5

LAS OPERACIONES DE INFORMACIÓN Y EL INFORME DE INTELIGENCIA CONTRATERRORISTA

Cel Inf Alexandre José Corrêa

RESUMEN:
A partir de la identificación de la era del conocimiento, se consolidó el entendimiento de que la gestión de las informaciones en la seguridad y defensa se tornó algo vital para la propia existencia y soberanía de los Estados. Las fuerzas de seguridad están cada vez más involucradas en asuntos que no son exclusivos a la esfera militar, pero que son igualmente esenciales para el éxito en la conducción de las operaciones contraterroristas. Por lo tanto, es creciente la necesidad de obtención y gestión de la información proveniente de todas las áreas del conocimiento. Las operaciones de información surgen como una poderosa herramienta para expandir el ambiente de información y realizar la gestión del conocimiento en diferentes áreas del saber, no solamente en el área tradicional de la inteligencia. El presente trabajo por medio de un análisis documental, pretende identificar si el informe de inteligencia contraterrorista, como producto del método de análisis actual integra datos y/o informaciones suficientes y oportunas para el combate al terror.

PALABRAS CLAVE:
Gestión del conocimiento, operaciones de información, inteligencia, terrorismo.

ABSTRACT:
From the characterization of the knowledge era, the understanding about information management was consolidated in security and defense and became vital for the very existence and sovereignty of States. The fight against terrorism is developing in an increasingly discontinuous, asymmetric and multidimensional operating environment. Security forces are increasingly involved in issues that are not exclusive to the military sphere, but are equally essential to the success of conducting counterterrorism operations. There is a growing need to collect and manage information from all areas of knowledge. Information operations emerge as a powerful tool to expand the information environment and realize the management of knowledge located in different areas of knowledge, not only in the traditional area of intelligence. The present work by means of a documentary analysis aims to identify if the counterterrorist intelligence report, as conceived by the current doctrine, integrates data and / or information sufficient and opportune for the fight against terror.

KEYWORDS:
Knowledge management, information operations, intelligence, terrorism.

Introducción

Planteamiento del Problema

La lucha para controlar las informaciones y el conocimiento en el campo de batalla, pueden ser ya vistas en las teorías de Sun Tzu hace 25 siglos. Al final de la primera década del siglo XXI, es posible constatar algunas consecuencias del fenómeno de la globalización, así como identificar algunas tendencias del mundo actual, donde el acortamiento de las distancias y su correlación variable temporal tal vez, sean las más visibles de sus consecuencias. Los cambios dinámicos que ocurren hoy, se acercan desde lo paradójico e imponen una fuerte inestabilidad en el escenario global donde ocurren las relaciones entre Estados, sociedades, grupos e instituciones civiles y militares. En ese contexto, es posible inferir una tendencia global de fragmentación política, en que Estados multinacionales tienden a fragmentarse en naciones menores. Por otro lado, también es lícita la observación de que varios grupos nacionalistas aumentan su influencia regional sobre las comunidades de su interes. Otra gran tendencia, es la interdependencia global, también llamada "interconectividad" por algunos autores. Tal idea demuestra que, aun si se fragmenta políticamente una organización, parece ser creciente la interconexión global a través de la red mundial de computadoras y la intensa utilización de todos las formas de medios de comunicación existentes.

Al inicio de la segunda mitad del siglo XX, la humanidad se sorprendió con su propia obra: el conocimiento creció sin parar de manera geométrica. El fenómeno fue acompañado con la inmediata difusión de informaciones sobre todas las áreas del saber, sin respetar soberanía ni fronteras, sumergiéndose así en el mundo globalizado en el que todo y todos eran impactados por sus efectos. Unas organizaciones desaparecían y otras surgían como las organizaciones no gubernamentales, empresas multinacionales, bandas criminales y organizaciones terroristas como actores internacionales, disputando los focos del escenario y los espacios de la prensa en los Estados Nacionales.

Durante el mismo período del siglo XX y paralelamente al desarrollo de la sociedad del conocimiento, la Guerra Fría colocó a las dos grandes superpotencias (EUA y URSS) en una disputa sin precedentes en todos los campos del poder, que incluyo a los servicios de espionaje que alcanzaron niveles de desarrollo jamás visto antes, donde la doctrina de inteligencia militar e inteligencia estratégica sirvieron de base para las decisiones de jefes políticos y militares.

La Era de la Información, como se presenta caracterizada en la obra de Heide y Alvin (Toffler, 1993), surge como elemento fundamental para la actual coyuntura internacional. La gestión de la información en Seguridad y Defensa de un Estado se vuelve vital para su propia existencia y soberanía. El ambiente del campo de batalla moderno, es cada vez más discontinuo, asimétrico y multidimensional, por lo que las Fuerzas Armadas están siendo forzadas, cada vez más, a involucrarse en asuntos que se escapan de la esfera militar, pero que son esenciales en la conducción de las operaciones, lo que viene a fortalecer el concepto de Operaciones de Información.

Una de las atribuciones del Estado es proveer de seguridad y defensa necesarias para que la sociedad pueda alcanzar sus objetivos, generando las condiciones para que el país no corra riesgo de una agresión externa ni esté expuesto a presiones políticas o imposiciones económicas insoportables, y sea capaz libremente de dedicarse al propio desarrollo y al progreso. Al ser una actividad de responsabilidad exclusiva del Estado, la

inteligencia tiene como característica el desarrollo de acciones especializadas y complejas, donde su principal objetivo es identificar, recopilar, analizar e interpretar datos e informaciones en las más variadas áreas del conocimiento y en los asuntos de interese de Estado.

Varios analistas que estudiaron el 11 de septiembre del 2001, indican que la falta de comunicación entre las diversas agencias estadounidenses habría sido la principal falla de seguridad que permitió el éxito del ataque a las Torres Gemelas por Al Qaeda. La necesidad de integración fue uno de los grandes aprendizajes estadounidenses con la tragedia que afectó a miles de personas de varias nacionalidades, y la falta de esa integración ha comprometido en la cualidad los informes de inteligencia contraterrorista.

Justamente en ese sentido, la doctrina de operaciones de información (Op Info) surgió con mucho más énfasis después del 2001, como un gran paraguas que busca integrar todas las fuentes del conocimiento, además de aquello que normalmente la inteligencia ya podía ofrecer, ya que no solamente la inteligencia es capaz de generar datos o informaciones útiles.

Consecuentemente, es posible plantear el siguiente problema: ¿En la era del conocimiento, el informe de inteligencia contraterrorista, como es elaborado doctrinariamente por la mayoría de las agencias, efectivamente integra datos y/o informaciones suficientes y oportunos para el combate al terror?

Esta investigación tiene por objetivo hacer una crítica constructiva de la metodología de elaboración de los informes de inteligencia actuales y del pensamiento dominante en la comunidad de inteligencia internacional en contraposición a la dinámica y velocidad de las informaciones en la era del conocimiento. Además, como objetivos parciales, se intentará mostrar como las Op Info pueden ser empleadas como una herramienta para la gestión del conocimiento y como favorece la calidad del informe contraterrorista.

Justificación de la Investigación

A pesar que el mundo occidental es responsable por casi todos los avances tecnológicos de la era del conocimiento, es paradójico pensar que los principales grupos terroristas de hoy utilicen esa tecnología para seleccionar sus blancos, entre los países occidentales, inventores de esa misma tecnología. También es curioso que todos los esfuerzos desarrollaos por las grandes potencias y los recursos empleados, parecen que no son suficientes para evitar la creciente ola de atentados, cada vez más osados y devastadores.

La inteligencia es, sin duda alguna, la herramienta capaz de ofrecer la ventaja necesaria para que los Estados enfrenten el terrorismo. Es claro también, que la era del conocimiento ofrece una gama infinita de informaciones y antecedentes disponibles para quien la quiera buscar. Sin embargo, hacer una gestión integrada de tanta información, con la tecnología disponible, no es tan fácil como parece.

Esta investigación se justifica en la medida que busca demostrar que el empleo de las operaciones de información como herramienta de la gestión del conocimiento, puede favorecer la calidad del informe contraterrorista.

Fundamentación: conflicto asimétrico, terrorismo y la era del conocimiento

Conflicto Asimétrico

Desde el final de la Segunda Guerra Mundial, sucedida por un largo período que se conoció como Guerra Fría, las formas de enfrentar las amenazas contra los intereses

nacionales han variado bastante. Los ejércitos experimentados en combate han aprendido de sus propios reveses, también las sociedades han cambiado y con ella también ha cambiado la forma de combatir. La era del conocimiento como consecuencia de la explosión tecnológica que se experimenta con una rapidez cada vez mayor, sustituyendo a la era industrial, no ha pedido permiso para transformar la sociedad, surgiendo nuevas formas de hacer política y de conducir la guerra. Estos cambios vienen alterando gradualmente las relaciones de poder, provocando inestabilidades, incertidumbres, generando la aparición de conflictos locales y regionales, involucrando la inserción de nuevos actores en el contexto de los conflictos, inclusive no estatales. Esta evolución en el ambiente operacional ha traído una significativa transformación en el modo de operar de las fuerzas de seguridad, potenciada por la facilidad de acceso a nuevas tecnologías en escala global, por la socialización de internet, por el surgimiento de las redes sociales y la actuación de los medios de comunicación, lo que ha contribuido al desarrollo de conflictos en áreas de gran concentración de población.

A pesar de estos nuevos ingredientes, los conflictos permanecen marcados por el empleo de la violencia. Por otro lado, la participación del vector militar es más compleja por ocurrir en ambientes con la presencia de la población civil, concentrada en núcleos urbanos que reducen la factibilidad de identificar al oponente y aumenta la posibilidad de efectos colaterales indeseados.

En la medida en que los conflictos interestatales se vuelven cada vez más anómalos, el ambiente híbrido de amenazas gana una mayor importancia para los estudiosos de la guerra. Por ello se definen conceptos adaptados a esa realidad, en los que el uso de la fuerza asume nuevas configuraciones descritas con nombres como; Guerra de 4ª Generación, Guerra Híbrida, Guerra Irrestricta o la Guerra Asimétrica, donde el arte de la guerra se enfrenta a amenazas que generan nuevos desafíos y complejidades en los actuales escenarios, incluyendo al terrorismo y las armas de destrucción masiva.

Sin embargo, en nuestros días, se puede deducir que en el campo de batalla contemporáneo, existen algunas características que tienden a repetirse. Se resalta en los conflictos asimétricos, la nítida presencia de nuevos actores y características, elegidos por la sociedad contemporánea, tales como: los medios de comunicación "In Situ" en el campo de batalla, influenciando de forma prevalente las decisiones políticas y el planeamiento de los niveles de decisión, poniendo más cerca el ámbito político del táctico.

La capacidad tecnológica no sólo evoluciona, sino que explota cada año; donde la exacerbación por la defensa de las minorías transnacionales; la influencia de las organizaciones no gubernamentales en los conflictos; la dificultad para definir líneas de contacto entre los beligerantes; el desafío de identificar al enemigo en el seno de la población: la utilización de la información como arma que influye en el poder de combate; la tendencia que los enfrentamientos se extienden a lo largo del tiempo y la conciencia de que las fuerzas militares no solucionan las causas de la guerra; la relevancia del papel de la población en el destino de los conflictos y la prevalencia de los combates urbanos con presencia de civiles, contra civiles y en defensa de civiles.

Así vive el mundo "posguerra" fría, bajo la mirada de los nuevos paradigmas impuestos por el acceso globalizado a las informaciones, donde un número cada vez mayor de personas recibe en tiempo real una

inmensidad de datos a través de los medios y redes sociales (entre otras tecnologías) generando cambios en las sociedades más abiertas. El modo de gestionar el conocimiento y las informaciones en el combate contra el terror, no puede quedarse ajeno a esas transformaciones.

Terrorismo

El terrorismo no es un fenómeno exclusivo de los días actuales. Su historia ha tenido numerosas variaciones de ideología, estilo, alcance, violencia y proporciones. Como si no bastaran los enfrentamientos armados a lo largo de la convivencia entre naciones, la historia de nuestra civilización todavía se ve obligada a asistir a otras explosiones de barbarie en la convivencia de los pueblos, nutridas por el fanatismo político, religioso o étnico. Lo que antes no era más que focos localizados de estas manifestaciones radicales, hoy se convierten en una amenaza global e interconectada, desconociendo fronteras políticas y cualquier otra limitación previsible por la mente humana. El terrorismo unido a la violencia extremista transnacional asume la condición de principal amenaza a la paz mundial y por ello moviliza las preocupaciones de todos los países implicados en la causa común de la seguridad internacional. El terrorismo transnacional contemporáneo es, indiscutiblemente, la mayor amenaza a la paz y la seguridad internacional en el siglo XXI, no existiendo lugares ni naciones inmunes a esta amenaza en el planeta.

Las organizaciones terroristas de hoy, operan su potencial destructivo a gran escala y, según las previsiones de algunos expertos, estarían a un paso del acceso a artefactos nucleares, además de armas químicas y biológicas, es decir, próximos a poseer armas de destrucción masiva.

Para tratar el tema terrorismo, inicialmente se hace necesario definirlo, sin embargo, ante las variables que envuelven el tema (tales como la naturaleza del objetivo, si es combatiente o civil; la autoría de la acción, si es estatal o no estatal; los objetivos de la acción, si es religioso, político o diverso), en la comunidad internacional, el alcance de una definición unánime ha sido una de las mayores dificultades.

De hecho, aún no hay un consenso acerca de la definición del término, ni siquiera en la ONU, no existiendo ninguna convención internacional que defina el término. Por ello se considera difícil llegar a una idea consensuada acerca de esta concepción, ya que son involucrados concepciones políticas, ideológicas, militares y religiosas.

Durante años, la ONU viene tratando de definir quién sería terrorista y lo que representa un acto de terror, controversias que han postergado la adopción de una nueva concepción sobre el terrorismo que incorporaría elementos clave de instrumentos legales ya existentes permitiendo que las naciones busquen un tratado internacional para luchar contra este.

La tarea de definición que implica necesariamente la transformación del terrorismo en términos analíticos útiles, en lugar de una herramienta polémica, debe considerarse a la luz de la relación entre lenguaje y política (Whittaker, 2001).

Como el terrorismo tiene efectividad política cuando el resultado de la acción se difunde, la comunicación ejerce el papel de crear en la opinión pública nacional e internacional, la sensación de pavor generalizado, de impotencia, de víctima indefensa y de perplejidad ante la inseguridad. Así, la publicidad oxigena la diseminación del horror y, al mismo tiempo, moviliza mentes en apoyo a la causa de los terroristas. En cualquier circunstancia, no se debe perder de vista la naturaleza delictiva de la actividad que se basa en apoyo logístico supeditado por contrabando de armas y de municiones, financiado por un flujo financiero

ilegal o de blanqueo de dinero.

Otro aspecto muy marcado del terrorismo es su frecuente unión con el crimen organizado. Como ejemplos de esta tendencia, hay vínculos entre Al Qaeda y el tráfico internacional de opio de origen afgano, entre los separatistas chechenos y la mafia rusa, entre fuerzas guerrilleras y los carteles de drogas de Colombia o entre el crimen organizado de otros países latinoamericanos con esos mismos carteles.

Los grupos terroristas se están asociando al crimen organizado y ambos actores se aprovechan de estructuras individuales y pasan a un actuar conjunto, buscando países donde la estructura político-social se encuentra inestable, logrando de esa manera infiltrarse (por medio de pequeñas células) en esos estados y por medio de una simbiosis, fortalecerse.

En un escenario tan complejo, que el informe de inteligencia contraterrorista debe valerse de todos los artificios posibles para que pueda ser efectivo, donde las doctrinas rígidas y convencionales no serán capaces de enfrentar un enemigo tan versátil y oculto.

La era del conocimiento

En 1969, en "La era de la discontinuidad", su libro más conocido, Peter Ferdinand (Drucker, 1992) escribió una sección sobre "la sociedad del conocimiento". Drucker añadió que, a finales de los '70, el sector del conocimiento generaría la mitad del PIB. En 1970, el tema del encuentro anual de la *"American Society for Information Science"* fue *"La Sociedad de la Información-Consciente"*, y un artículo presentado trató sobre *"El Advenimiento de la Sociedad de la Información"*. Para Drucker, las nuevas tecnologías de la información y la comunicación, que acompañan a la sociedad de la información y la sociedad del conocimiento, están transformando radicalmente las economías, los mercados y la estructura de la industria, los productos y servicios, los puestos de trabajo y los mercados laborales.

Drucker argumentó hacia 1946, que al regresar de los campos de batalla, los soldados estadounidenses exigían una matrícula en alguna universidad, y no sólo un empleo seguro como habían exigido sus antecesores al término de la I Guerra Mundial. Drucker sostenía que el cambio de comportamiento de los veteranos demostraba que el conocimiento estaba siendo más valorado que la simple ocupación laboral. Para el sociólogo estadounidense Daniel Bell, la nueva era comenzó en 1956 cuando el número de cuellos blancos superó al de obreros en Estados Unidos. Él advirtió: "¡Qué poder obrero que nada! La sociedad camina hacia la predominancia del sector de servicios". Es decir, el poder se dirigía hacia aquellos que poseían algún tipo de conocimiento que interesaba a otros. Para la llegada de la sociedad del conocimiento en los países desarrollados, el número de trabajadores sin especialización disminuyó, la cualificación del trabajador predominó y la educación se volvió vital. Esa sociedad se expresa por la conexión funcional de la universidad con la empresa y por el poder económico centrado en el conocimiento (Bell, 1973, pág. 408).

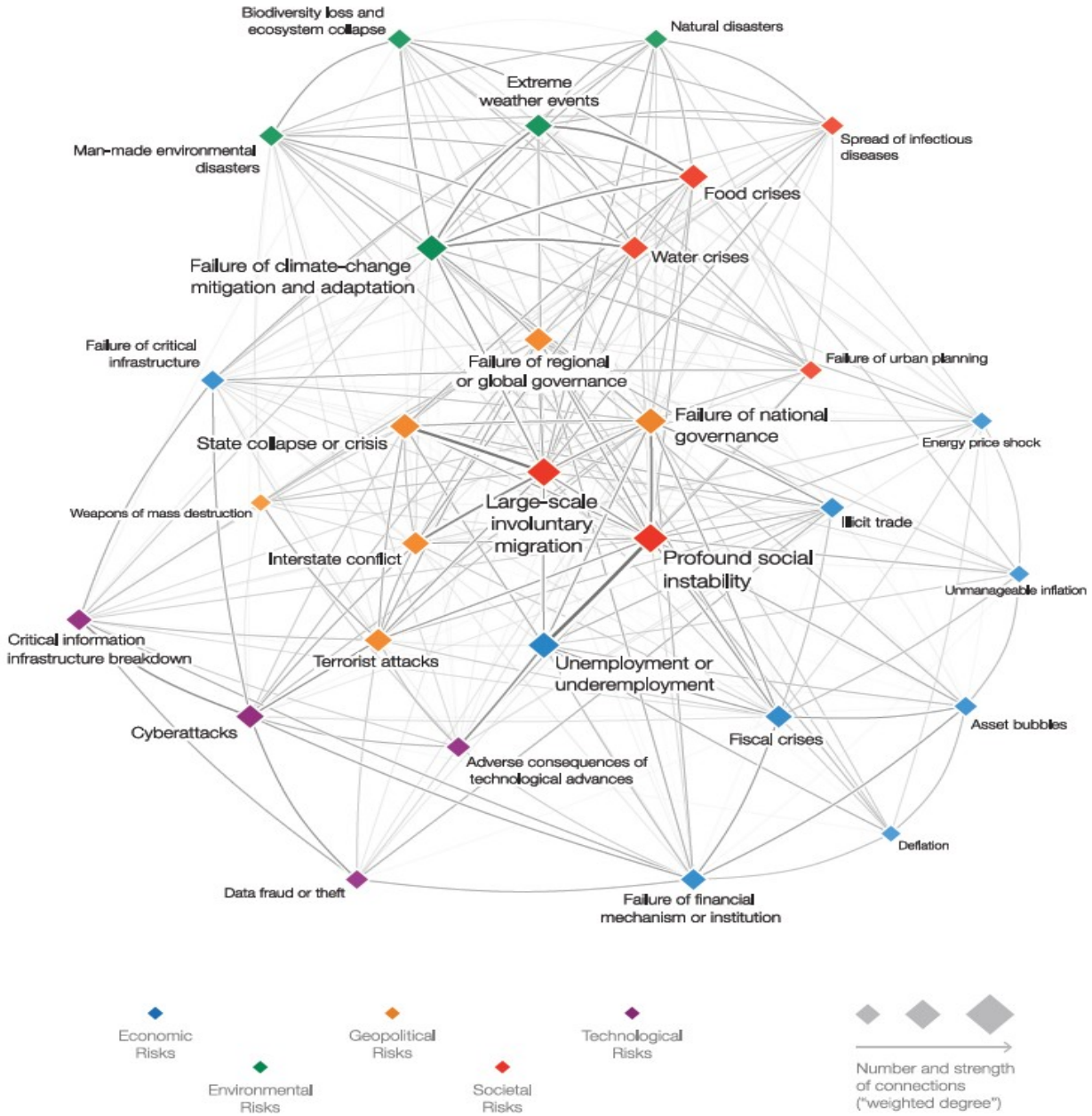
El poder, en su expresión más simple, es la capacidad de imponer la voluntad. Es una síntesis de voluntad y de medios económicos, tecnológicos, militares y otros para imponer esa voluntad. La era del conocimiento es deslumbrante y desafiante, en ella el poder está en manos de los hombres, de las naciones y de las instituciones que tienen el conocimiento. El capital mayor de cualquiera de esas organizaciones son sus recursos humanos. Preservarlos, enriquecerlos y estimularlos es la más sabia aplicación que pueden hacer sus líderes.

La necesidad de incluir la información

como factor preponderante en la conducción de la guerra, así como en los procesos que la anteceden y en aquellos que suceden las operaciones militares, haciendo surgir en diversos países numerosos estudios y documentos doctrinarios sobre el asunto.

El Informe de Riesgos Globales (World Economic Forum, 2017), producido por el Foro Económico Mundial, presenta un diagnóstico de los riesgos más marcados que involucran la actual coyuntura global, dentro de cinco grandes áreas de interés: economía, geopolítica, medioambiental, social y tecnológica. Según Klaus Schwab, fundador y Presidente Ejecutivo del WEF, el informe de 2017 destaca que el mundo de hoy se encuentra en un nivel sin precedentes de riesgos interconectados entre todas las áreas de interés. El tema destacado en el presente año fue, el proceso de decisión en ese mundo interconectado y la necesidad de incrementar la conciencia sobre los impactos globales de los riesgos derivados de esta situación. Es fácil inferir que, como consecuencia directa de ese ambiente complejo, el proceso de toma de decisiones deberá ser influenciado con el máximo de informaciones posibles, provenientes de las más diversas áreas de interés.

La figura siguiente (retirada sin traducción del informe original) busca mostrar las interconexiones entre los principales riesgos citados en el informe. Es interesante observar que el grosor de las líneas, el tamaño y la transparencia de los rombos indican, respectivamente, el grado de interconexión, la probabilidad de ocurrencia y la gravedad del impacto que deberá percibirse por el mundo por cada uno de los riesgos representados. Un ejemplo es el riesgo de ataques terroristas que, de acuerdo con la ilustración, se interrelaciona de forma marcada a más de otros diez riesgos, entre ellos: los ataques cibernéticos, el comercio ilícito, la ruptura de infraestructuras críticas, la profunda inestabilidad social, las armas de destrucción masivas, y otros. De esta forma, resulta fácil entender que, en este escenario complejo, las naciones necesitan un eficiente sistema de gestión de la información, donde todas las fuentes deben ser empleadas con la sinergia debida, para enfrentar los riesgos que se presentan.


Biodiversity loss and ecosystem collapse
Natural disasters
Extreme weather events
Man-made environmental disasters
Spread of infectious diseases
Food crises
Failure of climate-change mitigation and adaptation
Water crises
Failure of critical infrastructure
Failure of regional or global governance
Failure of urban planning
State collapse or crisis
Failure of national governance
Energy price shock
Weapons of mass destruction
Large-scale involuntary migration
Illicit trade
Interstate conflict
Profound social instability
Unmanageable inflation
Critical information infrastructure breakdown
Terrorist attacks
Unemployment or underemployment
Cyberattacks
Fiscal crises
Asset bubbles
Adverse consequences of technological advances
Deflation
Data fraud or theft
Failure of financial mechanism or institution
Economic Risks
Geopolitical Risks
Technological Risks
Environmental Risks
Societal Risks
Number and strength of connections ("weighted degree")

Discusión

Inteligencia

Al igual que los filósofos, los teóricos de la inteligencia, rara vez coinciden en definiciones claras de su trabajo, sin embargo, las teorías sobre la inteligencia generalmente la explican como la información que se recoge y analiza, a veces en secreto, y luego se utiliza para entender una situación particular y actuar con ventaja en base a ella. Este proceso ofrece información prescriptiva, por lo general a un tomador de decisiones o de políticas (de una empresa, institución, de una fuerza armada o de una nación), entendiéndose como inteligencia. Por lo tanto, más importante que la definición de inteligencia, es el proceso por la cual se obtiene. Sea cual sea su finalidad, lo que importa es la capacidad de una institución para recolectar datos y transformarlos en informaciones útiles y luego en conocimiento estratégico para el tomador de decisiones.

Según algunos autores clásicos, como el norteamericano Sherman Kent, el término inteligencia puede entenderse según en tres diferentes acepciones: organización, actividad y conocimiento. Como organización es un conjunto de recursos materiales y humanos especializados. Como actividad, es un método científico de trabajo y como conocimiento, es el resultado del proceso de obtención, análisis e integración de datos sobre fuerzas y áreas de operación (Kent, 1967).

Existe la tendencia a que todos los tipos de agencias de inteligencia concuerdan que la inteligencia puede ser creada por los analistas usando diferentes miradas y métodos de recolección y fuentes de información. Se utiliza todo, desde la comunicación actual y los registros de datos, hasta los diplomáticos, los espías, las fotografías, y los resultados y discusiones subsiguientes son desplegadas para ayudar al formulador de políticas a tomar decisiones. Tradicionalmente, aún hoy en día, estas informaciones se utilizan como parte del ciclo de inteligencia, especialmente cuando los comandantes y los responsables políticos toman decisiones tácticas y las ponen en acción. En una secuencia temporal más amplia, la inteligencia se utiliza como parte de un proceso operacional y estratégico de planificación para el futuro, que puede incluir pronósticos y predicciones de escenarios. Por lo tanto, la inteligencia puede incluir una comprensión de la realidad actual, a menudo incorporando algunos conocimientos actuales y pasados o creencias validadas sobre las intenciones de un individuo u organización en particular, sus acciones y las amenazas potenciales que representan (Rolington, 2013).

Debido a la creciente intangibilidad del ambiente contemporáneo, el informe de inteligencia en la prevención y en la lucha contra el terrorismo debe priorizar la valorización de las "fuentes abiertas" (es decir todas las que estén disponibles al público en general) y un monitoreo de los "factores de conocimiento", tales como: opiniones religiosas del oponente, su cultura, nivel de instrucción y entrenamiento, fuentes de información, entre otros. Además, se debe atribuir énfasis al empleo de fuentes humanas, armadas con sofisticadas tecnologías (incluso cibernéticas) y a la utilización de analistas expertos regionales, lingüistas y otros. Según Mark M. (Lowenthal, 2006), el primer y más importante objetivo de cualquier comunidad de inteligencia es rastrear amenazas, fuerzas, acontecimientos y desarrollos que pongan en riesgo la existencia de la nación.

Una relevante característica que la inteligencia contemporánea debe observar en la prevención y en el combate al terrorismo, es la importancia de la conectividad, ya que

los datos después de procesados, se convierten en información y, desde que se analizan creando conocimiento, no valen en las manos equivocadas y en el momento inoportuno. Hay necesidad de formular maneras de distribución de datos y/o informaciones de acuerdo con las exigencias, ya que la naturaleza de las redes de comunicaciones presupone hipótesis estratégicas muchas veces, mantenidas en secreto y producto de la capacidad de intercambiar información por la red permite que los especialistas puedan relacionar todos los conocimientos, desde el punto de vista de la gestión del conocimiento.

Se debe poner énfasis en la exactitud en la búsqueda de datos negados debiendo concentrarse, prioritariamente, en la calidad de las informaciones, que deben abarcar entre otros, los aspectos militares, políticos, psicosociales científico-tecnológicos, económicos, diplomáticos y otros que sean necesarios, utilizando las más variadas y avanzadas técnicas para obtenerlas. La inteligencia estratégica debe valorar la posibilidad de que el oponente o potenciales adversarios puedan utilizar información engañosa o la desinformación. En este contexto, se vuelve fundamental la actuación metodológicamente integrada de capacidades relacionadas a la información, en conjunto con otros vectores, que sean capaces de informar e influenciar a grupos e individuos y al ciclo decisorio de adversarios, al mismo tiempo que protege las informaciones de la propia institución. Esta es la búsqueda por la superioridad de informaciones, blanco permanente de las Op Info.

Esta investigación se focalizara en la inteligencia que una nación o fuerza armada (o fuerza de seguridad) utilizan para el combate al terror. Este tipo de inteligencia se clasifica como estratégica debido al hecho de servir como soporte directo y fundamental en las decisiones políticas y estratégicas de más alto nivel del Estado. Ya que en la prevención y la lucha contra el terrorismo y la violencia extremista transnacional, se debe tener la idea de que la información es un "activo estratégico", pues, además de servir como importante vector operativo y táctico, es una poderosa palanca capaz de cambiar decisiones de alto nivel por parte del oponente. La llamada "estrategia del conocimiento" prioriza la explotación de cuatro funciones clave en lo que concierne al conocimiento: adquirir, procesar, distribuir y proteger informaciones.

Normalmente, las agencias de inteligencia de la mayoría de los países occidentales suelen difundir el conocimiento producido a través de informes de inteligencia, evaluados por la credibilidad de la noticia y por la fiabilidad de la fuente, según una escala que poco varia de un país para otro, como muestra la tabla abajo:

Clasificación de la credibilidad	Clasificación de la fiabilidad
1 *Confirmado por otras fuentes*	***A*** *Completamente fiable*
2 *Probablemente cierta*	***B*** *Normalmente fiable*
3 *Creíble*	***C*** *Medianamente fiable*
4 *Dudosa*	***D*** *Normalmente no fiable*
5 *Improbable*	***E*** *No fiable*
6 *Certeza desconocida.*	***F*** *Fiabilidad desconocida*

Tabla 1: Evaluación del Informe de Inteligencia (Clase 58 del Máster Fenomenología del Terrorismo – UGR/2017)

En la clase 57 de ese posgrado, fue mencionado que *el informe de inteligencia debe presentar la información que aporta y que previamente ha sido recopilada de modo claro y conciso; debe poder leerse de forma rápida asimilando los datos que aporta sin problemas.* Pero ¿de qué datos exactamente se está hablando? ¿La doctrina actual de producción del informe de inteligencia contraterrorista, posee la velocidad y amplitud de fuentes compatibles con la tramitación de los datos en la era del conocimiento?

Operaciones de Información (Op Info)

El ejemplo de EUA

Durante la década de '90, los estadounidenses comenzaron a desarrollar su doctrina de Operación de Información (Op Info) que, de una forma u otra, maduró en un ambiente de conflictos en Oriente Medio, donde aplico las mejores prácticas de las Operaciones Basadas en Efectos (*Efect Bases Operations - EBO*) y de la Guerra Electrónica (GE).

La necesidad de que comandantes militares conduzcan operaciones conjuntas y combinadas (en las cuales ejércitos de tierra, mar y aire se integran a escalones más elevados y se articulan con fuerzas multinacionales), ha contribuido a expandir el ambiente de información situado en su tradicional área de interés. El nivel de planificación conjunto abarca, entre otras áreas, la necesidad de interconexión de sistemas de control complejos, en los diversos niveles de mando. Además, de la creciente la necesidad de captación y de la gestión de la información proveniente de todas las áreas del conocimiento, a través de una red de conocimiento global. De esta forma, las Fuerzas Armadas dependen cada vez más de la libre utilización de todo el espectro de información para cumplir sus misiones, con eficacia y eficiencia.

A partir del hecho de que la información ha desempeñado un papel de creciente importancia en toda forma de conflicto, Estados Unidos fue el país que primero decidió desarrollar un cuerpo doctrinal específico, orientado a sistematizar la utilización de la información en el ambiente del futuro campo de batalla. En la doctrina americana, las opciones de inteligencia integradas inicialmente en la guerra de mando y control (*Combat and Control War - C2W*), involucrando el ataque a los medios de mando y control enemigos (*C2 - Attack*) y la protección de la capacidad de mando y control amiga (*C2 - Protect*). Posteriormente, este concepto incluyó otras dos actividades de creciente importancia para la conducción de los conflictos: los Asuntos Civiles y la Información Pública. En el conjunto integrado de todas estas actividades se asignó la designación de Operaciones de Información, para la cual el ejército estadunidense elaboró, como soporte doctrinal para su conducción, el Field Manual 100-6 (US Army Staff, 1996).

De acuerdo con el FM 100-6, las Operaciones de Información se definen como las operaciones militares continuas, dentro del ámbito de la información militar, que facilitan, refuerzan y protegen la capacidad de las fuerzas amigas para obtener, procesar y actuar sobre la información, para obtener una ventaja en toda la gama de operaciones militares. Por lo que se refiere a los sistemas de información, el FM 100-6 ya presentaba una descripción de sus funciones y su papel en la conducción de las operaciones, distinguiendo los sistemas militares de los sistemas civiles y exponiendo algunos aspectos relacionados con su gestión y seguridad.

El problema era que el Comando Conjunto Norteamericano (*US JOINTCOM*) defendía que las Operaciones de Información deberían incluir la interacción con el ambiente de información global y la explotación o degradación de la información del enemigo y de los recursos que éste necesita para tomar decisiones. Se puede inferir que, esta concepción involucra los tres niveles de conducción de las operaciones (estratégico, operacional y táctico), ya que todos ellos se revelan necesarios para su planificación y ejecución.

La creciente importancia de las Op Info, en un contexto más integrado y completo (civil y militar), llevó al

Departamento de Defensa de los Estados Unidos (*US DoD*) a desarrollar una doctrina específica para la conducción de Op Info Conjuntas. Esta preocupación se tradujo en la Publicación Conjunta JP 3-13 (US DoD, 1998), donde los aspectos de interdependencia estructural y funcional entre sistemas civiles y militares condicionan el proceso de planificación y ejecución de las Op Info. Dentro de este marco, la guerra de información se definió como "el conjunto de las Operaciones de Información llevadas a cabo durante un período de crisis o conflicto con la finalidad de alcanzar o promover la consecución de objetivos específicos sobre uno o más adversarios." Esta definición alteró el concepto anteriormente establecido para la guerra de información (FM 100-6) e hizo que las Op Info se desarrollarse no sólo a nivel estratégico-militar, sino también a nivel político-estratégico.

Reflejo de esa visión y tras los atentados del 11 de septiembre de 2001, la Quadrennial Defense Review identificó las Op Info como uno de los seis objetivos operativos críticos para la transformación de las fuerzas armadas de EEUU. Ese documento apuntaba a la necesidad de que las Op Info sean tratadas no sólo como facilitadoras de las actividades, pero esencialmente, como una capacidad fundamental, al lado de las operaciones aéreas, terrestres, marítimas y operaciones especiales, condicionantes del éxito operacional de las futuras fuerzas armadas. La planificación de la Defensa pasó así a encarar a las Op Info como una competencia clave completamente integrada a la planificación y resolución de crisis, capaz de ser soportada y de poder soportar la conducción de las operaciones militares.

En esa misma línea de raciocinio, el 30 de octubre de 2003, el Secretario de Defensa de los EE. UU., aprobó la publicación de un guía para las operaciones de información, el *Information Operations Roadmap (IOR)* (Rumsfeld, 2003), cuya esencia fue hacer de las OP Info una competencia militar fundamental, estableciendo directrices y metas para todos los actores involucrados con la Defensa, desde el nivel político-estratégico hasta el nivel táctico de actuación. En vista de que el empleo de las Op Info se inicia en la paz, se extiende durante toda la crisis y sólo finaliza tras la restauración de la paz y la estabilidad, la citada publicación destacó tres funciones integrantes que debían alcanzarse, en su plenitud, a más corto plazo, que sean:

- Detener, desalentar, disuadir y dirigir a un adversario por medio de la desintegración de su unidad de mando e intención de combatir, mientras preserva su propia;

- Proteger sus planes y desorientar a los adversarios, permitiendo así maximizar el efecto de sus fuerzas, obteniendo exorbitante ventaja, mientras que el adversario gasta sus recursos para obtener efectos reducidos o limitados;

- Controlar las comunicaciones y redes del adversario y proteger a las suyas, incapacitando así la habilidad del enemigo para organizarse y defenderse mientras preserva el efectivo C2 de sus fuerzas.

Siguiendo las orientaciones emanadas por el Departamento de Defensa, el jefe del Estado Mayor Conjunto de las Fuerzas Armadas aprobó el 13 de febrero de 2006, una actualización del JP 3-13, cuya versión se convirtió en un compendio detallado de la doctrina de Op Info, para el nivel operativo de planificación y del que cabe resaltar algunos conceptos:

- Las OP Info se describen como el empleo integrado de **capacidades fundamentales**, como la Guerra Electrónica (GE), la Guerra Centrada en Redes (GCR), las Op. Psicológicas, la Decepción y la Seguridad. En lo que se refiere a sus especificidades y capacidades relacionadas

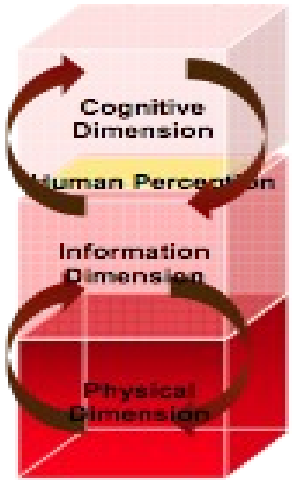
para influenciar, romper, corromper o usurpar el proceso de decisión humano o automatizado de un adversario, mientras se protege al de los aliados;

- Constituyen **capacidades de apoyo** de las OP Info: la Garantía de las Info, la Seguridad Física, el Ataque Físico, la Contrainteligencia y el Combate Transmitido por Cámaras (COMCAM);

- Constituyen **capacidades relacionadas**: las Relaciones Públicas, la Cooperación Civil-Militar y la Diplomacia Pública; y de los demás.

- Las OP Info tendrán prioridad en la comunidad de inteligencia, ya que las fuentes siempre serán limitadas y, normalmente, el plazo para la obtención de los productos necesarios suele ser largo, teniendo en cuenta las restricciones legales y las especificidades del público objetivo.

La última versión del JP 3-13 ha sido publicada el 20 de noviembre de 2014 y, sin duda, fue la que mejor interpreto las Op Info y el ambiente de la información. Así, las Operaciones de Información consisten en la actuación y metodología integrada de capacidades relacionadas a la información, en conjunto con otros vectores, para **informar e influenciar** a grupos e individuos, así como afectar el ciclo decisorio de oponentes y al mismo tiempo protegiendo el nuestro. Sus actores son los líderes, los que toman decisiones, los individuos y las organizaciones. Normalmente los recursos involucrados son materiales y sistemas empleados para recopilar, analizar, solicitar o diseminar información. De esta forma, el ambiente de la información es donde humanos y sistemas observan, orientan, deciden y actúan sobre las informaciones, constituyéndose así en el principal ambiente donde se toman las decisiones. Este nuevo ambiente está constituido de tres dimensiones distintas, como se muestra en el grafico siguiente:



Por otro lado, pretenden evitar, impedir o neutralizar los efectos de las acciones adversas en la dimensión informacional, la cual puede traducirse como un agregado de individuos, organizaciones y sistemas que recogen, procesan, diseminan o actúan sobre la información. Sus actores son los líderes, los que toman decisiones, los individuos y las organizaciones. Los recursos involucrados son los materiales y sistemas empleados para recopilar, analizar, solicitar o diseminar información.

De esta forma, el ambiente de la información es donde humanos y sistemas observan, orientan, deciden y actúan sobre las informaciones, constituyéndose así en el principal contexto donde se toman las decisiones. Es decir que la doctrina pura y tradicional de inteligencia debería se adaptar al ambiente informacional moderno de la era del conocimiento, especialmente cuando se tratar de un ambiente asimétrico y obscuro como es la guerra al terrorismo.

DIMENSIONES DE LA INFORMACIÓN
Dimensión Cognitiva - donde se toman las decisiones humanas. Es la dimensión del intangible, donde residen la moral, la cohesión de las unidades militares, la opinión pública, la conciencia situacional, las percepciones humanas, las emociones y los entendimientos.
Dimensión de la información - donde se toman las decisiones automatizadas, ya que es en esta dimensión que la información es recolectada, procesada, almacenada, diseminada, exhibida y protegida. Tiene una naturaleza ambigua, pues se trata de la propia información y el medio por el cual ella tramita, ocupándose del contenido, de la calidad y del flujo de las informaciones. Esta dimensión se une a otras dos.
Dimensión Física - donde ocurre la intersección del ambiente de la información con el mundo físico. Son las computadoras y las redes que componen los sistemas de datos y de comunicaciones, y que soportan toda la infraestructura.

Grafico Nr 1 – Dimensiones de la Información (JP 3-13)

El ejemplo de Europa

Al constatar que sus estructuras orgánicas dependían de forma significativa, de las informaciones y de sus procesos asociados, la OTAN comenzó a desarrollar una política para la conducción de Operaciones de Información. Tal política siempre tuvo por finalidad reducir las vulnerabilidades y aprovechar las oportunidades de la Alianza, en lo que se refiere al control de la información necesaria al proceso de toma de decisión.

La OTAN publicó por primera vez su política de Op Info en 1998, realizó una revisión en 2002 y otra en 2005. El 23 de noviembre de 2009, la Organización publicó el *Allied Joint Doctrine for Information Operations* (NATO, 2009), con el propósito de explicar, doctrinariamente, cómo las Op Info pueden apoyar la planificación, la conducción y la evaluación de las operaciones militares. A pesar de ser un documento centrado en el nivel operativo, el AJP-3.10 deja bien clara su subordinación al nivel político-estratégico, del que emanan las orientaciones para las acciones militares, que aisladamente no pueden resolver la crisis, pero pueden establecer condiciones para que otros actores la resuelvan, incluyendo el uso de todas las capacidades del poder nacional, ofrecidas por los estados miembros de la OTAN.

Este mismo documento define las OP Info como una función militar que ofrece tanto el asesoramiento como la coordinación de las actividades de información militar, siendo su propósito el crear el efecto deseado en la voluntad, en el entendimiento y en las capacidades de los adversarios, potenciales adversarios y otras amenazas aprobadas por el Consejo del Atlántico Norte, en apoyo a los objetivos militares establecidos por ese Consejo.

Para cumplir su objetivo, la doctrina de Op Info de la Alianza Atlántica se basa en los siguientes principios: enfoque de las operaciones basadas en efectos; implicación personal hacia el comandante; coordinación aproximada y secuencial; información e inteligencia exacta; planificación centralizada y ejecución descentralizada; designación de blancos conjuntos; la participación cuanto antes y la preparación en tiempo hábil; la continuidad; el seguimiento y evaluación continuos.

Estos principios se emplean en tres áreas de actividades que tienen los siguientes focos específicos:

- Actividades destinadas a cambiar, influenciar o reforzar las percepciones y actitudes de los adversarios;
- Actividades destinadas a preservar y proteger la libertad de maniobra de la Alianza en el ambiente de la información, a través de la defensa de datos e informaciones que apoyen el proceso y la toma de decisiones;
- Actividades que buscan alcanzar la capacidad de mando del adversario, afectando las informaciones que sirven de datos de soporte para el C2, inteligencia, vigilancia y adquisición de blancos, además

de aquellos de los cuales se valen los sistemas de armas inteligentes.

Dentro de las tres áreas de actividades descritas arriba, las tropas de la OTAN pueden valerse de una serie de técnicas, herramientas o capacidades inherentes a la Alianza, de forma que logren alcanzar los objetivos propuestos o el estado final deseado. Es decir, un gran paraguas bajo el cual varias otras operaciones se desarrollan, tales como: Operaciones Psicológicas, Operaciones de Seguridad, Seguridad de la Información, Disimulación, Guerra Electrónica, Combate a Líderes, Operaciones de Presencia, Postura y Perfil, Operaciones Centradas en Redes, Relaciones Públicas y Cooperación Civil-Militar.

Aunque la firma del Tratado que creó la Alianza Atlántica se remonta a 1949, las diferencias culturales y sociales que aún existen entre los Estados miembros han dificultado una orientación doctrinal clara por parte de la OTAN, especialmente por el desnivel doctrinario de los asuntos arriba descritos en cada uno de los estados miembros. Esas diferencias han suscitado cierta ambigüedad en cuanto a la forma en que se deben llevar a cabo las Op Info y cómo éstas pueden integrarse en la planificación y ejecución de las operaciones militares, revelando algunas dificultades en la asignación de responsabilidades en su ejecución.

La falta de unidad en el discurso y en el pensamiento, especialmente en el área de inteligencia, provoca retraso en la gestión del conocimiento y en el trámite de las informaciones, lo que ha permitido que grupos terroristas aprovechen las brechas de seguridad y defensa para acometer sus atentados.

Gestión del Conocimiento

Coincidencia o no, en ese mismo período, los conceptos de gestión de la información y de gestión del conocimiento trascendieron el ambiente militar y se adaptaron fácilmente al mundo corporativo, cuya mayor motivación es el lucro (estado final deseado) y el enemigo más importante es la competencia (si para los militares eliminar y / o neutralizar al enemigo es un objetivo relevante, sobrepasar la competencia significa a menudo la propia supervivencia de las empresas). Es decir que, la buena gestión del conocimiento puede ayudar y, en muchos casos, resolver los problemas relacionados con el escenario informativo, ahorrando esfuerzos, recursos, tiempo, sirviendo de base para la planificación estratégica y para la toma de decisión.

Es innegable la importancia que algunos términos reciben, ya sea en el ámbito académico, en la esfera operativa, o incluso en el mundo corporativo también es innegable el legado de conocimientos provenientes de la investigación doctrina de inteligencia, que servirá de base sobre la cual este trabajo pretende provocar una reflexión. De esta forma, es interesante aclarar, desde ahora, los conceptos más elementales sobre datos, información y conocimiento.

En "*Working Knowledge: Hoy Organizations Manage What They Know"*, Thomas H. Davenport y Lawrence Prusak (Davenport & Prusak, 1998) afirmaron que los datos son la mínima unidad semántica, y se corresponden con elementos primarios de información que por sí solos son irrelevantes como apoyo a la toma de decisiones. También se pueden ver como un conjunto discreto de valores, que no dicen nada sobre el "por qué" de las cosas y no son orientativos para la acción. Un número telefónico o un nombre de una persona, por ejemplo, son datos que, sin un propósito, una utilidad o un contexto no sirven como base para apoyar la toma de una decisión. Los datos pueden ser una colección de

hechos almacenados en algún lugar físico como un papel, un dispositivo electrónico (CD, DVD, disco duro...), o la mente de una persona. En este sentido las tecnologías de la información han aportado mucho a recopilación de datos. Como cabe suponer, los datos pueden provenir de fuentes externas o internas a la organización, pudiendo ser de carácter objetivo o subjetivo, o de tipo cualitativo o cuantitativo.

La información, a su vez, se puede definir como un conjunto de datos procesados y que tienen un significado (relevancia, propósito y contexto), y que por lo tanto son de utilidad para quién debe tomar decisiones, al disminuir su incertidumbre. Los datos se pueden transforman en información añadiéndoles valor. Contextualizando: se sabe en qué contexto y para qué propósito se generaron. Categorizando: se conocen las unidades de medida que ayudan a interpretarlos. Calculando: los datos pueden haber sido procesados matemática o estadísticamente. Corrigiendo: se han eliminado errores e inconsistencias de los datos. Condensando: los datos se han podido resumir de forma más concisa (agregación). Por lo tanto, la información es la comunicación de conocimientos o inteligencia, y es capaz de cambiar la forma en que el receptor percibe algo, impactando sobre sus juicios de valor y sus comportamientos.

Por último, el conocimiento es una mezcla de experiencia, valores, información y "*know-how*" que sirve como marco para la incorporación de nuevas experiencias e información, y es útil para la acción. Se origina y aplica en la mente de los conocedores. En las organizaciones con frecuencia no sólo se encuentra dentro de documentos o almacenes de datos, sino que también está en rutinas organizativas, procesos, prácticas, y normas. El conocimiento se deriva de la información, así como la información se deriva de los datos. Para que la información se convierta en conocimiento es necesario realizar acciones como: comparación con otros elementos, predicción de consecuencias, búsqueda de conexiones y conversación con otros portadores de conocimiento.

Según Ikujiro Nonaka y Hiro Takeuchi (Nonaka & Takeuchi, 1995), no es por el hecho de que las organizaciones no tienen conocimiento que acaban por tomar decisiones erróneas, sino por el hecho de que el conocimiento esté escondido en algún lugar de la organización o en la cabeza de alguien, es decir, el hecho de que el conocimiento esté implícito, inaccesible o no sea divulgado favorece la toma de decisión equivocada.

Otra figura interesante y esclarecedora, ya conocida por muchos, pero no tan bien comprendida, es la que Michael Polanyi (Polanyi, 1967) utilizó para definir los conocimientos tácito y explícito. El conocimiento tácito es la parte sumergida del iceberg, que sostiene todo el conocimiento. Este tipo de conocimiento es siempre personal, intransferible y específico al contexto. No es posible su codificación en libros u organización de teorías. El conocimiento explícito es la parte emergida del iceberg, que representa sólo una pequeña parte de todo el conocimiento del individuo. Es aquel conocimiento que puede ser compartido entre los demás.

La teoría presentada por Nonaka y Takeuchi considera que la creación se da partir de la distinción entre conocimiento tácito y explícito. El nuevo conocimiento generado pasa a no ser más individual y sí pertenecer al grupo. El proceso atraviesa cuatro modos de conversión de conocimiento: la socialización (tácito en tácito), la externalización (tácito en explícito), la combinación (explícito en explícito) y la internalización (explícita en

tácito). Con el ciclo completo, se genera el "Espiral del Conocimiento", que los autores consideran como un flujo continuo de creación y el compartir del conocimiento organizacional.

Pero es por causa del conocimiento tácito que el ser humano pasa a ser considerado fundamental para todo proceso de generación y de gestión del conocimiento. Por otro lado, el ser humano es naturalmente susceptible de resistencia a los cambios. Cambiar una manera de pensar y actuar siempre enfrenta barreras psicosociales e intelectuales. En plena era de la información, el inmenso volumen de datos, información y conocimientos explícitos requieren procesos automatizados para su buena gestión. Por lo tanto, las personas, procesos y sistemas (o herramientas de TI) forman la base triangular de la buena gestión. Los conceptos presentados, si se entienden bien, pueden ser aplicados de varias maneras en corporaciones privadas, instituciones gubernamentales y también las fuerzas armadas de todo el mundo ya disfrutan de las buenas prácticas de la gestión de información y conocimiento.

Como ya se ha dicho antes, la cuestión de la gestión de la información y del conocimiento ha sido observada como "piedra angular" de las Operaciones de Información. Es muy probable que el carácter permanente de este tipo de operaciónes sea el principal motivo de esta constatación. Es fundamental que los líderes, en todos los niveles, entiendan que no se puede pensar en conducir Op Info sólo durante las crisis. El escenario informacional necesita ser construido y constantemente actualizado, empezando mucho antes de la crisis y extendiéndose hasta después de ella.

Informar e influenciar a diversos públicos y audiencias no es tarea sencilla. Requiere personal especializado, recursos y tiempo de preparación para campañas bien elaboradas. Este tipo de operación debe ser conducida por el más alto escalón posible, de esta forma, el capital intelectual de la organización o del escalón responsable de conducir las Op Info se convierte en su bien más precioso. Algunas de las mejores prácticas observadas por países con mayor desenvoltura en esas operaciones apuntan a la mentalidad de gestión de la información y del conocimiento que sus Fuerzas Armadas poseían desde el período pre-crisis.

CONCLUSIONES

Dieciséis años después de los dramáticos atentados de 11 de septiembre de 2001, mucho ha sido hecho en la lucha contra la amenaza terrorista. Se multiplicaron las iniciativas de represalia, principalmente por parte de los Estados Unidos y de los países de la Comunidad Europea. A modo de ejemplo, se destaca el endurecimiento de la legislación, el refuerzo de la cooperación internacional antiterrorista, las acciones ostensibles y encubiertas de las agencias de inteligencia, el empleo de tecnologías avanzadas y las armas de última generación y el desarrollo de una doctrina común antiterrorista.. Como ya fue visto antes, eso es fruto de una inmensa gama de conocimiento sobre el tema terrorismo, que se multiplica a cada día y que necesita ser gestionada de alguna forma.

El entendimiento y el conocimiento de las motivaciones y capacitaciones de una organización terrorista posibilitan una sólida fundamentación en la conducta de operaciones contraterroristas exitosas (US Joint Chief of Staff, 2009). Debido al alto grado de letalidad y del largo alcance de los avanzados sistemas de armas, la tendencia de los terroristas será buscar operar en medio de la población, y el peligro a que combatientes y no combatientes van a estar expuestos será mucho mayor que en conflictos pasados. Es posible inferir que actores estatales y no estatales también van a utilizar todo su acervo de opciones, incluyendo los de carácter político, económico, psicosocial e informacional, para combatir ese enemigo común.

En ese escenario asimétrico, con excepción de las operaciones cibernéticas, todas las otras operaciones tenderán a ejecutarse en presencia de comunidades civiles no combatientes, lo que se constituye en uno de los más graves problemas que se plantean para la distinción del enemigo. Por lo que, en conflictos de esta naturaleza, los resultados finales se evaluarán en términos de efectos en los diferentes públicos en presencia.

Los entornos operativos siguen siendo extremadamente fluidos. Las coaliciones, alianzas y actores protagonistas cambian continuamente. Las operaciones multidisciplinares entre las diferentes agencias son altamente solicitadas para gestionar situaciones con esta variedad de actores. La presencia de los medios de comunicación es cada vez más relevante, en virtud de su actual postura independiente y la visión por la noticia de los acontecimientos ejerce una inmensa influencia sobre los diferentes públicos. Es decir, los ambientes operativos están interconectados de una forma tremenda, así como las amenazas también. La financiación de los grupos terroristas y sus interconexiones con varias organizaciones criminosas está emergiendo de forma clara, a cada día. Es evidente que el esfuerzo por la mayor efectividad en el monitoreo y en las acciones de pronta respuesta a los ilícitos transnacionales y domésticos debe ser mejorado, lo que probablemente reforzaría la capacidad de las organizaciones para cooperar en la lucha contra la amenaza terrorista.

Tras analizar ese escenario complejo de la era de la información y/o conocimiento y los mecanismos que confieren a las organizaciones responsables para la seguridad y la defensa la capacidad de contribuir a la prevención y lucha contra el terrorismo, dos palabras traducen el significado final del estudio: interacción e integración. La interacción que proporcionaría el conocimiento mutuo de las posibilidades y limitaciones de los vectores (militares y civiles), y la integración, que puede ofrecer complementariedad y calidad del producto, que es el mantenimiento de la soberanía y la paz social, en un lenguaje más técnico, la gestión del conocimiento obtenida en todas las áreas del saber, es la mejor arma que se puede emplear en el combate al terror. La inteligencia pura y simple como es concebida por la doctrina vigente no es capaz, por si sola, de gestionar todo el espectro informacional presente nos escenarios de hoy.

Volviendo al problema planteado: *¿En la era del conocimiento, el informe de inteligencia contraterrorista, como es hecho doctrinariamente por la mayoría de las agencias, integra datos y/o informaciones suficientes y oportunos para el combate al terror?* Es posible inferir que, a pesar de muchos avances en la lucha contraterrorista, hay que implementar la integración y la interacción de los datos e informaciones y mejorar la gestión del conocimiento. Las Op Info ya han demostrado que son una herramienta poderosa para unir diversas áreas del saber, no solamente bajo el análisis de expertos en inteligencia, pero también con ayuda y colaboración de otros expertos en diversas otras áreas. Esa forma pluridisciplinar de trabajo seguramente sería capaz de comprender mejor y más rápidamente los escenarios presentados.

De esa forma, al final de esa pesquisa, es posible admitir que la hipótesis que busca contestar al problema planteado es verdadera. Es decir que, por la falta de una buena gestión integrada del conocimiento, el informe de inteligencia contraterrorista, como es concebido por la doctrina de inteligencia vigente, no integra datos y/o informaciones suficientes y oportunos para el combate al terror.

Bibliografía:

Bell, D. (1973). O Advento da Sociedade Pós-Industrial. Cultrix.

Davenport, T. H., & Prusak, L. (1998). *Working Knowledge: How Organizations Manage What They Know.* Cambridge: Haravrd Business School Press.

Drucker, P. F. (23 de agosto de 1992). *The Age of Discontinuity - Guidelines To Our Changing Society .* New York: Harper & Row. Obtenido de Wikipedia: Drucker, Peter. La Era de la

Discontinuidad. https://es.wikipedia.org/wiki/Peter_F._Drucker#Drucker_y_las_sociedades_de_la_informaci.C3.B3n_y_el_conocimiento

Kent, S. (1967). *Informações Estratégicas.* (H. Freire, Trad.) Rio de Janeiro: Biblioteca do Exército.

Lowenthal, M. M. (2006). From Secrets to Policy (third edition). Los Angeles: CQPress.

NATO. (2009). *Allied Joint Doctrine for Information Operations, AJP 3-10.* Brusels : NATO.

Nonaka, I., & Takeuchi, H. (1995). *The Knowledge-Creating Company: How Japanese Companies Create the Dynamics of Innovation .* Boston: Harvard Business Press.

Polanyi, M. (1967). *The Tacit Dimension.* Chicago: University of Chicago Press.

Rolington, A. (2013). *Strategic Intelligence for the 21th Century - The Mosaic Method.* Oxford: Oxford University Press.

Rumsfeld, D. H. (2003). *Information Operations Roadmap.* Washington, DC: DoD.

Toffler, H. y. (1993). War and anti-War: Survival at the Dawn of the 21 Century. New York: Warner Books.

US Army Staff. (1996). *Fiel Manual 100-6. Information War.* Whashington, DC: US Army.

US DoD. (1998). *Joint Publication, JP 3-13. Information Operations.* Whashington, DC: DoD.

US Joint Chief of Staff. (2009). *JP 3-26, Counterterrorism.* EUA: DoD.

Whittaker, D. J. (2001). *The Terrorism Reader.* New York: Routledge.

World Economic Forum. (2017). *Global Risk Report.*