ISSN 2477-9253

Revista de Ciencias de Seguridad y Defensa

Número II

ESPE
UNIVERSIDAD DE LAS FUERZAS ARMADAS
INNOVACIÓN PARA LA EXCELENCIA

2016

Revista de Ciencias de Seguridad y Defensa

DEPARTAMENTO DE SEGURIDAD Y DEFENSA
UNIVERSIDAD DE LAS FUERZAS ARMADAS - ESPE
2016

Revista de Ciencias de Seguridad y Defensa
Revista oficial del Departamento de Seguridad y Defensa de
la Universidad de las Fuerzas Armadas - ESPE
2016

Periocidad
Trimestral (marzo-**junio**-septiembre-diciembre)

Número 2

Diseño de Portada y contraportada
David Cabrera R.

Edición gráfica, diseño y diagramación
David Cabrera R.

Preguntas y Correspondencia
Theofilos Toulkeridis
ttoulkeridis@espe.edu.ec

La revista de Ciencias de Seguridad y Defensa es un órgano de difusión científica semestral del Departamento de Seguridad y Defensa de la Universidad de las Fuerzas Armadas - ESPE, cuyos contenidos giran en base a temas como: seguridad, defensa, historia militar, sociología militar, geopolítica, eduación militar, estrategia, paz y desarrollo.

Como citar (ejemplo)
Dávalos Suárez, J., 2016: Una aproximación a la Oceanopolítica. Revista de Ciencias de Seguridad y Defensa, 1: 13-18

Revista de Ciencias de Seguridad y Defensa
2016
ISSN 2477-9253

Sumario

Número 2, 2016

MENSAJE INICIAL

En el mundo de la seguridad y la defensa, la velocidad con la que se vive hoy en día nos conduce a pensar y analizar en los "últimos escenarios", ya no en los "nuevos escenarios". Pese a esta versatilidad, la seguridad y defensa no dejan de ser espacios de ciencia y de acción. Pero, sobre todo, de bienestar colectivo. De allí que, publicar una revista sobre esta línea de investigación: es hacer eco de las ideas fraguadas en el ámbito académico, es alumbrar con el pensamiento aquellos rincones de paz y desarrollo, es apoyar a la prosperidad de los pueblos.

En este primero número de nuestra ***Revista de Ciencias de Seguridad y Defensa*** se tejen ideas, mensajes y reflexiones. En sí, esta publicación es un conjunto de páginas en las que se reflejan contenidos científicos relacionados con las tres dimensiones del accionar humano: el terrestre, el marítimo y el aeroespacial, a lo que se suman temas sociales e históricos, sin que por ello se marque territorio eminentemente militar, pues esta publicación es plural, cosmopolita y libre de estructuras jerárquicas.

Con un fraterno saludo

Milton Patricio Rodríguez Rojas
Teniente coronel de Estado Mayor
Director del Dpto. de Seguridad y Defensa
Universidad de las Fuerzas Armadas - ESPE

EDITORIAL

Escribir una revista sobre seguridad y defensa es, realmente, una tarea compleja pero necesaria; más aún, cuando las nuevas concepciones del bienestar están garantizadas en el contexto de las "responsabilidades estatales", líderes en garantizar una sociedad libre, cohesionada y productiva; pero, sobre todo, segura.

Dado que la seguridad moderna, tanto como la defensa, evitan y neutralizan las amenazas de todo tipo, protegiendo así la democracia y el desarrollo de los pueblos, la seguridad y la defensa también están identificadas como líneas paralelas que garantizan la estabilidad de los estados a través de un empleo equilibrado del poder y una visión estratégica alineada con los intereses nacionales. Todo esto, apuntando a un destino final: el bien público.

Bajo este breve enfoque conceptual, el Departamento de Seguridad y Defensa de la Universidad de las Fuerzas Armadas-ESPE, empeñado en compartir y difundir conocimientos puramente académicos, presenta en estas páginas los dieciocho artículos impresos en dos tomos. Estos artículos fueron seleccionados para formar parte de la primera edición de la revista científica de este Departamento, cuyos contenidos revelan ideas e informaciones de diferentes ejes temáticos pertenecientes a diversos escenarios y épocas: industrial-militar, aeroespacial, marítimo, social, histórico, estratégico y de seguridad y defensa, tal como su nombre lo anuncia.

En esta publicación, Sudamérica viene a ser el eje temático de mayor mención. Pues esto obedece a dos análisis comparativos sobre la defensa del subcontinente, especialmente cuando se trata de una pelea futura por el líquido vital, allá por tierras guaraníes, y otro sobre la industria militar. En este último tema, los autores relacionan la teoría del gasto militar con el crecimiento económico de los países dentro del escenario suramericano, de modo que el impacto de las empresas e industrias de armamento en la región, nos conducen a una interrogante: ¿es posible una industria militar de UNASUR?

A estas páginas llega, también, un artículo cuya palabra fuerza es nueva en el léxico geoestratégico, pese a que en la dimensión global resulta ser trascendental: *Oceanopolítica*. No se trata de un eufemismo. Simplemente es un nuevo término que acoge los valores políticos, económicos, militares y sociales de un Estado y su relación con el mar, tanto como su seguridad, desarrollo y crecimiento, elementos básicos del poder nacional.

Y no podía faltar el toque histórico que guarda la mayoría de documentos académicos. Aquí destaca un artículo que trae a la memoria las lecciones aprendidas de las operaciones aerotransportas desplegadas en octubre de 1983, en Granada, una pequeña isla del Caribe que años atrás fue colonia británica. Previo acuerdo establecido bajo una alianza militar caribeña, fueron empleados miles de soldados profesionales de los Estados Unidos de Norteamérica, con la misión de recuperar el gobierno prooccidental de Sir Eric Gairy, mismo que fue derrocado por un movimiento marxista. Se vivía tiempos de la Guerra Fría. Eso explica todo.

Alrededor del eje temático central, giran varios títulos que van desde la seguridad internacional, pasando por la delincuencia común, hasta la misma *ciberseguridad*. Dentro de este espacio académico, destaca el tema de los refugiados colombianos en el Ecuador. Al respecto, el autor de este artículo descifra este movimiento migratorio y sus nuevas formas de vida, esperanzas y desafíos, en una tierra que les acoge sin mayores condiciones.

Otro autor pone de manifiesto los elementos de planificación estratégica enfocados hacia las políticas de seguridad y defensa en el espacio aéreo. En términos más cotidianos, el artículo analiza el uso, desuso y abuso de este espacio "duramente militarizado" y con tendencias a una guerra tecnológica de vanguardia. No es que se trate de alarmar con una próxima guerra de las galaxias, pues para esto ya existen tratados internacionales que establecen políticas sobre estos panoramas.

Empero, alarma o no, El súper − volcán Chalupas, ubicado en la provincia de Cotopaxi, sale a la luz como una amenaza natural cuyos efectos serían considerados como una catástrofe global. Según el autor de este artículo, de darse la erupción de este súper − volcán, los daños serían incalculables, ahora la pregunta sin respuesta es ¿cuándo?

Cierran con broche de oro cuatro artículos de opinión. El primero establece un análisis conceptual sobre la palabra *amenazas* y su diversidad de adjetivos: viejas, nuevas, tradicionales… Esta palabra, que ha sido y seguirá siendo mencionada hasta la saciedad en todos los eventos académicos y publicaciones impresas y electrónicas, aquí tiene un baño de semántica y objetividad en su mención. Pues vale la pena que los académicos inspirados en el estudio de seguridad y defensa se retroalimenten con este artículo. Por último, hay un artículo de opinión al cual no haremos mención a su contenido sino a su autor. Es un joven cadete de la Escuela Militar cuyo anhelo era publicar sus ideas. Sueño cumplido.

Amigos lectores de esta línea de investigación, tienen en sus manos un trabajo de equipo con esa diversidad de temas que, de seguro, oxigenarán su lectura y su apego a viajar por el mundo de las letras y la investigación sobre seguridad y defensa. Asumimos a que su lectura sería incompleta si no existiera su crítica y análisis correspondientes. Bienvenidos al recorrido de estas páginas.

CHALUPAS
UN SÚPER-VOLCÁN ECUATORIANO QUE AMENAZA A TODO EL PLANETA

Theofilos Toulkeridis
Universidad de las Fuerzas Armadas - ESPE

Resumen

Un súper-volcán se ha reconocido en suelo ecuatoriano llamado Chalupas. Este volcán se manifiesta con masivos depósitos de ignimbritas, ubicados en varios sitios en el país. Una reactivación de este volcán podría resultar en la emisión mínima de ceniza expulsada de un volumen de 575 km3 y de un volumen mínimo de magma erupcionado de aproximadamente 230 km3, teniendo un Índice de Explosividad Volcánica de moderado a alto 7. La probabilidad de una reactivación en el siglo XXI es de unos calculados 0.1 - 6%. El daño potencial con una futura reactivación de este súper-volcán es incalculable.

Palabras claves: Chalupas, súper-volcán, índice de explosividad volcánica, destrucción masiva, invierno nuclear

Introducción

Dos veces en la historia del pasado próximo, el Homo Sapiens estaba al borde de la extinción debido a las explosiones volcánicas. Se trata de la explosión de la laguna de Taupo en Nueva Zelanda, la cual 23.000 años atrás expulsó mil veces más ceniza que cualquiera de las explosiones del siglo XX, y enfrió por varios años a todo el planeta. Una erupción anterior, 70.000 años atrás, fue aún peor. La erupción del volcán Toba, en Sumatra, oscureció el planeta Tierra por varios años. El invierno nuclear que siguió a esta catástrofe ha reducido la población de los humanos a pocos miles, como sabemos hoy, debido a las investigaciones de ADN entre otros descubrimientos arqueológicos. Los únicos volcanes que podrán generar una catástrofe global se llaman súper-volcanes. Hay unas tres docenas de estos súper-volcanes activos en el mundo, y uno de ellos está en el Ecuador, en la provincia de Cotopaxi. Se llama Chalupas.

Comportamiento de los Súper-volcanes

Tales volcanes de tipo súper-volcán o mega-caldera, no se notan a primera vista porque les falta el típico pico volcánico como es el caso del Fuji, Misti o Cotopaxi, y así se quedan fuera de la percepción de su potencial peligrosidad para el pueblo que vive cerca o hasta encima de estos gigantes. Después de una erupción y el vaciamiento de una enorme cámara de magma, se quedan morfologías similares a valles o casi calderas planas. A los súper-volcanes les pertenecen cámaras de magma, las cuales pueden alcanzar extensiones de hasta miles de kilómetros cuadrados. Las mismas morfologías de los súper-volcanes parece que están "respirando" porque ascienden y descienden, siendo un poco y medible su acumulación, pues el magma en su cámara correspondiente está en movimiento.

El despertar de estos volcanes puede ser demasiado rápido, como en el caso actual del volcán Uturuncu en Bolivia, tomando en cuenta que los planes preventivos simplemente no existen. Los súper-volcanes son bombas de tiempo. Solamente un centímetro de ceniza sobre un campo cultivado sería suficiente para destruir la cosecha. En el caso de la erupción de Toba se

precipitaron 15 cm. en una área que cubrió gran parte de India y de China, esta afectaría hoy en día a más que un billón de personas de forma severa. Sin embargo, estos volcanes son demasiado peligrosos para una enorme cantidad de personas, pero no son los más peligrosos del mundo. El súper-volcán globalmente más peligroso se encuentra en Estados Unidos y se llama Yellowstone. Este volcán tiene un diámetro de 70 a 30 kilómetros lo que hace imposible de verle sin utilizar imágenes satelitales.

Los súper-volcanes son una clase por sí misma y no se pueden comparar con ningún otro tipo de volcanes conocidos. En forma muy poderosa, como en ningún otro sitio del planeta, el calor de la parte interior de la tierra asciende con más fuerza hacia arriba. Pero la peligrosidad no emerge de este hecho, más aún, y al contrario de los volcanes comunes, no está buscando el magma de los súper-volcanes un camino directo hacia la superficie (Fig. 1a). El magma se acumula en la corteza superior donde derrite cada vez más roca de su alrededor. Así se infla el material licuado en la cámara de magma por miles de años (Fig. 1b). En la cámara misma predomina un infierno, donde el magma viscoso está en movimiento permanente. A cada rato se derrite la corteza superior hasta la superficie. La corteza se adelgaza más y más, mientras los gases bastante comprimidos dentro del magma se impulsan hacia arriba. Al mismo tiempo se forman fisuras en la corteza debido a estos movimientos; por una parte las inflaciones, debido a los movimientos de magma y gases hacia arriba y por otra, deflaciones por el derretimiento de las rocas encima de la cámara del magma (Fig. 1b). Algún momento podrá llegar una fisura a la cámara de magma la que iniciaría una descarga del calor atascado con un poder apocalíptico (Fig. 1c).

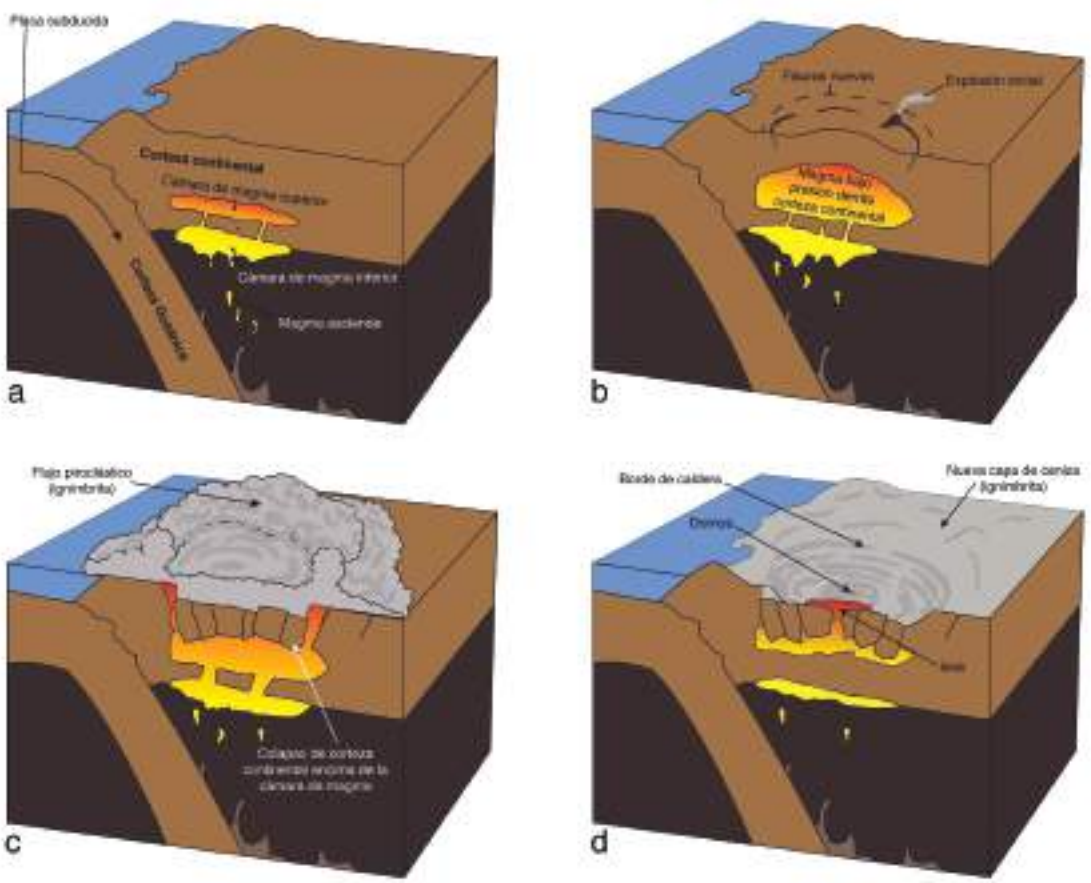

Fig. 1 a-d: Evolución y desarrollo de una explosión de un súper-volcán. Cortesía GEO1 - Theofilos Toulkeridis

Fig. 2: Índice de Explosividad Volcánica, con ejemplos mayormente del Ecuador

Magnitud de erupción (IEV)	Mínima masa erupcionada (kg)	Volumen mín. de magma erupcionado (km^3)	Volumen mín. de ceniza expulsada (km^3)	**Ejemplo** (de erupción tipica históricamente / ultimamente)	**Frecuencia** (numero promedio de erupciones por 100 años)	**Probabilidad** (min. que una erupción suceda en siglo 21)
7 (bajo)	1×10^{14}	40	100	Mas grande que Tambora 1815	0.1 - 0.5	10 - 50%
7 (mod.)	2.5×10^{14}	100	250	Posiblemente Ki-kai, Japón, hace 6000 años	0.01 - 0.06	1 - 6%
7 (mod.-alto)	**5×10^{14}**	**230**	**575**	**Chalupas, Ecuador**	**0.001 - 0.06**	**0.1 - 6%**
7 (alto)	8×10^{14}	300	750	Campaniana, Italia, hace 35000 años	0.001 - 0.01	0.1 - 1%
8 (bajo)	1×10^{15}	400	1000	Taupo caldera, NZ, hace 26000 años	<0.001>	<0.1%>
8 (alto)	8×10^{15}	3200	>5000	Evento tamaño Toba, hace 75000 años	0.0001	Aprox 0%

Lava, gases y ceniza se dispararán en una lluvia de fuego hacia el cielo. Y esto es solamente el inicio. La gota que iniciaría, el derrame empezaría apenas. Se multiplican las fisuras y el magma viscoso abre el camino dentro de las nuevas aperturas. Estas aperturas ahora se extienden tanto y en tal forma que se unificarían para formar un continuo resquicio elíptico hasta circular como un anillo (Fig. 1c). Cuando ocurre esto, la tapa de las rocas consolidadas de la corteza superior por encima de la cámara de magma, no tendría más una base y colapsaría de la misma forma como se quiebra un techo de una casa cuando los muros que la sostienen se colapsan. Se hunde esta masa consolidada de una o en varias partes en la cámara de magma, la cual se vacía al mismo tiempo, acelerando con esta presión de su peso quebrante la salida de más lava y gases fuera de los límites del anillo.

Después de esta erupción en forma vertical siguen varias más y el material expulsado – llamado ignimbrita – arrastra (Fig. 6), cubre y mata todo en su camino por cientos de kilómetros alrededor del centro volcánico (Fig. 1d). A nivel mundial, empieza un invierno nuclear donde comunicaciones, infraestructura, productividad agraria y movimientos aéreos entre otras catástrofes, fallarían por meses o hasta años. La expulsión de una enorme cantidad de dióxido de

Fig. 3: Vista aérea panorámica de gran parte del volcán Chalupas y del volcán Cotopaxi. Cortesía Instituto Geográfico Militar del Ecuador

Fig. 4: Vista panorámica del Chalupas y del volcán extinto Quilindaña. Cortesía Rafael Peña.

azufre generaría lluvia ácida, las temperaturas bajas se podrían comparar con una nueva era de hielo. En los meses siguientes se lamentará la muerte de cientos de millones de personas.

Situación Geológica del volcán Chalupas

Si pensamos sobre el súper-volcán ecuatoriano llamado Chalupas, el cual fue reconocido, evaluado y clasificado su IEV (Índice de Explosividad Volcánica) potencial, por el primer científico, autor de este articulo (Fig. 2; Tabla 1), Ecuador se acabaría casi totalmente y un máximo de 5% de la población actual podría sobrevivir conjuntamente con la población de Galápagos (Fig. 5). Pero solo si tenemos suerte. La pregunta del millón no es si va a erupcionar el Chalupas, sino más bien cuándo lo hará (Tabla 1).

Así, el volcán más peligroso del Ecuador es el único súper-volcán presente con un IEV de "7" en el país y está ubicado en la parte sur a suroriental del volcán Cotopaxi, a solamente 60 km de Quito (Fig. 3; 4). El volcán Chalupas tiene un diámetro entre 15 a 20 kilómetros y es mayormente plano (Fig. 3; 4), con típicas estructuras de una caldera y en su centro se encuentra un cono volcánico llamado Quilindaña con una altura de 4.878 msnm. compuesto inicialmente de andesítas anfibolíticas, más tarde de andesítas piroxénicas y olivínicas, terminando con un domo dacítico que es solamente un producto de actividad posterior de la fase eruptiva dominante.

La fase eruptiva fuerte del Chalupas ocurrió hace aproximadamente 200.000 años atrás, produciendo varios cientos de km3 de material piroclástico (Tabla 1), cubriendo una extensión de más que 2.000 km2 (Fig. 5). Muchos de los depósitos riolíticos se encuentran hoy en día en el valle interandino. El Chalupas era un estratovolcán con lavas andesíticas en su base antes de su colapso. Parece que después de un extenso reposo de actividad, el Chalupas erupcionó de nuevo en siete ocasiones entre 6.300 y 15.000 años atrás. Dos centros eruptivos jóvenes (domos riolíticos) se encuentran en la zona norte del Chalupas, llenando los valles y correspondientes ríos de Yanaurcu, Barrancas y Valle del Río.

Los depósitos del gran evento del Chalupas son casi exclusivamente predominados de ignimbritas (Fig. 5; 6). La mayoría de las estructuras calderitas están borradas debido a la intensa actividad glaciar en este sector. Sin embargo, estudios en las últimas décadas ubican al sector de Chalupas como la zona más productiva para el uso de energía geotérmica en el Ecuador. La reactivación masiva de este súper-volcán sería similar con la casi completa destrucción del Ecuador.

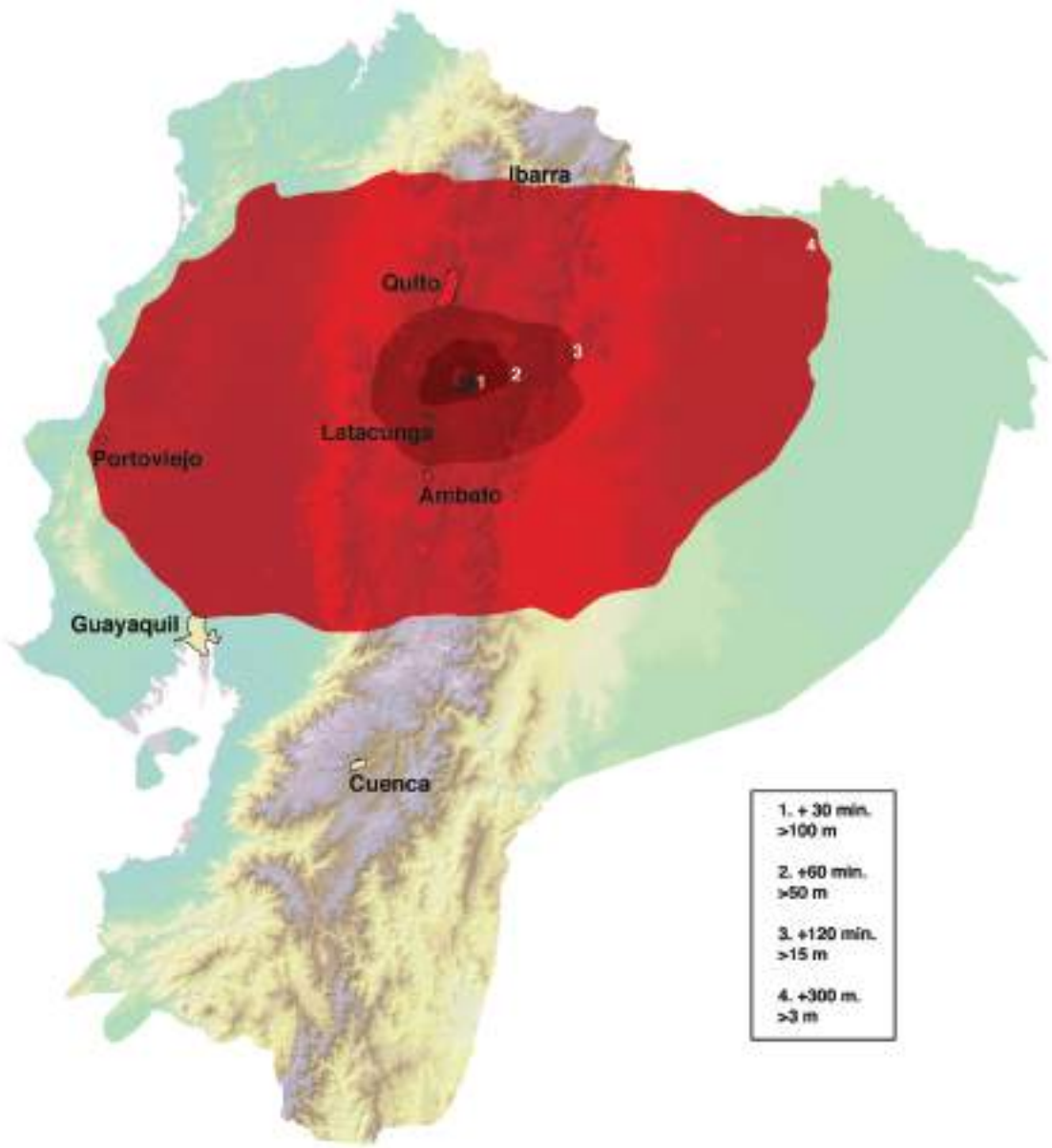

Fig. 5: Distribución de ignimbritas, su espesor y el tiempo de la llegada en una eventual fase eruptiva fuerte del súper-volcán Chalupas. Cortesía GEO1 - Theofilos Toulkeridis

Fig. 6: Depósitos de ignimbrita en una cantera algunos 31 km al sur-occidente del volcán Chalupas. Nota la persona como escala y que no se vea ni base ni tope (erosionado) de este depósito de 56 m visibles de la última fase eruptiva del volcán Chalupas. Cortesía GEO1 - Theofilos Toulkeridis

Conclusión

El daño potencial en una futura reactivación de este súper-volcán sería incalculable. Sin embargo, se puede predecir que el Ecuador dejará de tener vida humana después de la próxima explosión de este volcán andino que amenaza todo el planeta.

Referencias

Breining, G, (2007). Super Volcano: The Ticking Time Bomb Beneath Yellowstone National Park Paperback. Voyageur Press: 256 pp.

Hall, M.L., Samaniego, P., Le Pennec, J.L., Johnson, J.B, (2008). Ecuadorian Andes volcanism: A review of Late Pliocene to present activity. J. Volcanol. Geotherm. Res. 176, 1–6.

Mason, B.G., Pyle, D.M. and Oppenheimer, C, (2004). The size and frequency of the largest explosive eruptions on Earth. Bull. Volc., 66: 735-748.

Oppenheimer, C., Eruptions that Shook the World. Cambridge University Press: 408 pp.

Schminke, H.U, (2004). Volcanism. Springer, Berlin-Heidelberg: 324 pp.

Sigurdsson, H., Houghton, B.F., McNutt, S., Rymer, H. and Stix, J, (2000). Encyclopedia of Volcanology. Academic Press, San Diego: 1417 pp.

Toulkeridis, T, (2011). Volcanic Galápagos Volcánico. (bilingual Spanish-English). Ediecuatorial, Quito, Ecuador: 364 pp

Toulkeridis, T, (2013). Volcanes Activos Ecuador. Santa Rita, Quito, Ecuador: 152 pp

Toulkeridis, T., Buchwaldt, R. and Addison, A, (2007). When Volcanoes Threaten, Scientists Warn. Geotimes, 52: 36-39

Zeilinga de Boer, J., Sanders, D.T., Ballard, R.D, (2004). Volcanoes in Human History: The Far-Reaching Effects of Major Eruptions. Princeton University Press: 320 pp

Siebert L, and Simkin, T, (2002). Volcanoes of the World: an Illustrated Catalog of Holocene Volcanoes and their Eruptions. Smithsonian Institution. Global Volcanism Program Digital Information Series, GVP-3, (http://www.volcano.si.edu/gvp/world).

ESTRATEGIAS INCONEXAS EN LOS SISTEMAS DE SEGURIDAD

Oswaldo Jarrín R
Universidad Internacional del Ecuador - UIDE

Resumen

La denominada arquitectura de seguridad hemisférica, que se trata más bien de un sistema de seguridad del Régimen Interamericano, ha tenido una gran evolución en el escenario de la seguridad continental, desde antes de la creación de la OEA, 1948.

Las iniciativas para la creación y actualización de las organizaciones intergubernamentales a nivel regional y subregional, para preservar y mantener la estabilidad y la paz regional, han sido múltiples y variadas; no obstante, las políticas provenidas en las organizaciones subregionales no han logrado los propósitos que regularmente han motivado los encuentros internacionales, más aún cuando las estrategias determinadas a nivel Estado, muchas veces se independizan de los compromisos que regularmente se adquieren.

Palabras claves: Seguridad colectiva, seguridad cooperativa, control político, seguridad humana, seguridad pública

Escenario evolutivo de la seguridad

La Unión de Repúblicas Americanas, como se conocía en origen a la Asociación de Países del Continente decide, en 1942, la creación de la Junta Interamericana de Defensa JID, ante una situación internacional de amenaza a la paz, seguridad e independencia futura del hemisferio Occidental, derivada de la Segunda Guerra Mundial. La misión encomendada a la Junta era preparar gradualmente a las repúblicas americanas para la defensa del continente americano.

Sin embargo, los análisis y el debate acerca del escenario de la seguridad hemisférica, normalmente toman como referencia al Tratado de Asistencia Recíproca, TIAR, que habiendo sido firmado en 1947, lo convirtieron en uno de los pactos de defensa de pos guerra más antiguo en cuanto a defensa colectiva a nivel global, producto de la resolución de la Conferencia Interamericana sobre problemas de la guerra y la paz, según consta en el primero de sus considerandos.

Cuando se trata de analizar la evolución del escenario de la seguridad interamericana, se considera al TIAR, como referencia principal de un primer periodo de la defensa colectiva, a partir del cual se avanza en el continente hacia la seguridad colectiva con la firma de la Carta de la OEA y el Pacto de Bogotá en 1948. En su inicio, el TIAR, enfatizaba procesos políticos y compromisos pendientes que existían en el régimen internacional americano y que sin duda sirvieron de inspiración y aun de modelo para conjurar las amenazas de agresión contra cualquiera de los estados del hemisferio. El más antiguo de ellos fue la Doctrina Monroe de 1823, declaración elaborada cuando los conflictos derivados de influencias económicas y de las rivalidades entre las potencias europeas, miraban a los recientemente independizados países americanos, como una oportunidad de reconquista.

Esta visión geopolítica continental adquirió una gran y permanente trascendencia a partir de 1826, en que se ratifican y amplían los acuerdos entre los países americanos en el célebre Congreso de Panamá. A pesar de su limitada convocatoria y corta permanencia política, el

Congreso significó un gran aporte a la integración y posicionamiento de los países americanos, dentro del marco de las relaciones internacionales en materia del derecho internacional y la defensa. Sus propósitos políticos eran lograr la unión y confederación de los países americanos basados en una renovación de tratados, en la organización de normas del derecho internacional y solución pacífica de conflictos, pues no desconocía sino más bien promocionaba la Doctrina Monroe con una convención de contingentes militares y navales en apoyo a la independencia de Cuba y Puerto Rico.

Este antecedente histórico, de visión geopolítica, se reforzó y adquirió la importancia de una verdadera escuela geopolítica norteamericana con la teoría de Spykman , que aportaba un enfoque diferenciado de las regiones en el continente americano, mientras que la Europa de entonces colocaba planteamientos contrapuestos a la teoría de Mackinder en cuanto al cambio del concepto de control del corazón del mundo.

Empero en el mundo, ocurren importantes acontecimientos de pos Segunda Guerra Mundial, ya que no obstante haberse logrado la creación de la Organización de las Naciones Unidas ONU, se incrementan las diferencias entre los países vencederos, produciéndose un cambio en la correlación de fuerzas por la búsqueda de supremacía de las potencias, como un efecto contrario a lo que se esperaba con el reordenamiento mundial instituido en 1945 con el Tratado de Yalta.

De hecho era el nacimiento del bloque comunista con pactos bilaterales de amistad y asistencia por parte de la URSS, aunque inicialmente su propósito era vista solo como una reacción al Plan Marshall desarrollado por los Estados Unidos para la recuperación económica de Europa occidental. De esta manera cobra importancia la denominada Doctrina Truman, que impulsó la estrategia de la contención al comunismo y que en las américas se ve reflejada en ayuda militar y económica. Con esto, el mundo vive dos enfoques sobre un mismo concepto de seguridad que alimentan el conflicto ideológico. La seguridad se basa entonces en el desarrollo socio–económico, pues el dilema es cómo lograr en cada Estado ese desarrollo con ideologías contradictorias que son la base de la confrontación Este - Oeste, que identifica a la época de la bipolaridad.

Así se pasa de la defensa colectiva del TIAR hacia la Seguridad Colectiva, entendida como el comportamiento de Estados que graviten su política exterior en intereses compartidos, según acuerdos y compromisos formales institucionalizados y reconocidos por estructuras jurídicas y políticas, evitándose la conformación de contrapoderes.

Se trata de que la seguridad colectiva tenga capacidad de movilización de una coalición internacional multinacional para detener, disuadir y defender a la comunidad de una amenaza externa común, con aprobación de una autoridad internacional y en conexión con el artículo 51 de la Carta de las Naciones Unidas. En este sentido, el capítulo VI de la Carta de la OEA , define la seguridad colectiva como la inviolabilidad del territorio y de la soberanía de los Estados y la garantía de la legítima defensa individual o colectiva o de cualquier acto que ponga en peligro la paz. Por lo tanto, los aspectos de carácter político, confianza mutua, solución pacífica de los conflictos, control de armamento, diplomacia preventiva y de desarrollo social y económico, abren una segunda etapa en la evolución del escenario de la seguridad hemisférica.

El "Balance del terror" - se pensaba - había logrado la estabilidad y la paz en base del temor y el miedo permanente a la represalia masiva y aun a la Destrucción Mutua Asegurada, MAD En ese ambiente se produjeron varias crisis: Berlín, Praga, Checoeslovaquia, Canal de Suez; que, tratándose del continente americano, tienen la máxima significación para el mundo la Crisis de los Misiles, producida luego de que Cuba fuera expulsada de la OEA en 1962, y donde el mundo se encontraba al borde de un conflicto nuclear.

Apenas resuelta la situación de crisis de los misiles, el presidente Kennedy evaluó la política exterior y de seguridad basada en la disuasión nuclear. Así mismo, fortaleció la centralización del control de las armas nucleares , que en etapas sucesivas lograría acuerdos con la URSS para la celebración de las conversaciones y acuerdos de limitación de armas nucleares, conocidos como los acuerdos SALT . El Continente Americano no se alejó de esta política de control de armas nucleares, antes la asoció a la política de seguridad del régimen interamericano y en 1967 se firma el Tratado de Tlatelolco para la proscripción de armas nucleares en América Latina y el Caribe.

La mayor perturbación a la paz se produjo en los países americanos debido a los impulsos de una revolución que recorrió como un efecto dominó en los países latinoamericanos y del Caribe, ansiosos por alcanzar cambios en sus estructuras sociales, económicas y políticas, creándose oportunidades para que actuaran líderes populistas, partidos políticos que impulsaban la insurrección y grupos subversivos que proliferaron en el continente, elevando a Cuba como el adalid de la lucha revolucionaria a partir de la guerrilla organizada por Fidel Castro contra la dictadura de Batista.

Se incrementaron mecanismos de cooperación y de fomento de la confianza, como fue la designación de la Alianza para el Progreso como una comisión ejecutiva del Consejo interamericano de lo económico y social, de la OEA, como una réplica de la Doctrina Truman en el continente. Se trató de abrir mercados supranacionales con la creación de la ODECA o Carta para América Central, BID y el Mercado Sudamericano, según el Acuerdo de Montevideo.

La Perestroika de Gorbachov, si bien contribuyó a suprimir los criterios ideológicos en las relaciones internacionales, por otra parte dejó un especio inestable perdiéndose un factor de estabilización, donde las evoluciones repercutirían tanto en la periferia de Europa Oriental como en el resto del mundo.

En el contexto de una extensión de la teoría de la contención al comunismo y por otra parte con el patrocinio comunista externo para el impulso de la revolución armada en los países latinoamericanos, se implementó en varios países de la región la Doctrina de la Seguridad Nacional, que condujo a una lógica de preeminente protección del Estado ante el supuesto enemigo interno representado en los grupos ideológicos de extrema izquierda subversivos que desencadenaron violencia armada hasta legar a brotes de guerra civil al interior de los países con grave afectación a los derechos humanos.

En el ámbito político – militar, las instituciones armadas debían mantenerse en nivel de su especialidad y responsabilidades profesionales, subordinadas y orientadas por las decisiones políticas y no ser utilizadas para fines partidistas. Frente a estos aspectos, la OEA recoge los contenidos de la Declaración de Santiago de 1991en la que determinan que la democracia representativa era y debía ser la forma de gobierno común de todos los países de la región, con lo cual se elabora la Carta Democrática Interamericana en el 2001, coincidente con el 11 de Septiembre como dice en su texto "precisamente cuando la democracia enfrenta en todo el mundo un terrible desafío" refiriéndose al terrible atentado terrorista del World Trade Center en los Estados Unidos, como una oportunidad para crear un compromiso de consolidación y sustento de la democracia en la región.

Los múltiples cambios en el escenario de la seguridad hemisférica como producto de la post Guerra Fría y del advenimiento de la globalización, produjeron a nivel global otros cambios menos dramáticos pero igualmente importantes y definitivos especialmente para los países de la periferia, porque la globalización no se desarrolla sobre una base plana o neutral, sino que más bien tienen un efecto híbrido; es decir, tiene como resultado una mezcla de los efectos de

la globalización con los significados locales, sociales, económicos y políticos y culturales, no suficientemente superados.

Países poseedores de deudas inmensas, aparatos estatales ineficientes y corruptos que han tenido que realizar serios ajustes estructurales, adoptar políticas de austeridad, frecuentemente recortando presupuesto a programas de asistencia social, viven nuevamente escalas de fricción, inestabilidad y nuevas formas de violencia.

Por otro lado, la globalización ha facilitado la conformación y expansión de redes del crimen organizado con ramificaciones internacionales, convertidos en poderes que llegan a compartir con la guerrilla o grupos ilegales armados zonas geográficas para la producción de droga y desarrollo de comercios ilegales. Sus enormes ingresos y poder económico desarrollado, les permite organizar, equipar y mantener fuertes contingentes armados con capacidad de amenazar a los poderes del Estado.

En el año 2000, la UNESCO - con la presión de movimientos antiglobalización - desarrolló la Cumbre del Milenio, para exigir un nuevo orden mundial y tomar medidas ante las situaciones de inseguridad. La agenda se concretó en la determinación de los ocho objetivos del milenio para afrontar de la mejor forma los problemas más graves de la vida cotidiana en materia de pobreza, educación, salud, pandemias, medio ambiente, igualdad de género, mortalidad infantil y compromisos para fomentar una asociación mundial para el desarrollo. Sin embargo, cuando se trata de tomar medidas en forma más directa ante las diferentes amenazas que no son esencialmente de tipo militar, o de orden interestatal, se siente el problema de cómo conceptualizar a la seguridad en el nuevo escenario mundial.

El debate surge el momento de dar un tratamiento a la seguridad con el enfoque de la seguridad humana y constatar que la seguridad de la gente, pasa a ser prioritario en contraposición a la seguridad nacional de la Guerra fría. En este nuevo enfoque se toma en cuenta los riesgos y amenazas de orden económico, ambiental, de identidad étnica, cultural, de identificación, ejercicio político y de derechos humanos, con lo cual la seguridad sufre una expansión que no se sabría en donde parar, retornándose al problema de la militarización de la seguridad, característica de épocas pasadas.

Tomando en consideración todos estos condicionantes del escenario de la seguridad en el hemisferio, la Cumbre de las Américas de Santiago, en el año 1998, encomendó a la OEA, un análisis sobre el significado, alcance y proyección de los nuevos conceptos de seguridad, con el propósito de desarrollar enfoques comunes y revitalizar las instituciones del sistema interamericano.

La Declaración sobre Seguridad de las Américas, OEA - 2003, establece que la nueva concepción de la seguridad en el hemisferio es de alcance multidimensional, e incluye las amenazas tradicionales y las nuevas amenazas, preocupaciones, y otros desafíos a la seguridad de los Estados del hemisferio.

La cobertura e instrumentación de los diferentes mecanismos y medidas para afrontar en forma especial a las nuevas amenazas, denominadas no tradicionales, advierten claramente que cada Estado tiene el derecho soberano de identificar sus prioridades nacionales de seguridad y definir estrategias, planes y acciones para hacer frente a las amenazas a su seguridad, conforme a su ordenamiento jurídico y con respeto al derecho intencional.

La OEA, consciente de la problemática y para una mejor comprensión y por supuesto adopción de políticas de seguridad que sean diferenciadas y acordes con las amenazas que existan en los escenarios de seguridad de los países, logró la celebración de un Compromiso por la Seguridad Publica de las Américas, en octubre del 2008, con la participación de los ministros

del Interior, o Gobierno, bajo cuya responsabilidad se encuentra la administración y gestión de la seguridad pública de sus respectivos países.

Para dar una mayor profundización y mejor cooperación contra la delincuencia organizada transnacional en cumplimiento de la VI Cumbre de las Américas 2012, en la OEA se firma el Compromiso de Chapultepec, mediante la cual se establecieron un Esquema Hemisférico de cooperación contra la delincuencia organizada transnacional, con el propósito de coordinar esfuerzos y acciones.

Se establecen dos mecanismos de cooperación con un pilar operativo del esquema que funciona en el Centro de Coordinador de las Américas CCA, creado en México y uno político técnico a cargo de la OEA, con la finalidad de crear una Comisión Interamericana contra la delincuencia organizada transnacional. Las capacidades a ser incrementadas tienen que ver con el intercambio de información, la elaboración de productos estratégicos, y la incorporación de redes internacionales para intercambio de información, tecnificación en investigación y persecución penal.

Arquitectura de la seguridad hemisférica

El SSH, Sistema Seguridad Hemisférico, ha sabido mantenerse a tono con el pensamiento político y de seguridad que se ha ido evolucionando en el mundo, en coherencia con lo cual se ha ido modificando las estructuras; sin embargo, a pesar de ser el hemisferio un pionero en los propósitos de la integración regional y de la seguridad regional, sufre altibajos cíclicos, debido al fundamento neorrealista y la impregnación ideológica que ha acompañado al proceso de decisiones en la política exterior de los países.

El antagonismo ideológico Este-Oeste de la Guerra Fría, la infiltración antiimperialista derivada de la teoría Centro Periferia y el retorno a la confrontación Norte - Sur con el desarrollo de modelos socioeconómicos neo populistas, se han mantenido con diferentes fisonomías en la política internacional del hemisferio, dejando siempre incompletos los procesos de integración.

Una de las debilidades del SSH, radica en que no obstante ser la región una de las más estables y pacificas del mundo, muchas veces no se puede mantener una comunidad en la que sus miembros, para evitar pelearse entre sí, saben colocar sus disputas en otra vía. Esporádicamente se retoman diferendos ideológicos, económicos o territoriales para reavivar tensiones entre los países.

No siempre se escucha decir, por ejemplo, lo que dijo el presidente Piñera acerca del diferendo territorial, “Dejemos a la Haya lo que es de la Haya”.

Organizaciones subregionales

La compatibilidad que existe entre el SSH y las organizaciones subregionales, abre oportunidades y mecanismos de apoyo desde las subregiones, para en forma más específica, tratar los problemas y elaborar planes de acción para la solución de problemas de seguridad. Temas como las operaciones de paz, de la MINUSTAH en Haití, es un buen ejemplo en el que aportan varios países en coordinación con la ONU.

Junto con la OEA participan en el Régimen Interamericano de Seguridad, organizaciones subregionales y otros instrumentos y mecanismos que de manera formal contribuyen a la estabilidad, a la democracia y a la seguridad.

En este gran conjunto de mecanismos del régimen interamericano, se encuentran cumbres, reuniones extraordinarias, tratados, convenciones, comisiones, conferencias, declaraciones, compromisos, acuerdos. Para citar algunos tenemos:

- Cumbres de las Américas,
- Cumbres extraordinaria del Sistema de Integración de Centroamérica SICA
- Tratado Marco de Seguridad Democrática en Centroamérica
- Convenciones Interamericana como CICAD; CICTE; CIFTA
- Reuniones Extraordinarias de Seguridad de Centro América
- Compromisos como el de Lima, de la Seguridad Publica de las Américas
- Acuerdo Marco como el de Seguridad Regional entre los Estados parte del MERCOSUR
- Declaración de Santiago, San salvador, Costa Rica, Quito
- Conferencia de Ministros de defensa de la Américas
- Declaraciones Conjuntas de países de ministros de Defensa de los Países Bolivarianos

De las organizaciones subregionales del hemisferio, cinco están directamente comprometidas con la preservación de la seguridad. Pese a que han nacido casi todas ellas de un acuerdo de comercio, pronto vieron la conexión e importancia de involucrar a los países de su organización en el debate y toma de acuerdos, resoluciones o decisiones según sus protocolos para coparticipar en la solución de problemas de la seguridad subregional.

Una de las organizaciones más antiguas y efectivas para lograr la integración, acuerdos y planes de seguridad subregional ha sido el Sistema de Integración de Centro América SICA, 1991, con su tratado marco de seguridad democrática en Centroamericana, 1995, con frecuentes cumbres y comisiones que han efectivizado planes para atención y cooperación en desastres y en el control de las nuevas amenazas a la seguridad. Solo basta considerar la integración de los siete países centroamericanos con cuatro europeos, Reino Unido, Francia, Holanda, España y Canadá, para implementar el Plan Martillo y realizar operaciones militares aeronavales de interdicción para controlar las rutas de comunicaciones y comercio marítimas del Caribe y combatir el narcotráfico y el crimen organizado transnacional.

El MERCOSUR, es otro de los ejemplos de organización subregional que ha realizado gran aporte a la estabilidad, la democracia y cooperación regional. Este organismo ha logrado la determinación de Zona de Paz Regional, ha implementado acuerdos bilaterales, trilaterales, entre Argentina y Uruguay; Argentina, Brasil y Chile, pero especialmente los acuerdos de control y desarrollo nuclear entre Argentina y Brasil.

En esta consideración la Política de Defensa de los Estados Unidos, reconoce que en el hemisferio hay una transformación admirable en la defensa regional a partir de alianzas bilaterales, subregionales y multilaterales, con capacidades crecientes para convertirse en exportadores de seguridad, ayudar a vecinos y desarrollar operaciones multinacionales, en cooperación de la defensa en el hemisferio.

El Grupo Contadora, una de las organizaciones con gran prestigio y efectividad para alcanzar la paz de Centroamérica, se transformó en el Grupo de Rio, dándose continuidad a la representatividad de los países sudamericanos proyectó en el 2010 a la creación de la Comunidad de Estados Latinoamericanos y del Caribe CELAC, un proyecto subregional en ciernes.

La UNASUR, sin embargo, nacida como comunidad, es la que demuestra gran actividad y capacidad de integración, con el propósito de "Crear un espacio de integración y unión, cultural, social, económica entre los pueblos, dando prioridad al dialogo, con la finalidad de eliminarla

desigualdad, lograr la inclusión social y participación ciudadana y fortalecer la democracia, reduciendo las asimetrías y fortaleciendo la soberanía e independencia de los Estados".

En este caso, y prácticamente en todos los relacionados con los complejos de seguridad, es probable que el criterio (Buzan 1992:185-186), de que es muy difícil la estructura y funcionamiento de un complejo de seguridad, se deba a la presencia de los Estados Unidos, a la sobre cobertura de la OEA y a la falta de interacción de los países. Antes bien, la experiencia indica que las diferentes organizaciones creadas siempre parten de propósitos comunes, apenas con variaciones en ciertos enfoques pero que convergen en el interés social regional.

Lo más apropiado sería pensar que el factor ideológico de confrontación no ha dejado de ser un elemento disociador en la conformación de los complejos de seguridad.

En conclusión, la compatibilidad puede y debe mejorar con la institucionalidad intergubernamental, no solamente al interior de las organizaciones regionales de seguridad cuando se tengan las reuniones de concertación, sino después, cuando se tengan que implementar las decisiones a las que se han llegado. Eso significa que la gestión política es la parte más difícil.

Finalmente, la multiplicidad de organizaciones, mecanismos e instrumentos que conforman el Régimen de Seguridad Interamericano, da la imagen de una saturación y neutralización de acción debido al "entrecruzamiento" de instrumentos que entorpecen el accionar y causan confusión.

Más practico, inmediato y efectivo, según Jay Cope , es buscar oportunidades de coparticipación política e interinstitucional, para trabajar en conjunto, fortalecer las medidas de confianza entre los países, promover el cumplimiento efectivo de los compromisos internacionales, antes que seguir incrementando otros nuevos.

Los dos sistemas, tanto el Sistema Interamericano de defensa SID, como la Organización de Estados Americanos OEA, se basan en los mismos compromisos fundacionales desde 1945, sin dejar de seguir creando mecanismos en el régimen internacional, con finalidades similares y sin resultados efectivos.

Cada uno de los sistemas se encuadran en teorías diferentes; por una parte el SID refleja los fundamentos del estructuralismo, desde el momento en que concibe a la defensa y posteriormente a la seguridad como un proceso de construcción en el que los diversos componentes del sistema deben interactuar, generándose un problema entre los agentes; es decir, entre los representantes institucionales y la estructura conformada.

Para Alexander Wendt , el problema entre el agente y la estructura se basa en que el ser humano y su naturaleza tienen un propósito y sus acciones ayudan a transformar la sociedad y las estructuras en las que se desenvuelven; por lo tanto, esas interacciones de los agentes y afanes de poder, conllevan a propósitos que se reflejan en las estructuras o entidades creadas, tratando de lograr éxitos por si mismos al margen del funcionamiento sistémico.

La OEA, por su parte tiene una inclinación funcionalista, es decir, se encuentra desde su formación en el utilitarismo, con intereses comunes compartidos que le llevan a formar un sistema integral que atiende a las preferencias del sistema y no las de los líderes políticos En este sentido, el SID tiene una fundamentación teórica que se esfuerza permanentemente por ser incorporado en la OEA, y luego de haberlo logrado, busca una participación efectiva, no admitida ni reconocida.

El narcotráfico por ejemplo es un problema transnacional que atenta a los valores, la justicia, las instituciones, la salud, la moral, la educación, la economía, el ambiente y a la prosperidad. La gobernanza de la seguridad por lo tanto debe ser la nueva estrategia para hacer de la seguridad un bien público internacional de la región; empero, para esta amenaza cada institución tiene una responsabilidad y cada una debe hacer lo suyo; es decir, obedecer a su naturaleza específica, sin desviar el objetivo común de seguridad.

Referencias:

Haftentorn, H, (2006). Comming of Age Foreign Policy Since 1945, Rowman & Littefield Publ. Maryland, 2006, pp.98

Palma, H, (2007). Seguridad Alcances y desafíos, Ed. CEPEI

Taylor, P, (s.f). Geografía Política, Economía -Mundo, Estado- Nación y localidad, Colin Flint, segunda edición, Ed. Trama Editorial, Quito

Junta Interamericana de Defensa, Reseña Histórica, Washington D.C

Cope, J, (2007). Partners of Choice, A Regional Security Conundrum, Senior research Strategic Fellow INSS, Western Hemipheric Security, Colloqium

Wendt, A, (1987). The Agent Structure problem: in International relations Theory, Mit Press

Revista Caretas, "Seco y cargado", diciembre de 2010

America´s strategy in world Politics, Spikman 1942, El geopolítico Nicholas Spikman, José Luis Fiori, La onda digital, http://www.laondadigital.com/laonda/laonda/301-400/368/b1.htm

Carta de los Estados Americanos y protocolos de reformas http://www.oas.org/dil/esp/tratados_A41_Carta_de_la_Organizacion_de_los_Estados_Americanos.htm

LOS CERTs COMO HERRAMIENTA DE APOYO A LA CIBERDEFENSA EN LAS FUERZAS ARMADAS

Juan Carlos Polo González
Academia de Guerra del Ejército ecuatoriano

Resumen

El presente trabajo busca establecer una orientación en el manejo de la seguridad informática y su relación directa con la ciberdefensa, a través del desarrollo de una estrategia que facilite la detección, prevención, mitigación y eliminación de ataques informáticos, los mismos que son considerados como principales amenazas de una organización. Para esto, se analiza las diferentes formas en las que puede aparecer y desarrollarse un delito informático y el ámbito en el que se desenvuelve las normas ISO 27000, las mismas que pueden ser administradas en forma eficiente con la implementación de un centro de respuesta inmediata de seguridad informática, propuesta que ya es visualizada en este caso por parte del Comando Conjunto de las Fuerzas Armadas ecuatorianas para controlar esta amenaza.

En la actualidad, el problema radica principalmente en la falta de capacidad de respuesta que tienen las organizaciones contra eventuales ataques informáticos, los mismos que vulneran los protocolos de seguridad y las estrategias de prevención y control. Países europeos considerados a la vanguardia en este campo, ya han considerado entre sus prioridades la preparación de estas políticas.

Una estrategia para solucionar estos eventos es la incorporación de un centro de respuesta a incidentes informáticos inmediatos (COMPUTER EMERGENCY RESPONSE TEAM, CERT), el mismo que debe tener la capacidad de evaluar, coordinar y promover el desarrollo de servicios de prevención ante amenazas informáticas, las mismas que pueden presentarse en toda la infraestructura de una organización. Tomando como premisa fundamental que el personal que trabaje en esta organización debe contar con la capacitación y el entrenamiento especializado y que sus actividades deben orientarse a reaccionar en forma inmediata ante un evento de estas características.

Palabras clave: Ciberseguridad, ciberdefensa, Certs, seguridad informática, doctrina de seguridad

Desarrollo

El hombre nace como un individuo solo, pero su naturaleza de supervivencia lo encamina a agruparse, conformar un grupo para defenderse de los riesgos y peligros que se encuentran en su entorno. Así nacen las organizaciones estatales que permiten a base de un tributo, asegurar la estabilidad emocional y física de sus miembros. Con el advenimiento y desarrollo tan avanzado de la tecnología y los medios electrónicos se puede determinar que no todas las amenazas, en este caso informáticas, son físicas. El uso de la violencia no siempre termina en ataques físicos o en un conflicto. Hoy en día las guerras son asimétricas con acciones en varios campos como el político, económico, psicológico, electromagnético o cibernético.

En este caso puntual, el Estado como ente regulador, es el responsable de la seguridad nacional y para ello dispone de organismos e instituciones estatales, las mismas que deben enfocar sus misiones para asegurar, dominar y controlar sus campos de acción. Este carácter multidimensional debe alinearse con una doctrina de seguridad, doctrina que debe ser flexible en

sus organizaciones y que se adapte a los nuevos fenómenos que surgen como posibles factores de riesgo, amenazas y oportunidades.

Para ir a la par del entorno geopolítico regional, es necesario mejorar los procesos de seguridad informática organizacional. En la actualidad, con los nuevos escenarios planteados, se debe considerar que los ataques no solo provienen de otro Estado, sino de las nuevas amenazas tales como: narcotráfico, crimen organizado, terrorismo, ataques de piratas informáticos, grupos humanos opuestos a un determinado régimen, los desastres naturales, entre otros. Específicamente en las Tecnologías de Información y Comunicaciones, TICs., las amenazas principales son el espionaje, ataques dirigidos, ransomware, la ingeniería social, los crackers, el ciberterrorismo, entre otros.

Bajo este concepto se debe considerar a los ataques informáticos con una amenaza, no solo a los organismos estatales de seguridad sino a todas las organizaciones públicas y privadas en general, organismos que deben manejarse bajo un marco doctrinario que abarque la ciberdefensa y ciberseguridad. Para ello, se debe diferenciar estos dos conceptos que van de la mano y que engloban características similares, pero que no son iguales, y es necesario que todos los actores involucrados en estos sectores de la sociedad asuman la importancia estratégica del ciberespacio, así como de su uso seguro y responsable. En la actualidad, los organismos estatales de seguridad, algunos organismos públicos y algunas organizaciones privadas están llevando campañas de concienciación, especialmente dirigidas a estudiantes.

La tendencia del uso de la tecnología en nuestros días ha evolucionado el medio en el que se desenvuelve la sociedad. Directa o indirectamente, el ser humano necesita y hace uso de estas herramientas en su diario vivir. Cada día son más los incidentes relacionados a la violación de las seguridades informáticas. Todo esto, lleva a una desestabilización, vulnerabilidad y compromiso de la seguridad de una red de computadoras utilizando varios métodos y con distintos objetivos.

En el campo de la ciberseguridad, existen varios acontecimientos que podemos tomar en consideración a nivel internacional y nacional, tales como, el ataque a la página oficial de entidades públicas y privadas como Sony, Honda, Paypal, Fondo Monetario Internacional u otros delitos como: fallos de seguridad a servidores web, intrusión a copias de seguridad en la web, denegación de servicio, robo de datos, publicación dolosa de información estrictamente personal o los actuales ataques a dispositivos móviles. En base a los expertos en seguridad, la mayoría desarrolladores de antivirus, protocolos de seguridad o herramientas que ayudan a la seguridad, estos delitos siguen un mismo patrón de actividad: acceder al sistema explotando una vulnerabilidad y depositar una carga dañina de software maliciosa con un determinado fin.

La ciberdefensa y la ciberseguridad, son dos conceptos íntimamente ligados y abarcan procesos similares que los identifican en su naturaleza. Para comprender de una mejor manera esta relación, primero se debe entender los conceptos de amenaza, ciberespacio, ciberconflicto y ciberataque, para evitar futuras confusiones. La amenaza es la percepción de la capacidad que un potencial adversario posee para infringir un daño o perjuicio, el ciberespacio es el ámbito artificial creado por medios informáticos (RAE), el mismo que no tiene fronteras, el ciberconflicto es la confrontación entre dos partes utilizando la tecnología, y el ciberataque es un ataque desarrollado en el ciberespacio.

Ahora bien, Ciberseguridad es el conjunto de herramientas, procesos, directrices y métodos para proteger a los activos y usuarios de una organización, de un ataque malicioso ejecutado en el ciberespacio. La Ciberseguridad surge como un componente que garantiza el cumplimiento de las propiedades de seguridad de los recursos de una organización (UIT, 2012). La definición de Ciberdefensa comprende la aplicación de todas las acciones y medidas para proteger la

infraestructura de los sistemas de información y comunicaciones frente a los ciberataques y garantizar la Ciberseguridad (NATO, 2013). Una vez que se encuentran claros estos conceptos, es importante evaluar el grado de incidencia que tiene la afectación a la infraestructura crítica respecto a las Tecnologías de Información y Comunicaciones (TICs). Para conocer sus vulnerabilidades y por lo tanto para preparar una estrategia defensiva, tomando en consideración que mientras más la infraestructura critica se acerca al entorno remoto y administración por la vía de redes informáticas a través de redes LAN, MAN o WAN con accesos el internet, más será la vulnerabilidad a un ataque, sin que esto se considere una premisa, porque bien conocido es que también se puede sufrir un ataque al software y hardware, antes de que se conecte a la gran red o a un sistema en explotación.

Uno de los problemas más importantes que se debe plantear, es la implantación de procesos de seguridad informática, amparados en las ISO 27001/27002 (OSI) que son las normas de seguridad de la información desarrolladas por la Organización Internacional para la Estandarización como una guía de buenas prácticas, a fin de precautelar la información que se encuentra considerada como uno de los activos intangibles más importantes de una organización. La información obedece a cuatro principios fundamentales que son: confidencialidad, integridad (no repudio) disponibilidad y autenticidad, todo ello conocido como transabilidad. La seguridad informática puede clasificar su acción en medidas físicas y lógicas, las mismas que permiten evitar un daño producido por un ataque informático caracterizado por el deseo principal de robo de información. Los ataques informáticos pueden ser producto del conocimiento de hackers, cracker u otras dimensiones de piratas informáticos como los ataque de la ingeniería social entre otros, los mismo que pueden atacar a las diferentes capas del ciberespacio: física de infraestructura, lógica de hardware y cognitiva de percepción social (Ventre, 2012).

Existen muchos motivos por los cuales se cometen ataques informáticos, tales como el factor económico, político, protesta, ciberterrorismo. Los delitos informáticos a considerar deben estar enfocados no solo a robo de contraseñas o ingreso a perfiles de redes sociales. Debe ir más allá.

El desarrollo de los virus informáticos son cada vez más complejos, códigos de software maligno para realizar procesos como vaciar cuentas bancarias, el reciente ataque utilizando el ransomware dirigido contra copias de seguridad en la nube o explotar alguna vulnerabilidad en la infraestructura informática, narcotráfico, tráfico de armas, sistema de apuestas ilegales, stack pivoting y return and jump, nuevas técnicas de evasión de mecanismos de cuarentena sandboxing, envio masivo de correo no deseado spam, suplantación de los reminentes de mensajes con la técnica sppofing, uso de troyanos, uso de archivos Bot del Irc para el control remoto de sistemas y sustracción de información, ataque de fuerza bruta, de interposición man in the middle, ataques de waterring hole, botnet, secuestro de dominio, sidejacking o secuestro de sesiones, sniffer, sniffing, ciberbullying o grooming. Todos estos ataques se encuentran camuflados en software que circula en la red, ataques criminales que, desde el mundo virtual, están encaminados a destruir la infraestructura financiera y hasta económica de un país.

Un ejemplo de ello es el ataque mediático de ANONYMUS, el ataque de LULZSEC, o el ataque Dragonfly, una amenaza avanzada dirigida especialmente contra sistemas de control industrial en el sector energético en Europa, el robo de información personal en Orange – Francia, en el cual el incidente de seguridad permitió acceder a información de un millón trescientos mil clientes en el que se incluía nombres, apellidos, direcciones de correo electrónico, números de teléfono móviles y fijos, así como fechas de nacimiento. Los atacantes tienen un gran nivel de control y un amplio rango de recursos, además tienen la ventaja de decidir la naturaleza de la amenaza, como y cuando se va a realizar el ataque, empleando un sinnúmero de herramientas

disponibles en la red, las mismas que incluyen servicios legítimos. Independientemente del origen y naturaleza de la amenaza, la Ciberdefensa de una nación debe construirse sobre un conjunto de capacidades que le permitan alcanzar un estado de riesgo conocido y controlado.

Todos estos ataques sufridos en varios campos, ponen en alerta y revelan la necesidad de contar con protocolos de seguridad a fin de evitar estos actos ilegales. Una de las suposiciones más peligrosas que puede tener una organización, es que tienen conocimiento de cómo un atacante puede llegar a afectar la red. Por otro lado, se debe tomar en cuenta que la brecha digital se ha disminuido en los últimos años, tomando en consideración que la política estatal es brindar a la población servicios de internet más robustos y a un mayor número de individuos. La empresa privada ofrece mejores planes de acceso a internet: El 90% del tráfico internacional en Ecuador se realiza mediante dos cables de fibra óptica; en ambos casos, Ecuador solicitó "la entrega de una determinada capacidad internacional con acceso a la Internet, para uso de desarrollo social y educativo en la estación terminal de cable submarino" a ser administrada por el Fondo de Desarrollo de las Telecomunicaciones (FODETEL). Este recurso llega al 67% de los cantones del territorio nacional. El número de hogares conectados a Internet de banda ancha en 2013 es 891.000 (7.7%), el porcentaje conectado a la Internet de alta velocidad es 0.89%" (DELGADO, 2014). Según el Censo poblacional del 2010 el 33% de pequeños, el 46% de adolescentes y el 41% de jóvenes afirma tener un computadora, el 14% de los niños entre 6 y 9 años se declara internauta, mayores a 10 y menores de 18 años se declara usuario de internet (INEN, 2010).

La serie ISO 27000 aglomera todas las normativas en materia de seguridad de la información. Lo más importante de esta familia son las normas ISO 27001 e ISO 27002. La última de estas, antes conocida como ISO 17799 (modificó su nombre en el año 2007), y basada en la norma británica BS 7799, es un código de buenas prácticas para la realización de un Sistema de Gestión de Seguridad de la Información (SGSI). Está dividida en once dominios (por ejemplo, Seguridad física y del entorno o Control de accesos), y en cada uno de ellos se destacan cuáles son las mejores prácticas o los controles recomendados para dar seguridad en la organización. Esta norma no es certificable, para ello, está la norma ISO 27001, que es la que las organizaciones deben certificar. La misma contiene los requisitos que debe cumplir una organización, para estar acorde a las buenas prácticas enlistadas en las otras normas de la familia (especialmente la 27002).

Publicada en octubre 2005, hoy es la certificación en seguridad más popular y es aplicada por empresas de todo tipo en todo el mundo. Por último, la ISO 27001 también extiende, respecto a la importancia de "concientizar a los usuarios acerca de los peligros del software no autorizado o malicioso […] En particular, es esencial que se tomen precauciones para detectar y prevenir virus informáticos en computadoras personales" (BORTNIK, 2010).

Del mismo modo, y en relación con la defensa, las Fuerzas Armadas dependen de las Tecnologías de Información y Comunicaciones para comunicarse, ejercer el mando y control de las operaciones, obtener y distribuir información e inteligencia, realizar labores de vigilancia, reconocimiento o adquisición de objetivos o coordinar los fuegos. Todas estas tareas, como parte de la misión fundamental de la institución armada que es la defensa de la soberanía y la integridad territorial. En cada una de estas actividades, las TICs actúan como elemento multiplicador de la fuerza y optimizan la concepción, planificación y ejecución de las operaciones, pudiendo condicionar el desarrollo y resultado de una contienda. Por lo tanto, la posesión de una infraestructura tecnológica robusta, segura y resiliente, la sistematización de las dimensiones que componen el ciberespacio y su integración en la planificación operativa o la capacidad para actuar en este dominio, son algunos de los asuntos que más atención están recibiendo desde las Fuerzas Armadas (THIBER).

En el ámbito de operaciones militares, se debe tomar en cuenta los ataques informáticos especialmente en el componente del campo de batalla de mando y control y considerarlos como una amenaza a la libertad de acción. La pérdida de ella, en la conducción de las operaciones militares, es considerada como negativa para la operación. El Ministerio de Defensa Nacional indicó que considera al espacio cibernético como "vital" para la seguridad del Estado y sus ciudadanos, por lo que anunció el desarrollo de capacidades operativas pertinentes y políticas específicas (NACIONAL, 2014), es por ello que desde el año 2014, con el anuncio de la creación de un Comando de Ciberdefensa por parte del Ministerio de Defensa Nacional, a través del Comando Conjunto de las Fuerzas Armadas. Entidad que se dedicaría principalmente a la protección de infraestructura crítica para las operaciones del Estado. Con una inversión de 8 millones de dólares, se desea liderar el concepto de Ciberseguridad en esta institución militar y llegar a ser una organización a la vanguardia de la seguridad informática en Ecuador, ya que un ataque a la infraestructura informática en Fuerzas Armadas puede causar un impacto bastante fuerte en la seguridad integral del país o la intervención remota y maliciosa en la infraestructura de servicios básicos de un país como el caso de luz eléctrica o agua potable.

Existe varias estrategias de ciberseguridad y/o ciberdefensa, para determinar las tendencias y características más relevantes en base a: detección de activación maliciosa, detección mitigación y terminación de ataques, análisis dinámico de riesgos, ataque y daños, recuperación de ciberataque, toma de decisiones a tiempo, gestión de la información de Ciberdefensa o técnicas como pruebas de penetración, medidas de sensibilización y educación (España, 2012).

Planificar, desarrollar y establecer un centro de respuesta a incidentes informáticos, es otra respuesta que está tomada en cuenta por los países más desarrollados y que cuentan con los recursos necesarios. Estos centros conocidos como CERT (Computer Emergency Response Team) o CSIRT (Computer Security Incedent Response Team) por sus siglas en Ingles. Esta iniciativa ya ha sido tomada por países vecinos, en la región trece países cuentan con Equipos de Respuesta a Incidentes de Seguridad Cibernética (CSIRT).

Los ataques informáticos en los últimos tiempos, han demostrado que todavía no se tiene una infraestructura adecuada para prevenirlos, y se evidencia la incapacidad de las organizaciones para enfrentar este tipo de amenazas, lo que ha obligado a considerar la importancia de la ciberdefensa en el entorno público y privado. Inicialmente, un CERT puede ser destinado para proporcionar servicio de respuesta inmediata a incidentes a nivel de la infraestructura informática critica clasificada en: software, hardware, base de datos, sistemas, redes internet, y posteriormente elaborar proyectos de investigación, innovación y transferencia tecnológica relacionados a temas de respuesta a incidentes y delitos informáticos.

Entre los procesos agregados de valor de un CERT se puede considerar: detección o identificación de la amenaza, bloquearla, monitorearla, reportarla, guardar registros y evidencias de la amenaza, responderla, pedir información a los organismos o actores involucrados, hacer uso de la infraestructura, comunicación transversal y horizontal con otros centros de apoyo.

El CERT debe estar en condiciones de identificar inconvenientes fundamentales, por ejemplo que las instituciones públicas y privadas no han coordinado sus políticas de manejo de información frente a la impunidad que existe actualmente en los delitos informáticos, a pesar que la normativa ya tiene implementado una serie de recursos legales. Otro de los objetivos de estos centros es el fortalecimiento de las capacidades técnicas y operativas de las instituciones gubernamentales para afrontar las amenazas y ataques cibernéticos, monitoreando la infraestructura critica, minimizando los riesgos vinculados a la información crítica de un Estado, reforzar la protección de los sistemas informáticos de las Fuerzas Armadas y Policía Nacional, reaccionar adecuadamente

ante los ataques cibernéticos que atenten contra la seguridad de una organización. Además, se debe coordinar con la Policía Judicial a fin de realizar programas de prevención, atención, investigación y apoyo a la judicialización de los delitos.

En resumen, un CERT tiene objetivos específicos enmarcados en cuatro grandes áreas que son: la autoridad, el escalamiento, la coordinación y la capacitación, todos ellos afianzan una sociedad de información segura. En base a los estándares internacionales, las mejores prácticas, la administración física y técnica de la seguridad y la personalización se puede establecer dos vías de manejo de la información; primera, la conveniencia que tiene la demanda; y, la segunda, la confianza en la entrega de la misma. Los objetivos que se desprenden son: la coordinación con los organismos estatales para la promoción de políticas, procedimientos, recomendaciones, protocolos y guías de seguridad informática y velar por su implementación, promover el desarrollo de nuevos centros en todos los niveles del Estado, ya sea público o privado, ofrecer servicios de información y prevención de amenazas informáticas y su respectiva respuesta a los incidente, coordinar en la formación de talento humano especializado en el campo de la seguridad que tiene relación con estas tecnologías, apoyar a otros organismos estatales de seguridad integral, fomentar un sistema de gestión del conocimiento, proveer al Estado la inteligencia necesaria para mitigar estos delitos tomando en consideración que el análisis necesario para identificar un atacante puede llevar meses de estudio, con la utilización de recursos informáticos y el respectivo personal capacitado.

Conclusiones

La tecnología avanza con mayor rapidez y con ello las amenazas informáticas a través del cometimiento ilícito de actos cibernéticos, especialmente ligados al manejo de información. Las principales amenazas están relacionadas con el narcotráfico, crimen organizado, fraude al fisco, fraudes económicos, resentimiento político, robo de información organizacional. Todos y cada uno de ellos, aprovechándose de las vulnerabilidades de la infraestructura informática de las organizaciones o de la ingeniería social en la parte humana de este campo, sin contar que los usuarios cada día comprometen más su privacidad, al no tener un adecuado manejo de contraseñas.

Los estados, como vigilantes de la seguridad integral, han adoptado mecanismos y herramientas para protegerse de estos ataques, y entre las principales estrategias es la creación de centros de atención a ataques informáticos con una respuesta inmediata en su accionar a través del uso de las tecnologías de visualización y análisis de datos, manejo de planes de contingencia y el aumento de alianzas corporativas entre la industria de la seguridad y los gobiernos.

En el Ecuador ya se han realizado algunos proyectos pilotos sobre este tema, y es el Ministerio de Defensa, a través del Comando Conjunto, quien quiere liderar el campo de la seguridad informática con la creación de un Comando de Ciberdefensa, el mismo que se encargará de protocolizar todas las actividades encaminadas a asegurar los procesos informáticos relacionados con la Información.

Referencias:

Bortnik, S, (2010). La serie de las normas ISO 27000. Obtenido de Seguridad Corporativa

CICTE-OEA, (2011). CERTS en América Latina

Delgado, J. A, (2014). Gobernanza de Internet en Ecuador: Infraestructura y acceso. Artículo presentadohttp. Quito.

España, M. d, (2012). El ciberespacio, nuevo escenario de confrontación. Imprenta del Ministerio de Defensa.
INEN, (2010). Censo poblacional
NACIONAL, M. D, (2014). Agenda Política de la Defensa. Quito
NATO, (2013). MC0571.
OSI, (s.f.). Organización Internacional de Estandarización.
RAE, R. A, (s.f.). Diccionario de la RAE.
Thiber, T. C, (s.f.). Instituto de Ciencias Forenses y de la Seguridad de la Universidad Autónoma de Madrid.
UIT, (2012).
Ventre, D, (2012).

REFUGIADOS COLOMBIANOS EN EL ECUADOR

Hernán Moreano Urigüen
Universidad Internaciona del Ecuador - UIDE

Resumen:

El presente trabajo brinda un balance panorámico de la situación política que ha vivido Colombia desde inicios del presente siglo para dar solución a su conflicto interno, el cual se expresa desde hace varios años a través del narcotráfico y la presencia de la guerrilla y grupos paramilitares a lo largo de su territorio. Por tal motivo, es primordial analizar la reacción del Ecuador para atender fenómenos sociales como refugiados hacia el país debido a las estrategias ofensivas implementadas desde Bogotá. Se estudiará información proveniente de distintas fuentes institucionales, oficiales y de diversas entidades de la sociedad que trabajan directamente o indirectamente con las relaciones de Ecuador y Colombia frente a la ayuda a refugiados.

Palabras clave: Seguridad fronteriza, migración, guerrilla, violencia, relaciones binacionales

Inmigración de colombianos hacia el Ecuador

Para entrar en el contexto, es necesario resaltar otro de los temas que afecta a la política colombiana y evidencia cómo el repliegue del conflicto interno hacia las fronteras se está desbordando hacia el Ecuador: los desplazados y los refugiados. Hasta diciembre de 2010, el 98% de los 53.342 refugiados registrados en territorio ecuatoriano fueron colombianos, aunque se estima que el número de refugiados en el Ecuador se eleva en realidad a unas 135 mil personas.

El siguiente gráfico demuestra la evolución de ciudadanos desplazados por la guerra interna que se vive en Colombia. Actores armados ilegales (GIAC) con las guerrillas de las FARC y el Ejército de Liberación Nacional (ELN), las Bandas Criminales (Bacrim) compuestas por disidentes de las antiguas Autodefensas Unidas de Colombia (AUC), hoy narcotraficantes, son los causantes de centenares de familias de los departamentos internos y fronterizos colombianos huyan hacia el Ecuador.

Los años de mayor desplazamiento fueron 2008 y 2009 con tendencia a la baja en el 2010. Durante la administración del expresidente Álvaro Uribe Vélez se vivió una cruente guerra entre las fuerzas ofensivas del Estado, GIAC y Bacrim, con el fin de recuperar presencia pública. Desde la etapa del presidente Juan Manuel Santos (2010 hasta la actualidad) la intensidad de la guerra se ha reducido debido a los intentos de diálogos por la paz que se celebran en La Habana – Cuba.

Muchos inmigrantes colombianos cruzaron (y lo siguen haciendo) la frontera hacia el Ecuador con el fin de solicitar el carné de refugio al Estado a través de la Cancillería y la Oficina de Naciones Unidas para el Refugiado (ACNUR). Los procesos de selección son bien rigurosos, por eso es bastante más elevado el número de solicitudes, frente al número de personas a quienes se les concede la condición de refugio.

La ACNUR calcula que unas 1.500 personas entran mensualmente al país por la frontera norte (2013). Para algunos grupos defensores de los Derechos Humanos como Pro Refugio…

"…todos estos aspectos muestran la importancia que tiene el impulsar una coordinación interestatal consistente entre los dos países, que asuma los temas sensibles que los involucra y forje, además, objetivos comunes para diseñar una relación futura de respeto y cooperación siguiendo los parámetros que dictan el derecho internacional y la prudencia" .

Gráfico 1, Número de refugiados colombianos en el Ecuador, 1999-2013. Fuente: Dirección de Refugio, Ministerio de Relaciones Exteriores y Movilidad Humana del Ecuador

Ahora surge una pregunta, ¿qué hacen los ciudadanos colombianos una vez que obtienen el refugio por parte del Estado ecuatoriano?, ¿a qué se dedican?, ¿qué tan fácil es para ellos conseguir empleo, educación y salud? Para muchos organismos del Gobierno Nacional es un enigma. No hay registros oficiales sobre las labores que realizan, sean están legales o ilegales.

El siguiente gráfico muestra la cantidad de refugiados en los últimos seis años.

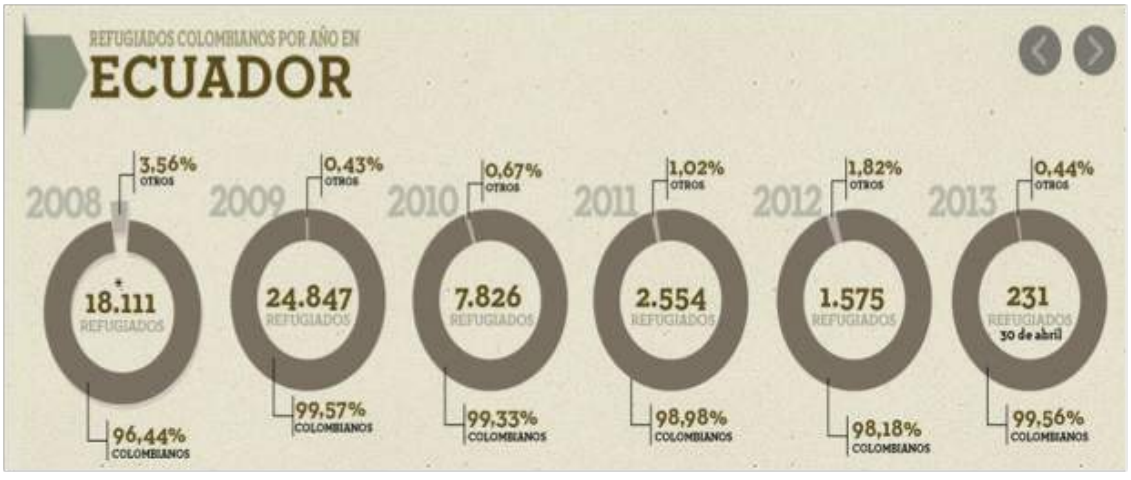

Gráfico 2, Refugiados colombianos por Año 2008-2013. Fuente: Dirección de Refugio, Ministerio de Relaciones Exteriores y Movilidad Humana del Ecuador, diario El Universo.

Cabe recalcar que para ACNUR, el refugiado es la persona que "sale de su país debido a que su vida corre peligro". A la vez, el Estado ecuatoriano considera que "las personas refugiadas tendrán en el territorio nacional los mismos derechos y deberes que las personas ecuatorianas de acuerdo a la Constitución de la República y la legislación pertinente".

Lo anterior implica que es obligación del Estado ecuatoriano brindar seguridad, atención médica y educativa al refugiado. Además, a través de fundaciones como el caso de "Pro-refugio" , se puede otorgar pequeños préstamos para la conformación de pequeñas empresas. Lastimosamente no existen datos estadísticos oficiales sobre el número de negocios establecidos por ciudadanos colombianos refugiados en el Ecuador.

La Cancillería ecuatoriana, en conjunto con el Instituto de Seguridad Social (IESS) y el Registro Civil , han construido una red de monitoreo de refugiados colombianos en el país. El siguiente gráfico muestra la ubicación geográfica de refugiados colombianos a lo largo y ancho del país.

Gráfico 3, Fuente: Dirección de Refugio, Ministerio de Relaciones Exteriores y Movilidad Humana del Ecuador, diario El Universo.

Tal como se evidencia en la imagen anterior, la provincia céntrica de Pichincha concentra la más alta cantidad de número de refugiados colombianos en el Ecuador (14.992), luego le sigue la provincia amazónica fronteriza de Sucumbíos (13.050), que limita con el departamento fronterizo de Putumayo, y en cuyas selvas operarían los frentes 38 y 42 de las FARC. En tercer lugar le sigue la también provincia fronteriza costera de Esmeraldas (6. 063) las cual colinda con el departamento colombiano de Nariño, donde operaría el frente 49 de las FARC y se concentraría el mayor número de hectáreas de hoja de coca de toda Colombia. Luego le siguen otras provincias céntricas, cuyos puntos de concentración serían los centros comerciales en ciudades principales, tal es el caso de Imbabura (3.166), Guayas (3.056), Azuay (2.217), Santo Domingo de los Tsachilas (2.006), entre otras.

Desde el punto de vista de la seguridad ciudadana, las varias cárceles del país se encuentran sobrepobladas, tal como lo demuestran algunos diarios del Ecuador. Preocupa la cantidad de ciudadanos extranjeros que han sido detenidos por riñas callejeras, microtráfico de drogas, crímenes, robo a mano armada, entre otras.

Hasta finales del año 2013 la cantidad de detenidos en las cárceles de las principales ciudades del país fue la siguiente:

Ciudad	# PPL
Guayaquil	331
Sucumbíos	243
Quito	196
Esmeraldas	150
Cuenca	20

Tabla 3, Personas Privadas de Libertad (PPL). Colombianos en el Ecuador. Fuente: diario El Comercio, enero 2014

A pesar de que las cifras no son muy altas, la mayoría de los detenidos responden por el delito de microtráfico de drogas y actos violentos en las calles y vecindarios de las grandes urbes.

Según ACNUR, en el Ecuador residían 26.167 refugiados colombianos hasta el año 2012. Mientras tanto, la Cancillería ecuatoriana considera que en todo el país residen aproximadamente unos 500.000 colombianos no registrados por las instituciones competentes. Muchos de ellos

huyeron de los efectos del Plan Colombia (2000-2007), como son los caso de violencia generada por paramilitares, guerrilleros y militares: paros armados, secuestros, fumigaciones y despojo de tierras por parte de grupos violentos. Se estima que el número de refugiados se elevaría ante un eventual fracaso de los diálogos de paz en La Habana y Oslo.

En caso de que las negociaciones se tornen a favor de un desarrollo agrario en Colombia, un sector podría regresar con el fin de recuperar sus tierras, mientras que otro permanecería para no afrontar los antecedentes del pasado judicial. Por otro lado, está la estrategia del Estado colombiano de empujar a la guerrilla y bandas criminales hacia las fronteras, lo que podría empeorar la situación de inseguridad en el lado ecuatoriano frente a actividades ilícitas como narcotráfico, robo de armas, minería clandestina, lavado de activos, secuestros, prostitución, entre otros. Las medidas planificadas por el Estado colombiano para reinsertar a la sociedad a los ex guerrilleros aún no están claras. De hecho, se proyecta que la composición social y del mercado de trabajo actualmente existente en Colombia, no estaría lista para enfrentar los retos que significa un proceso de paz exitoso.

Ante esta posibilidad, es necesario que el Estado ecuatoriano desarrolle una estrategia que prevenga la movilización de grupos delictivos desde Colombia hacia el Ecuador.

Conclusiones:

El proceso de negociaciones ha generado una polarización en las posiciones de los dos principales representantes políticos de Colombia: Santos y Uribe. Durante el mandato de Uribe, la guerra interna contra las FARC y demás grupos irregulares se intensificó, mientras que Santos dio un cambio radical al iniciar negociaciones con las FARC para establecer la paz.

En medio de este panorama han surgido acusaciones de parte de Uribe sobre los temas fundamentales que se estarían negociando en La Habana como "posibles acuerdos con las FARC que afectarían directamente al estamento militar colombiano y otras áreas vitales del Estado", lo cual ha sido desmentido totalmente por el presidente Santos.

Otro de los rumores que han afectado seriamente a la imagen del proceso de las negociaciones es el posible indulto o amnistía que se otorgaría a los miembros de las FARC, lo cual ha sido también desmentido por Santos, señalando que se procederá a aplicar la justicia transicional.

Cabe indicar que este punto es sumamente sensible ya que la sociedad en general, especialmente las víctimas de las actividades ilícitas de las FARC, reclaman que se haga justicia ante lo sucedido y tendría incidencia directa en el apoyo de parte de la sociedad al proceso de negociaciones.

Por otra parte, esta polarización que se origina desde los principales actores políticos influye también en la percepción de la población para brindar o no apoyo al proceso para lograr la paz. Los cuestionamientos sobre los resultados del proceso de las negociaciones generan desconfianza en la opinión pública sobre sus resultados.

Bibliografía:

Bonilla, A, Moreano, H, (2009). "La lucha contra el narcotráfico en el Ecuador, 1989-2009". En: La guerra contra las drogas en el mundo andino: hacia un cambio de paradigma, Juan Gabriel Tokatlian, (compilador), / 1a ed. Buenos Aires: Libros del Zorzal.

Chávez, N, (2007). "Cuando los Mundos Convergen". Tesis de Grado. Facultad Latinoamericana de Ciencias Sociales – FLACSO sede Ecuador. Quito.

Moreano, H, (2012). "Frontera, Pobreza y Vulnerabilidades". Consejo Latinoamericano de Ciencias Sociales – CLACSO. Programa Las Relaciones Internacionales de la Pobreza y el Caribe. Buenos Aires.

Moreano, H, (2010). "Entre Santos y Traquetos: el narcotráfico en la frontera colombo ecuatoriana". Revista Colombia Internacional. Universidad de los Andes. Enero a junio. Bogotá.

Rivera, F, Torres, F, (2011). "Ecuador ¿país de tránsito o país productor de drogas?" Programa de Cooperación en Seguridad Regional. Fundación Friedrich Ebert. Quito.

Rivera, F, (2007). Aspectos Sociodemográficos. "Migración forzada de colombianos. Colombia, Ecuador, Canadá". Corporación Región, UBC, FLACSO. Bogotá.

UNODC, (2012, 2013). Censo de Cultivos de Coca. Colombia

Vargas, A, (2014). "La paz vendrá una vez termine el conflicto armado". Ponencia presentada en el diario El Nuevo Día. 4 de junio. Tolima-Colombia.

Medios de Comunicación:

- Diario El Comercio www.elcomercio.com
- Diario Hoy www.hoy.com.ec
- Diario El Universo www.eluniverso.com
- Diario La Hora www.lahora.com.ec
- Radio Visión. www.radiovision.com.ec
- Revista Semana de Colombia www.semana.com

Páginas Oficiales:

- Departamento de Defensa de los Estados Unidos www.defense.gov
- Departamento de Estado de los Estados Unidos www.state.gov
- Ministerio de Defensa de Ecuador www.defensa.gob.ec
- Ministerio Coordinador de Seguridad del Ecuador www.nuestraseguridad.gob.ec
- Ministerio de Defensa de Colombia www.defensa.gov.co
- Ministerio del Interior del Ecuador www.mininsteriointerior.gob.ec
- Oficina del Alto Comisionado de Naciones Unidas para el Refugio www.acnur.org
- Oficina de Naciones Unidas para la Droga y el Delito www.unodc.org
- ONGs:
- Fundación Friedrich Ebert Ecuador www.fes.org.ec
- Fundación Friedrich Ebert Colombia www.fescol.org
- Fundación Ideas para la Paz en Colombia www.ideaspaz.org.co
- Critical Analysis www.plancolombia.com
- Universidad de Miami - Florida www.miami.edu
- Washington Office for Latin America www.wola.org

MANEJO RESPONSABLE DE LAS MUNICIONES Y EXPLOSIVOS, CONFIANZA, SEGURIDAD Y NOBLEZA

Ricardo Javier Acuña López
Ejército ecuatoriano

Las tragedias suscitadas el 20 de noviembre del año 2002 en la Brigada de Caballería Blindada N° 11 Galápagos, el 23 de marzo del año 2003 en la Base Naval de Guayaquil, han sido el punto de partida para emprender varios planes en la administración y custodia del material bélico en los repartos militares. Quienes son custodios del material deben poseer la habilidad, conocimiento y capacidad de almacenar las municiones y explosivos que la norma técnica lo revela para este tipo de material. Las normas INEN, MILITARY ESTÁNDAR, NORMAS NATO, son algunos de los procedimientos que se han puesto sobre la mesa para encontrar la fortaleza del manejo de municiones y explosivos, hoy considerados como peligrosos, para evitar y lamentar errores como los ya anunciados.

Los aportes para eliminar estas deficiencias se han venido dando por varios estamentos, uno de estos es la FABRICA DE MUNICIONES SANTA BARBARA (F.M.S.B.); que, bajo su proyecto de "Proceso de Certificación de la Munición", se realizó en varias fases:

- Limpieza de polvorines.- Retirar todo material considerado como basura, de tal manera que todo material inservible sea direccionado directamente a su destrucción.
- Ordenamiento.- Seguidamente realizar el ordenamiento de los polvorines de acuerdo a la norma técnica, lotes y compatibilidad de explosivo.

- Muestreo.- De cada lote de municiones, tomar una muestra representativa para que sea valorada y posteriormente certificada.
- Análisis de los componentes.- Las muestras fueron llevadas a los laboratorios donde - desarmados en sus componentes primarios - se sujetaron a varias pruebas química, físicas y dinámicas poniendo a prueba sus performances para certificar su uso, almacenamiento o su destrucción.
- Certificación.- Finalmente, luego de varias pruebas de campo y laboratorios, se certificó qué munición está apta a ser almacenada, enajenada, desmilitarizada o destruida.

Este proyecto llevado a cabo desde el año 2002, avanza en su fase final, el mismo que se encuentra en espera de recursos económicos para completar el mismo.

Al momento los polvorines del Ejército se encuentran almacenados de acuerdo a las normas y procedimientos establecidos (directivas e instructivos), sin descuidar las recomendaciones de la F.M.S.B. y descartar impases con gran tragedia como los ya vividos. Es así que muchos de estos conocimientos se encuentran ya en las mallas curriculares de los cadetes y personal de tropa del servicio de material de guerra, para realizar una excelente administración, manipulación y transporte de las municiones y explosivos.

Normas de seguridad aplicadas a los polvorines militares

Varias obras relatan las mejores opciones para minimizar los efectos destructivos de los artefactos militares. Las Normas INEN, las cuales son avaladas por la República del Ecuador, muestran algunas medidas de gran importancia tales como:

- El almacenamiento de explosivos se debe realizar en lugares seguros construidos específicamente para esta finalidad, denominados polvorines.
- Deberán estar ubicados, cumpliendo las distancias de seguridad con respecto a las áreas pobladas y rutas de tráfico públicas, con la finalidad de limitar los alcances y efectos de una eventual explosión.
- Deben estar separados por una distancia establecida entre polvorines, a fin de que la comunicación de la explosión del uno al otro no sea probable.
- Su ubicación depende de las características constructivas y el tipo de polvorín; además, por la cantidad y compatibilidad de municiones y explosivos que contengan.
- No se deberán construir polvorines en zonas que puedan verse afectadas por incendios forestales o inundaciones.
- El almacenamiento de municiones y explosivos dentro de un polvorín, se deberá realizar de acuerdo a la "clasificación por la peligrosidad y a los grupos de compatibilidad de almacenamiento".
- En un polvorín cubierto por tierra, la puerta será técnicamente débil para que la fuerza de la onda ocasione daños menores.
- Los polvorines estarán circundados en un radio mínimo de 25 metros por una malla o cerca de alambre de 2.20 metros de altura o mayor, con puerta y candado.
- Los explosivos y agentes de voladuras, almacenados dentro de los polvorines, deben apilarse de manera tal que faciliten la estabilidad, la revisión de las unidades de empaquetamiento y el retiro de los materiales más antiguos.
- Las cajas que contienen explosivos se deben mantener en pilas de almacenamiento de amplia base y poca altura (máximo 1,6m) y deben estar asentadas sobre estibas de madera, para evitar que estén en contacto directo con el piso.
- Las cajas deben estar separadas de la pared entre 5 y 10 cm. para protegerlas de posible humedad.
- ¡No se permite fumar!, portar ni manipular fósforos, encendedores, armas de fuego o municiones e instrumentos que puedan producir chispas o fuego. Tampoco se puede mantener depósitos de material combustible dentro de un área de 25 m. a la redonda de cualquier polvorín.

De esta manera se permite el trabajo profesional de cada uno de los custodios del material, incluso se debe tener las mismas consideraciones para su transporte; es decir, no descuidar su compatibilidad, utilización de vehículos adecuados para este propósito, evadir recintos poblados y mantener una cadena de evacuación de ser el caso (Plan de Contingencia). Para todo esto, el mando militar ha considerado la aplicación de todos estos procedimientos en el Manual Técnico MT-154-01 A-5.

Esto nos permitirá mantener un Ejército de gran confianza y nobleza para la sociedad, como lo ha sido hasta estos días, una labor en la cual se sintetice la operatividad de los combatientes y sus armas y por el trabajo profesional de sus miembros, tanto en el almacenamiento, manipulación, mantenimiento y transporte de las municiones y explosivos, desarrollando el aspecto cognitivo de nuestros repartos militares, custodios de este material y con la responsabilidad que caracteriza a cada uno de los miembros de la institución armada.

Referencias:

Revista Military Review - 1999
Albán, R, (s.f). Proyecto SICEM, FABRICA DE MUNICIONES SANTA BARBARA
YELLOW BOOK, (COMPATIBILIDAD)
http://www.fremap.es/BuenasPracticasPrevencion/Manuales/MAN.023.
Manual técnico de transporte de Municiones y Explosivos MT-154-01 A-5

EL CIBERESPACIO: EL NUEVO TEATRO DE GUERRA GLOBAL

Luis Recalde H.,
Universidad de las Fuerzas Armadas - ESPE

Resumen

Finalizada o controlada la tradicional guerra convencional, el mundo tiene un nuevo teatro de operaciones llamado ciberespacio. De allí se han desprendido diversos ataques que traspasaron las fronteras virtuales; así, la tecnología de vanguardia ha formulado el nuevo campo de batalla global, desarrollado por los nuevos sistemas cibernéticos.

Palabras clave: ciberespacio, fronteras virtuales, espacio tridimensional, ciberguerras

Introducción

El teatro de guerra es una zona del globo terráqueo relativamente extensa, compuesta por los espacios terrestres, marítimos y aéreos que están - o estarían - potencialmente implicados en operaciones de guerra. Bajo esta perspectiva, estaríamos hablando de una determinada zona geográfica "tangible" de la tierra compuesta por los dominios tridimensionales de las operaciones militares convencionales, y que puede estar involucrada en una acción bélica determinada.

Hace algunos siglos, cuando se comenzaron a estudiar las guerras, generalmente se analizaban las formas de enfrentamientos básicos, por ejemplo la falange griega o la romana, éstas se enfocaban en el empleo táctico de las fuerzas en un determinado teatro de operaciones, hasta que Jomini (1838) pensó que, siguiendo una serie de leyes, un contingente militar podría estar en condiciones de vencer más fácilmente. Estas leyes se referían no solo al enfrentamiento y al combate en sí (es decir, la táctica de la que todos se habían ocupado hasta ese entonces), sino también a la maniobra de aproximación y retirada y a la logística de sostenimiento de las operaciones. A la combinación sincronizada en el terreno de estos aspectos previos al hecho táctico se lo conoce hoy como el "arte operacional" (Vergara, 2003).

Mientras Clausewitz (1831), concebía que la guerra era demasiado compleja, impredecible y un arte muy especial, porque se ejercía sobre elementos que reaccionan en función de su empleo y conducción. Pero lo más importante es que quería probar la naturaleza fundamental de la guerra y su lugar en el espectro de la actividad humana, por lo que la guerra fue orientada a una sistematización en el pensamiento de la conducción militar que, para una mejor interpretación, la guerra podía definirse en tres niveles:

- El que fijaba las causas por las que se debía ir a la guerra, al que llamaron nivel estratégico
- El que entendía los movimientos (maniobras) y la logística de las tropas en el terreno, al que llamaron nivel operacional
- El de los enfrentamientos en sí, al que llamaron nivel táctico (Vergara, 2003).

Por lo tanto en la guerra tradicionalmente visualizada, las fuerzas militares beligerantes emplean sus medios en un espacio tridimensional definido (aire, mar y tierra), y que es uno de los elementos decisivos para la consecución de un objetivo preestablecido en el nivel estratégico militar.

Con el vertiginoso desarrollo de las Tecnologías de Información y Comunicación (TIC), de la era posmoderna, se ha dado origen a un sin número de aplicaciones basadas en sistemas satelitales y terrestres de telecomunicaciones, redes de informática, telemática, dispositivos móviles que procesan, almacenan y transmiten información en tiempo real, elementos que sirven fundamentalmente para la conducción y toma de decisiones en el campo militar. Es aquí donde se origina un espacio intangible para realizar operaciones militares en los niveles operacionales y estratégicos. Este campo se lo denomina "Ciberespacio" y es donde - en los últimos años - se han librado ya grandes batallas.

Breve reseña de las guerras recientes en el ciberespacio

A finales del siglo pasado, ya se produjeron varios ataques utilizando el ciberespacio como un campo de batalla virtual. Con el pasar de los años, estos tipos de conflictos cibernéticos han ido creciendo y cada vez son más sofisticados y letales. A continuación se realiza una breve reseña de las principales "ciberguerras" producidas en los últimos años.

1999 - Guerra de Kosovo

Durante la intervención de los aliados en la Guerra de Kosovo, más de 450 expertos informáticos, al mando del Capitán Dragan, se enfrentaron a los ordenadores militares de los aliados. Este grupo integrado por voluntarios de diferentes nacionalidades, fue capaz de penetrar a los computadores estratégicos de la OTAN, la Casa Blanca y al portaaviones norteamericano Nimitz. Esto solo como una demostración de fuerza, ya que dicho portaaviones no era su objetivo principal; además, de ser una fuente alternativa de información en Internet, sirvió como grupo coordinador de actividades contra la guerra fuera de Yugoslavia.

2003 - Taiwán

En 2003, Taiwán fue amenazado con un "posible" ataque maquinado por las autoridades chinas. No hay pruebas pero dejó sin servicio a diversas infraestructuras como hospitales, la Bolsa y algunos sistemas de control de tráfico. El supuesto ataque provocó un caos progresivo y con una aparente organización; que, además, incluyó virus y troyanos, llegando a la conclusión de que el objeto no sólo sería robar información sensible, sino también paralizar al país.

2007 - Estonia

En ese año, Estonia culpó a las autoridades de Rusia de diversos ataques continuados que afectaron a medios de comunicación, bancos y diversas entidades e instituciones gubernamentales. El origen del conflicto habría sido el retiro de una estatua en memoria del Ejército soviético que se hallaba en la principal plaza de la capital.

2008 - Georgia

Durante la guerra Rusia - Osetia del Sur – Georgia, se produjeron ciberataques a esta última nación por parte de Rusia, orientados hacia sitios gubernamentales.

2010 - Irán

Este país del Medio Oriente también registró un ataque a las centrifugadoras del programa de enriquecimiento de uranio -programa nuclear iraní-. El troyano, virus o programa infiltrado recibió el nombre de Stunex. Irán acusó a Estados Unidos de su autoría.

2011 - Canadá atacada desde China

Según las autoridades canadienses, los sistemas de contraseñas del Ministerio de Finanzas fueron víctimas de un ciberataque procedente de máquinas instaladas en China.

Guerra cibernética en el 2012

EE.UU, Reino Unido, Alemania, India y China ya cuentan con equipos especiales de hackers y centros técnicos para proteger sus bases de datos estratégicas, e incluso para responder proporcionalmente en caso de un ciberataque. Especialistas en seguridad de redes advirtieron de una guerra cibernética para el 2012. Numerosos ataques podrían perpetrarse gracias al avance de las tecnologías de robo de datos y espionaje.

Holanda - 2013

En este año se realizó el mayor ciberataque del mundo, cuando diez millones de holandeses se quedaron sin firma digital y no pudieron acceder a la declaración de renta. La agresión se basó en la modalidad de denegación de servicio (DDOS), que consiste en el bloqueo del portal debido a una avalancha de solicitudes. Desde el Ministerio del Interior holandés explicaron que: "Es como si sonara una alarma continuamente y la puerta estuviera cerrada. Los ladrones están fuera pero desgraciadamente los visitantes normales también".

Ciberataques masivos a Estados Unidos - 2015

En los últimos años, Estados Unidos ha sufrido un sinnúmero de ataques que, de acuerdo a los organismos de seguridad de este país, provienen de hacker chinos, uno de los cuales pudo haber accedido a las bases de datos de cuatro millones de empleados y ex colaboradores del Gobierno federal. La oficina de administración de personal del Gobierno estadounidense, que es la encargada de las investigaciones de los potenciales funcionarios de gobierno, informó que podrían haberse contaminado los datos de altos funcionarios del gobierno (Huerta, 2013).

Definición del ciberespacio desde el enfoque militar

El Departamento de Defensa de Estados Unidos precisa que:

"El ciberespacio es un ámbito operativo cuyo carácter distintivo y único está enmarcada por el uso de la electrónica y el espectro electromagnético para crear, almacenar, modificar, intercambiar y explotar la información a través de las tecnologías de información y comunicación (TIC) y basadas en sistemas interconectados con sus infraestructuras asociadas" (Kuelh, 2006)

Por notro lado, Greg Rattray plantea que:

"El ciberespacio es un entorno artificial para la creación, transmisión y uso de la información en una variedad de formatos, fundamentalmente constituido por el hardware electrónico, redes, sistemas operativos, estándares y políticas de transmisión ".

Bajo estos conceptos, se podría reconocer que el ciberespacio es un teatro de guerra global creado en forma virtual o artificial, y que es una mezcla de electrónica, energía electromagnética, infraestructuras de red y la información en su conjunto.

Para la conducción de las operaciones militares convencionales, los Estados Unidos habían establecido cuatro dominios físicos para sus operaciones, a saber: terrestre, marítimo, aéreo y aeroespacial. Cada uno de ellos tienen radicales diferencias y características físicas únicas, y son valiosos sólo a través de la utilización de la tecnología para explotar esas características. Ahora han añadido al ciberespacio como el quinto dominio, ya que se ha constituido como un factor decisivo y de supremacía militar, por lo que en la actualidad se trata de controlarlo y explotarlo con fines políticos, estratégicos, económicos y militares del poder nacional.

Según el Departamento de Defensa estadounidense, el ciberespacio tiene las siguientes características:

- Es creado, mantenido, operado y de propiedad de los actores públicos, privados y de gobierno, y está disponible en todo el planeta
- Varía dependiendo de la tecnología, arquitectura, procesos y conocimientos para generar nuevas capacidades para su empleo militar
- Está sujeto a la disponibilidad del espectro electromagnético
- Permite altas tasas de maniobra operativas y toma de decisiones ya que capitaliza el hecho de que la información se mueve a velocidades que se acercan a la velocidad de la luz
- Facilita las operaciones a través de los dominios aéreo, terrestre, marítimo y espacial
- Trasciende Fronteras geopolíticas y organizacionales
- Se constituye por la interconexión de los sistemas de transmisión de información y datos, infraestructuras de soporte crítico, dispositivos que recopilan, procesan y transmiten datos, el uso de software, hardware y sistemas de información
- Incluye los datos de voz y vídeo " en reposo " y " en movimiento "
- Es de fácil acceso en distinto grado y a otras naciones, organizaciones, al sector privado, a los cibernautas y también para los enemigos de una nación
- Es la base del almacenamiento y trasmisión de la información y el conocimiento en tiempo real (The National Military Strategy For Cyberspace Operations, 2006).

Conclusiones

La aparición del ciberespacio como un nuevo teatro operacional, presenta nuevas oportunidades para el empleo de sistemas electrónicos, redes e infraestructura en operaciones militares. Por otro lado, es necesario determinar sus vulnerabilidades para diseñar estrategias de defensa en este domino virtual. Entonces podríamos decir que la ciberestrategia es el desarrollo y el empleo de las capacidades para operar y explotar el ciberespacio, integrada y coordinadamente con los otros teatros operacionales para lograr - o contribuir - al logro de los objetivos a través de los componentes de un poder nacional.

En los dominios de la guerra (aire, mar y tierra), las fronteras nacionales están claramente delimitadas; en tal virtud, se puede determinar cuándo existían acciones hostiles externas contra un país o acciones provocados por agentes internos; siendo el espacio cibernético, un campo

virtual donde las fronteras tradicionales desaparecen y se origina un campo de batalla global, puesto que un ataque puede producirse desde países alejados geográficamente o desde el interior del mismo.

Los países que no tienen una gran capacidad económica que les permita adquirir sistemas militares para la guerra convencional, deberían desarrollar capacidades para dominar y explotar los sistemas cibernéticos, de tal forma que se puedan formar profesionales con conocimientos multidisciplinarios para enfrentar las nuevas amenazas de este teatro de guerra global y contribuir a la seguridad nacional.

Referencias Bibliográficas

Impresos

Dan, K, (2006). From Cyberspace to Cyberpower: Defining the Problem, Information Resources Management, College/National Defense University, Washington

Chairman of the Joint Chiefs of Staff, (2006). The National Military Strategy for Cyberspace Operations, Washington

Rattray, G, (2001). Strategic Warfare in Cyberspace, Cambridge, Mass.: MIT Press, UK

Páginas WEB.

Artículo las Guerras Informáticas, Documentos varios, Estudio sobre Ciber Guerra Informática tomado en línea, septiembre 2014, http://www.gitsinformatica.com/descargas.html

Huerta Pablo, Ciberguerras: Las Batallas del Futuro, Hoy, Investigation Discovery, tomado en línea septiembre 2014, http://id.tudiscovery.com/ciberguerras-las-batallas-del-futuro-hoy/.

Vergara, Evergisto de, Los Niveles de la Guerra o del Conflicto, Instituto de Estudios Estratégicos de Buenos Aires, Sep-2003, tomado en línea, http://www.ieeba.com.ar/docu/ Los niveles de la guerra y del_conflicto.pdf.

LA DELINCUENCIA EN LA SOCIEDAD ECUATORIANA

Jorge Miño
Universidad de las Fuerzas Armadas - ESPE

Resumen

El siguiente artículo trata de un análisis sobre la evolución de la delincuencia ecuatoriana, considerando el cómo se desenvolvía la comunidad hace algunas décadas y el acelerado cambio hasta la actualidad. Al respecto, se hace un estudio de las causas de la delincuencia, muchas de las cuales son lógicas y las percibimos, pero hay otras que no se las puede concebir ya que constituyen y son producto de la crisis económica global que afecta a la sociedad mundial y que puede ser solucionada en cada país

Se ha comprobado que en nuestro país hace algunos años ya se conocieron hechos delincuenciales que conmocionaron a la sociedad en aquellos tiempos y se los ha tomado como el punto de partida en la escalada de violencia que nos ha llevado a ser considerados como noticia a nivel mundial por asesinatos a sangre fría, argumentados por la complicidad del alcohol y la droga; que, al decir de los delincuentes, trastorna sus conductas.

La delincuencia se encuentra localizada en las dos principales ciudades del país como son Quito y Guayaquil, donde se han podido descubrir verdaderas redes delincuenciales que operan en las diferentes modalidades y que constituyen una amenaza a la sociedad.

Palabras clave: Delincuencia, sociedad, asesinato, tranquilidad, violencia

Introducción

Este artículo conduce a nuestra mente a épocas remotas donde la vida se desarrollaba en armonía y en convivencia pacífica, tanto en las poblaciones grandes como en las ciudades y pueblos pequeños. Las tiendas y almacenes se mostraban abiertos para atender al público con cordialidad. Pero de pronto este espejismo desapareció. Sin embargo, ahora es tema de añoranza y conversaciones de padres e hijos que les hacen conocer cómo era la vida en aquellos tiempos, ya que ahora hay farmacias, tiendas de víveres, licorerías y almacenes pequeños que aparecen con barrotes de hierro en las puertas de ingreso a sus locales, aparentando celdas autoconstruidas en la gran cárcel de la población. También las viviendas, sean casas o departamentos, aparecen con barrotes de hierro en puertas y ventanas, con lo que se puede concluir que nos hemos enclaustrado voluntariamente en pleno siglo XXI.

Para nosotros, esta forma de vida es normal, no así para los turistas del primer mundo que nos visitan. Para ellos es motivo de filmación y fotografías que revelan a su retorno el periplo en un país extraño, cuyos ciudadanos se han encarcelado debido al auge de una amenaza latente llamada en términos generales delincuencia. "A manera de paradoja, ahora los que pertenecemos a una sociedad libre vivimos entre rejas, mientras que los delincuentes viven libres"

De un tiempo acá, nuestro país dejó de ser aquel sitio de paz y tranquilidad, diferente en el contexto regional por la ausencia de violencia y agresión delincuencial. Los tentáculos de la delincuencia han logrado penetrar hasta los más recónditos parajes de nuestra geografía. Los pretextos para el incremento delincuencial son de múltiples dimensiones que no justifican su accionar. El tema delincuencial figura en las portadas de los periódicos como un tema de lectura diaria, con detalles otrora no publicables. ¿Será que nuestra sociedad se acostumbró a vivir con la delincuencia o es que la delincuencia es parte de la vida misma?

Desarrollo

Actualmente los delincuentes, cuando no pueden cumplir con su objetivo, pueden incurrir en el delito de asesinato a sangre fría, por el hecho mismo de conseguir el botín, que muchas veces puede ser un teléfono celular o una ínfima cantidad de dinero. Nos preguntamos si ¿la delincuencia ha tenido influencia extranjera? O tal vez ¿la delincuencia ecuatoriana ha adoptado un modelo propio sin escrúpulos?

La delincuencia en el Ecuador ya no es la de años atrás, ahora existe perfeccionamiento y la razón radica en la influencia extranjera, especialmente la de origen colombiano, dado su entrada libre a territorio ecuatoriano (La Hora Nacional, 2006).

Conocedores en temas de seguridad manifiestan que la delincuencia fue importada con la presencia de delincuentes extranjeros que llegaron al país en algún momento, influyendo e instruyendo a nuestros delincuentes que todavía mantenían métodos tradicionales, sin mayor violencia. (Biblioteca Univ. El Salvador- Repositorio). Pero hay otras corrientes que consideran que la delincuencia fue creciendo conforme se incrementaba el desempleo, mientras se agrandaba la brecha de la inequidad. Así mismo, que la juventud y niñez habían abandonado las aulas escolares para atender necesidades de su entorno familiar, debido al desempleo, subempleo y otras causas. Todos los temas descritos, de seguro que al ser desarrollados nos tomaría tiempo para escribir sendos ensayos de profunda investigación. (ESPOL-4-ABR-2011)

Un estudio realizado por la Universidad Técnica Particular de Loja, UTPL, en una investigación sobre cómo afecta la delincuencia en la sociedad; da como resultado las causas por las que una persona se vuelve un delincuente, las mismas que se detallan a continuación:

- La pérdida de valores éticos y morales
- La mala administración de los gobiernos
- La falta de aplicación de las Leyes
- Corrupción de la función Judicial y en todos los estratos sociales
- La crisis económica
- El desempleo masivo
- La migración campesina
- La inflación de los últimos años
- La falta de alimentación, vivienda, salud, educación entre otras

Es alarmante cómo el tema de sicarios se ha ido impregnando en la sociedad, a tal punto que ya se puede encontrar mercado a través de la Internet. Los lectores pueden ingresar a través de cualquier buscador, allí podrán comprobar la oferta y demanda por estos servicios, es por eso que se ha considerado preocupante la información sobre la presencia agresiva y criminal de los llamados sicarios, personajes que ofrecen sus servicios a la sociedad, con audacia y descaro sin precedentes.

Poco a poco la delincuencia se ha ido perfeccionando y los malhechores se van inventado tácticas de las más diversas, como por ejemplo el uso de disfraces para que la víctima no se percate del delito, la utilización de vehículos robados o motocicletas que les facilite su escape luego de cometido el delito. Utilizan guantes de látex para no dejar huellas, y ahora ya ni siquiera utilizan pasamontañas, ya que luego del delito viajan a sus lugares de origen que normalmente son poblaciones en los países vecinos o ciudades del Norte o del Austro.

En los casos en que han sido capturados los delincuentes luego de haber cometido sus jugarretas y una vez que han sido interrogados por la Policía, con el más grande cinismo y sangre fría han narrado todos los pormenores o formas como han sido contratados y el pago que han recibido, el cual no es ni siquiera digno de ser publicado.

Considero que el punto de partida del incremento de la actividad delincuencial en el Ecuador se dio a partir del 21 de noviembre de 1.991, con el caso de Juan Fernando Hermosa Suárez (nacido en 1976), apodado "El niño del terror", quien acabó con la vida de 22 personas en Ecuador. Estos hechos de violencia máxima fueron narrados por el propio joven, con lujo de detalles y asombrosa frialdad. Sus víctimas fueron taxistas y homosexuales. (El Diario Manabita, 2013)

Según las autoridades, Hermosa era el cabecilla de una agrupación delictiva denominada "La banda del terror", dedicada al asalto y robo de vehículos e integrada en su mayoría por menores de edad. La banda sólo robaba carros, pero no había obstáculo de ninguna índole que impida lograr su propósito. Esto explica la gran cantidad de asesinatos. (YouTube, 2011)

Lo que se podría sostener es que la delincuencia traspasa fronteras y este mal no es propio de nuestro país, sino del continente y del mundo, el cual, fusionado con el narcotráfico, constituyen un caldo de cultivo ideal para la proliferación de la delincuencia. (Repositorio ESPOL, 2011)

Por lógicas razones considero necesario centrar mi análisis en el campo de la educación, por ello acudo a estadísticas que nos dan los siguientes resultados del auge delincuencial, aclarando que los temas presentados son solo una muestra informativa de los cientos de delitos cometidos cada día en el Ecuador. Así tenemos que se cometen 6 violaciones al día.

En el primer semestre de 2013, hubo 14.596 delitos denunciados, 480 de los cuales tuvieron participación jóvenes que cometieron asaltos o robos a vehículos privados o taxis.

De cada 10 mujeres, 8 son víctimas de algún tipo de violencia.

El 51% del total de denuncias contra mujeres son por maltrato físico y el 47% por maltrato psicológico.

El mayor problema de Guayaquil está relacionado con las pandillas juveniles, pues se calcula que existe alrededor de 200, integradas por cerca de 70.000 niños y jóvenes entre los 12 y los 25 años de edad (Clery, 2011).

Por tratarse de un tema de actualidad, el asesinato a dos jóvenes mujeres argentinas en Montañita, un poblado de la Costa ecuatoriana, esta información ha circulado por el mundo entero, por lo que me permito hacer mención del mismo para cerrar el tema del artículo y que los lectores puedan sacar sus propias conclusiones, entre otras, que todos somos proclives a ser presa de la delincuencia en cualquiera de sus modalidades.

La muerte de las jóvenes argentinas Marina Menegazzo (21 años) y María José Coni (22), ha generado el debate sobre la igualdad de género y la violencia contra las mujeres. Con cartas y mensajes difundidos en redes sociales, diversas personas y agrupaciones feministas han tomado el caso como una bandera de lucha. "Ayer me mataron", "Todas somos pibas viajeras" y "Qué va a ser de ti lejos de casa", son tres de los mensajes que se han difundido las redes sociales en los últimos días. (El Universo, 2016)

Uno de los presuntos asesinos de las dos jóvenes argentinas presentó versiones contradictorias de los hechos. Tras la audiencia desarrollada en Manglaralto, provincia de Santa Elena, el fiscal informó que inculpó del delito de asesinato a los acusados, identificados como Segundo P. y Eduardo A., contra quienes se dictó prisión preventiva.

El ministro del Interior Serrano dijo a la prensa que las dos chicas abandonaron el hostal donde se hospedaban en Montañita el 22 de febrero a las dos de la tarde. Esa misma noche, los sospechosos habrían conocido a las chicas en un bar llamado "La Abogadita". Ellas habrían

dicho que no tenían dinero y que iban a regresar a Guayaquil haciendo dedo, por lo que les ofrecieron que se quedaran a dormir en la casa de uno de ellos. Allí las dejaron y los dos hombres se habrían marchado hasta cerca de las dos de la mañana, cuando regresaron. Las chicas también habrían salido de la casa, pero al volver habrían encontrado a ambos hombres borrachos. (El Universo, 2016)

Según la versión, las autoridades atribuyen a Segundo P., éste se quedó a solas con Coni e intentó abusar de ella, pero la chica intentó escapar, por lo que él la golpeó en la cabeza con un palo, causándole la muerte. Luego, tras escuchar un grito en la otra habitación, Segundo P. habría ido allí donde descubriría que Eduardo D. había acuchillado a Menegazzo. Según la misma versión, Segundo P. limpió el lugar, guardó los cuerpos en unas bolsas y los llevó con una carretilla a unos 400 metros de su casa, donde intentó ocultar uno de los cadáveres, dejando abandonado el otro. (Teleamazonas, 2016)

Conclusiones

Como sociedad responsable, no podemos dejar de pensar, analizar y reflexionar sobre este tema que es noticia diaria de la prensa nacional. Considero que hay - entre otras - una vía de solución para el problema, y es la educación, pero para lograr esto, se necesita solucionar una serie de problemas de índole social, iniciando por la educación infantil y fortaleciendo valores en la juventud; así, recibir a futuro los resultados que todos esperamos.

Pero la manera más idónea de combatir este mal que nos aqueja, es con una educación permanente que llegue a los lugares más recónditos de nuestra geografía. Está demostrado a nivel mundial que los seres humanos con una educación efectiva desde temprana edad, forman ciudadanos que luchan por el buen vivir en todo sentido, pues aplaudamos el esfuerzo de jóvenes educadores que se sacrifican en los lugares más recónditos, brindando conocimiento y sabiduría a compatriotas dignos que luchan por ser mejores, por verse alejados de la delincuencia.

Todos somos responsables de la falta de educación de nuestros niños y jóvenes, por ello la campaña nacional a favor de la educación debe ser reforzado en todos los niveles de la sociedad, que bien la podríamos llamar "Más educación menos delincuencia".

Bibliografía

Arteaga, M. (2000) Inicios del pensamiento sociólogo en el Ecuador. Edit. Casa de la cultura ecuatoriana. Núcleo del Guayas.

Cabanellas, G. Diccionario Jurídico elemental. Edit. Heliastas ISBN 950-9065-98-6

Clery, A. (2011). Problemas sociales en el Ecuador. Edit. Universidad Vicente Rocafuerte. Guayaquil.

Dalmau F. (1983) El joven delincuente en Guayaquil. Edit. Unión Gráfica. Guayaquil.

Estarellas C. (2010) La delincuencia en el Ecuador. Edit. Desde mi trinchera. Guayaquil.

Merino D. (2012) Delincuencia y Sicariato en el Ecuador. Edit. ESPOL. Guayaquil.

Narváez N (2008) La delincuencia en el Ecuador. Edit. Blog de Word Press.com. Quito.

Moreno B (2010) Causas sociales de la delincuencia y la impunidad. Edit. Revista judicial. Quito

Doña T. (2009) La delincuencia en el Ecuador. Edit. ESPOL. Guayaquil.

Dalmau F. (2011) Acciones para mejorar la delincuencia. Edit. ESPOL. Guayaquil.

CYBER DEFENSAS: LOS NUEVOS CHICOS BUENOS

Robert Vargas Borbúa
Universidad de las Fuerzas Armadas - ESPE

La creación de un mundo mejor no es sólo una tarea de los gobiernos y políticos. Es una responsabilidad de todos. Después de los ataques terroristas en París, Francia envió soldados a las calles de París para proteger a los ciudadanos. Se sabe que puede haber más terroristas dentro de las fronteras de Francia. Las Fuerzas Armadas francesas, individuos y otros servicios de seguridad tienen que definir quién es amigo y quién podría ser el enemigo, qué es bueno o malo. Será una tarea difícil y se pueden cometer muchos errores porque en las operaciones, las personas inocentes podrían ser afectadas. El orden en la batalla se está difuminando, es difícil saber quién es el enemigo, dónde está el enemigo, o cuáles son los límites del área enemiga. Además, la batalla ocurre en el mundo cibernético donde el grupo de piratas informáticos conocido como ANONYMUS ha hecho una declaración de guerra contra ISIS, perpetradores de los ataques en París. Sin embargo, los piratas informáticos, quienes se encuentran fuera del estado de derecho, no pueden defender esta guerra por nosotros.

ANONYMUS ha cerrado y eliminado más de 25.000 cuentas de Twitter de ISIS, incluso exponían sus paraderos virtuales. Este grupo se ha comprometido no sólo a defender a los parisinos, sino a otros en las redes sociales en contra de ISIS.

Estas declaraciones y acciones deben despertar muchas preocupaciones en los parisinos y en todos los ciudadanos comunes en el mundo. ¿Deben los parisinos agradecer a ANONYMUS? ¿Por qué los servicios de seguridad francesa o la Policía no cerraron los tweets y las cuentas de Twitter antes? ¿Por qué no usaron Twitter con la misma eficiencia cuando rastreaban a Gadafi en Libia? Hay muchas posibles respuestas a estas preguntas. Aunque ellos no tengan la capacidad para luchar en contra de los terroristas cibernéticos, no creyeron que cerrar estas cuentas en las redes sociales fuera necesario, ya que la ley no les permitía a estas organizaciones legales utilizar esos procesos.

Muchos presidentes, ministros, parlamentarios y ciudadanos, así como las instituciones públicas y privadas usan Twitter y otras redes sociales para transmitir información. No hay duda de la influencia que el Internet tiene en nuestra política, nuestra economía y en nuestro mundo social, incluso influye en nuestra apreciación de que es correcto e incorrecto fuera de las definiciones de "normal". Si publicas algo que está mal, tal como ANONYMUS u otros grupos lo definen, sus cuentas podrían cerrarse o podrían ser acosados en línea.

La semana pasada el Gobierno ecuatoriano hizo varias modificaciones a la Constitución. ANONYMUS argumentó en contra de las enmiendas, por lo que decidió publicar vídeos, imágenes y mensajes de correo electrónico que afectan a la reputación de ministros, asambleístas y otros políticos. Los criminales (piratas informáticos) se convierten en defensores de la ley y el orden según su conveniencia. Por otro lado, algunos gobiernos y proveedores (como Google, Microsoft y otros) cierran publicaciones y cuentas de redes sociales de algunos ciudadanos que podrían "afectar negativamente" a la sociedad de un país. Dado que no existe un sistema legal cibernético, no existe un marco legal para juzgar el bueno o mal comportamiento.

El mundo cibernético tiene que estar asociado con el objetivo de crear una sociedad mejor y tiene que ser un mecanismo a través del cual la Internet genere una justicia social, no injusticia social. Si el estado de derecho en el mundo es difícil de lograr, el estado de derecho en el espacio cibernético sigue siendo vago y ambiguo. Como hemos visto, los estados ya no tienen el monopolio de la violencia ni son los únicos jugadores que tratan de proteger a los ciudadanos de un país.

Otros grupos, legales o ilegales, pueden tomar medidas con el fin de proteger a los demás, como el sentido moral de la ley.

Todos somos ciudadanos cibernéticos, con derechos y responsabilidades, defensores cibernéticos, si esperamos a que grupos como ANONYMUS apoyen el estado de derecho y que peleen nuestras batallas. Estamos dejando el futuro a fuerzas oscuras, eso puede conducirnos a una situación peor de la que ya estamos.

La gente común en las calles puede presionar a los políticos y a las organizaciones a hacer más o a hacer algo completamente diferente. Como en las imágenes del niño sirio muerto en las orillas del Mediterráneo que provocaron ira y reacciones en todo el mundo, sobre la guerra civil de Siria y la migración forzada de sus habitantes. Los primeros refugiados sirios están llegando a Canadá. Este no es un debate sobre el control de la Internet, más bien se trata de una discusión acerca de cómo crear una sociedad mejor e igualitaria. La era de la información y la Internet nos dan la oportunidad de estar involucrados. Nuestras opiniones y mensajes en las redes sociales podrían promover la equidad y la igualdad. Esta es la oportunidad.

"HACIA NUEVOS CONCEPTOS Y VISIONES ESTRATÉGICAS DE SEGURIDAD Y COOPERACIÓN PARA LA SEGURIDAD NACIONAL Y ESTABILIDAD REGIONAL"

Gabriel Recalde G.
Universidad de las Fuerzas Armadas - ESPE

Visión general de seguridad

Una visión panorámica y reflexiva del mundo, nos presenta ciertos procesos de consolidación de una triada de poder mundial conformada por una América unida, la Unión Europea y una pujante Asociación de Países Asiáticos de la Cuenca del Pacífico, que disputarán la hegemonía global en función de su creciente población y cada vez menos recursos naturales. Pero en esta visión miramos con preocupación a una América todavía con dificultades en materia de integración, pero aún convencida de alcanzar la gran unidad continental como fortaleza para enfrentar los desafíos globales.

En la subregión andina se continúa luchando por un nuevo orden basado en democracia y estabilidad política y social, economía libre y abierta, defensa del medio ambiente y de los recursos naturales y energéticos estratégicos. Integración, más allá de la cooperación; seguridad de las áreas e instalaciones estratégicas y enfrentamiento oportuno y adecuado a las contingencias de origen natural y antrópico que puedan afectar la continuidad de las actividades vitales para el Estado, a la población, sus recursos y los bienes nacionales. Pero, a la par, nuevas preocupaciones, amenazas y factores de riesgo aparecen en la visión integral de seguridad, cuyas soluciones no dependen solo del factor militar, sino de la relación auténtica, transparente y dinámica entre las instituciones que conforman la estructura de seguridad de los estados, y la sociedad civil.

Preocupa la continuidad del conflicto interno de la hermana república de Colombia, así como la presencia cada vez más agresiva de las nuevas amenazas asimétricas como el narcotráfico, sus delitos conexos y sus nuevos ingenios con tecnología de punta: la transnacionalización del crimen internacional, los cíber ataques, la delincuencia organizada y la común, la pobreza, la miseria y la indigencia, generadoras de violencia y males sociales; la corrupción, el sicariato, la trata de blancas, las movilizaciones descontroladas, los efectos del cambio climático; y, en algunos casos, la reactivación de amenazas tradicionales de soberanía que aparentemente estaban sepultadas en el pasado por los Acuerdos de Paz. Situaciones que han sobrepasado la capacidad de control de ciertos estados, convirtiéndolos en Estados en Indefensión recurrentes a Estados de Excepción, como mecanismos normales de gobernabilidad.

En el escenario de paz, cooperación e integración americana, se debe reconocer las importantes iniciativas y persistencia de los organismos de seguridad y desarrollo hemisféricos, la CAN y la UNASUR, y particularmente de las conferencias de ministros de Defensa, las conferencias de Seguridad Andina y las conferencias de los Comandantes de FF.AA. del continente, sin el éxito esperado, pues, entre otras dificultades de fondo, persisten actitudes matizadas por recelos, desconfianza, incertidumbre, inexperiencia, improvisación, intransigencia, falta de renunciamiento, nuevas visiones ideológicas en la conducción de los estados, discontinuidad en la aplicación de políticas de Estado en defensa, falta de cultura democrática y falta de cultura de seguridad, a más del accionar de ciertos intereses desestabilizadores, todo lo cual ha conducido a éxitos relativos típicos de un marco de formalidad social y diplomática, rescatándose el beneficio de la relación personal entre autoridades civiles y militares. El resultado es una percepción de escepticismo generador de actitudes negativas que no favorecen los objetivos superiores de unidad nacional y regional.

En materia de seguridad, se ha cuestionado la vigencia, por obsolescencia, de ciertos tratados de la antigua, estática y reactiva seguridad colectiva, por no haber cumplido con los objetivos para los que fueron creados, permitiendo así la prevalencia del liderazgo impositivo y de la discrecionalidad de los países hegemónicos. Por ello se señala que la cultura de seguridad y defensa se ha circunscrito al ámbito formal y académico y no a la efectividad de sus propósitos.

Es imperativo entonces, iniciar nuevos procesos, empezando por sincerar los resultados de los análisis de nuestras realidades nacionales para definir amenazas y factores de riesgo que, proyectados a nivel regional, nos permitan encontrar denominadores e intereses comunes que nos unan; y, acto seguido, diseñar líneas de acción estratégicas que incluyan la revisión y actualización de los instrumentos de paz y seguridad a efecto de alcanzar un nuevo enfoque cooperativo, preventivo, flexible, dinámico y efectivo, basado en la buena fe y transparencia como ejes para una limitación mutua en el uso de las armas, el mantenimiento multilateral de la paz, el fortalecimiento de medidas de confianza mutua y seguridad, y así contribuir a prevenir conflictos, fortalecer las instituciones democráticas y ahorrar ingentes recursos económicos.

En la ruta hacia la seguridad cooperativa, la seguridad nacional y regional debe concebirse como un concepto integral donde no se concibe la seguridad política sin seguridad económica, y ésta no existe sin justicia social. Nada será posible si no se ubica al ser humano como objetivo supremo de los estados y de la región, debiéndose agregar la seguridad ambiental y la seguridad humana así como el reconocimiento pleno del individuo como sujeto del derecho internacional.

Amenazas y factores de riesgo nacionales y regionales: Escenarios prospectivos de preocupación para la seguridad nacional y estabilidad regional

Las nuevas amenazas son de naturaleza diversa y alcance multidimensional. Su asimetría hace difícil su identificación y neutralización oportuna en un contexto de cambio e incertidumbre; y, para enfrentarlas, es necesario ampliar los conceptos tradicionales de seguridad para incluir nuevos enfoques más flexibles, creativos y efectivos, a la par de su acelerada dinámica. Una apertura indiscriminada de fronteras - mientras los demás países se blindan - es la punta de lanza para la inseguridad ciudadana actual y de los bienes nacionales, oportunidad que toman los países emergentes para aliviar su presión interna y favorecer la migración indeseable.

Se pone a consideración un cuadro general de amenazas y factores de riesgo elaborado en base a la propuesta de la Junta Interamericana de Defensa - 2003, resultado del análisis de la realidad nacional del Ecuador, como un aporte que podría servir de referencia para otras visiones de los países emergentes.

Criterio de elaboración: Las amenazas se han diferenciado de los factores de riesgo bajo la premisa de que para enfrentarlas, es necesario la respuesta militar del Estado; en cambio para los segundos, no necesariamente, aunque las FF.AA. ecuatorianas están interviniendo en actividades de apoyo a la acción del Estado y del Gobierno, más allá de sus competencias directas, lo que podría ser mañana, objeto de reclamos jurídicos.

Los elementos expuestos en el orden de prioridades han incrementado su accionar, afectando a todos los factores del poder nacional que podrían afectar también a los países de la región de acuerdo a sus realidades. Lo que más preocupa es la reactivación de ciertas amenazas de soberanía, las afectaciones del conflicto interno de Colombia, los cíber ataques, y las secuelas de la pobreza, generadoras de violencia y males sociales; así como la injusticia social, la corrupción y la impunidad, como factores de desestabilización e inseguridad.

Cuadro general de amenazas y factores de riesgo. Visión Particular desde la Realidad Nacional del Ecuador

Para atender las demandas, y en cumplimiento de sus misiones constitucionales de defensa de la soberanía e integridad territorial y apoyo al desarrollo nacional, las Fuerzas Armadas ecuatorianas han terminado un arduo e intenso proceso de reestructuración para optimizar su eficiencia, eficacia y competitividad. Al momento están apoyando con su contingente en más de veinte y cinco subsidiarias, que van desde el control de actividades ilícitas hasta la conservación del medio ambiente, en atención a desastres naturales, siendo los primeros en llegar y los últimos en salir del lugar de la tragedia.

Propuestas para la seguridad nacional y estabilidad regional: Líneas de acción estratégicas para enfrentar las nuevas amenazas

El Sistema Nacional y Regional de Seguridad debe adoptar inmediatamente una arquitectura flexible basada en los principios de seguridad cooperativa, con responsabilidad compartida, interacción y coordinación permanente entre todos los países, organismos, instituciones y sociedad civil de todas las naciones. Además, fortalecer los organismos que conforman las estructuras de seguridad de los estados para volverlos más operativos, dinámicos, ágiles, eficientes y efectivos, estableciendo mecanismos concretos y oportunos de intercambio de información e inteligencia estratégica y construir escenarios prospectivos en base a la realidad regional, por encima de escenarios negativos como los proyectados a la región por el conflicto interno de Colombia.

Los nuevos escenarios deberán estar basados en primer lugar en el estado nacional de derecho, de respeto a la ley, que permita consolidar con posibilidades de éxito en el estado regional de derecho, donde los conflictos internos y externos de los países se resuelvan por medios pacíficos y a través de la observancia y el cumplimiento de los acuerdos y convenios internacionales en los

cuales impere la reciprocidad, el respeto mutuo, la igualdad, la equidad, la justicia y la economía humanizada.

Las aspiraciones futuristas y ambiciosas de la Declaración de Santa Cruz lo dicen todo; empero, en el afán de aportar, se expresan las siguientes líneas de acción estratégicas de cooperación institucional, nacional y regional:

Seguridad nacional y regional cooperativa

- Actuación anticipada y enfrentamiento oportuno a las nuevas amenazas a fin de prevenir conflictos, con el esfuerzo coordinado de cada una de las naciones, priorizando el sistema diplomático
- Fomento del multilateralismo, como factor esencial, y los principios de la seguridad cooperativa

Fortalecimiento de la fuerza pública

- Fortalecer la cobertura estratégica para negar rutas de actividades ilícitas
- Planificar, de manera conjunta y combinada, las operaciones militares y el empleo de las instituciones que conforman la estructura de seguridad de los estados.

Protección de la población y sus recursos

- Fomentar en la población una conciencia nacional y regional sobre la responsabilidad de todos en la seguridad y defensa
- Fortalecer los valores cívicos, éticos, morales, culturales y de cohesión social
- Proteger la infraestructura nacional
- Prevenir y neutralizar el desarrollo de actividades ilícitas
- Organizar, planificar, capacitar y coordinar en atención a desastres naturales

Respeto a la ley y los derechos humanos

- Actualizar las leyes para sancionar los delitos relacionados con terrorismo, narcotráfico, secuestros, sicariato, etc., exhortando a los parlamentos de los estados a armonizar las legislaciones nacionales con respecto a la legislación internacional, a fin de contribuir en el diseño de estrategias regionales más efectivas y de común aceptación
- Educar y monitorear en las instituciones militares el respeto a los derechos humanos.

Fortalecimiento de la cooperación interinstitucional e internacional

- Priorizar la ejecución de proyectos de desarrollo social, particularmente en las zonas fronterizas y en aquellos lugares olvidados por el Estado
- Cooperar en la lucha contra el crimen internacional
- Fortalecer las instancias de cooperación en inteligencia estratégica y el intercambio oportuno de información
- Apoyar a las operaciones de paz

Comentarios Finales

Sudamérica vive una difícil situación de inseguridad y falta de cooperación que dificulta la construcción de escenarios de unidad nacional y regional, lo cual amerita perseverar hasta obtener una Declaración de Verdaderas Voluntades Políticas que permita fortalecer el sistema democrático y viabilizar acciones estratégicas concretas, apoyando iniciativas políticas y diplomáticas e impulsando espacios de diálogo de interés común, para llegar a soluciones integrales de manera definitiva y duradera, buscando el equilibrio y la armonía regional, y evitando armamentismos con alto costo social.

La mejor alternativa es caminar hacia el futuro por la senda del Estado de Derecho en cada una de las naciones, de derechos y libertades, pero también de responsabilidades, de observancia de la ley, de fiel cumplimiento de los acuerdos internacionales, especialmente los de paz y seguridad.

La solución será integral. La realidad exige superar el aislamiento y recelo mutuos y construir mecanismos para fortalecer la seguridad nacional y regional. Aquí, la responsabilidad es de todos: "Hacia un mundo libre, sin miedo y sin temores", objetivo supremo de los hombres, de las Naciones Unidas y de los Estados Americanos.

INSTRUCCIONES GENERALES PARA LOS AUTORES

Todo artículo debe ser original y se enviará al comité editorial, quién decidirá la aceptación o no para la publicación en base a la revisión de pares conformados por especialistas del área.

Ediciones: La revista "REVISTA DE CIENCIAS DE SEGURIDAD Y DEFENSA" se publica cuatro veces al año, en los meses de abril y octubre, tiempos de semestres activos de la Universidad de las Fuerzas Armadas ESPE.

Temas: La revista "REVISTA DE CIENCIAS DE SEGURIDAD Y DEFENSA" abarca con todos los temas relacionados con seguridad y defensa, ya sea a nivel nacional como internacional. Las temáticas pueden incluir historia y educación militar, geopolítica, soberanía e integridad territorial, seguridad alimenticia, seguridad y desarrollo nacional, seguridad de salud, sociología militar, estrategia, mantenimiento de la paz y seguridad internacional, investigación y desarrollo tecnológico para la defensa nacional, transporte y movilidad, patrimonio natural y cultural, gestión de riesgos, prevención, mitigación y otros temas afines.

Idioma: Los artículos pueden ser escritos en español o en inglés.

Extensión: La extensión de los artículos como de opiniones puede ser de hasta 15 páginas. Deberán ser escritos en papel tamaño Ejecutivo (18.41x26.67 cm), en procesador de palabras, a doble espacio, con el tipo de letra TIMES NEW ROMAN, tamaño 12.

Márgenes: Arriba 2.5 cm - Izquierdo 2cm - Abajo 2.5 cm -Derecho 1.5 cm

Carátula: La carátula deberá incluir el título del artículo (14 ptos en mayúsculas, negrito y justificado); nombre(s) completo(s) del(os) autor(es) (10 ptos, mayúsculas, negrito y justificado), el nombre de la Institución, dirección de la institución, correo electrónico. Las páginas no deben estar numeradas.

Resumen: Cada artículo debe ser precedido por un resumen corto (no debe exceder de 500 palabras), el cual debe permitir al lector tener una idea de la importancia y el campo que abarca el artículo, debiendo incluir este resumen en inglés y ubicado luego de las palabras clave. En caso de que el artículo sea en inglés, después del "abstract" deberá presentarse el resumen en español.

Palabras clave: Un máximo de cinco, las cuales facilitan el contenido del texto. Se ubicarán luego del abstract.

Páginas del texto: El texto se escribirá con TIMES NEW ROMAN 12 ptos. Los títulos de capítulos de primer orden, serán escritos con mayúsculas, negrito y justificado. Los de segundo orden con mayúsculas, sin negrito y justificado. Los de tercer orden, sin negrito, justificado y las primeras letras con mayúsculas. Después de cada título dejar un espacio.

Ecuaciones: Se debe dar especial atención a la ubicación de índices y subíndices con el propósito de evitar errores. Las ecuaciones deben ser numeradas secuencialmente en paréntesis en el lado derecho de la página. Se debe dar especial atención a las ecuaciones a fin de que los símbolos sean claramente identificados.

Tablas: El título debe ser colocado en la parte superior y la primera letra con mayúscula (11 ptos), debe estar numerada secuencialmente.

Figuras, gráficos, imágenes: Sólo podrán incluirse ilustraciones originales (fotografías de alto contraste, gráficos, mapas, dibujos, figuras, etc.) listos para impresión. El título debe ser colocado en la parte inferior y la primera letra con mayúscula (11 ptos), debe estar numerada secuencialmente.

Agradecimientos: En caso de existir colocarlos a 11 ptos con negritas y mayúsculas

Referencias: Las referencias deben ser citadas de la siguiente forma con 11 ptos con negrillas y mayúsculas:

- Para un libro, debe ir el apellido del autor(es), año de publicación, seguido del título con mayúsculas las primeras letras y en cursivas, editora, edición, lugar.
- Para una revista, debe ir el apellido del autor (es), año de publicación, seguido del nombre del artículo, nombre de la revista con mayúsculas la primera letra, volumen, número, páginas del artículo separado por guión, lugar.

Sólo podrán incluirse ilustraciones originales (fotografías de alto contraste, gráficas, mapas, dibujos, figuras, etc.) listos para impresión. Debe adjuntarse una lista completa de ilustraciones. Cada ilustración será numerada y acompañada de una leyenda de identificación e indicación de su ubicación exacta dentro del texto; adicionalmente deberá ser suavemente etiquetada en la parte posterior a fin de identificar claramente la parte superior e inferior y el número que le corresponde. Las figuras, fotos, imágenes, y otros, cuyos archivos deberán ser generadas con una resolución mínima de 600 pixeles en formato .tiff, o .jpg. Recomendamos comprimirlas para su envío (formato .zip).

Textos electrónicos: Los autores deberán enviar sus contribuciones por correo electrónico en procesador compatible con PC (Office) a: ttoulkeridis@espe.edu.ec

Quinta presidencial asignada a la Escuela de Oficiales de Ingeniería, 1922. Estaba ubicada en la Av. Patria, fue derrocada en 1949 para la construcción de la Embajada de los Estados Unidos en el Ecuador (Foto: Alfonso Ortiz)

1922 ECUADOR
ESPE
UNIVERSIDAD DE LAS FUERZAS ARMADAS
INNOVACIÓN PARA LA EXCELENCIA
SEGURIDAD Y DEFENSA
UNIVERSIDAD DE LAS FUERZAS ARMADAS-ESPE