta marco analítico. Para lo primero se ensayó en la dirección que indica la Ciencia Post normal y la Teoría deSistemas

Evolutivos (TSE) para configurar así un nuevo paradigma que recogiera los avances producto de la crisis de la "vieja inteligencia" y las propuestas de "Inteligencia Anticipatoria".

De la frustración de este proceso parte mi tesis uno: la ruptura operada por la pandemia global y la nueva tendencia hacia la necesaria integración de los sistemas de información de riesgos del Estado, no cancela sino modifica el contexto de la discusión sobre el nuevo paradigma de la IE.

Interrupción y Nuevo Punto de Inflexión: la Pandemia Global.

Esta discusión o tendencia hacia la búsqueda de un nuevo consenso entre la masa crítica de especialistas en la disciplina de la Inteligencia de Estado, en lo fundamental, quedó interrumpida y modificó los contextos de actuación de los aparatos de inteligencia a partir de otro gran fracaso: la incapacidad para anticiparse a un fenómeno global que pronto puso en crisis aguda los sistemas de salud pública y privada de los Estados Nacionales, incluso de aquellos Estados regionalizados (como los de la Unión Europea) con sistemas de salud mixtos integrados.

Los servicios de IE en todo el mundo, no sólo no pudieron anticipar el grave evento sanitario multinacional, sino que con la problemática encima se comportaron de distinta manera, unos con más eficacia que otros en los procesos sanitarios de contención, control y reversión. Destaca el servicio israelí, el Mossad en el trabajo coadyuvante de monitorear con minuciosidad cada hospital receptor de grupos sociales infectados, y evolución hospitalaria.

la Inteligencia Anticipatoria vs la integración de servicios públicos de información sobre riesgos.

El paradigma de la Inteligencia Anticipatoria, en vías de despliegue, se derrumbó ante el fracaso de sus herramientas de análisis preventivas para el caso de la pandemia global. No hubo un solo aparato nacional de inteligencia que haya podido anticiparse y actuar proactivamente a semejante cataclismo mundial que abarcó a más de 140 países y costó millones de víctimas, muertes, y un costo desorbitado en la reconversión de los sistemas de salud nacionales en el curso mismo de la catástrofe sanitaria. Aquí quedaron enterradas las bases de aquella propuesta impulsadas por sus autores, formulada al influjo dominante de las dos administraciones de George W. Bush en los EUA, y su nueva estrategia de seguridad nacional y doctrina de defensa nacional, que Obama relegó y reformuló. Trump administró la crisis y quiso culpar a China sin éxito. Ni la CIA apoyó su hipótesis.

Lo que los Estados Nación y los Estados Región (agrupados por tratados de integración regional) demostraron durante el desarrollo de la pandemia global, fueron los inmensos vacíos que había en cuanto a la falta de una simbiosis integral de los servicios de información nacional y de los modelos de riesgo con los cuales operaba cada agencia: de desastres naturales, de emergencias sanitarias, de movimientos sísmicos y telúricos en general, de desastres climáticos, de inteligencia nacional de Estado, no sólo diferenciados como es normal, sino con sistemas de datos (DATA) absolutamente disociados en la detección de amenazas, lo cual acentúa su efecto pernicioso en el desarrollo de una crisis de alto impacto.

Este tipo de eventos potencialmente destructivos, son parte de la Agenda Nacional de Riesgos y Amenazas en muchos países, incluyendo México. Los temas de posible afectación colectiva que desestabilizan al Estado y sus instituciones y se vuelven amenazas directas a la seguridad interior pasan a formar parte de las amenazas cuyos riesgos gestiona el poder público con distintas instituciones. Los aparatos de prevención y protección del Estado especialmente no se han diferenciado correctamente de los servicios de información clasificada, como los de la inteligencia de Estado, civiles, policiales y militares. Usamos este concepto de información clasificada de Estado para indicar acción de prevención y protección nacional,

Nuestro concepto se refiere a los procesos informativos que pretenden prever eventos de afectación colectiva mayor, en donde el Estado a través de su gobierno nacional, gestiona los riesgos a los que está sujeta la colectividad nacional. Son una comunidad muy amplia de organismos de distinto tipo que conforman un gran aparato de recepción informativa, análisis, estudio, prevención, protección, de seguridad y ayuda, que gestionan los múltiples riesgos en que estamos inmersos la sociedad, nuestro territorio, instituciones, ecosistemas, etcétera, y cuyo insumo fundamental es la información, lo más amplia, exacta, a tiempo y oportuna posible. Son una parte fundamental de la gobernanza y la estabilidad político-social, por tanto, del Estado.

En consecuencia, si este magno aparato de información falla, la capacidad de respuesta queda comprometida, en entredicho, y la afectación en cualquier magnitud, no es principalmente para el Estado, sino para la sociedad nacional misma. Ello se paga con destrucción de riqueza material (infraestructura, instalaciones, bienes públicos diversos, e incluso, vidas humanas). De allí su relevancia estratégica y el contar con dicho aparato como el conjunto de instrumentos y herramientas de las que depende una parte sustantiva de la estabilidad nacional. De allí su trascendencia.

Si no logran anticiparse a procesos socialmente e institucionalmente lesivos, fallan en su cometido con relevantes consecuencias. Este fenómeno de la pandemia global no pudo ser detectado por ningún servicio de inteligencia del mundo. Algunos esbozaron indicios de que "algo fuerte" se venía desarrollando, pero no hubo la claridad suficiente para organizar la respuesta. Nuestro aparato de inteligencia para la seguridad nacional adolece de una deficiencia o vulnerabilidad relevante puesto que el cruzamiento de la inteligencia civil-militar con la inteligencia sanitaria, era muy necesaria como afirma un especialista como Jonathan D. Clemente, desde la segunda guerra mundial, nadie se ocupó de ello, y el no poseerlo apropiadamente a estas alturas del siglo XXI es una falla monumental.

Lo cierto es que la pandemia global sumergió al mundo en una grave crisis de seguridad internacional, de salud pública global, sanitaria y a los Estados nacionales, en una severa crisis de seguridad nacional, colapsó los aparatos públicos de prevención, protección y gestión de riesgos (incluyendo la inteligencia nacional) que lograron seguir operando a pesar de nuevas amenazas. Pero no pueden volver a ser los mismos después de este evento.

En México esta brutal experiencia debe llevarnos a replantear el modelo de la información de Estado, es decir, el aparato preventivo convertido en proactivo y el aparato de gestión de riesgos, incluyendo principalmente lo relativo a la inteligencia para seguridad nacional, la militar y la civil. En la etapa de las muy sofisticadas tecnologías de la información y la comunicación, de las plataformas informáticas, de las bases de datos y metadatos, de la revolución digital y de la cooperación de los sistemas de inteligencia de Estado en todas las regiones del planeta, deben reconfigurarse los servicios de información y riesgos sobre la base de una visión más amplia.

Aquí nuestra tesis dos: la tarea de con-

struir el nuevo paradigma para la Inteligencia de Estado debe estar estrechamente articulada al proyecto de fusión integral de los servicios de información del Estado, de los que manejan información clasificada, apoyadas en la Inteligencia Artificial (IA). La adopción de distintos aspectos en seguridad, inteligencia y gestión de riesgos diversos para lograr su anticipación proactiva, se ha venido dando en distintos países mediante el uso de la IA.

Búsqueda del nuevo paradigma para la IE y la IA.

La propuesta de uso de la Inteligencia Artificial (IA) en la IE para la seguridad multi dimensional cambia el eje estratégico de la discusión sobre estos temas, a partir de que modifica la base de sustentación tecnológica para la IE (civil, policial, militar y criminal) que son una base fundamental de soporte para proveer la seguridad a la nación, a los ciudadanos y a las instituciones.

La eclosión y desarrollo de la IA desde sus primeros pasos ha generado inmensas posibilidades y capacidades de cambio en los diversos espacios del orden social, y particularmente en la inteligencia para la seguridad, ya que posee un potencial enorme al ser la tecnología más importante de nuestro tiempo, en el contexto de lo que los especialistas llaman "la tercera ola de la digitalización", particularmente debido a sus aplicaciones en la industria tecnológica de la seguridad, incluyendo la empresarial. También hay muchos que le temen por su capacidad de reemplazo de trabajos operativos, de los cuales prescinde.

Por sus aplicaciones y desarrollos tecnológicos para la seguridad y contra el crimen transnacional organizado, hasta las "smart cities", la infraestructura estratégica, el rastreo de virus y la prevención de desastres, los líderes se orientan por soluciones vinculadas al uso y desarrollo de IA.

Tenemos entonces un binomio dinámico nuevo: IA/Seguridad que es el eje de una nueva propuesta, que modifica sustantivamente los términos de la discusión respectiva y búsqueda de soluciones, porque provee instrumentos inéditos de control y anticipación a hechos empleando algoritmos, siendo capaces tales instrumentos de aportar vigilancia y control preventivo, identificación precisa de tipología de incidencias, víctimas o consecuencias de hechos y se convierte por todo ello, en base de un nuevo paradigma para la seguridad multidimensional.

En las instituciones de inteligencia en distintos países que han avanzado en estos usos, aplicaciones y desarrollos tecnológicos de última generación, mediante el análisis e investigación de señales de comunicaciones y tecnologías de video vigilancia, la inteligencia nacional accede a información exhaustiva que maximiza la efectividad de sus tácticas y estrategias contra el crimen transnacional con la operatividad de IA aplicada a la seguridad. En suma, efectividad, conocimiento en tiempo real, prevención de incidencias, identificación mediante análisis de imágenes.

Una crítica preventiva: en el pensamiento contemporáneo de la última revolución tecnológica, de la "era digital", de las TIC, etc. Se tiende a sobredimensionar la capacidad y potencial de la tecnología moderna para solucionar los problemas agudos del orden social contemporáneo. No olvidar, como ejemplo, que cuando surgieron las TIC y el comercio electrónico se llegó a sostener que "las crisis económicas del capitalismo contemporáneo habían desaparecido", era la "Nueva Economía", y sobre ello corriendo miles de toneladas de tinta sobre este despropósito falaz.

Pero haciendo a un lado este "endiosamiento" con la revolución tecnológica de nuestro tiempo, no utilizar todo el potencial y desarrollos, usos y aplicaciones de la IA para potenciar, reconvertir y aumentar nuestras capacidades al máximo en las instituciones de inteligencia y seguridad sería un gravísimo error histórico. Adelante entonces con el impulso de este nuevo paradigma del binomio virtuoso IA/Seguridad.

Ahora bien: todo esto exige la inversión para la reconversión tecnológica, pero también, la reconversión organizativa que implica lo administrativo, lo operativo, los recursos humanos y la estructura jerárquica, y por supuesto, el marco jurídico de avanzada para todo ello. Personalmente he disentido del gobierno anterior en México en la omisión intencional que ha hecho sobre los temas del nuevo marco constitucional para replantear toda la organización de la inteligencia nacional.

He dicho, que no hay nueva Ley de Seguridad Nacional (la actual es de principios del siglo y debe incluir la ciberseguridad), tampoco una Ley de Inteligencia Nacional (que plantee la transparencia en todo aquello que sea posible y prohíba y penalice rigurosamente el espionaje privado desde plataformas compradas mediante corrupción con proveedores), que debe establecer con mucha mayor rigurosidad la adquisición de equipos tecnológicos de alto valor financiero (que favorece la corrupción) y la falta de un Sistema Nacional de Inteligencia, SNI (que hay en casi todo Sudamérica), imperativa también, una reconceptualización teórica para no llamar a todo crimen un tema de "seguridad pública", concepto superado como visión del siglo XX para la seguridad de los Estados nacionales y que el poderío del crimen transnacional modificó radicalmente.

La seguridad es un sistema institucionalizado que comprende la conjunción integrada y organizada de siete instituciones (no hay espacio para desglosar). O funciona todo el sistema o no se garantiza la seguridad. Pensar solo en la policía, el ejército, la guardia y la tecnología parcializa la problemática del sistema institucional. Esta es toda la agenda pendiente de la inteligencia y la seguridad para México, El tercer gran mérito de la propuesta hecha es que plantea no sólo el uso de las aplicaciones e instrumentos existentes de IA, plantea la construcción de los propios como robots y drones capaces de realizar tareas físicas y operativas usando sensores y sistemas de vigilancia y control sobre ellos, que permiten a las instituciones tener capacidad de interpretar y analizar mediante imágenes diversas objetivos señalados y/o la detección de objetos (armas), así como la identificación facial morfológica, generando información situacional en tiempo real.

Todo ello requiere otro gran esfuerzo en la capacitación y alta especialización del recurso humano, reduciendo la estructura administrativa, como se ha hecho en todo Sudamérica. Por cierto, he estudiado la experiencia de 8 países de nuestro subcontinente que han transitado desde la doctrina de seguridad nacional de las dictaduras hasta nuevos paradigmas en la función de inteligencia para la seguridad.

El cuarto gran mérito, va en sentido de lo que ya hemos dicho sobre el manejo del software adecuado para nuestro sistema de IA/Seguridad el cual deberá ser operado por analistas altamente capacitados que sean capaces de identificar falsificaciones posibles y/o anticiparse a eventos desfavorables.

Tendríamos por delante u camino de capacitación altamente especializada que recorrer, sobre todo en la inteligencia civil y policial. Para el tema de la ciberseguridad necesitaríamos también profesionales altamente calificados. El ejército puede ayudar en su capacitación. Nunca se parte de cero, algo existe ya de camino andado.

Es evidente la necesidad de provocar en forma planificada un gran salto

tecnológico (un bigbang), que pondrá en la línea de obsolescencia acelerada o quizá sólo de la necesidad de un cierto proceso avanzado de adaptaciones o interconexiones, lo que hoy son los equipos y el software fundamentales de la inteligencia para la seguridad, que son las plataformas tecnológicas de contenido ofensivo y defensivo, que hoy provee la telemática.

En suma el potencial de transformación y asentamiento de un nuevo paradigma tecnológico aplicado a la inteligencia y la seguridad en el binomio planteado AI/Seguridad conlleva, un cambio tecnológico que acelera el desarrollo de procesos y su optimización.

Hoy la seguridad y protección ciudadana, el paradigma del siglo XXI, requiere un enfoque de estructura institucional integrada por siete instituciones articuladas bajo un marco jurídico-constitucional general: 1) institucionalidad administrativa; 2) la institucionalidad de los cuerpos armados (policiales y otros del tipo intermedio, como en México la Guardia Nacional); 3) la institucionalidad de la inteligencia para la seguridad; 4) la institucionalidad abocada a la promoción, administración, procuración e impartición de la justicia; 5) el marco jurídico institucional para la seguridad; 6) el sistema tecnológico aplicable; 7) la institucionalidad referida al modelo de reclusión y rehabilitación penitenciaria.

Este enfoque de entender la seguridad como un sistema institucional integrado ha estado ausente en las políticas públicas como en las disertaciones académicas y parlamentarias, se habla de los cuerpos policiacos, de la inteligencia, de las plataformas tecnológicas, la corrupción, pero no se conciben las variables dentro de un modelo sistémico integrado. Grave falla.

Dejamos enunciadas las piezas del sistema que prefiguramos ligado a la incorporación de la IA a la inteligencia y la seguridad que pueden ser la base de un nuevo modelo de IE para la seguridad multidimensional. En oro ensayo podemos desarrollarlas con precisión y cierta amplitud.

El nuevo paradigma y los sistemas de análisis integrados.

En paralelo a todo ello, la metodología y las técnicas, así como los cuerpos teóricos para el análisis en inteligencia y contrainteligencia, así como para la ciber protección usando la telemática para reforzar los mismos, puede transitar-no si una amplia discusión pormenorizada- con los dos pivotes referidos antes que señaló el maestro Jordi Serra del Pino de la Universidad de Barcelona: el enfoque de la ciencia post normal que aportaron Funtowicz y Rvetz (1993) cuyo planteamiento es el de trascender la ciencia normal basada en el cuerpo teórico e histórico desarrollado por T.S Khun "cuando los datos son inciertos, los valores en disputa, los riesgos altos y las decisiones urgentes".

La ciencia normal orientada a evaluar la calidad de los resultados, la ciencia post normal se orienta mejor a un examen integral basado en "las cuatro pes": los productos obtenidos, los procesos desarrollados, los propósitos planteados previamente y las personas idóneas involucradas, al que denominaron un modelo de ciencia post normal.

Personalmente considero que las bases del modelo de avance científico paradigmático de T.S. Khun sigue vigente por cuanto enfoca los cambios estructurales científicos como rupturas epistemológicas que abren una nueva etapa científica del conocimiento sistemático, al cual no escapa la IE y la seguridad multi dimensional.

El segundo pivote epistémico planteado por el maestro Serra del Pino que es la herramienta analítica acorde con la Inteligencia Proactiva que es la Teoría de Sistemas Evolutivos (TSE), considero la necesidad de confrontar las fortalezas de esta teoría frente a la Teoría de los Sistemas Complejos (TSC). Se indica que el primer cuerpo teórico-analítico posibilita un tipo de análisis sistémico que se requiere en la inteligencia y contrainteligencia de Estado, dado que parte de una premisa: la necesidad de lograr la capacidad para evolucionar hacia estadios superiores para maximizar las condiciones del conocimiento. Y ello lo permite los sistemas evolutivos, que van desde la partícula más sencilla hasta la estructura más sofisticada, como pueden ser los sistemas integrados por matrices superiores.

La TSE establece un modelo evolutivo de los sistemas de conocimiento, integrado por cinco etapas: la emergencia, el desarrollo, la madurez, la desestabilización y la ruptura transformativa. En los primeros tres estadios se experimenta un proceso de crecimiento de tipo cuantitativo o incremental que conduce a la madurez del proceso, a partir del cual, llegó a su umbral de tolerancia de la complejidad (entendida como el límite de la información procesada) y entra entonces en una etapa de desestabilización porque el sistema puede mostrar limitantes para integrar mayor información, pero sus impulsos evolutivos lo conducen a entrar en un proceso transformativo, ante la sensibilidad de los cambios operados con la nueva información, entando finalmente al ciclo de ruptura que marca el final del proceso evolutivo, debido a su capacidad de capturar y procesa nueva información de manera más efectiva.

Esto aplicado al análisis de inteligencia proporciona herramientas para un tipo de inteligencia más proactiva.

Un razonamiento analítico que tendríamos que aplicar de manera concreta, este nivel de abstracción en la explicación de sus componentes, hacen muy difícil determinar su factibilidad en el trabajo de inteligencia y contrainteligencia, a la que legítimamente se le busca hoy una nueva base teórica, metodológica y analítica con las técnicas respectivas aplicables, que las haga realmente operativas, útiles para nuestros fines.

La TSC podemos perfilarla en sus términos generales sobre cuatro ejes centrales: i) un sistema complejo se entiende en relación con una determinada filosofía del movimiento; ii) ésta filosofía implica cierta filosofía del tiempo; iii) sobre esta base los sistemas complejos comportan una cierta filosofía social, cultural, política o histórica; y iv) los sistemas complejos definen una auténtica revolución científica en curso, consideramos, en los términos definidos por T.S. Khun, como un nuevo saber aceptado por la masa crítica de expertos en las temáticas concernidas.

A partir de ello debemos considerar a la IE y la seguridad multidimensional como parte de las "disciplinas complejas", no "sencillamente complejas", sino de una "complejidad creciente", es decir, como sistemas no lineales, como sistemas emergentes o adaptativos, así, los objetos de estudio de aquellas, deben estar comprendidos como "ciencias de la complejidad" que han creado una variedad de otras ciencias, metodologías, técnicas, lenguajes, enfoques, teorías y disciplinas con utilidad creciente en nuestra reali-

dad macro social, política, histórica. Dentro de tales disciplinas de complejidad creciente, el objeto de estudio de la criminalidad transnacional organizada, por supuesto que dada su amplitud y realidad multifacética, debe ser considerado para su estudio científico como materia de un sistema complejo en los términos aquí esbozados. En fin.

La discusión es compleja, requerimos regresar a ella en otro momento, dado que la búsqueda de un nuevo paradigma de componente integral sobre las temáticas que nos ocupan, sobre la IE y sus objetos de estudio, la seguridad multidimensional y el crimen transnacional organizado en su complejidad multifacética lo demandan imperativamente, para abordarlos con una trayectoria de aproximación científica cada vez mayor, con lo cual nuestro trabajo será cada día más útil para nuestro país, para el bienestar de la nación y la fortaleza de nuestras instituciones públicas.

Noviembre, 2024.