Inteligencia Estratégica en un mundo globalizado en Latinoamérica: Retos y desafíos en el siglo XXI*

Boris Saavedra

Centro William J. Perry de Estudios Hemisféricos de Defensa, Universidad Nacional de Defensa, Washington, D.C
saavedrab@ndu.edu

Recibido: junio 27 de 2015
Aceptado: noviembre 2 de 2015

BIBLID [2225-5648 (2015), 5:2, 75-106]

Resumen

La inteligencia en general ha sido catalogada como algo misterioso por las experiencias históricas en Latinoamérica así como por el desconocimiento en general sobre la verdadera esencia de la inteligencia como actividad primordial del Estado. Este trabajo se enfoca en el análisis del papel de la Inteligencia Estratégica como elemento fundamental de la política pública de seguridad y defensa de la nación en Latinoamérica. Los cambios ocurridos en los albores del presente siglo para la recolección y análisis para la producción de inteligencia son fundamentales. El análisis del poder, internet, la tecnología digital, robótica y computadoras inteligentes son responsables de los cambios más acelerados de nuestra historia. La Inteligencia Estratégica requiere una reforma integral de funcionamiento, en cinco aspectos a destacar: 1) Distinción en materia de competencia de los organismos de inteligencia. 2) la dependencia de los organismos de inteligencia. 3) Limitar la asignación de competencias en materia de inteligencia interior. 4) Establecimiento de un órgano de coordinación al máximo nivel del Estado y 5) Controles externos eficaces. Estos aspectos son imprescindibles para un sistema de inteligencia estratégico acorde con las exigencias del presente y futuro.

Palabras clave

Globalización, inteligencia estratégica, espacio cibernético, poder, tecnología digital, internet, robótica, inteligencia artificial.

* Estudio original elaborado para la revista "Policía y Seguridad Pública" en el marco de las gestiones de apoyo académicas internacionales realizadas por el Centro de Investigación Científica (CINC-ANSP)

Strategic Intelligence in a globalized world in Latin America: Challenges in the XXI century*.

Boris Saavedra

William J. Perry Center for Hemispheric Defense Studies, National Defense University, Washington, D.C
saavedrab@ndu.edu

Received: june 27, 2015
Accepted: november 2, 2015

BIBLID [2225-5648 (2015), 5:2, 75-106]

Abstract:

In general, intelligence has been classified as something mysterious due to the historical experiences in Latin America and the general ignorance about the true essence of intelligence as a primary activity of the State. This paper focuses on the analysis of the role of strategic intelligence as a fundamental element of public security and defense policy of a nation in Latin America. The changes occurring at the dawn of this century for the collection and analysis of intelligence are critical. The analysis of power, internet, digital technology, robotics and intelligent computers is responsible for the rapid changes of our history. Strategic Intelligence requires a comprehensive operational reform in five points: 1) Distinction as far as competition of intelligence agencies is concerned. 2) The dependence of the intelligence agencies. 3) Limiting the allocation of responsibility for domestic intelligence. 4) Establishing a coordinating body at the highest level of the State and 5) Effective external controls. These aspects are essential for a strategic intelligence system in line with present and future demands.

Key words:

Globalization, strategic intelligence, cyber space, power, digital technology, internet, robotics, artificial intelligence.

* Original study written for the "Police and Public Security" Journal within the framework of the international academic support efforts conducted by the Centro de Investigación Científica (CINC-ANSP)

Introducción

Hablar de los servicios de inteligencia en general (o simplemente "inteligencia") ha sido catalogado como algo misterioso y confidencial, tanto por las lamentables experiencias históricas en Latinoamérica como por el desconocimiento en general sobre la verdadera esencia de una actividad primordial del Estado en un mundo globalizado. Sin embargo, hoy día la inteligencia es una herramienta de máxima utilidad no solo en el área pública del gobierno sino en el área privada de los negocios. Este trabajo se enfoca en el análisis del papel de la Inteligencia Estratégica como elemento fundamental de la política pública de seguridad y defensa de la nación en Latinoamérica en el siglo XXI.

Entre las razones que llevan a reexaminar la teoría y la práctica para la producción de Inteligencia Estratégica se encuentran los cambios ocurridos a partir de la década de los noventa en el proceso de recolección y análisis, en el tipo de productos requeridos y en los retos que la comunidad ligada a este tema enfrenta en el presente.

La Inteligencia Estratégica comprende diferentes componentes tales como: una misión, una habilidad y una capacidad nacional. Adicionalmente, es también un elemento de política pública y, como todos los elementos de políticas públicas, debe ser discutido inteligentemente por el público en general. Estos debates son necesarios para lograr desarrollar una política eficiente, que pueda satisfacer los requerimientos de la política de seguridad del Estado y las expectativas de los ciudadanos en general.

A mediados del siglo XX el profesor Sherman Kent (2015) de la Universidad de Yale, quien prestó servicios por mucho años en el gobierno de los Estados Unidos, escribió un libro titulado "Strategic Intelligence for American World Policy" en él se describen los principios para el análisis comprensivo de la información que permitan satisfacer las necesidades de los Estados Unidos como potencia mundial en forma eficiente. De esta manera se comienza a utilizar este término para identificar la rama de la inteligencia encargada de elaborar análisis de carácter compresivo que incluye la evaluación de los potenciales escenarios en el futuro.

La evolución de los servicios de inteligencia y su profesionalización contiene diferentes factores que han dado forma a la estructura y sus responsabilidades. Sin embargo, en Latinoamérica se enmarca dentro de los procesos de adaptación, modernización y transformación del sector de seguridad y defensa en la región en las últimas décadas, a raíz de la llamada Tercera Ola de Democratización a finales de los años setenta del siglo XX (Huntington, 1991). La Inteligencia Estratégica como la conocemos, hoy en día, es el análisis producido en un proceso separado del usado para desarrollar una política. Es la combinación de diferentes

ISSN: 2225-5648, Año 5, Vol. 2, p. 75-106

fuentes de información para lograr un análisis que va mucho más allá de una simple descripción de un despliegue militar o un evento político; se amplía en áreas como **el análisis del poder en todas sus manifestaciones, las comunicaciones, el espacio cibernético, y la tecnología en un mundo globalizado e interdependiente.**

En este orden de ideas, la metodología CAPA "Evaluación del Conflicto y Análisis de las Políticas" (Raza, 2015) empleado por el Centro William Perry de Estudios Hemisféricos de Defensa constituye una herramienta fundamental para el análisis de situaciones potenciales que pueden generar conflictos violentos entre grupos políticamente organizados en el ámbito internacional.

En la primera década del siglo XXI, Naim, (2013), en su obra "The End of Power" considera que estamos viviendo la transición del poder en todas sus manifestaciones y que éste se mueve de norte a sur, de este a oeste, de grandes corporaciones a ágiles e incipientes compañías, de gobiernos autoritarios y represivos al individuo en plazas públicas, y en el espacio cibernético. En definitiva el poder en la actualidad es fácil de obtener, difícil de mantener y fácil de perder.

En medio de esta difusión del poder en todas sus expresiones, los medios de comunicación para masas han transformado la vida de las personas y sus relaciones con el entorno, al cambiar sus percepciones sobre la sociedad y la forma que se tiene de relacionarse con sus semejantes. A partir de la creación de la imprenta, la disponibilidad de materiales escritos se multiplicó. En el siglo del telégrafo nacen dos sistemas de comunicación que revolucionan el mundo de la información: el cine y la radio. Sin embargo, la televisión, en solo unos años, supuso la verdadera revolución. Considerado el rey de las comunicaciones, el televisor modificó incluso los hábitos vitales domésticos.

La llegada del Internet y la consideración del espacio cibernético como "Quinto Dominio" por el gobierno de Estados Unidos, es una de las recientes creaciones de la humanidad que no se ha entendido bien. Lo que comenzó como un medio de información y transmisión con computadoras del tamaño de un cuarto en la década de los setenta a un cuarto lleno de computadoras en la actualidad, se ha transformado en un medio omnipresente y de emisión de un sinfín de energía e ideas. A su vez, es intangible y no responde a los cinco sentidos del ser humano, además de estar en constante mutación que crece y se hace más complejo segundo a segundo. Es una fuente de muchas cosas buenas pero con potencial para la maldad. Internet y las redes sociales que operan en el espacio cibernético han cambiado ciertamente el panorama político-mediático. La habilidad y el poder que tiene hoy día el individuo de crear y difundir su propia opinión transmitiéndola al mundo, genera una interactuación sin precedentes en la historia de la humanidad.

ISSN: 2225-5648, Año 5, Vol. 2, p. 75-106

La combinación de tecnología digital, robótica y computadoras inteligentes es responsable de los cambios más acelerados de nuestra historia. Se están experimentando muchas transformaciones a pasos acelerados, muchas más que en generaciones anteriores; estos cambios se producen por instrumentos que se tienen al alcance de la mano y hacen que se participe mucho más de lo que se podría imaginar. Cada dos días se produce más contenido digital que todo el que fue creado desde el inicio de la civilización hasta el año 2003 (aproximadamente cinco exabytes) y esto solo con dos mil millones de personas de los siete mil millones que integran la población mundial (Schmidt & Cohen, 2013). Con la inclusión global es inimaginable cuántas ideas, creaciones y perspectivas se van a producir y cuál será el impacto en la vida del día a día de las personas. El beneficio colectivo con el intercambio de conocimiento y creatividad crece a una rata exponencial, en el futuro la tecnología de la información estará en todas partes como la electricidad, será un hecho muy difícil de describir a las nuevas generaciones cómo era la vida antes de este periodo de tecnología digital.

En los últimos diez años los adelantos tecnológicos no tienen precedentes en la historia, ya que han impulsado la gestión del conocimiento a tiempo oportuno en los más altos niveles de la toma de decisiones, no tan solo en el gobierno sino también en el sector privado empresarial. La función de inteligencia como elemento de política pública a nivel nacional y estratégico está experimentando cambios importantes dentro de la sociedad global e interdependiente actual.

El análisis de la Inteligencia Estratégica en los términos descritos en este ensayo requiere contar con una reforma institucional de funcionamiento, caracterizada por cinco aspectos a destacar: 1) Distinción en materia de competencia de los organismos de inteligencia. 2) Establecimiento de la dependencia de estos organismos de inteligencia. 3) Limitada asignación de competencias en materia de inteligencia interior. 4) Establecimiento de un órgano de coordinación bajo dependencia del máximo nivel del Estado y 5) Creación de controles externos eficaces. Estos aspectos son imprescindibles para un sistema de inteligencia estratégico congruente con el régimen democrático representativo de gobierno.

Transición del poder en un mundo globalizado

El mundo hoy día está atravesando un cúmulo de problemas, circunstancias y oportunidades sin precedentes. Nuevos centros de poder e influencia emergen e impactan con cambios continuos en el balance del poder económico, político, social y militar, alterando radicalmente las reglas mediante las cuales las naciones y las instituciones internacionales operan. En la realidad, las naciones del mundo están actualmente más integradas de lo que estaban hace pocas décadas.

ISSN: 2225-5648, Año 5, Vol. 2, p. 75-106

La acción de pequeños grupos armados con capacidad para alcanzar sus intereses mientras infligen daños considerables a las fuerzas militares del Estado, es una de las maneras en que el ejercicio del poder a través de la fuerza ha cambiado; así mismo, es cada vez menor la habilidad y voluntad política del Estado de hacer uso de la fuerza a su disposición con gran capacidad de destrucción. Está claro que estos pequeños grupos militarizados no pueden enfrentar las fuerzas militares del Estado en un combate regular. No obstante, estos colectivos son capaces de negar la victoria a las fuerzas gubernamentales mejor preparadas y tecnológicamente más capacitadas, en un conflicto de naturaleza asimétrica. Esto explica los cambios fundamentales en la forma en que el poder opera en la actualidad. Es decir, el poder está transitando del Estado a los actores no estatales, legales e ilegales (empresas de seguridad y defensa y grupos armados al margen de la ley respectivamente)

El caso del autodenominado "Estado Islámico" (ISIS por sus siglas en inglés) constituye el mejor ejemplo de la transición del poder del Estado a las organizaciones criminales no Estado que surge en Irak en el año 2004, adoptando ese nombre dos años después. Al Qaeda e ISIS eran dos organizaciones aliadas entre sí enfrentadas al mundo occidental, pero esta última reniega de Al Qaeda en el año 2014, probando ser más brutal y eficiente al controlar una franja territorial entre Siria e Irak, implantando estructuras de gobierno en los territorios capturados tales como gabinete de gobierno, organizaciones financieras y cuerpos legislativos bajo la interpretación radical de la religión musulmana.

Cuando se trata del despliegue y uso del poder de la fuerza militar que representa la expresión máxima de poder físico del Estado, la política busca persuadir la guerra o la amenaza de guerra a través de la coerción. El poderío militar medido por el tamaño, equipamiento y capacidad tecnológica demuestra ser la idea más compleja de poder. La fuerza militar es un hecho contundente que queda cuando las sutilezas de la diplomacia, la influencia cultural, y el poder blando han fracasado.

Sin embargo, al hablar de poder blando hoy día y de acuerdo con (Nye, 2011), el poder de una nación no es orgánico como un ser humano, con un ciclo de vida predecible, sino que este poder se ejerce a través de tres dimensiones: el poder físico representado por el aparato militar, el poder económico representado por la infraestructura productiva de la nación y, en las relaciones transnacionales donde los actores no Estado juegan un papel muy importante tanto los buenos representados por instituciones privadas financieras y de seguridad, como los malos representados por las organizaciones criminales como Al Qaeda, Boko Haram e ISIS entre otras.

ISSN: 2225-5648, Año 5, Vol. 2, p. 75-106

Los grupos armados que operan al margen de la ley se han incrementado en relevancia y efectividad en el conflicto moderno. Estos han puesto en peligro uno de los principios fundamentales que han regido la política y adjudicación del poder en los últimos siglos. De acuerdo con Max Weber (2009) el Estado es una asociación que reclama el monopolio del uso legítimo de la violencia, es decir parte de la definición y razón de ser del Estado moderno es su habilidad para centralizar el uso del poder militar de la nación.

La convergencia del Estado moderno y la modernización de la institución militar no ha sido solamente asunto de ideología o filosofía política. Esto tiene una profunda razón práctica, ya que refleja el análisis del costo y de la tecnología de la guerra. A través de los siglos el costo de los medios de violencia ha escalado desde el aumento del precio de los fusiles de guerra hasta la artillería pesada, pasando por los tanques, los aviones de combate y la estructura de computadoras, lo cual incrementa los requerimientos logísticos para lograr la efectividad militar.

Al lado del crecimiento de las instituciones militares en las democracias occidentales, se presenta el crecimiento de una gran variedad de empresas privadas para prestar servicios de seguridad y defensa que hasta hace poco tiempo se consideraban reservados y de dominio absoluto de las instituciones militares y de seguridad del Estado. Esto, no obstante, no es completamente nuevo ya que en la Edad Media y el Renacimiento las actividades de la seguridad y defensa eran proporcionadas por particulares. Sin embargo, hoy día el mercado de la seguridad y defensa supera los cien mil millones de dólares en comparación con la generación anterior donde este mercado era casi inexistente

Tal como lo afirma (Naim, 2014), desde la creación del Estado moderno después de Westfalia en el siglo XVII, la institución militar posee el monopolio de la fuerza por ser importante e impresionante desde el punto de vista de su papel y sus capacidades en la defensa de la soberanía de la nación. Tiene ventajas en cuanto a los recursos públicos asignados por considerarse prioritarios en el presupuesto nacional, dándole el peso moral que los justifique para el gasto e inversión, además de la legitimidad política para actuar. Sin embargo, podemos ver que este monopolio ha perdido espacio en dos aspectos cruciales desde el punto de vista filosófico y práctico. En primer lugar, lo ha perdido en la concepción filosófica del monopolio de la legitimidad del uso de la fuerza y en segundo, desde el punto de vista práctico, en el monopolio conferido a la fuerza militar por la competencia geopolítica entre los Estados soberanos y la necesidad de la siempre compleja tecnología para ganarlo. El surgimiento de poderosos actores no Estado y la difusión vertiginosa de la tecnología más allá del campo de los especialistas han destruido las bases de la ventaja.

ISSN: 2225-5648, Año 5, Vol. 2, p. 75-106

Esta difusión de poder en la institución militar hacia organizaciones no estatales, aunada a las fuerzas centrífugas, han desmembrado el conflicto, desempaquetando las capacidades militares y transformándolas en un hibrido militar/civil que no tiene límites en el impacto en las fuerzas militares de la nación. Inclusive, los nuevos actores en conflicto están en riesgo de perder su objetivo por las mismas causas que les han permitido surgir tan rápido en los últimos años del siglo XXI.

En resumen, la nanotecnología aplicada a la investigación y desarrollo de la industria militar con robótica y aviones no tripulados, espacio cibernético provisto de armas de naturaleza variada, municiones de alta precisión, terroristas suicidas, redes transnacionales del crimen organizado y una serie de otros actores armados, han alterado el ambiente de seguridad global. La configuración de este ambiente está en plena evolución, por lo tanto es imposible describirlo con exactitud. No obstante, podemos asumir con cierto nivel de certeza que el poder de las grandes instituciones de seguridad y defensa será menor de lo que ha sido en el pasado.

Nuevas tecnologías de comunicación política

El 11 de septiembre de 2001, de acuerdo con algunos autores, marcó posiblemente un punto de inflexión en los servicios de inteligencia para la seguridad y defensa nacional en los Estados Unidos de America. En la reiterada sociedad de la informacion fueron precisamente la falta de ésta o de coordinacion para la integracion de los datos disponibles, lo que generó una defectuosa gestion, que permitió los atentados ocurridos en esa fecha.

En consecuencia se necesitan soluciones concretas, capaces de controlar y convertir en conocimiento útil las ingentes cantidades de informacion que deben procesar las agencias de inteligencia de un país; en esta búsqueda se encuentran con la gestion del conocimiento, para permitir que los organismos de inteligencia operen como una fuerza basada en el conocimiento rapidamente desplegable y globalmente enfocada para que pueda ver primero, comprender primero, actuar primero y terminar con una decision exitosa.

Otro enfoque que se debe analizar con detenimiento es el de los avances tecnológicos en el ámbito de las comunicaciones y en particular en la comunicación política, el cual ha sufrido grandes cambios. La llegada de Internet y las redes sociales ha modificado ciertamente el panorama político-mediático en función del cambio del ejercicio del poder político y cómo se transmiten los mensajes al público.

La nueva Red Web 2.0 (es una herramienta de comunicación política que consiste en una plataforma que involucra todos los dispositivos conectados. Su elemento esencial es su propio contenido generado por el

ISSN: 2225-5648, Año 5, Vol. 2, p. 75-106

usuario e incluso a veces solo admite la aportación de éste. Ello ocurre en portales como Youtube, Tuenti, Facebook, Flicker y MySpace, entre otros. No obstante, en muchas ocasiones y cada vez más, estas aplicaciones son utilizadas por entidades, como los partidos políticos y empresas, y no por individualidades, como camino más corto para llegar a la ciudadanía disfrazándose de usuarios.

Esta red Web 2.0 da paso a un nuevo entendimiento de la comunicación en la que el ciudadano puede expresar su opinión directamente, tomando los medios de comunicación un papel secundario. Sin embargo, la sobrecarga de datos que se generan conlleva una intoxicación informativa que afecta no solo al individuo sino a todas las instituciones del Estado y particularmente del gobierno para discernir lo importante y veraz frente a lo desechable.

Las tecnologías han cambiado a lo largo de la historia la forma de entender y elaborar la comunicación política. En la actualidad se goza de una opulencia informativa que pone en peligro su correcta lectura para producir análisis de inteligencia. La intoxicación informativa por sobrecarga de datos, puede llevar al receptor a dificultades graves en el discernimiento de aquellos datos importantes y veraces frente a los desechables o distorsionados, esto indudablemente puede afectar drásticamente la calidad y veracidad del análisis para la toma de decisiones.

De todas formas, todo dependerá del nivel de información de la sociedad o país. Parece que la Web 2.0 ha abierto una nueva era en la comunicación política, aunque aún no sabemos si será cuestión de moda, se afianzará en los próximos años o surgirán otras herramientas que acapararán el interés de los políticos. De cualquier forma, el analista de Inteligencia Estratégica deberá tener la capacidad para discernir el uso de esta herramienta y sus consecuencias en la lectura de la información para producir un análisis realista y confiable para la toma de decisiones al más alto nivel del gobierno.

No olvidemos que Internet y, sobre todo, la web 2.0 suponen un pequeño paso político para el hombre, pero un gran salto para la humanidad. Nuestro aquí y ahora supone una evolución herramental, pero no un cambio de finalidad en los mensajes políticos. Este debe ser el criterio que maneje el analista de Inteligencia Estratégica cuando utilice la información proveniente de estas nuevas herramientas en la comunicación política presente y futura.

La nueva revolución de la red de redes ha abierto una brecha de oro para los políticos, siempre más preocupados en convencer a la opinión pública y conseguir votos que en rendir cuentas. Las redes sociales, las bitácoras y las aplicaciones de video como Youtube, permiten a los equipos de campaña conformar bases de datos mucho más ricas y fiables que las realizadas en base a las tradicionales encuestas. Sin embargo, desde el punto de

ISSN: 2225-5648, Año 5, Vol. 2, p. 75-106

vista del analista de Inteligencia Estratégica esta revolución implica un entendimiento claro de la naturaleza de estas nuevas herramientas y cómo afectan la labor de análisis de información para poder comprender primero y proveer, al tomador de decisiones, del conocimiento a tiempo que le permiten decidir y actuar para asegurar el éxito.

El espacio cibernético

El quinto dominio, como se le denomina en el mundo de la seguridad y defensa en la actualidad, se caracteriza entre otras cosas porque los espías nos acechan sin darnos cuenta. Desarrollan sus actividades sustrayendo información sin tomar ningún documento de la institución o espiando a los ingenieros en sus sitios de trabajo o de descanso ya que lo hacen en forma remota a través de una conexión de computadoras.

De acuerdo con el Director del FBI, James Comey, las actividades criminales en el espacio cibernético, incluyendo el espionaje y el fraude financiero, serán las amenazas más significativas a la seguridad nacional en las décadas por venir. Las posibilidades de un ataque cibernético paralizante se ubican en el tope de las amenazas globales (Harris, 2014).

Los gobiernos de las naciones más desarrolladas del mundo no están informando la totalidad de los acontecimientos que ocurren en el espacio cibernético. Se han limitado a comentar y quejarse de ser víctimas de ataques incesantes de enemigos invisibles. Sin embargo, la agresividad de los ataques que se desarrollan en este quinto dominio no tiene límites. El ataque perpetrado por los Estados Unidos e Israel denominado “Olimpic Games” contra el centro de enriquecimiento de uranio en Natanz, República de Irán desde 2008 hasta 2010 (Singer, 2012) tomó por sorpresa a los ingenieros de la planta que no tenían idea del ataque del cual estaban siendo objeto.

Esta realidad que tiene lugar en el espacio cibernético está cambiando la Internet de forma fundamental y no necesariamente para bien. Con gran celo de protección del espacio cibernético, los gobiernos, y en particular con la cooperación de empresas privadas especializadas en la seguridad y defensa del espacio cibernético, están haciendo este dominio más vulnerable de lo que es posible imaginar.

El motivo principal por qué la seguridad del espacio cibernético se ha hecho tan importante y por qué se están haciendo grandes esfuerzos en este sentido, es por el control, para usarlo como arma y como herramienta de espionaje. Esta es la razón por la cual los Estados Unidos han incorporado el ataque en el espacio cibernético como parte de la guerra convencional y lo han usado para desmantelar infraestructura en otros países. Se trata, precisamente, del mismo acto de agresión que según fuentes oficiales del gobierno, temen a nivel doméstico y hay que tomar medidas extraordinarias para prevenirlo.

ISSN: 2225-5648, Año 5, Vol. 2, p. 75-106

La guerra cibernética y el espacio cibernético son términos amorfos que se aplican a un espectro de actividades ofensivas. Así como el espionaje, parte de la inteligencia, es inseparable de la guerra tradicional, también el espionaje en computadoras es un prerrequisito para el ataque en el espacio cibernético. Es decir, en la guerra cibernética el éxito estará asociado a la combinación de espionaje y ataque.

En este orden de ideas, la protección del espacio cibernético no es una exclusividad del gobierno. El desarrollo de la defensa y la guerra en él es cada día más una actividad privada. Los gobiernos no pueden operar en el espacio cibernético solos; defendiendo sistemas de computadoras o atacándolas, requiere la participación y voluntad del sector privado.

Una vez más los Estados Unidos se mantiene indiscutiblemente como líder militar del mundo en el espacio cibernético con la alianza público-privada en asuntos de seguridad y defensa (Harris, 2014). En el 2014 se gastaron 13 billones de dólares en los programas de defensa del espacio cibernético con énfasis en la protección de las redes de computadoras del gobierno y compartir el conocimiento para detectar la amenaza con la industria de la seguridad y defensa del sector privado. Para colocar esta alianza en perspectiva es importante tener en cuenta que en los próximos cinco años solamente la Secretaria de Defensa tiene en sus planes invertir 26 billones de dólares (Ibíd.). Sin embargo, la pregunta es ¿cuánto será la inversión en defensa y en ofensa? Evidentemente, esto es secreto, no obstante, la línea entre ofensa y defensa en el espacio cibernético es muy tenue y difusa.

Los negocios relacionados con el espacio cibernético están en plena ebullición. Las compañías, gobiernos e individuos gastan un promedio de 67 billones de dólares anuales protegiendo sus sistemas de computadoras (Ibíd.). Muchos de los expertos contratados por la empresa privada provienen del gobierno, particularmente del sector militar, lo cual ha motivado una gran deserción hacia el sector privado por las expectativas salariales.

La lucha por el control del espacio cibernético está definiendo los asuntos de seguridad y defensa del mundo. Cada nación deberá hacer todo lo que está a su alcance para contar con los recursos materiales, humanos y financieros para asegurar la soberanía de su espacio cibernético con las características que éste presenta y que tendrá una gran influencia en la soberanía de los otros cuatro dominios tradicionales.

Las decisiones que tomen los gobiernos y los líderes empresariales, hoy día, tendrán un profundo impacto no tan solo para sus connacionales en el campo de los dominios tradicionales, sino en la dependencia de un espacio ancho, distribuido y difícil de definir que no es enteramente común, no es la propiedad de una corporación o gobierno, no responde a nuestros

sentidos comunes como humanos ya que nadie lo ha visto, tocado, oído u olfateado para identificarlo como tal. Sin embargo, lo que es cierto e indudable es que la amenaza existe en el espacio cibernético. Responder a esta amenaza en forma apropiada es en la actualidad desconcertante y a menudo un ejercicio peligroso, pero uno en el cual todos tenemos participación.

Es evidente que corresponderá a los analistas de Inteligencia Estratégica, como componente fundamental de la política de seguridad nacional, proceder a dar respuesta a este reto que el nuevo dominio de la defensa y seguridad presenta en el siglo XXI, a fin de hacer posible la vida en el planeta bajo la condición de una paz relativa y duradera.

Se trata de repensar la Inteligencia Estratégica para adaptarla no solo porque el mundo es diferente sino preguntarse cómo, cuándo y por qué medios la amenaza debe ser considerada y entendida en un nuevo dominio; cómo debe ser pensada desde el punto de vista de su naturaleza para ser capaces de formular un análisis confiable y valedero a los tomadores de decisión y formuladores de políticas públicas de seguridad y defensa.

Tecnología

Al final del siglo XX la tecnología fue capturada por proyectos ambiciosos en la industria militar. La ciencia ha dado pasos avanzados en la creación de máquinas que pueden ser controladas a distancia y con autonomía de movimiento. La era de la robótica se ha ido perfeccionando a pasos agigantados y rápidos, entrelazándose con el mundo de la guerra y el conflicto. Sin embargo, es de hacer notar que los primeros esfuerzos fueron desarrollados por Thomas Edison y Nikola Tesla, dos científicos rivales y los primeros en el campo de lo que hoy día se conoce por ingeniería eléctrica. En realidad el trabajo más sobresaliente en el campo de instrumentos con control remoto fue el de Tesla con un sistema de comunicaciones inalámbricas en 1893 (Singer, 2009). Adicionalmente, cinco años más tarde hizo una demostración de un control remoto para un bote eléctrico en el Madison Square Garden en la ciudad de Nueva York.

A medida que en la guerra se comenzaron a emplear menos armas heroicas y más armas tecnológicas de gran capacidad de destrucción, los sistemas de armas no tripuladas comenzaron a ganar el interés de las fuerzas militares. Ejemplo de esto es que en el ejército se comenzó a utilizar el "Perro eléctrico", un triciclo que servía para abastecer a las tropas en las trincheras. En la fuerza aérea fue un misil de crucero denominado "Kettering Bug" o torpedo aéreo pequeño, no tripulado, al cual se le asignaba un giróscopo y un barómetro para volar automáticamente un curso directo a un blanco predeterminado y se estrellaba a una distancia máxima de 50 millas.

Después de la Segunda Guerra Mundial surgió la dicotomía de robótica

ISSN: 2225-5648, Año 5, Vol. 2, p. 75-106

y computadora, evolucionando durante toda la época de la Guerra Fría aunque con poco interés por parte de la fuerza aérea en lo referente a vehículos no tripulados, dejando este desarrollo en manos de la armada y el ejército de los Estados Unidos.

La evolución tecnológica del vehículo no tripulado continuó, pero sin mucho énfasis durante los años sesenta y hasta finales de los ochenta. Sin embargo, fue en 1991 durante la primera Guerra del Golfo que el sistema de vehículos no tripulados capturó, en forma gradual, el interés de las fuerzas militares después de las llamadas Bombas Inteligentes con dos versiones diferentes: las bombas guiadas por láser y los misiles de cruceros.

El momento mágico del empleo de la tecnología digital llegó en 1995 cuando los vehículos no tripulados se integraron con el Sistema de Posicionamiento Global (GPS). El GPS es una constelación de satélites militares que pueden proveer la información de localización, velocidad y dirección a un recibidor en cualquier parte del globo terrestre. Esto permite a los vehículos no tripulados (drones) y sus operadores conocer automáticamente dónde están en cualquier momento. Los drones comenzaron a ser más confiables para volar, a medida que la información que estos pasaban era de suma utilidad tanto para los generales como para las tropas en el terreno de operaciones. Es así que los drones como el Depredador y el Halcón Global hicieron su debut en la guerra de los Balcanes, y algunos años más tarde recolectaron información sobre el sistema de defensa aérea de los serbios y el flujo de refugiados. Sin embargo, el pleno empleo de esta tecnología digital se consolidó a raíz del ataque terrorista del 11 de septiembre de 2001 en los Estados Unidos cuando el liderazgo político norteamericano se convenció de la necesidad de invertir dinero en esta tecnología de punta.

Mientras más se usa este equipamiento digital y la robótica en las fuerzas militares, más se consolida el convencimiento de sus ventajas en el campo de batalla, ya que esta tecnología no tiene las debilidades psicosomáticas y físicas del ser humano de disgusto, miedo, cansancio, sentimiento, etc. Otro aspecto de gran ventaja de estos dispositivos es la velocidad de acción y reacción en situaciones de alto riesgo. No obstante, es de hacer notar que el número de muertos civiles no combatientes con el uso de esta tecnología (drones) en el combate al terrorismo internacional ha traído controversia no solo a nivel internacional sino también nacional en los Estados Unidos por la muerte de ciudadanos norteamericanos en estas operaciones lo cual contradice el mandato constitucional.

En sólo 60 años el empleo de la tecnología digital, robótica y computadoras inteligentes ha cambiado la actitud del liderazgo político en los Estados Unidos, lo cual se puede evidenciar en la preferencia de la Comisión de la Fuerzas Armadas del Congreso por un programa de adquisiciones de

ISSN: 2225-5648, Año 5, Vol. 2, p. 75-106

sistemas no tripulados de tecnología digital para la Secretaria de Defensa. Adicionalmente se ha incluido un criterio que exige que para la aprobación de un sistema de desarrollo bajo control humano se deba contar con una certificación que explique por qué un sistema no tripulado es incapaz de cumplir los requerimientos del programa. Si las fuerzas militares van a comprar un nuevo sistema, deberán justificar por qué no es un sistema robótico.

La tecnología es el gran separador pero a la vez el gran igualador en el arte de la guerra (Boot, 2006). Los Estados Unidos puede ser la nación más poderosa militarmente en la historia del mundo por su tecnología; sin embargo, su gran poder no siempre le ha permitido obtener la victoria. Por el contrario, grupos que no son ni siquiera un Estado han sido capaces de frustrarlo y defraudarlo usando armas de bajo costo y baja tecnología como el ataque terrorista de septiembre 11, 2001, o los ataques en Irak a sus fuerzas militares con dispositivos explosivos improvisados (IED por sus siglas en Ingles).

Quizás el mejor ejemplo de estos cambios tecnológicos es el caso del conflicto en el Medio Oriente con la participación de Hezbollah, una de las organizaciones no estatales más innovadoras en la actualidad. Desde su creación en 1985 se ha transformado en una multitud de identidades y formas, como organización paramilitar capaz de movilizar miles de combatientes (terrorista) y simultáneamente una organización política con representantes en el parlamento, con su propia estación de televisión, radio e Internet. Aún más, es una organización caritativa de ayuda a hospitales, clínicas y escuelas dedicada al bienestar público en el sur de Líbano.

Esta pequeña organización ha sido capaz de cumplir lo que una coalición de naciones no pudieron lograr en 1948, 1967 y nuevamente 1973: derrotar a Israel en lo que ha sido llamado por el General de la Infantería de Marina de los Estados Unidos James Mattis, una Guerra Hibrida. Hezbollah es muy amorfa en su estructura; mezcla el poder militar, político, religioso y económico. Han sido capaces de desplegar sus tropas en el terreno en forma descentralizada como un enjambre en ataque, pero con capacidad de dispersión cuando las fuerzas militares de Israel tratan de identificarlos y destruirlos

Los actores no estatales se presentan sorprendentemente incoativos. De acuerdo con los reportes del gobierno de Israel, no solo Hezbollah ha sido capaz de penetrar el sistema de computadoras y comunicaciones del ejército Israelí, sino que al hacerlo lo ejecutó en forma magistral, haciendo creer que el ataque provenía de compañías localizadas en Estados Unidos y Canadá, las cuales ya habían sido penetradas y tomadas bajo control por esta organización terrorista con todas sus identidades y características descritas.

ISSN: 2225-5648, Año 5, Vol. 2, p. 75-106

Hezbollah ha demostrado que los actores no estatales pueden no solo desarrollar estrategias asimétricas para neutralizar las ventajas de las fuerzas del Estado, sino que son capaces de retar al Estado con su propio juego tecnológico. Se impone entender y conocer la naturaleza de esta clase de enemigo que tiene una mejor preparación para combatir contra una fuerza militar superior y particularmente contra la fuerza militar mejor preparada de estos tiempos. Si bien es cierto que David no mató a Goliat en este momento, pero sí fue capaz de propinarle un gran dolor de cabeza.

Una mirada al futuro promete y a la vez reta. Se enfrenta un futuro difícil e incierto con pasos acelerados y un periodo de expectativas en la historia de la humanidad. Se están experimentando cambios más acelerados que en otras generaciones y estos cambios se producen en parte por los aparatos que están al alcance de las manos. Por lo tanto estas transformaciones son más personales y comunes al individuo de lo que se podría imaginar.

Se está en la era donde las computadoras exceden la inteligencia humana (Kurzweil, 1999). La tecnología es la continuación de la evolución por otros medios y es, en sí misma un proceso evolutivo, tal afirmación lleva a un crecimiento exponencial tecnológico y a un acelerado retorno en el tiempo, ya que está hecho en su propio orden de incremento tecnológico acelerado.

La computación, digitalización y robótica son las bases fundamentales de cualquier tecnología del presente y futuro, inclusive con sus limitaciones eventuales. Las leyes de Moore prometen procesadores infinitamente pequeños en cuestión de pocos años. Como se señaló anteriormente, se están creando cada día aproximadamente cinco exabytes de información con solo 2 mil millones de personas con acceso a Internet. ¿Qué pasará cuando los 7 mil millones de personas que habitan la tierra tengan acceso a esta tecnología? La llegada de más internautas al espacio cibernético es buena para ellos, pero también para todos. Sin embargo, es un reto para los analistas de inteligencia que deben producir la información para los tomadores de decisiones a todos los niéveles de gobierno: local, nacional e internacional, a fin de dar respuestas adecuadas, coherentes y a tiempo a las complejas situaciones de seguridad y defensa

Los intentos de contener la información y la diseminación de la conectividad fallarán a lo largo del tiempo. La información es como el agua, siempre conseguirá la forma de llegar a todos. El Estado, los ciudadanos, las compañías, las ONG, los consultores, los terroristas, los ingenieros, los políticos y los hackers tratarán de adaptarse a estos cambios y gestionar sus efectos pero nadie será capaz de controlarlos.

La gran mayoría de los habitantes del mundo se beneficiará de esta tecnología que generará gran eficiencia y oportunidades y mejorará la calidad de vida de la humanidad. Sin embargo, esto no llegará en forma

uniforme a todos; el sistema de clases sociales se fortalecerá y la gente mejor preparada se beneficiará grandemente de acuerdo con su ubicación en la estructura social. Es decir, una pequeña minoría en el tope se beneficiará más por su riqueza, acceso o ubicación social.

La Inteligencia Estratégica

El ambiente actual de seguridad y defensa caracterizado por difusión de poder, el sistema de comunicación de la nueva Red Web 2.0, el espacio cibernético y la tecnología digital, han impactado la Inteligencia Estratégica como elemento fundamental de la política de seguridad nacional desde la creación del Estado moderno. En el mundo antiguo, por ejemplo, los cartagineses y fenicios llegaron a tener gran experiencia en el desarrollo del conocimiento de sus adversarios a través de la inteligencia; sin embargo, esta inteligencia tenía un enfoque muy limitado en cuanto a su empleo por ser de alcance muy reducido. Hoy sabemos que se requiere de un conocimiento del contexto con todas sus características complejas, interdependientes y de grandes retos para lo cual se necesita el empleo de la llamada Inteligencia Estratégica. Ésta constituye la herramienta fundamental diseñada y utilizada para proveer al gobierno de pronósticos de visión ampliada a mediano y a largo plazo de la situación nacional con su interdependencia, complejidad y potenciales riesgos.

A través de la historia la comunidad de los servicios de inteligencia ha cometido muchos errores tales como: la falla en prever la invasión a Corea del Sur por pate de Corea del Norte en junio de 1950; la falla de prever la respuesta que daría el nuevo régimen de gobierno comunista en China a la aproximación del General Douglas MacArthur al río Yalu en noviembre de ese año, al enviar cientos de miles de tropas a lo largo de la frontera en un contraataque masivo y finalmente, la falta de consideración de la acción terrorista en el territorio americano el 11 de septiembre de 2001. Estas fallas han tenido un costo muy elevado para la política y estrategia de seguridad nacional de los Estados Unidos de América.

Las lecciones aprendidas de estas experiencias, en particular de las dos primeras, trajeron como consecuencia que el director de la Agencia Central de Inteligencia Walter Bedell Smith (Berkowitz and Goodman, 1989) actuará con determinación para evitar la ocurrencia de hechos de esta naturaleza y creara y desarrollara una unidad responsable de analizar y evaluar las situaciones con una visión futurista y comprensiva. Estos estudios comenzaron a mediados de los años cuarenta del siglo pasado por el profesor Sherman Kent de la Universidad de Yale, quien escribió un libro donde introdujo el nuevo término de Inteligencia Estratégica; también prestó servicios en la Oficina de Servicios Estratégicos durante la Segunda Guerra Mundial. Él desarrolló estos análisis bajo ciertos principios que deberían cubrir varios aspectos importantes como: planeamiento

ISSN: 2225-5648, Año 5, Vol. 2, p. 75-106

de inteligencia, desarrollo de métodos y sistemas de recolección de información, desarrollo de análisis, y gestión de las organizaciones, con la finalidad de proveer al más alto nivel de gobierno de estimados mediante el análisis de inteligencia comprensiva que pudieran ser útiles para la toma de decisiones y su impacto en los años por venir.

La Inteligencia Estratégica se diferencia de la inteligencia operacional tradicional llamada por el Duque de Wellington "el conocimiento de lo que hay al otro lado de la colina". La Inteligencia Operacional o la llamada Inteligencia Táctica por Wellington es la que se enfocaba en la situación actual y la observancia directa del enemigo. La Inteligencia Estratégica tiene una base mucho más amplia con un objetivo comprensivo al integrar los estudios políticos, sociales, económicos y tecnológicos para proveer un análisis de visión amplia y un pronóstico de largo alcance de las necesidades para la planificación del futuro.

Es importante destacar que la Inteligencia Estratégica surge, como un elemento clave y oportuno después de la Segunda Guerra Mundial, como necesidad en la transición de los Estados Unidos de una política de aislacionismo a un papel activo como gran potencia mundial. En este sentido, el libro de Inteligencia Estratégica de Kent se convirtió en un libro de texto de los estudiantes de inteligencia en los Estados Unidos e inclusive en el mundo, al publicarse en varios idiomas tales como francés, ruso, alemán y otras lenguas, incluyendo el chino con una edición hecha en Taiwán en forma ilegal sin respetar los derechos de autor.

En este breve estudio se trata de explicar la evolución de la Inteligencia Estratégica en los últimos años, particularmente en el transcurso del siglo XXI y los retos que enfrenta en el ambiente de seguridad a escala mundial con la evolución del poder en todas sus dimensiones: las comunicaciones, el espacio cibernético y la tecnología en un mundo globalizado e interdependiente

La Inteligencia Estratégica como se conoce hoy día es el producto de un proceso de análisis combinado de diferentes y variadas fuentes de información que pretende ir mucho más allá de un evento político o un despliegue militar a un análisis que logre encapsular todos los elementos que identifican las dinámicas sociales, políticas, económicas y tecnológicas a nivel mundial, que casualmente es la razón de reexaminar las teorías y prácticas de esta especialidad de la inteligencia con el enfoque de los cuatro aspectos antes mencionados

De esta forma se realiza un análisis de algunos aspectos que caracterizan el ambiente de seguridad donde se desarrollan las actividades de la Inteligencia Estratégica a la luz de los cuatro enfoques del estudio como se ha dicho, poder, comunicaciones, espacio cibernético y tecnología.

ISSN: 2225-5648, Año 5, Vol. 2, p. 75-106

La diversidad de objetivos

La comunidad de Inteligencia Estratégica debe analizar gran cantidad de información con mayor alcance y profundidad para producir un análisis actualizado de acontecimientos en pleno desarrollo y a gran velocidad. De esta forma estos acontecimientos, desde el punto de vista del análisis de lo que representa el poder en la seguridad y defensa en proceso de transición del Estado a los actores no estatales como lo son las agencias de seguridad privada o los grupos armados ilegales que actúan al margen de la ley tales como Al Qaeda o ISIS, requieren conocer y entender la verdadera naturaleza de la amenaza a la luz de una multiplicidad de actores a escala nacional e internacional, como por ejemplo, las 192 naciones que integran las Naciones Unidas y solamente a nivel regional en el hemisferio occidental más de 30 organizaciones internacionales.

El hecho de la gran cantidad y variedad de actores a escala nacional e internacional representa un problema para la comunidad que produce los análisis de Inteligencia Estratégica, ya que demanda más monitoreo a las personalidades a quienes hay que hacerles un seguimiento de sus decisiones y actuaciones, no tan solo a nivel nacional en sus países sino a los funcionarios en estas instituciones internacionales.

La proliferación de la tecnología de las comunicaciones ha avanzado a una velocidad sin precedentes. En la primera década del siglo XXI el número de personas conectadas a internet a nivel mundial se incrementó de 350 millones a 2 mil millones. En el mismo periodo de tiempo el número de teléfonos móviles ha pasado de 750 millones a más de 5 mil millones de unidades (Schmidt & Cohen, 2013). Desde el punto de vista de las comunicaciones, el impacto que han tenido las redes sociales y en cómo han evolucionado las comunicaciones en cantidad y en calidad, representa un gran problema para los analistas de Inteligencia Estratégica, ya que hoy en día todos nos comunicamos con todos en forma simultánea y permanente. Esto dificulta la labor del analista para producir un examen adecuado y pertinente a tiempo y acertado para los tomadores de decisiones, ya que todos estamos en condiciones de acceder a la información en forma permanente y en tiempo real.

Internet es una de los pocos inventos que la humanidad ha creado que todavía no logra entender bien. Lo que sí es cierto es que se ha convertido en el campo de batalla. En los últimos años la alianza entre soldados y espías ha crecido, expandiendo el terreno en que combaten juntos. Ellos han trasladado, por ejemplo, una técnica de cacería del enemigo que probó ser eficiente en Iraq y Afganistán. Los hackers de la Agencia Nacional de Inteligencia trabajaron en equipo con las tropas en el terreno logrando combatir y eliminar gran cantidad de combatientes Talibanes. Sin embargo, esta combinación de espías y soldados no es la única, hoy día, en el campo

ISSN: 2225-5648, Año 5, Vol. 2, p. 75-106

de batalla del espacio cibernético. La línea entre la defensa y la ofensiva es muy difícil de determinar por las mismas características que presenta lo que se ha denominado el quinto dominio después del terrestre, naval, aéreo y espacial. De esta forma es sumamente importante y difícil para el analista de Inteligencia Estratégica determinar no sólo este escenario en la actualidad y su impacto en los otros dominios, sino también en medio de la gran multiplicidad de objetivos a tomar en consideración; así como en todas las actividades de la sociedad en general y de esta forma tener la visión de su evolución e impactos futuros en el mundo globalizado e interdependiente actual.

La revolución de la tecnología y la información ha traído beneficios impensados a los ciudadanos. Esta tecnología permite a cualquiera conocer cómo otra persona podría estar pensando, comportándose y cumpliendo o desviándose de la norma establecida, tanto en su hogar como en la sociedad en general. La nueva tecnología disponible permite cada día conocer con más exactitud la información y verificarla en línea en forma inmediata, ilimitada e inclusive en su idioma nativo. Esto marca el comienzo de una era del pensamiento crítico en las sociedades alrededor del mundo que anteriormente estaban aisladas.

El futuro marcará una era sin precedentes de opciones y selecciones. Mientras algunos tratarán de controlar su identidad exponiéndose al mínimo a la participación virtual, otros consideran y consiguen oportunidades para participar, tomando el riesgo que esto conlleva. Esta participación alcanzará su máxima expresión a medida que se incremente el uso de teléfonos móviles y el ingreso a Internet. El empoderamiento del ciudadano incrementa la participación y las exigencias por la entrega de cuentas y transparencia de los líderes políticos, empresariales y sociales en el presente y aún más en el futuro. En medio de estas transformaciones que empoderan a la ciudadanía en general, se exige a los analistas de Inteligencia Estratégica entender las transformaciones sociales económicas y políticas y su impacto en la multiplicidad de objetivos para poder predecir los cambios e impactos en cada uno de estos campos.

Multiplicidad de consumidores de análisis de Inteligencia Estratégica

La creciente demanda de los consumidores de inteligencia podría hacer que la información se dificulte, adicionalmente a esto hay más consumidores de Inteligencia Estratégica que la demandan. A medida que la globalización se consolida, el número de analistas de Inteligencia Estratégica se ha incrementado en términos generales, sino también la sociedad en general ha diversificado esta actividad que otrora era exclusiva del gobierno, particularmente del sector de la seguridad y defensa.

El sector privado empresarial emplea, hoy día, las bondades de la Inteligencia Estratégica por la misma consideración de la globalización

de los mercados y la gran competencia que demanda, la cual no sólo se desarrolla a nivel nacional sino también en el mercado internacional por la dinámica económica y comercial que hoy vive el mundo que cada día se hace más pequeño y sin fronteras.

La interacción de aspectos sociales, económicos y políticos requiere a la comunidad de Inteligencia Estratégica profundizar en temas que anteriormente eran de poco interés para los asuntos de seguridad y defensa del Estado. El análisis de tipo económico, por ejemplo, que anteriormente se enfocaba en los potenciales adversarios, hoy día requiere hacerse a nivel global por las implicancias que puede haber de orden económico y que tienen impacto directo e indirecto en asuntos de seguridad nacional e internacional. Por ejemplo, hasta hace pocos años las decisiones de la Organización de Países Exportadora de Petróleo (OPEP) eran de las más importantes en el análisis de la Inteligencia Estratégica para conocer las tendencias de los precios de esta materia prima y su impacto en la geopolítica mundial. Sin embargo, en la actualidad esto no es así por la evolución que ha tenido el mercado del petróleo a escala mundial con una proliferación de la oferta por diferentes organizaciones legales e ilegales como es el caso del Califato Islámico en el Medio Oriente. Esta proliferación en el área económica se puede observar también en las áreas social y política por lo cual se observa una gran cantidad de consumidores que demandan análisis de Inteligencia Estratégica tanto en los organismos del gobierno, instituciones multilaterales internacionales y empresas del sector privado.

Finalmente, el incremento burocrático del gobierno con nuevas organizaciones e instituciones, así como el de las organizaciones no gubernamentales y el sector empresarial privado con necesidad de coordinación interinstitucional para poder enfrentar los retos y demandas que se presentan, necesitan de estos análisis en forma constante y con carácter de inmediatez para que sus líderes estén en condiciones de tomar decisiones oportunas y acertadas.

Nuevos retos a la recolección de información

La tercera característica que presenta el nuevo ambiente de Inteligencia Estratégica es la dificultad para la recolección de información y la complejidad de transformar ésta en análisis útil de información, por razones como son la capacidad que tiene el individuo de informarse y comunicarse a través de las redes sociales, todos nos comunicamos con todos y con gran velocidad es decir, el mundo es plano (Friedman, 2005).

Otro aspecto que debemos tomar en consideración es el tecnológico que así como puede ayudarnos para la recolección de información también es de fácil acceso a nuestros potenciales y reales oponentes, lo que les da

ISSN: 2225-5648, Año 5, Vol. 2, p. 75-106

una gran capacidad de penetrar nuestros centros vitales y atacar nuestras vulnerabilidades, sobre todo en el quinto domino o sea en el espacio cibernético

La recolección de información hoy día es mayor y de mejor calidad, sin embargo, el problema es cómo mantener esta información a buen resguardo con el cifrado que asegure la información y por cuánto tiempo, de manera que permita disminuir las vulnerabilidades por las capacidades que en algún momento puedan desarrollar los opositores o enemigos para penetrar las fuentes de información y análisis.

A diferencia del pasado, sobre todo durante la guerra fría, que se usaba una gran cantidad de medios aéreos, terrestres y marítimos para la recolección de información, hoy día la tecnología digital y el espacio cibernético permite recolectar información sin ni siquiera moverse del sitio de trabajo y sin ser detectados fácilmente. Esta es una de las mayores características que ha impactado a la Inteligencia Estratégica por la facilidad del acceso a la información a un menor costo y con menos riesgos. Sin embargo, esta capacidad también es de fácil acceso a los opositores y enemigos con lo cual aumentan su capacidad de recolección de información.

Los nuevos retos para el análisis de Inteligencia Estratégica

En el contexto de los cuatro elementos analizados en el ambiente de seguridad mundial actual y en particular en el Hemisferio Occidental, la información para el análisis es más compleja de lo que era hace pocos años. Imagine el volumen y velocidad de la información a analizar y su impacto directo, indirecto y cruzado, no solo en el ambiente de seguridad sino también su interacción y efectos en toda la dinámica social y particularmente en los cinco dominios de acción de la defensa, para determinar las consecuencias que se puedan generar en poco tiempo para satisfacer la variedad de consumidores con intereses variados pero interrelacionados entre sí. Hoy en día, por ejemplo, el análisis político y económico que debe producir la comunidad de Inteligencia Estratégica es muy complejo; para estimar el comportamiento económico de un país se han desarrollado un número impresionante de modelos de estadística econométrica que es tan compleja como la utilizada en sistemas técnicos de armas. Estos modelos son a su vez útiles para predecir posibles resultados electorales así como otros eventos políticos.

La complejidad del análisis podría generar un efecto dominó en el proceso de inteligencia. En el pasado cuando dos análisis entraban en desacuerdo, las diferencias se subsanaban al determinar la mejor fuente de información. Hoy día las diferencias radican en los supuestos y los complejos modelos utilizados en este sentido. El supervisor en la cadena de mando debe tener un entendimiento claro de la utilización de estos modelos para establecer

ISSN: 2225-5648, Año 5, Vol. 2, p. 75-106

las diferencias y desarrollar nuevos proyectos para lograr un medio que supere las diferencias en los análisis. Eso obviamente incrementa la demanda de habilidades analíticas muy sofisticadas.

Otro aspecto a considerar es la planificación de personal para el desarrollo de análisis de Inteligencia Estratégica. Esto puede ser tan dificultoso como planificar máquinas y organizaciones. Las habilidades y destrezas que se requieren de un analista de Inteligencia Estratégica se reflejan en lo que debe cubrir un análisis, particularmente en los temas discutidos anteriormente que requieren de áreas de alta especialización y sofisticación. Como ejemplo se puede tomar a un analista del espacio cibernético o de la tecnología al respecto, para ambos se debe tener un conocimiento muy complejo de la naturaleza del área, su evolución y los modelos analíticos para poder interpretar el acontecimiento y así predecir un potencial escenario. Se podría concluir que este personal requiere poder anticipar las tendencias políticas, económicas, tecnológicas y del espacio cibernético en forma correcta. Sin embargo, es muy dificultoso hacer estos pronósticos.

En la actualidad, se vive un ambiente de seguridad y defensa caracterizado por la presencia de amenazas multidimensionales sumamente complejas; la presencia de Conflictos Adaptativos Complejos así identificados por (Raza, 2015) pueden ser analizados por la Metodología CAPA (Análisis de Políticas y Evaluación de Conflictos por sus siglas en Inglés) constituye una arquitectura novedosa para edificar y sostener el proceso de Institucionalización de la seguridad pública y la defensa para desarrollar políticas y estrategias proactivas y exitosas ante las amenazas que hoy afectan a Latinoamérica.

La nueva política de seguridad y defensa y la Inteligencia Estratégica

La comunidad de Inteligencia Estratégica debe analizar más información con mayor alcance para un número muy superior de actores y de clientes. Por ejemplo hace 50 años la ONU contaba con 152 países cuando en la actualidad cuenta con 192, sin tomar en cuenta las organizaciones internacionales. Sólo en el hemisferio Occidental en los últimos años se han creado varias organizaciones como la UNASUR, CELAC, CDS, CFAC, SICA, etc. Esta situación demanda una política de Inteligencia Estratégica más abierta para satisfacer las necesidades de la multiplicidad de actores en todas las dimensiones y direcciones.

Es sumamente difícil entender los cambios de actitud hacia el secretismo de la Inteligencia Estratégica. No es que no deben haber secretos y confidencialidad, pero el cambio cultural con el advenimiento de la democracia como el sistema de gobierno más practicado en el mundo y los valores que sustentan su práctica, así como la toma de consciencia de

ISSN: 2225-5648, Año 5, Vol. 2, p. 75-106

los derechos humanos, hace que derechos como la libertad de expresión y la libertad a la información constituyan parte de nuestras vidas cotidianas en cualquier parte del mundo. Los casos de Julián Assange y Edward Snowden son ejemplos de estos cambios culturales a escala mundial en lo relativo a los derechos de privacidad, información y libertad de expresión. Esto impacta a la Inteligencia Estratégica no solo en la complejidad del análisis sino también en el uso y ejercicio de esta rama tan importante de la inteligencia. Hasta ahora estos casos recientes tocan las prerrogativas de los medio de comunicación para publicar información restringida, algo que hace sólo algunos años hubiese sido impensable. Por esta razón es que a los dos casos mencionados, tradicionalmente se les habrían impuesto penalidades severas en dos ámbitos: a los empleados de gobierno responsables de entregar información clasificada a los medios y más aún usar las redes sociales para divulgar información y, en segundo lugar, a los medios que se atrevieran a divulgar información secreta o confidencial del gobierno.

Estará por verse el desenlace de ambos casos que implican a la inteligencia como función fundamental del Estado y particularmente su ejercicio en un mundo que ha cambiado el ejercicio de la información con el advenimiento del Internet. El otrora monopolio de la información es parte del pasado. Estos son los aspectos de mayor realce que están cambiando la política del uso de la Inteligencia Estratégica a escala global y particularmente en Latinoamérica donde persiste la errónea interpretación de confundir la inteligencia con operaciones encubiertas que aunque podrían estar relacionadas como fuente de información, las segundas para la primera, es sólo una más de las múltiples fuentes de recolección de información para el análisis de Inteligencia Estratégica.

Papeles y expectativas de la Inteligencia Estratégica

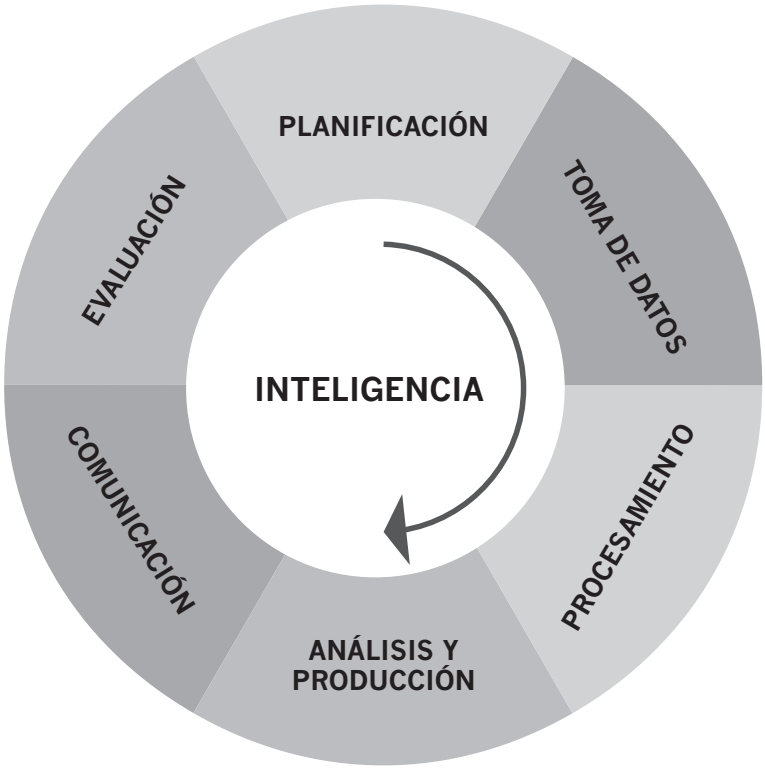
El ambiente actual de inteligencia es totalmente diferente de lo que era hace algunos años. Los cuatro aspectos de este análisis: poder, comunicación política, espacio cibernético y tecnología han impactado en forma significativa la labor de la Inteligencia Estratégica en su desarrollo, así como en los resultados que se esperan de su producto.

El futuro éxito de la Inteligencia Estratégica dependerá grandemente de cómo logre realizar su función y generar el análisis con la calidad y cantidad necesaria y suficiente. Afortunadamente, a diferencia de épocas anteriores ahora se cuenta con un cúmulo de experiencia en las cuales se pueden basar los cambios necesarios para cumplir las misiones y expectativas necesarias en forma eficaz. Como mucha de esta información es pública, es posible poner en práctica ciertas ideas concernientes a la producción de inteligencia, tomando en consideración los cuatro aspectos

ISSN: 2225-5648, Año 5, Vol. 2, p. 75-106

para lo cual se requiere repensar el proceso en función de la naturaleza de todos y cada uno de los actores, consumidores y el impacto que puede tener en el producto que servirá como la base fundamental para la toma de decisiones de los líderes políticos del mundo.

A continuación en la gráfica (Esteban y Bonilla, 2003) se presenta el proceso del ciclo de Inteligencia Estratégica que producirá el conocimiento justo y necesario requerido para proveer a los tomadores de decisión al más alto nivel del gobierno en función de los seis elementos del proceso: planificación, toma de datos, procesamiento, análisis y producción, comunicación y evaluación.



El ciclo de Inteligencia Estratégica para la Seguridad y Defensa

ISSN: 2225-5648, Año 5, Vol. 2, p. 75-106

Planificación. Consiste en determinar las áreas de interés estratégico del organismo para el que actúa el servicio de inteligencia y las necesidades de información concretas requeridas por sus responsables. Es una etapa crucial, ya que la Inteligencia Estratégica es el resultado de un proceso metódico que se origina en las necesidades de los usuarios.

Toma de datos. Trata de la adquisición, selección, autentificación y reunión de datos e información en bruto, mediante medios tecnológicos, humanos o documentales.

Procesamiento. Es el control y conservación de los datos recopilados por medios diferentes para su conversión e integración en conjuntos estructurados de información, que puedan adoptar la forma de mensajes documentales tras su recuperación. En este sentido se trabaja con sistemas electrónicos de gestión de datos y sistema de apoyo para la toma de decisiones.

Análisis y producción. Consiste en extraer con precisión y rapidez información a partir de los depósitos de datos, que induzca a la construcción de conocimiento. Esta fase marca la frontera entre información e inteligencia.

Comunicación. Radica en la distribución y puesta a disposición del documento creado al demandante del análisis o, por iniciativa propia del analista, al responsable de su departamento o del servicio de modo seguro.

Evaluación. La comunicación de informes de inteligencia no supone el final de un proceso iniciado con una petición general o especifica de información. Es necesario analizar las reacciones de los usuarios ante la información suministrada, identificar los objetivos cumplidos con las decisiones adoptadas sobre su base, y valorar la importancia que la información ha tenido en el logro de esos objetivos.

Es necesario hacer un esfuerzo en la producción de Inteligencia Estratégica para reducir la brecha entre los servicios de inteligencia y la gestión del conocimiento, si se considera la comunicación y la interacción entre esas tareas un elemento positivo para el progreso de ambas, en pro de la seguridad y defensa de la nación con una visión estratégica de la función.

ISSN: 2225-5648, Año 5, Vol. 2, p. 75-106

Conclusiones

La función de inteligencia como elemento de política pública a nivel nacional y estratégico experimenta cambios de índole evolutivo o involutivo, que permiten, a sus cuadros profesionales, reflejar y ejecutar lo democrático tan bien como lo represivo, en cualquier país.

Si se atiende a la naturaleza y al fin de la Inteligencia Estratégica y sus actividades, y al hecho de que la información obtenida por diversas fuentes es el elemento con el cual se trabaja, se está ante lo que se denomina la Inteligencia Estratégica en un mundo globalizado e interdependiente y que se refiere a un proceso de gestión del conocimiento. Sin embargo, la tradicional mutua ignorancia entre el cerrado y reservado mundo de los servicios de inteligencia para la seguridad y defensa, así como el abierto universo de la Inteligencia Estratégica con fuentes abiertas y cerradas para procesar la información documental, dificultan la necesaria osmosis de conocimiento y habilidades que enriquecería a ambas esferas. Su origen se encuentra, principalmente, en el diverso ámbito de aplicación de sus trabajos, los diferentes valores culturales que están detrás de los modos de adquisición, selección, tratamiento, difusión y uso de la información e incluso la procedencia y el estatus profesional de sus miembros.

No obstante, se debe reconocer los continuos progresos en los modos de producción de inteligencia y conocimiento por parte de los servicios que se integran en el marco disciplinario de la gestión del conocimiento a la luz de las cuatro áreas analizadas en este ensayo, lo que favorece el entendimiento de un mundo globalizado e interdependiente y la reconocida recepción de estos análisis de información en los diferentes ámbitos de gobierno como de la empresa, la industria, las finanzas y la administración pública en general.

En los últimos diez años, los adelantos producidos no tienen precedentes, ya que han impulsado la gestión del conocimiento a tiempo oportuno en los más altos niveles de la toma de decisiones, no tan solo en el gobierno sino también en el sector privado empresarial. La captura de datos por medios electrónicos en las redes sociales, el tratamiento y análisis electrónico de las cantidades ingentes de datos, la observación y seguimiento de la evolución del entorno, la integración de datos de diversa procedencia y modos de obtención, y la producción de información, análisis y evaluación, han sido tan grandes en su cantidad y calidad que, hoy día, sería casi imposible realizar la labor de Inteligencia Estratégica sin la tecnología digital. Esta tecnología se evidencia en el espacio cibernético, en los vehículos no tripulados de toma de información, en los espacios aéreos, acuáticos y terrestres, respectivamente, en pleno acontecimiento para el análisis y conversión de esa información en conocimiento para la toma de decisiones a todos los niveles públicos y privados del acontecer mundial.

ISSN: 2225-5648, Año 5, Vol. 2, p. 75-106

Resulta innegable en perspectiva, la consolidación del sistema democrático en Latinoamérica, a pesar de las marchas y contramarchas. Tal consolidación deberá reflejarse también en los sistemas de Inteligencia Estratégica latinoamericanos, en los que puede advertirse una clara tendencia a la institucionalización. En esta materia no faltan en la región profesionales altamente capacitados tanto en materia estratégica como en las diferentes áreas del análisis presentado con conocimiento, mucha técnica, y un equipamiento moderno de redes de información y comunicación.

El Centro William J. Perry de Estudios Hemisféricos de Defensa (WJPC por sus siglas en Inglés) está aplicando la metodología CAPA descrita anteriormente creada por el profesor Salvador Raza, experto en la materia, para la evaluación de conflictos y análisis de las políticas en ambientes donde se desarrollan los Conflictos Adaptativos Complejos (CACs) y de esta manera lograr identificar las variables intervinientes que generan la crisis y proceder a desarrollar las potenciales respuestas institucionales mediante el fortalecimiento de la institución de la seguridad y defensa.

El análisis de la Inteligencia Estratégica en Latinoamérica en los términos descritos en este ensayo requiere contar con una reforma institucional de funcionamiento caracterizada por cinco aspectos a destacar:

Primero, distinción en materia de competencia de los organismos de inteligencia, entre inteligencia exterior, inteligencia interior (incluyendo a la contrainteligencia dentro del propio país), e Inteligencia militar, con asignación de las respectivas competencias a distintos organismos para evitar el generalizado uso de la inteligencia militar en otras áreas fuera de su competencia.

Segundo, el establecimiento de la dependencia de los respectivos organismos de inteligencia respecto de los ministerios titulares de esas competencias, vale decir, Relaciones Exteriores, Interior, y Defensa.

Tercero, limitada asignación de competencias en materia de inteligencia interior, en particular a la inteligencia militar circunscrita a las amenazas contra el Estado y el sistema democrático tales como: terrorismo, narcotráfico, sedición, tentativas de cambio del sistema democrático por medios ilegales, contrainteligencia, espionaje, sabotaje, verificaciones de seguridad relativas a personal que accede a información secreta, medidas de seguridad de contrainteligencia.

Cuarto, establecimiento bajo dependencia del máximo nivel del Estado de un órgano de coordinación del sistema, planeamiento de inteligencia, y de elaboración de Inteligencia Estratégica nacional,–sin medios propios de obtención de información, ni de realización de operaciones encubiertas–, presidido por el máximo funcionario de inteligencia y constituido por los

ISSN: 2225-5648, Año 5, Vol. 2, p. 75-106

jefes de los organismos de inteligencia, representantes políticos de alto nivel de las áreas de relaciones exteriores, defensa, interior y economía. Por supuesto, con el apoyo de los mejores analistas de inteligencia de que se disponga, y de un conjunto de analistas en materias sustantivas de los sectores público y privado;

Quinto, controles eficaces integrados por las comisiones parlamentarias constituidas en cada una de las Cámaras, o Asambleas Unicamerales con amplias facultades, incluyendo investigativas, y la creación de un cargo de Comisionado Parlamentario para Asuntos de Inteligencia.

Es imprescindible un cambio en la cultura de inteligencia, sustituyendo el criterio de servicio a los intereses políticos y personales del gobierno de turno y de los de la propia estructura de inteligencia, por el de servicio a la Nación. Erradicar la acción coyuntural y sustituirla por la planificación estratégica, perfeccionar las capacidades técnicas adquiridas, pero perfeccionar y jerarquizar significativamente las capacidades de análisis; reclutar a los mejores, no a los amigos; administrar cuidadosa y adecuadamente los fondos de la actividad de inteligencia, actuar, en definitiva, con clara conciencia del rol de la actividad de Inteligencia Estratégica en el sistema democrático, consistente en contribuir a proteger al Estado y a los ciudadanos de las amenazas, informando sobre ellas a los decisores políticos, posibilitando de ese modo el necesario prestigio y reconocimiento social de la actividad.

En definitiva, así como se ha avanzado en Latinoamérica hacia la consolidación del sistema democrático, puede y debe avanzarse hacia una actividad de Inteligencia Estratégica base fundamental para el eficaz y legítimo uso del servicio congruente con el sistema democrático representativo de gobierno.

ISSN: 2225-5648, Año 5, Vol. 2, p. 75-106

Bibliografía

1. Bacalao-Pino, Lázaro Magdiel (2009). *Poder y Comunicación: Una segunda revisión crítica.* Universidad de la Habana. La Habana, Cuba. http://www.researchgate.net/publication/28314979_Poder_y_comunicacin_una_segunda_revisin_crtica

2. Berkowitz, Bruce D. & Goodman, Allan E. (1989). *Strategic Intelligence for American National Security*. New Jersey: Published by Princeton University Press. ISBN: 0-691-02339-5 198

3. Boot, Max. (2006). Technology Warfare, and the Course of History 1500 to today. Macrohistory and World Timeline. Disponible en: http://www.fsmitha.com/review/Boot.html

4. Caldevilla Dominguez, David. (2010). Las Nuevas Tecnologías Cambian el Panorama de la Comunicación Política. Disponible en: http://www.jourlib.org/paper/2640649#.VbeXIT8w-os

5. Esteban, Miguel A. y Bonilla Navarro, Diego. (2003) *Gestión del Conocimiento y servicios de inteligencia: la dimensión estratégica de la información.* Recuperado de http://www.elprofesionaldelainformacion.com/contenidos/2003/julio/3.pdf

6. Friedman, Thomas L. The World is Flat. *A brief history of the Twenty First Century*. (2005) Flattener # 4 Open Sourcing ISBN: 13-978-0-374-29288-1

7. Gómez de la Torre, Rotta Andrés. (2009). *Servicios de inteligencia y democracia en América del Sur: ¿Hacia una segunda generación de reformas normativas?* http://repositorio.pucp.edu.pe/index/handle/123456789/15918

8. Harris, Shane. (2014) *War the Rise of the Military-Intelligence Complex.* Copyright@2014 by Shane Harris. ISBN 978-0-544-25179-3. New York, New York 10003.

9. Huntington, Samuel P. (1991). The Third Wave: Democratization in the late twentieth century Published by the University of Oklahoma Press, Norman, ISBN 0-8061-2346-X

10. Jordan, Javier. (2011). Introducción al análisis de inteligencia. http://www.seguridadinternacional.es/?q=es/content/introducci%C3%B3n-al-an%C3%A1lisis-de-inteligencia

11. Kent, Sherman. (2015). Strategic Intelligence for American World Policy. Princeton Legacy Library Series. ISBN 978-069-162-4044

ISSN: 2225-5648, Año 5, Vol. 2, p. 75-106

12. Kurzweil, Ray. (1999). The Age of Spiritual Chines. When computers exceed human intelligence. Published by the Penguin Books ISBN 0-670-88217-8

13. Lewis, Bobbi Kay. (2009). *Social Media and Strategic Communication: Attitudes and Perceptions among College Students.* https://shareok.org/handle/11244/7479

14. McFATE, Sean. (2014). The Modern Mercenary Private Armies and What they mean for World Order. *Oxford University Press is a department of the b of Oxford.* New York, N.Y. ISBN: 978-0-19-936010-9 10016.

15. Naim, Moises. (2013). The End of Power. From Boardrooms to Battlefields and Churches to States, Why Being in Charge ins't what it used to be. Published by Basic Books, Member of the Perseus Books Groups. ISBN 978-0-465-03156-6 New York

16. Navarro Bonilla, Diego. (2004). El Ciclo de Inteligencia y sus límites. *España: Universidad Carlos III de Madrid.* http://dialnet.unirioja.es/servlet/articulo?codigo=2270935

17. Nye, Joseph, Jr. (2011). *The Future of Power. Part One Type of Power.* New York, N.Y.: Published by Public Affairs member of Perseus Book Group. ISBN 978-1-58648-891-8

18. O–Reilly, Tim. (2005). *"Qué es Web 2.0. Patrones del diseño y modelos del negocio para la siguiente generación del software".* Traducción del Portal de Comunicación de la Fundación Telefónica. Extraído de Internet. 23 de julio 2015. http://issuu.com/bibliotecas_duocuc/docs/la_biblioteca_en_la_web2.0/93

19. Raza, Salvador. (2015) *The CAPA Method for Conflict Assessment and Policy Analysis for the Security and Defense Sectors.* Disponible en: http://www.caei.com.ar/sites/default/files/working_paper_ndeg_38.pdf

20. Russel, Swenson y Lemozy, Susana. (2009). El Nexo de la Cultura Nacional y la Inteligencia Estratégica. Artículo en Internet. *National Defense Intelligence College. Washington D.C. En Democratización de la Función de Inteligencia Center for Strategic Intellegence Research*. Disponible en Internet AVISORA.com extracto del libro del mismo título. http://www.avizora.com/colaboradores/textos_jorge_serrano_torres/0011_democratizacion_de_la_funcion_de_inteligencia_comentario.htm

21. Sánchez Hernández, Carlos. (2011). Competitive intelligence: De los Estados a las empresas. *Nómadas, Revista Crítica de Ciencias Sociales y Jurídicas. España: Universidad Compútense de Madrid.* http://revistas.ucm.es/index.php/NOMA/article/view/NOMA1111140133A

22. Sanger, David E. (2012). *Confront and Conceal Obama's Secret Wars and Surprising use of American Power.* New York: Published by Crown Colophon are registered trademark of Random House, Inc. ISBN: 978-0-307-71802-0.

23. Scahill Blackwater, Jeremy. (2007) *The rise of the world's most powerful mercenary army.* New York: Published by MJF Book Fine Communications.

24. Schmidt, Eric & Cohen, Jared. (2013). *The New Digital Age Reshaping the Future of People*. Nations and Business. New York: Published by Alfred A. Knopf. ISBN: 978-0-307-95713-9

25. Singer, P.W. (2009). Wired for War The Robotics Revolution and Conflict in the 21st Century. New York, N.Y.: Published by The Penguin Group (USA) Inc. ISBN: 978-1-59420-198-1.

26. Weber, Max. (2009). *La Política como Vocación.* Alianza Editorial. Traducido por Francisco Rubio Llorente. pág. 83-84. Disponible en: http://www.lasangredelleonverde.com/el-estado-como-monopolio-de-la-violencia-segun-max-weber/