

**COLEGIO INTERAMERICANO DE DEFENSA  
DEPARTAMENTO DE ESTUDIOS  
CLASE XLIV**

# **MONOGRAFIA**

## **EL DESARROLLO TECNOLÓGICO Y SU IMPACTO EN LA SEGURIDAD Y LA DEFENSA NACIONAL**



**TCNEL. DAGOBERTO CABRERA ARGUETA  
EJERCITO DE EL SALVADOR**

**FORT LESLEY J. McNAIR,  
WASHINGTON, DC. MAYO 2005**

**EL DESARROLLO TECNOLOGICO Y SU IMPACTO EN LA SEGURIDAD Y LA DEFENSA  
NACIONAL**

POR

TCNEL. DAGOBERTO CABRERA ARGUETA  
REPUBLICA DE EL SALVADOR

Monografía presentada al Colegio Interamericano de Defensa como requisito para la obtención del Diploma aprobatorio del Curso Superior de Defensa y Seguridad Hemisférica.

FORT LESLEY J. McNAIR,  
WASHINGTON, DC. MAYO 2005

Certifico que he revisado este Trabajo  
de Investigación y lo he encontrado  
ajustado a la normativa y metodología  
del CID.

---

CNEL. GUILLERMO RAMIREZ CHOVAR

EJERCITO DE CHILE

ASESOR COORDINADOR

---

**FECHA**

## **NOTA ACLARATORIA**

Las opiniones emitidas en el presente trabajo son de la exclusiva responsabilidad del autor y no representan la posición del CID.

## **AGRADECIMIENTO**

Agradezco a Dios, nuestro Señor, quien me ha dado la fe y la confianza para elaborar este trabajo, porque con su ayuda nada es imposible.

Un agradecimiento muy especial al Sr. Coronel Guillermo Ramírez Chovar de Chile, quien realizó un excelente asesoramiento, poniendo de manifiesto su profesionalismo y muy especialmente su don de gente, a nuestros asesores y a mis queridos compañeros de la clase No 44, “La Mejor de las Mejores”.

A mi esposa Tesla, por entregarme todo su respaldo, paciencia y palabras de aliento, durante mis largas horas de trabajo; a mis hijas Teslita, Dorita y Michelle, por comprender mis ausencias y el tiempo que dejé de compartir con ellas. A mis queridos padres Francisco Antonio Cabrera (QDDG) y Dora Argueta Santín Vda. De Cabrera, por el apoyo que siempre me brindaron en mi carrera profesional.

Para terminar no quiero dejar de mencionar que durante la elaboración de ésta monografía, nuestro Señor, llamó a su presencia a mi querida suegra Gloria Soledad Ramírez, a ella también le dedico éste esfuerzo, por el amor que siempre me entregó.

## **AUTORIZACIÓN**

Autorizo al Colegio Interamericano de Defensa la publicación de este trabajo como artículo de lectura seleccionada o en la revista del Colegio, con la condición que se incluyan en dicha publicación, la totalidad de notas bibliográficas consideradas en el trabajo de investigación.

---

Tcnel. Dagoberto Cabrera Argueta

República de El Salvador

## INDICE

	Páginas
<b>RESUMEN</b> .....	<b>1</b>
<b>CAPITULO 1- INTRODUCCION</b> .....	<b>4</b>
<b>CAPITULO 2- INFLUENCIA DE LA POLITICA DE DEFENSA DE LOS ESTADOS EN RELACION CON SUS VECINOS</b> .....	<b>7</b>
2.1 La defensa y la seguridad nacional en el hemisferio.....	7
2.2 Los libros blancos y su importancia en la política de defensa.....	13
2.3 Las amenazas tecnológicas a la defensa y la seguridad nacional.....	18
2.4 Influencia del desarrollo tecnológico dentro del poder militar.....	24
<b>CAPITULO 3- LOS AVANCES TECNOLOGICOS COMO AMENAZA A LA SEGURIDAD Y LA DEFENSA NACIONAL</b> .....	<b>27</b>
3.1 Experiencia de ataques con las nuevas tecnologías de informática.....	27
3.2 Las empresas transnacionales como nuevos actores al servicio de la tecnología.....	30
3.3 La era de la información y su impacto en los sistemas de seguridad, defensa e inteligencia.....	34
3.4 El desarrollo tecnológico como posibilidad de cooperación, integración y estabilidad de la región.....	36
<b>CAPITULO 4- CONSECUENCIA DE LA TECNOLOGIA CONTRA LA SEGURIDAD Y LA DEFENSA NACIONAL EN LAS EXPRESIONES DEL PODER</b> .....	<b>40</b>
4.1 La expresión económica.....	40
4.2 La expresión política.....	41
4.3 La expresión Psicosocial.....	43
4.4 La expresión militar.....	44
<b>CAPITULO 5- CONCLUSIONES</b> .....	<b>46</b>
<b>GLOSARIO</b> .....	<b>I</b>
<b>BIBLIOGRAFIA</b> .....	<b>II</b>

## RESUMEN

El desarrollo tecnológico y su impacto en la seguridad y la defensa nacional, es un tema muy amplio que encierra muchas áreas en el campo de la tecnología, que pueden afectar de diversas maneras la seguridad y la defensa nacional de los Estados.

En ese contexto se ha desarrollado la presente monografía dentro de un espectro tan amplio, dando énfasis principalmente a la informática y las comunicaciones, que en las últimas dos décadas, ha tenido una diversidad de adelantos, por supuesto que en éste mismo orden de ideas podemos mencionar la robótica, la energía nuclear, las pandemias, las armas de destrucción masiva, entre otras que requieren de tecnología, pero que pueden ser detectadas o por lo menos identificadas. No obstante por tratarse de un trabajo de monografía con limitantes en el volumen del mismo se centra en las dos áreas antes mencionadas, considerando la potencial amenaza al hemisferio, pero especialmente señalando lo difícil que puede resultar para los estados que no cuentan con tecnología adecuada, contrarrestar este tipo de amenazas.

La monografía consta de cinco capítulos, inicialmente con una introducción que sirve como una antesala donde se determinan los aspectos generales, haciendo el planteamiento de tres premisas que son las siguientes:

- 1.- Los avances tecnológicos como una amenaza a la seguridad y a la defensa nacional;
- 2.- Como una herramienta que favorezca a la integración del hemisferio, para enfrentar las crecientes amenazas antes mencionadas.
- 3.- Como una disuasión para los países del hemisferio dentro del poder militar.

A partir de estas tres premisas se trata de llamar la atención sobre como los avances tecnológicos afectan o favorecen al hemisferio, considerando la seguridad y la defensa nacional.

El objeto principal de la investigación es establecer cómo estamos preparados para contrarrestar por ejemplo las amenazas cibernéticas, las vulnerabilidades ante el empleo de los equipos electrónicos, como los teléfonos celulares, las cámaras fotográficas, los Jump Drive o incluso las agendas electrónicas, así como los Hacker, los virus, las bombas lógicas, los gusanos etc. Con mucha preocupación se puede apreciar las grandes vulnerabilidades en la seguridad de las instalaciones de áreas sensitivas como lo son las sedes de las diferentes carteras de estado de los países del hemisferio, así como las instituciones financieras.

Basados en estos adelantes se hacen las siguientes interrogantes:

¿Cómo nos impactan estos avances?

¿Podremos tener la capacidad de enfrentar éste tipo de amenazas?

¿Serán las leyes y las instituciones de un Estado suficientes para proteger su soberanía e integridad territorial?

En esa perspectiva se desarrolla una visión del entorno que tiene la seguridad y la defensa de los Estados, citando en el capítulo 2, algunos conceptos generales de ambas áreas, considerando al hemisferio para poder abordar con objetividad necesaria ésta investigación.

Dentro de los aspectos que se resaltan es la preocupación hemisférica con el establecimiento de los libros de defensa, como base para establecer sus políticas de defensa. Asimismo se señalan las grandes diferencias existentes entre Estados Unidos y Canadá, con el resto del Hemisferio, no sólo en el orden tecnológico y económico, sino de interés en los temas de seguridad y defensa nacional.

No menos importante es el señalamiento que se hace de la falta de preocupación en el hemisferio, por los adelantos tecnológicos, con la excepción de Cuba con su tradicional desconfianza de los Estados Unidos y su poderío tecnológico en todos los ámbitos incluyendo la informática y las comunicaciones.

La globalización se señala como una fuente de aspectos positivos para la integración del hemisferio, considerando los beneficios de los avances tecnológicos en la lucha contra los desastres naturales, la educación, la salud, la economía y el fortalecimiento social.

En el capítulo 3, se hace mención de cómo “Los avances tecnológicos como amenaza a la seguridad y la defensa nacional”, por lo cual se citan algunas experiencias señaladas en los Estados Unidos por considerar que dentro de la potencia hegemónica se han detectado los casos con mayores daños y donde se involucran algunas de las principales transnacionales.

Asimismo en este capítulo se registra a las empresas transnacionales como nuevos actores al servicio de la tecnología, por la importancia que éstas tienen en el desarrollo del armamento, la informática, los equipos de comunicación, los satélites y los equipos de guerra electrónica.

Otro aspecto importante es la era de la información y su impacto en los sistemas de seguridad, defensa e inteligencia, enfocando los campos económico y político, los desafíos que esta presenta incluso a la inteligencia misma de los Estados.

Sin embargo así como existen amenazas con la tecnología, también podemos señalarla como instrumento de cooperación, integración y estabilidad de la región, donde se señala el aprovechamiento en beneficio de los países del hemisferio, por ejemplo ante los desastres naturales, la globalización, los

tratados de libre comercio, el combate al crimen organizado, el narcotráfico y los acuerdos regionales como el Plan Puebla-Panamá. También se presentan algunos ejemplos importantes como el sistema nacional de alarmas de maremotos en Chile, que son esfuerzos que demuestran que el desarrollo tecnológico también puede ser positivo.

En el capítulo 4 “Las consecuencias de la Tecnología contra la Seguridad y la Defensa Nacional en las expresiones del poder”. El esfuerzo principal de este capítulo es el señalar las consecuencias directas que se dan en cada expresión, fundamentalmente los aspectos más significativos, obteniendo como resultado que las expresiones política y económica pueden ser las más afectadas, la psicosocial y la militar sin embargo tienen repercusiones que atentan incluso para la consecución de los Objetivos Nacionales de los Estados. También es importante señalar la incidencia directa que tienen el poder u órgano judicial en la gran mayoría de países del hemisferio.

Para finalizar el presente trabajo de investigación, en el capítulo 5 “Conclusiones”, se trata de puntualizar los aspectos más importantes que proporcionen en el contexto de las tres premisas señaladas al inicio del resumen:

- 1.- Los avances tecnológicos como una amenaza a la seguridad y a la defensa nacional.
- 2.- Como una herramienta que favorezca a la integración del hemisferio considerando la seguridad y la defensa nacional.
- 3.- Como una disuasión para los países del hemisferio dentro del poder militar.

Por supuesto que el tema es por demás interesante, por tratarse de dos principios que son fundamentales en la gobernabilidad de un estado: La seguridad y la defensa nacional, pueden tener diferentes enfoques cuando hablamos del desarrollo tecnológico, pero se considera que el esfuerzo puesto en la elaboración de la presente monografía, puede abrir el espacio a otras investigaciones, considerando la constante evolución de la tecnología, solo basta ver en los Estados Unidos como funcionan su sistema de informática, en cuya plataforma giran, sus comunicaciones, el armamento y sus fuerzas aérea y naval.

# **CAPITULO 1**

## **INTRODUCCION**

El presente trabajo tiene por finalidad determinar como impactan los avances tecnológicos a la defensa y la seguridad nacional, desde la siguiente óptica:

- a.- Como una amenaza a la seguridad y a la defensa nacional.
- b.- Como una herramienta que favorezca a la integración del hemisferio, para enfrentar las crecientes amenazas antes mencionadas.
- c.- Como una disuasión para los países del hemisferio dentro del poder militar.

Asimismo se pretende llamar la atención en el desarrollo de capacidades de los medios técnicos específicamente en la informática y las comunicaciones, que no amenazan solamente al campo militar, sino también al económico, político y al psicosocial, presentando acciones que han ocurrido o pueden ocurrir, como el ciberterrorismo que es una posibilidad abordada seriamente por los Estados Unidos ante el uso público del Internet y la posibilidad de que grupos terroristas puedan sabotear los sistemas militares, sistemas financieros y las instituciones gubernamentales entre otros posibles blancos.

Los adelantos tecnológicos son una parte muy sobresaliente en el escenario mundial. En las postrimerías del siglo XIX y el siglo XXI la informática y las comunicaciones han pasado a ser parte importante relacionada con el proceso de la información que afecta directamente a la seguridad y la defensa nacional de un Estado.

Nuestro hemisferio por supuesto no esta excluido de eso, principalmente por ser un continente donde está la potencia dominante, los Estados Unidos, el cual por su importancia hegemónica atrae amenazas de empleo de armas de destrucción masiva o atentados terroristas, que no se limitan a las acciones del 9/11, pues el terrorismo cibernético como veremos en el desarrollo de este trabajo, ya no es una utopía. Esto puede afectar a todos los campos del poder, principalmente al económico y al político, afectando directamente la estabilidad no sólo del hemisferio sino del mundo.

Al hablar de seguridad y defensa nacional nos encontramos con un factor que trasciende las fronteras y es la base legal que garantiza que los Estados tengan las herramientas necesarias para poder emplear a las instituciones armadas, los organismos de seguridad pública y los organismos de inteligencia del estado que juegan un papel muy importante en el manejo de la información de las amenazas crecientes. Estas instituciones deben de estar fundadas en la constitución de la república o las leyes auxiliares que permitan afrontar las amenazas emergentes.

Los extraordinarios avances de la tecnología en el área de la informática y las comunicaciones sin embargo nos llevan a hacernos las siguientes interrogantes:

¿Cómo nos impactan estos avances?

¿Podremos tener la capacidad de enfrentar este tipo de amenazas?

¿Serán las leyes y las instituciones de un estado suficientes para proteger su soberanía e integridad territorial?

Todas las interrogantes anteriormente planteadas nos llevan a pensar que estamos ante un problema muy complejo, puesto que estas tecnologías tienen un altísimo costo, que para los países del hemisferio, exceptuando Estados Unidos y Canadá, son demasiado elevados y no tienen la capacidad de afrontar, si tomamos en cuenta que no estamos hablando solamente de armamento, sino de equipos de comunicaciones, informática y guerra electrónica.

Actualmente existe un amplio despliegue de servicios inalámbricos fijos y móviles, el crecimiento de la Internet en escala mundial, avances que han permitido extender la cobertura geográfica de los servicios básicos de telecomunicaciones en los países en vías de desarrollo que son acordes a las políticas de universalización de estos servicios puestos en marcha, por los gobiernos del hemisferio.

La utilización masiva del Internet por la gran mayoría de la sociedad, incluyendo las grandes esferas gubernamentales nos pone vulnerables a las acciones de los delincuentes comunes, el crimen organizado, las organizaciones terroristas y a las amenazas externas tradicionales. Todas afectan a la seguridad y la defensa nacional, por ser un concepto tan amplio para mencionar un ejemplo existen casos de hurto de información a las instituciones financieras utilizando los diferentes mecanismos técnicos que están al alcance de todos en la red, el espionaje corporativo es una realidad, el acceso a estrategias, planes e información de los depositantes es sólo un ejemplo, esto puede causar problemas en estas instituciones, pero lo más grave es la inseguridad de los usuarios de los bancos que puede crear un alto grado de desconfianza y por lo consiguiente existiría la posibilidad de que los depositantes retiren sus ahorros, creando falta de liquidez para operar y esto puede causar una crisis económica en cualquier país; por esa razón en el capítulo 3 se hace mención de casos muy graves acaecidos principalmente en los Estados Unidos, donde éstos delitos cibernéticos que son reales y han tenido su impacto en los Estados Unidos especialmente en la administración Clinton y se menciona éste país y no otro del hemisferio por existir información más clara y documentada. En este sentido existe una

vinculación directa entre una indebida utilización de estos recursos y la seguridad y la defensa nacional, en virtud de las amenazas que estos ataques traen a toda la sociedad.

Otro aspecto importante que está muy relacionado a las amenazas es la globalización por estar influyendo de manera directa en las relaciones internacionales, impactando en todo sentido, pero esto nos debe llevar a pensar que así como influyen negativamente, puede ser un gran aliado en el proceso de integración regional. Por lo que hay que considerar que también los avances tecnológicos impactan positivamente a la integridad hemisférica, un ejemplo práctico, es el plan Puebla-Panamá, que ahora puede incluir hasta Colombia, es un buen ejemplo del empleo de la tecnología de punta para fortalecer esta integración regional de mesoamérica; en ese sentido se prevé la instalación de un sistema de fibra óptica de alta capacidad intercomunicando a todos los países de esta región, que será la base para la construcción de la supercarretera de la información de Centro América, Panamá y Colombia. A través de estos sistemas se podrá mejorar la calidad y reducción del precio de los servicios telefónicos y de Internet entre los países antes mencionados, así como la gestión de acuerdos de enrutamiento de tráfico de Internet con backbones en Norteamérica específicamente en los Estados Unidos, con bases más favorables para todos<sup>1</sup>.

Lo anterior es sólo un ejemplo de lo que la tecnología puede hacer en beneficio de los países del hemisferio, otro ejemplo muy importante es el apoyo en las regiones ante los desastres naturales; la obligatoriedad de todas las personas naturales, instituciones públicas y privadas; y las entidades de cualquier naturaleza de participar en la prevención, mitigación, preparación, respuesta, rehabilitación y reconstrucción junto a la comunidad.

La base legal la podemos encontrar principalmente en la constitución de la república, las leyes auxiliares creadas para ese mismo fin, también las encontramos en los sistemas jurídicos de los diferentes países del hemisferio; los aspectos referentes a la soberanía y la integridad territorial en la mayoría de los países son referidos a las cartas magnas de los estados del hemisferio.

---

<sup>1</sup> Clovis Baptista secretario ejecutivo de la CITEI, consideraciones proporcionadas a las interrogantes efectuadas por correo electrónico dentro del proceso de investigación de la presente Monografía.

## **CAPITULO 2**

### **INFLUENCIA DE LA POLITICA DE DEFENSA DE LOS ESTADOS EN RELACION CON SUS VECINOS**

#### **2.1 La defensa y la seguridad en el hemisferio.**

Existe en el hemisferio un creciente interés por definir los conceptos de seguridad y defensa nacional para lo cual se han realizado una serie de paneles auspiciados por la OEA<sup>2</sup>, donde han desarrollado un análisis muy amplio sobre su evolución, al efectuar la recopilación de la información emitida en ese tipo de actividades se encuentran una serie de factores entre los que se pueden mencionar: la poca preparación de algunos países latinoamericanos, especialmente cuando no se maneja una política de defensa en forma adecuada, para lo cual se citan algunos casos como los siguientes:

a.- La transparencia en la formulación de la política de defensa, en el establecimiento del presupuesto y en la rendición de cuentas; esto es un concepto que refleja en gran medida el porqué de las vulnerabilidades de los estados en cuanto a su seguridad y defensa nacional, las instituciones no son fortalecidas con la adquisición de tecnología vigente, por tener presupuestos que en su mayoría cubren del 80% al 90% solamente para el pago de salarios, lo que no permite disponibilidad para las inversiones.

b.- La subordinación de las instituciones militares a las autoridades políticas constitucionales, de los diferentes países del hemisferio y a los procesos de administración pública donde se establecen las leyes del presupuesto. Las crecientes obligaciones de los gobiernos por satisfacer las necesidades de educación, salud, alimentación y trabajo, para mencionar algunos, son las causas por las cuales no se invierte en tecnología, para las instituciones armadas y de seguridad pública.

c.- La integración de la política de defensa con la política exterior, la evolución de la reforma del estado y las transformaciones de las políticas internas en el sistema nacional<sup>3</sup>

El anterior concepto es una muestra de la necesidad de que en nuestros gobiernos exista una verdadera integración dentro de las mismas carteras de estado, de lo contrario esto se convierte en un obstáculo para que las instituciones armadas mejoren sus sistemas de armas, sus medios aéreos, navales y sus equipos de comunicaciones e informática.

---

<sup>2</sup> Panel No 2 de seguridad nacional, políticas de defensa y fuerzas armadas, de la OEA 20 de Mayo de 2002 ([www.libroblancoecuador.org/panel2p.pdf](http://www.libroblancoecuador.org/panel2p.pdf))

<sup>3</sup> Profesor Thomaz Guedes Da Costa Universidad Nacional de Defensa, Washington, expositor del panel No 2, 20 de mayo de 2002. ([www.libroblancoecuador.org/panel2p.pdf](http://www.libroblancoecuador.org/panel2p.pdf))

d.- La integración operativa de las Fuerzas Armadas bajo la modernización material, administrativa y doctrinaria.<sup>4</sup> De este concepto se pueden desprender la necesidad de modernización que requieren las instituciones armadas, es importante resaltar el interés existente en los países del hemisferio por modernizar sus Fuerzas Armadas, países como México, Chile, Colombia, Ecuador, El Salvador, Perú, Brasil y Argentina, están presentando avances con planes a largo plazo para estar en condiciones de cumplir su misión constitucional, pero siempre existe el problema cuando hay una falta de definición de los nuevos niveles o grados de modernización tecnológica.

Cuando se evalúa la condición tan desigual que existe entre los Estados Unidos y Canadá, con el resto de países del hemisferio, nos damos cuenta que los avances tecnológicos impactan en gran medida a la seguridad y la defensa nacional, si lo vemos por regiones en Norteamérica a parte de las dos excepciones antes mencionadas, México, si bien es cierto tiene mucha capacidad aérea y naval, posee medios de comunicación satelital, un sistema de guerra electrónica establecido, no tiene la capacidad tecnológica de sus vecinos del norte, en Centro América anteriormente se mencionó a El Salvador por su plan de modernización de la Fuerza Armada, que están basados en los planes Arce 2000, 2005 y en proceso de autorización el 2010, obviamente por la escasez de recursos económicos será muy difícil que alcance los niveles de desarrollo tecnológico de punta requeridos, aunque por ejemplo en el área de comunicaciones e informática se han hecho grandes adelantos para modernizarla.

En el cono sur la situación es un poco mejor especialmente para Brasil, Chile, Colombia y Argentina, posiblemente Venezuela con la capacidad económica actual pueda mejorar en este sentido, pero vemos que la situación es similar a la de México cuando nos referimos a los Estados Unidos y Canadá. No están a la altura de la tecnología que estos dos países han alcanzado, principalmente los Estados Unidos y si vemos lo que pasó el 9/11, cuando se refiere a ataques terroristas todavía hay que recapacitar que no sólo la falta de tecnología en las instituciones responsables constitucionalmente, sino también a los organismos de inteligencia que requieren de tecnología para poder obtener la información que pueda prevenir a un Estado de una amenaza de esta índole.

Cuando se habla por ejemplo de los equipos de comunicaciones lo preocupante es que las organizaciones terroristas como lo fue el actual partido político de El Salvador, el Frente Farabundo Martí para la Liberación Nacional (FMLN) o como lo es actualmente las Fuerzas Armadas Revolucionarias de Colombia (FARC), tuvieron con apoyo de países como Cuba especialmente en el primer país y con una combinación de Cuba y el narcotráfico con el segundo, la capacidad de atentar

---

<sup>4</sup> profesor Thomas Guedez Da Costa. Universidad Nacional de Defensa, Washington, Idem No 3.

contra la defensa y seguridad nacional, ante vulnerabilidades para poner un ejemplo con el empleo de la guerra electrónica, especialmente por los altos costos de estos equipos.

Para poder tener una visión clara de los conceptos de seguridad y defensa nacional, se han analizado diferentes conceptos de algunos países del hemisferio que han publicado en sus libros de defensa nacional o en leyes auxiliares.

Se pueden observar muchas similitudes entre los conceptos de seguridad nacional, teniendo algunos componentes que pueden destacarse entre los cuales se encuentran los siguientes:

“Es un conjunto de medidas preventivas de distensión, disuasión, defensa y control de todo orden, que adopta un gobierno, con la finalidad de garantizar la consecución o mantenimiento de los intereses nacionales, que constituyen los objetivos nacionales permanentes, frente a cualquier crisis y contra todo riesgo potencial.<sup>5</sup>”

Sin embargo para los Estados Unidos el concepto de seguridad nacional es más amplio principalmente por su carácter de potencia mundial, el cual se enmarca dentro de lo siguiente:

“Es un término que abarca en forma colectiva las relaciones extranjeras de los Estados Unidos especialmente la condición proporcionada a cerca de:

- a.- Militares o una ventaja de la defensa sobre cualquier nación extranjera o un grupo de naciones.
- b.- Una posición extranjera favorable a las relaciones de los Estados Unidos.
- c.- Una postura de defensa capaz de resistir con éxito una acción hostil o destructiva dentro o fuera de los Estados Unidos.<sup>6</sup>

El señor Rodrigo Atria quien fungió como jefe del comité asesor de la exMinistra de la Defensa de Chile, manifestó en el año 2002, al participar en el “Panel de Seguridad Nacional, Políticas de Defensa y Fuerzas Armadas”, lo siguiente:

“Al inicio del siglo XXI el concepto de seguridad nacional es distinto al que fue hasta el fin de la guerra fría, en 1989” haciendo posteriormente el siguiente resumen:

A grandes rasgos desde la paz de Westfalia en 1648, y hasta mediar el siglo XX el mundo vivió una era centrada en la preeminencia de los actores fundamentales de las relaciones internacionales, el Estado, la nación políticamente organizada, era el actor indiscutido del escenario mundial y el objeto único de seguridad, este enfoque genérico ya no es sostenible en la actualidad. Ciertamente el Estado es

---

<sup>5</sup> General de Brigada Víctor Zabala, Secretario general del consejo de seguridad nacional COSENA (Ecuador), Idem No 4

<sup>6</sup> Definición publicada por la Agencia de Seguridad Nacional el 07 de Mayo de 2002, en el documentó" as Atended Through página 295”.

y seguirá siendo el futuro avizorable, la unidad básica del orden internacional. Sin embargo también es evidente la pérdida de preeminencia del Estado frente a actores no estatales en el sistema internacional; frente a los gigantescos volúmenes de capital que algunos de esos actores generan y mueven; frente a los variados regímenes internacionales que suponen renunciar a una parte del ejercicio de la soberanía y frente a la creciente valoración de la persona humana como objeto de seguridad.

El fin de la Guerra Fría amplió el impacto de esos elementos dando paso a la globalización particularmente de las comunicaciones y de la economía. Un fenómeno complejo e incluso contradictorio que expresa la configuración de un ambiente internacional nuevo”.

Por todo lo anterior el carácter de la respuesta a las nuevas amenazas “por que al ser diferentes en ubicación geográfica, tamaño, grado de control sobre los territorios nacionales y organismos de seguridad y de defensa, estas amenazas no afectan a los estados de la misma forma y mucho menos tienen las mismas capacidades para enfrentarlas.

Después de los atentados del 11 de septiembre del 2001 en los Estados Unidos se reorientó el debate sobre seguridad, la sola presencia de una nueva forma de terrorismo, conceptualizado como una amenaza asimétrica, dio un nuevo giro en los Estados Unidos en sus prioridades, en su agenda de seguridad con el combate contra el terrorismo como su eje.

Esto tiene diversas consecuencias, una de ellas es la aparición de nuevas coaliciones y alianzas bajo el común denominador de su combate con diferentes roles, como la contribución militar, política o ambas, esto trae de nuevo tecnología, en este caso puede fortalecer la integración hemisférica, pero como una reflexión preguntémonos entonces ¿Con qué medios podemos integrarnos?.

Cuando nos referimos a la defensa nacional, vemos que es un concepto que está establecido en los libros de defensa de los diferentes países del hemisferio y cuyo significado recoge los siguientes aspectos:

a.- Es la actitud la disposición, la integración y la acción coordinada de todas las capacidades, voluntades, recursos, fuerzas morales y materiales del Estado, ante cualquier forma de agresión o amenaza, incluyendo las de seguridad interior como los desastres naturales.

b.- Tiene por finalidad permanente garantizar la unidad, la soberanía, la independencia del Estado, la integridad territorial, el ordenamiento jurídico, la protección a la vida de la población y la de sus recursos.

c.- Se busca asegurar el logro de los objetivos nacionales, orientados especialmente para asegurar su soberanía e integridad territorial.

d.- El Estado para cumplir con su deber de proporcionar seguridad, defender o mantener sus derechos territoriales, soberanía y ordenamiento jurídico debe contar con una institución armada para garantizarla, los Estados que no cuentan con esta valiosa herramienta, están a expensas de que otros lo ayuden.

Cuando se analizan los conceptos anteriores se entiende claramente que a pesar de que todos los recursos y actividades que en forma coordinada desarrolla el Estado permanentemente en todos los campos de acción, las Fuerzas Armadas claramente necesitan para cumplir con su misión constitucional no tener tantas limitaciones con los recursos y esto incluye la tecnología en todo su sistema de armas y de comunicaciones, cuando un grupo terrorista amenazó a El Salvador por tener tropa en Irak en el año 2004, surgieron muchas interrogantes en el consejo de seguridad nacional de ese país, por la falta de recursos técnicos con los que cuentan tanto la institución armada como la policía nacional civil, para poder detectar por ejemplo coordinaciones entre estos terroristas para realizar dichas acciones. Las amenazas actualmente trascienden a las tradicionales amenazas externas, cuando vemos que la seguridad interior puede ser también vulnerada por el narcotráfico, el crimen organizado, los grupos terroristas, que en muchas ocasiones cuentan con mejor armamento y equipo de comunicaciones, que superan especialmente a las instituciones de seguridad pública, que en algunos países son parte de sus Fuerzas Armadas, ejemplo: Venezuela, Colombia y Ecuador.

En cuanto a la defensa existen factores que son muy importantes, un ejemplo es Chile<sup>7</sup>, el cual no agota su política de defensa en la protección del territorio por lo demás plenamente vigente, esta se ha enriquecido en virtud de su economía, del proceso de reforma de las instituciones políticas internacionales donde el país participa de la dinámica de la globalización y de la importancia creciente de las crisis internacionales originados en conflictos intra-estatales o en amenazas no estatales. En ese sentido la agenda de seguridad internacional de Chile es hoy más global que antes y plantea un claro desafío a la capacidad del estado chileno para elevar el nivel de su participación en la toma de decisiones internacionales.

Lo más importante de lo anterior es que existe un aspecto fundamental la dimensión internacional occidental, su política de defensa y su política exterior, ésta es de participación crítica y activa en el régimen internacional occidental de gobernabilidad articulado en torno a valores e intereses compartidos por las naciones del hemisferio; la consolidación de la democracia, la vigencia de los

---

<sup>7</sup> Rodrigo Atria exjefe del comité asesor de la exministra de defensa de Chile, expositor del panel No 2, 20 de mayo de 2002. ([www.libroblancoecuador.org/panel2p.pdf](http://www.libroblancoecuador.org/panel2p.pdf))

derecho humanos, la cooperación internacional, el apoyo al libre comercio y a los regímenes de regulación que permitan tanto un funcionamiento sano de los mercados internacionales como un desarrollo sustentable.

Para efectos de comprender la nueva dimensión que tiene ahora la defensa nacional de nuestro hemisferio ante las crecientes amenazas, se rescata de la política de defensa de Chile cuatro ámbitos que son los siguientes:

a.- La política de alcance global.

El país se encuentra interesado en el fortalecimiento de las Naciones Unidas, como la institución global de legitimidad para realizar operaciones militares. Por lo que este país se ha propuesto incrementar su participación en operaciones de paz bajo mandato de la ONU.

b.- La manutención de la paz y el desarrollo de la cooperación con nuestro continente.

c.- Los vínculos entre el Cono Sur y sus vecinos. Con Argentina se impulsa un camino creciente de colaboración político-estratégica, el que se ha mantenido pese a las dificultades que ese país atraviesa.

d.- Con Perú también está teniendo un importante incremento en la cooperación especialmente en el marco de la cooperación económica, se espera elaborar una metodología común para medir el gasto de defensa militar a la desarrollada con Argentina.

Se resaltan estos aspectos por que es importante ver como en el hemisferio existen grandes retos y se necesita crear conciencia en las necesidades de los estados de contar con todo un marco legal para poder respaldar a las instituciones armadas y de seguridad pública, que son la columna vertebral cuando hablamos de la defensa y la seguridad nacional, para responder adecuadamente a la misión disuasiva que se les confiere, por lo que las Fuerzas Armadas claramente tienen un reto, mantener un proceso de modernización para afrontar con éxito los nuevos desafíos como tener acceso a la nueva tecnología con un modesto presupuesto. Así como la de afrontar los retos de la globalización, existe un cuestionamiento sobre si ¿se considera que los conceptos de seguridad y defensa nacional se hallan disminuidos con la globalización?, al buscar una respuesta con hechos en nuestro hemisferio se encuentran dos ejemplos bastante claros, el primero es el caso de Argentina y Brasil actualmente reflexionan sobre la posibilidad de construir un libro de defensa común. Otro caso es el de Argentina y Chile que han avanzado en cuestiones antes impensadas. Incluso ahora se está definiendo una colaboración estrecha en el plano político-estratégico pese a las dificultades Argentinas. Se camina hacia una adecuación de los conceptos de soberanía y defensa a cuestiones más generales.

Hace no mucho tiempo el desarrollo estaba condicionado por la defensa y algunos proyectos quedaron relegados por ésta. Ahora las cosas han cambiado, y más que una disminución, hay una adecuación en función de intereses regionales comunes que se puede ir descubriendo.

Otra región que está teniendo avances en ese sentido es Centroamérica, la constitución de la Conferencia de Fuerzas Armadas de Centro América (CEFAC), es una muestra de ello, el grado de confianza logrado por las instituciones militares del área a pesar de los conflictos entre Honduras y El Salvador por cuestiones limítrofes y Honduras con Nicaragua por las mismas razones, han logrado crear una confianza que se refleja hacia la política exterior de estos países, un ejemplo son los acuerdos alcanzados en materia aduanera, donde Guatemala y El Salvador tienen sus fronteras abiertas y sin los tradicionales controles migratorios, el apoyo entre estos países ante los desastres naturales, ejemplo el huracán Mitch en 1998, donde después de mucho tiempo El Salvador provee ayuda por medios aéreos a Honduras y este último país a El Salvador en el 2001 con los terremotos, junto a Guatemala y Nicaragua, son ejemplos esperanzadores del entendimiento que las regiones deben tener para apoyarse mutuamente, por eso la globalización no disminuirá los conceptos de soberanía y defensa, sino por el contrario, los fortalece considerando la evolución que ha tenido en el hemisferio.

## **2.2 Los libros blancos y su importancia en la política de defensa.**

Los países del hemisferio aunque reconocen en sus diferentes leyes la necesidad de tener instituciones militares y de seguridad pública para la seguridad y la defensa nacional, principalmente en la constitución política o constitución de la república, de los diferentes Estados. Sin embargo al analizar los libros blancos de Argentina, Brasil, Bolivia, Chile, Ecuador y Perú<sup>8</sup> se puede observar que es un instrumento que proporciona un respaldo que se traduce en acciones que van encaminadas a permitir que los países expongan sus puntos de vista, objetivos y políticas en relación de la defensa, motivar la participación de la sociedad civil en asuntos de seguridad y contribuir a fortalecer las prácticas democráticas. tienen un respaldo que se traduce en acciones que van encaminadas a permitir a los países exponer sus puntos de vista, objetivos, y políticas en relación a la defensa, motivar la participación de la sociedad civil en asuntos de seguridad y contribuir a fortalecer las prácticas democráticas.

Un aspecto bastante común es la misión constitucional que tiene la generalidad de los países del hemisferio ejemplo de ello son: Guatemala, Honduras, El Salvador, Nicaragua, Colombia, Ecuador,

---

<sup>8</sup> Tomado del estudio de Daniel Atahuichi Quispe “Los Libros Blancos de Defensa”.

Es investigador de la Universidad de la Cordillera, Bolivia . ([www.cda-acd.forces.gc.ca/.../publications/research/background/doc/Defence\\_White\\_Papers\\_in\\_Bolivia\\_s.pdf](http://www.cda-acd.forces.gc.ca/.../publications/research/background/doc/Defence_White_Papers_in_Bolivia_s.pdf))

Perú, Chile, Argentina, Bolivia y Brasil, en el caso de los Estados Unidos y Canadá, lo ven desde el punto de vista de la seguridad nacional. Los diferentes estudios realizados en ese sentido recogen diversas opiniones especialmente sobre la importancia de los Libros Blancos de la Defensa de las diferentes naciones, una de las cuales es la siguiente:

- a.- Un marco de referencia que describa aspectos relacionados a la seguridad y defensa y permita explicar la visión y objetivos del gobierno y sociedad en torno al tema.
- b.- Antecedentes acerca de la definición de políticas de seguridad y defensa de un país.
- c.- Descripción de los entornos de naturaleza histórica, geográfica y estratégica sobre los que se define la política de defensa.
- d.- Marco constitucional y legal con respecto a la defensa, así como las responsabilidades de cada actor social.
- e.- Organización, proceso de toma de decisiones, roles y responsabilidades del Jefe de Estado, Parlamento, Ministerio de Defensa e Instituciones Armadas.
- f.- Aspectos operacionales, tales como reclutamiento, entrenamiento y despliegue de Fuerzas Armadas.
- g.- Información sobre capacidades, presentando indicadores básicos posibles de verificar en fuentes especializadas.
- h.- Aspectos presupuestarios, que incluyen: requerimientos, la evolución del nivel de gastos y comparación con gastos en otros sectores.
- i.- Detalle de capacidad existente y planificada, así como acuerdos y negociaciones sobre desarme.

Las Fuerzas Armadas del hemisferio han encontrado en la elaboración de los Libros Blancos de la Defensa un fundamento, muy importante para poder establecer un fomento al debate parlamentario en aspectos que van mas allá del tratamiento de temas presupuestarios al sector de defensa, pero más importante aún para los siguientes aspectos:

- a.- Fomentar el debate parlamentario en áreas que van más allá del tratamiento de temas presupuestarios al sector de Defensa.
- b.- Promover una comunicación más amplia sobre este tópico entre lo Ministerios de Finanzas, Defensa, Relaciones Exteriores, Gobierno y el mismo Jefe de Estado.

- c.- Estimular el debate acerca de misiones, despliegue y roles militares.
- d.- Incentivar el estudio y participación de sectores académicos.
- e.- Incrementar el interés de la sociedad en temas de defensa.

Tradicionalmente las Fuerzas Armadas del hemisferio han trabajado con mucho recelo en relación con las otras carteras del Estado, no existiendo una integración como la planteada por ejemplo por Chile, Ecuador y Perú, donde se están logrando avances en ese sentido que benefician el fortalecimiento de sus instituciones. Por lo que estos medios son un mecanismo que sirve para fortalecer la posición de las instituciones armadas en la búsqueda de obtener mejores presupuestos que redunden en la obtención de los recursos materiales que son los que facilitan la compra de una tecnología que esté acorde para poder enfrentar las amenazas crecientes que se tocaron en el numeral anterior. Constitucionalmente las Fuerzas Armadas y las Instituciones de seguridad pública, que es un caso particular en los países del hemisferio, donde en países como El Salvador y Guatemala, como resultado de los Acuerdos de Paz de estas dos naciones, la Fuerza Armada ya no tiene bajo su responsabilidad la seguridad pública, sin embargo vemos que en países como Colombia, Ecuador y Venezuela, las Fuerzas Armadas si la mantienen bajo su jurisdicción.

Estas variantes algunas veces lejos de ayudar a una institución armada la puede perjudicar tomando en cuenta que el monto del presupuesto a una Fuerza Armada que tenga las dos responsabilidades, no está acorde en muchos casos a la misión que tiene que cumplir. Esto se complica más cuando se tienen que considerar amenazas tan serias como los ataques del terrorismo internacional, el crimen organizado, el narcotráfico y las de origen técnico como los ataques cibernéticos que son una realidad que con el empleo del Internet pone al descubierto las graves vulnerabilidades existentes en los países latinoamericanos especialmente, aunque esta nueva amenaza puede afectar incluso a los Estados Unidos y Canadá.

La República Federativa de Brasil es uno de los países que en base a su libro de política de defensa<sup>9</sup> muy bien articulada, presenta algunos artículos que gran medida se identifican con el pensamiento del hemisferio, específicamente de los países latinoamericanos, donde claramente se pone de manifiesto algunos aspectos sobresalientes como los siguientes:

---

<sup>9</sup> Tomado del Libro [Política de Defensa Nacional 1996](#) (Traducido por el Departamento de Traducciones de la OEA), pagina de la OEA, sobre el Fomento de la Confianza y la Seguridad) Numerales del 4.3 al 4.7.

a.- El aspecto preventivo de la defensa brasileña consiste en colocar la acción diplomática en primer lugar cuando se trata de la solución de conflictos y de contar con una estructura militar suficiente como para producir un efecto disuasivo.

b.- El carácter defensivo, no quiere decir necesariamente que las Fuerzas Armadas se tengan que limitar exclusivamente a operaciones de defensa cuando se presente una situación de conflicto. En circunstancias más amplias de defensa, y a los efectos de rechazar una eventual agresión armada, el país empleará todo el poderío militar necesario para que el conflicto se resuelva en el plazo más breve y con el mínimo de daños a la integridad y a los intereses nacionales, imponiendo condiciones que propicien el restablecimiento de la paz.

c.- Es esencial el fortalecimiento equilibrado de la capacitación nacional en el campo de la defensa, con la participación de los sectores industrial, universitario y técnico-científico. El desarrollo científico y tecnológico es primordial para lograr la mayor autonomía estratégica y la mejor capacidad operativa de las Fuerzas Armadas.

d.- El poderío militar se debe basar en la capacidad de las Fuerzas Armadas, en el potencial de recursos nacionales y de reservas que se pueden movilizar, a los efectos de inhibir las posibles acciones que puedan constituir un desacato de las normas para la convivencia pacífica de las naciones.

Las Fuerzas Armadas deberán guardar relación con la postura política y estratégica de la nación y su estructura deberá ser flexible y versátil para que puedan actuar con celeridad y eficacia en distintas situaciones y lugares.

e.- Corresponde a las Fuerzas Armadas la misión que le atribuye la Carta Magna de defender a la nación cuando sea necesario, a los efectos de asegurar el mantenimiento de su integridad y soberanía. Para ello es fundamental que se perfeccione constantemente la composición de las Fuerzas Armadas, tanto en lo que se refiere a su apresto como a su utilización y, asimismo, que se racionalicen las actividades afines.

Cuando se analizan los literales antes mencionados se pueden rescatar la necesidad de un Estado de contar con instituciones armadas que sean capaces de ser disuasivas, por lo que adquiere mayor significado la política de defensa, de esta podemos determinar que los campos del poder se ven

relacionados, de ahí la importancia de que éstas sean representadas con carteras de estado que trabajen de manera integral, por eso se expone en el numeral anterior la presentación del ejemplo Chileno, porque también en base a una clara política de defensa, no se limita a la defensa de la soberanía y la integridad territorial, sino que busca mayores posibilidades de cooperación, integración y estabilidad para la región.

Las diferentes Cartas Magnas de los países del hemisferio contemplan la defensa de la nación cuando sea necesario, porque a pesar del sentimiento de integración hemisférica, los Estados siempre consideran potenciales amenazas a su soberanía e integridad territorial. La modernización, la flexibilidad, la versatilidad y la eficiencia son los objetivos que se persiguen cuando la base legal es parte fundamental en el mantenimiento de las Fuerzas Armadas del hemisferio.

La Política de Defensa Nacional, debe de ser importante para las sociedades de los países que componen este hemisferio, porque tiene como fundamento, los objetivos y los principios estipulados en las respectivas Constituciones de la República, lo cual tiene relación con la posición de los Estados en su política exterior, basada en la búsqueda de soluciones pacíficas para las controversias y el fomento de la paz y de la seguridad en el ámbito internacional.

En cuanto a los Estados Unidos y Canadá, su posición es extremadamente opuesta a la del resto del hemisferio, puesto que obedecen a intereses extra continentales, por lo que no se pueden considerar los mismos parámetros, por ejemplo la disuasión de estos países con su poderío militar va más allá de la capacidad latinoamericana.

Los recursos económicos son fundamentales para poder contrarrestar las amenazas tecnológicas que descansan principalmente en la informática, que es motivo de reacción por las diferentes potencias mundiales, en nuestro hemisferio existe una iniciativa bastante reducida sobre estos aspectos y orientadas a la educación, la formación y el desarrollo de los recursos humanos<sup>10</sup>

De la página de la OEA relacionada a la “Ciencia y la Tecnología” recogemos un apartado que enmarca muy bien la inquietud existente en el hemisferio en relación a los avances tecnológicos el

---

<sup>10</sup> Tomado de la Oficina de Ciencia y Tecnología de la OEA, infraestructura de redes (Cumbre de las Pericas, plan de acción, Miami 1994)

cual dice textualmente: “La infraestructura de la información de un país [...las telecomunicaciones, la tecnología de la información y la radiodifusión...] es un componente esencial del desarrollo político, económico, social y cultural”. Las necesidades del desarrollo de la infraestructura de la información de las Américas son inmensas”.

No se aprecia una preocupación de lo que las amenazas informáticas pueden realizar contra la defensa y la seguridad nacional de los países del hemisferio, sin embargo como se trata de enfocar en el siguiente numeral existen amenazas reales contra los mismos, en mayor o menor escala pero de mucho significado principalmente para los Estados Unidos como potencia mundial.

### **2.3 Las amenazas tecnológicas a la defensa y la seguridad nacional.**

La tecnología está teniendo un desarrollo constante que si bien está favoreciendo a las sociedades de nuestro hemisferio, también se convierte en una amenaza ante las debilidades de las economías especialmente de los países latinoamericanos, las potencias como los Estados Unidos y Canadá que son parte también del hemisferio aunque tienen diferencias muy grandes, con las economías del resto de países, son concientes de las amenazas que representan los sistemas informáticos y de comunicaciones, no solamente en el campo militar, sino también en la información que se convierte como le dijo el Señor General Gordon Sullivan de los Estados Unidos “En una moneda corriente de la victoria en el campo de batalla”<sup>11</sup>.

Esto nos mueve a pensar en el origen de estas preocupaciones y para ello al analizar los documentos escritos dentro de los Estados Unidos, encontramos las siguientes afirmaciones:

“Estamos en peligro, Norteamérica depende de las computadoras. Estas controlan la distribución de energía, las comunicaciones, la aviación y los servicios financieros. Las computadoras se utilizan para guardar información vital: desde archivos médicos hasta planes de empresas y expedientes penales. Y aunque confiamos en ellas pueden fallar ya sea debido a un mal diseño o a un control de calidad deficiente o a accidentes y lo que es todavía peor, debido a una agresión deliberada.

---

<sup>11</sup> Citado por Arthur S. Degroat, Capt. USA and David C. Nilsen, “Information and Combat Power on the Force XXI Battlefield,” Military Review 75, No 6 (November-December 1995) 56.

“El ladrón de hoy puede robar más cosas con una computadora que con un revolver. El terrorista del mañana podrá hacer mas daño con un teclado de computadora que con una bomba” <sup>12</sup>

Probablemente al leer este comentario en el año 2005, no sea un tema nuevo, sin embargo cuando analizamos que fue escrito en los inicios de la era de la informática en 1991, se puede ver el nivel de importancia que 14 años después esta tiene. Los Estados Unidos hasta hace 1998 no le había prestado tanta atención como ahora y tanto el hemisferio como los demás países del mundo se han ido adentrando de lleno en la revolución cibernética, esta tecnología es parte de nuestra sociedad y por ende en las economías de la comunidad mundial. Realmente la supercarretera de la información se ha convertido en el elemento económico vital de las naciones del hemisferio. Aunque los Estados Unidos actualmente esté liderando al mundo en la era de la informática, este país se ha vuelto especialmente dependiente de ésta tecnología, de las computadoras y de la red mundial que las conecta, ésta dependencia se ha convertido en una clara y apremiante amenaza al bienestar económico no sólo de los Estados Unidos, sino del hemisferio y del mundo, a nuestra seguridad ciudadana y a la seguridad nacional.

Las redes del mundo, que muchos llaman "ciberespacio", no saben de fronteras físicas, la capacidad cada vez mayor de conectarnos a través del ciberespacio nos deja cada vez más expuestos a los adversarios tradicionales y los emergentes. Los terroristas, los grupos radicales, los narcotraficantes y el crimen organizado pueden unirse para aprovechar la creciente serie de medios informáticos de agresión avanzados. Las agresiones cibernéticas complementarán o reemplazarán las tradicionales agresiones militares, lo cual complicará y exacerbará las vulnerabilidades que se deben prevenir y combatir. Entre los recursos que corren riesgo se encuentra no sólo la información que se almacena o que recorre el ciberespacio, sino además todos los componentes la infraestructura nacional que depende de la tecnología de la informática y de la disponibilidad oportuna de información exacta. Estos incluyen la infraestructura de las telecomunicaciones misma; los sistemas bancario y financiero; el sistema de energía eléctrica; otros sistemas de energía, como los oleoductos y los conductos de gas natural; las redes de transporte; los sistemas de distribución de agua; los sistemas médicos y de salud; los servicios de emergencia, como la policía, los bomberos y los cuerpos de rescate, y el funcionamiento del

---

<sup>12</sup> Agenda de la política exterior de los Estados Unidos de América -- noviembre de 1998, “LA DEFENSA DE LA NACION ANTE UN ATAQUE CIBERNETICO: LA SEGURIDAD INFORMATICA EN EL MUNDO DE HOY LA DEFENSA DE LA NA CION ANTE UN ATAQUE CIBERNETICO”, por el Teniente General Kenneth A. Minihan, Director de la Agencia de Seguridad Nacional de Estados Unidos (NSA)

gobierno a todos los niveles. Estos aspectos por supuesto afectarán en mayor medida a los Estados que tengan más dependencia de estos recursos, por ejemplo en el hemisferio, países como los Estados Unidos, Canadá, México, Venezuela, Colombia, Ecuador y Bolivia, poseen recursos naturales muy importantes, como el gas natural y el petróleo. Los Estados Unidos ha tenido el interés de tomar acciones que aseguren la seguridad de la información, lo cual ha significado un objetivo a alcanzar. Por esa razón el expresidente de los Estados Unidos Bill Clinton firmó el 22 de Mayo de 1998, la Directiva de Decisión Presidencial 63 (PDD-63)<sup>13</sup> sobre la Protección de la Infraestructura Crítica. En ésta señala: "Mi intención es que Estados Unidos tome todas las medidas necesarias para eliminar con prontitud cualquier vulnerabilidad significativa a las agresiones tanto físicas como cibernéticas contra nuestras infraestructuras críticas, especialmente nuestros sistemas cibernéticos. La meta nacional es que, para el año 2000, a lo sumo, Estados Unidos haya logrado una capacidad operativa inicial, y que para dentro de 5 años, a más tardar, Estados Unidos haya logrado y pueda mantener la capacidad de proteger las infraestructuras críticas de nuestra nación de actos intencionales que debilitarían considerablemente la capacidad del el gobierno federal de desempeñar las misiones esenciales de seguridad nacional y garantizar la salud y seguridad de los ciudadanos; los gobiernos estatales y locales de mantener el orden y proporcionar un mínimo esencial de servicios públicos; el sector privado de asegurar el funcionamiento ordenado del sistema económico y proporcionar servicios esenciales de telecomunicaciones, energía, financieros y de transporte.

Lo anterior deja claro que debe existir un esfuerzo nacional para lograr metas tan ambiciosas como la planteada por el entonces presidente de los Estados Unidos. Significa entonces que se necesita una cooperación muy importante entre el gobierno y el sector privado de un Estado, esto queda plenamente demostrado cuando una nación como los Estados Unidos que es la primera potencia mundial lo plantea como una meta nacional. Y es que el documento antes mencionado PDD-63 instruye al gobierno federal que dé ejemplo asegurando la confiabilidad de los sistemas federales pero también determina que el sector público no puede resolver este problema de manera unilateral.

Para los Estados Unidos<sup>14</sup> es claro que los departamentos y agencias federales dependen sobremanera de los servicios proporcionados por el sector privado: energía, telecomunicaciones, transporte, etc. Por lo tanto, la PDD prevé una Asociación Pública y Privada para desarrollar y poner en

---

<sup>13</sup> Publicación Electrónica del USIS, Vol. 3, No. 4, noviembre de 1998, ([www.usis.com/](http://www.usis.com/))

<sup>14</sup> Ídem al No 13 de la Pagina 20.

práctica un Plan Nacional de Seguridad de la Infraestructura, para resolver la amenaza del terrorismo electrónico. El punto principal radica en cómo lograr que el sector privado se comprometa con el Plan de Seguridad de la Infraestructura desde una perspectiva nacional. Debido a la gran competitividad actual, el sector privado tiende por lo general a buscar las ventajas en el mercado incluyendo la reducción de los costos operativos para aumentar las utilidades. El logro de mejores medidas de protección cibernética requerirá tanto una mayor inversión como una colaboración entre competidores. Elementos esenciales cualquier estrategia que haga que las Infraestructuras Críticas sean más fiables (resistentes) debe comprender tres elementos básicos:

a.- Una mayor protección frente a las agresiones cibernéticas, la capacidad de detectar cuándo ocurre una agresión y la capacidad de responder y recuperarse cuando una agresión ha sido detectada.

b.- La protección frente a la agresión cibernética se basa en la tecnología del cifrado de datos incluyendo las firmas codificadas digitalmente la cual proporciona servicios de autenticación, integridad, prevención de la posibilidad del repudio y privacidad y confidencialidad necesarios para garantizar la información. Quizá la mejor arma de protección contra la agresión cibernética sea la autenticación basada en la codificación digital que se emplea para dar acceso a la información.

c.- El cifrado se emplea en computadoras, en los servidores y en todas las redes para asegurar que la información referente a asuntos confidenciales de gobierno y de particulares se mantenga en esas condiciones.

La primera potencia mundial tomó las previsiones desde hace cinco años contra las amenazas que la tecnología a través de la informática podría traer, por supuesto que a diferencia de Canadá el interés de los Estadounidenses es más por la responsabilidad que éste tiene por ser el principal proveedor de los servicios de informática y todas las redes que de ella se desprenden, pero la interrogante que debemos hacernos es ¿Qué pasa con el resto del hemisferio?, y es aquí donde difícilmente podamos encontrar un Estado que esté en condiciones de contrarrestar estas amenazas.

Desde 1998 hasta la fecha los Estados Unidos han trabajado a través de muchas iniciativas de investigación tecnológica una de las cuales fue publicada por el Washington Post en el año 2003, donde textualmente escribieron lo siguiente:” El presidente de los Estados Unidos George W. Bush a firmado

una directiva secreta en la que ordena al gobierno desarrollar, por primera vez, un plan nacional que fijará cuando y como lanzar ciber-ataques contra las redes informáticas del “enemigo” según ésta información, el pentágono está actualmente preparando los planes para establecer todos los pasos necesarios para desarrollar una actuación hostil contra la infraestructura informática de un país enemigo”<sup>15</sup>. Se compara esta directiva con la existente para el uso del armamento nuclear, que establece las situaciones en las que puede utilizarse dicho armamento, la selección de objetivos que se consideren legítimos y quien debe autorizar un ataque de este tipo.

En cuanto al diagnóstico, detección y respuesta a la agresión cibernética, la tecnología no está tan avanzada ni es tan efectiva. Hoy día, Estados Unidos tiene muy poca capacidad de detectar o reconocer una agresión cibernética dirigida a las infraestructuras del gobierno o del sector privado, y todavía tiene menos capacidad de respuesta. La capacidad de identificar una agresión cibernética estratégica contra uno o varios componentes de la infraestructura crítica, y responder de un modo apropiado, es claramente un tema de seguridad nacional importante.

Uno de los factores que complica la situación es el hecho de que tradicionalmente los intrusos que interfieren con las computadoras se han considerado delincuentes que incumben a las agencias encargadas de ejecutar la ley. Cuando aparece alguno, es de esperar que se le rastree, detenga y enjuicie. Además, el sector privado no ha estado muy dispuesto a compartir información sobre algún caso de intrusión en sus sistemas computarizados, por miedo de recibir mala prensa (Vg., titulares en los diarios tales como: "Se estima en millones las pérdidas bancarias en allanamiento de computadoras" o "Piratas cibernéticos dislocan el servicio telefónico") y por la reacción del público. Para llegar a tener una capacidad de defensa nacional efectiva frente a las agresiones cibernéticas, han de crearse nuevas normas de acción recíproca que permitan la colaboración abierta y dinámica entre el sector privado, las fuerzas policiales y la comunidad de seguridad nacional.

En los Estados Unidos la Agencia de Seguridad Nacional (NSA), tiene la función en la seguridad de la información, que va más allá de la seguridad de la información de los Estados Unidos, debido a que en la era de la informática, las misiones tradicionales de esta agencia [...inteligencia de comunicaciones y seguridad de sistemas de información...] confluyen en una: proporcionar superioridad de información a Estados Unidos y sus aliados. Teniendo en cuenta este esquema, es

---

<sup>15</sup> [www.washingtonpost.com/wp-dyn/articles/A38110-2003Feb6.html](http://www.washingtonpost.com/wp-dyn/articles/A38110-2003Feb6.html)

fundamental comprender bien la Infraestructura de Información Mundial y las vulnerabilidades de los Sistemas de Información de Redes ante las agresiones cibernéticas. Desde una postura defensiva, la NSA ha llevado a cabo una serie de iniciativas para establecer la base técnica para proteger nuestras infraestructuras críticas.

Los Estados deben de integrar en sus organizaciones dedicadas a prevenir las amenazas planteadas en este numeral, como a manera de ejemplo lo está realizando Estados Unidos con la NSA, se requiere entonces que se desarrolle la tecnología necesaria para crear un sistema nacional de detección y respuesta ante una agresión cibernética, que es una debilidad en el hemisferio por carecer de los recursos necesarios, tanto técnicos como económicos.

La NSA está desarrollando un modelo que consiste en crear un sistema nacional de detección y respuesta ante una agresión cibernética. Este modelo integra una variedad de sensores que pueden colocarse en lugares críticos de la infraestructura y en la infraestructura de telecomunicaciones misma, y comprende técnicas analíticas avanzadas y de amplio alcance para proveer un panorama dinámico de cualquier amenaza a las infraestructuras críticas desde el ciberespacio mundial. Estas técnicas deben compartirse entre los diferentes componentes nacionales: los de seguridad nacional, federal, industrial y regional, para que, concurrentemente, puedan detectar, defender, reconstituir y recuperar los servicios vitales.

Sin embargo existen otros factores que también son importantes en este contexto como lo es el desarrollo nuclear que está teniendo Brasil en su esfuerzo por reducir los costos en la producción de energía; el objetivo inicial es lograr la autosuficiencia en combustible nuclear para abastecer sus propias centrales, lo que representaría un ahorro de 14 millones de dólares al año que se gastan ahora en la importación de ese insumo., en un esfuerzo conjunto con Alemania, Argentina que son fundamentales para el éxito de sus economías y su seguridad nacional. Pero también trae consecuencias para los el resto de países del hemisferio que se benefician con la compra de éste tipo de recursos naturales. Contando con grandes yacimientos de uranio, Brasil podrá en el futuro disputar el mercado mundial de materiales combustibles, que moviliza cerca de 11.000 millones de dólares al año, destacó el físico.<sup>16</sup> Además ya existen movimientos ecologistas en contra del desarrollo nuclear en Brasil y

---

<sup>16</sup> Tomado de la página Tierra América Noticias, artículo del Sr. Mario Osava, del 20 de octubre 2004. ENERGIA-BRASIL: Lucha por ingresar al club nuclear.

Argentina, como el “Seminario de Energía para Sociedades Sustentables”, en continuación del año anterior donde se había presentado la “Plataforma: Soberanía energética y Sociedades Sustentables”, organizado por CENSAT Colombia y otras organizaciones. “El Taller contra la expansión de la energía nuclear en Brasil y en Argentina” debatió las perspectivas para la expansión nuclear en Brasil y Argentina, los acuerdos bilaterales entre Argentina y Australia, Brasil y Alemania, Brasil y Francia y sus impactos para los países del MERCOSUR, financiamiento internacional para energía nuclear y estrategias para evitar la finalización de Angra III en Brasil, y Atucha II en Argentina. Otro tema discutido es “La Globalización y la necesidad de una estrategia global de energía” fue el tema de un seminario que mostró las tendencias que surgirán en la última década en el sector de energía como la concentración del mercado de energía en manos de unas pocas corporaciones transnacionales y la privatización del sector y las posibles estrategias globales para proponer políticas energéticas sustentables, con la Fundación Heinrich Böll.

#### **2.4 Influencia del desarrollo tecnológico dentro del poder militar.**

La mayor maquinaria científica y tecnológica del mundo se desarrollo bajo el auspicio de la industria militar estadounidense, a la par de los intereses de la defensa de Estados Unidos.

El gobierno estadounidense subsidió toda la investigación científico tecnológica mediante grandes contratos de investigación y desarrollo de defensa, traspasando capital fiscal a corporaciones privadas como la Boeing, la IBM y muchas otras mas, de manera que todo el caudal de tecnología que hoy circula en gran medida proviene de las subvenciones; hay que incluir toda la investigación y estudio en ciencias básicas sustentadas en universidades. Esas herramientas tecnológicas, por lo visto hoy están al servicio una amplia gama de usuarios.

Los programas de aviones de combate para los Estados Unidos por ejemplo, conseguirán la increíble cifra de US\$ 400 mil millones en nuevos contratos multianuales. Lockheed Martin obtendrá más de 225 mil millones de dólares en 12 años para construir cerca de 3.000 aviones *Joint Strike Fighter (JSF)* para la Fuerza Aérea, Infantería de Marina y Armada. Según *The Business Week*, Lockheed también espera conseguir US\$ 175 mil millones en ventas a clientes extranjeros en los próximos 25 años. El retorno del triángulo de hierro, la nueva propuesta militar 75 Sumergido en un déficit comercial record, los Estados Unidos necesitan desesperadamente un impulso para equilibrar su balanza comercial a través de las exportaciones de armas. Si el *JSF* consigue los esperados US\$ 175 mil millones en ventas de exportación, puede pasar a la historia como el mayor producto individual

para equilibrar la balanza de pagos. Actualmente Estados Unidos controla 50% del mercado global de armas, con ventas militares al extranjero que en 1999 bordearon los 16.500 millones de dólares.

La ampliación tecnológica de los horizontes político estratégicos postulados taxativamente, en una febril producción de paradigmas en competencia para comprender los cambios y el porvenir de las relaciones entre los Estados, donde brillaron Francis Fukuyama y su Fin de la Historia y el Último Hombre, y Samuel Huntington con su Choque de Civilizaciones pocos de ellos imaginaron la importancia que tendría Internet en el surgimiento, la organización y comunicación de nuevas y viejas asociaciones políticas, económicas y militares.

Internet ha creado un nuevo espacio para lo político y estratégico, entendiéndose por esto el espacio donde los actores estratégicos globales despliegan sus intereses, poder y probabilidades. Así se pasaría de una geopolítica centrada en el territorio, y en las dimensiones tradicionales del tiempo y el espacio, hacia una crono política, orientada a la dominación y control de la dimensión cero de la instantaneidad, la fuente del poder por excelencia del mundo global: la información y el conocimiento.

Los avances tecnológicos son para las diferentes Fuerzas Armadas del hemisferio un tema de vital importancia para la seguridad y la defensa nacional, principalmente para este último concepto que es la razón de ser constitucionalmente de las mismas.

Como se mencionó en el primer capítulo la disparidad existente entre las potencias como Estados Unidos y Canadá, en comparación con Latinoamérica es una brecha muy amplia, principalmente porque los presupuestos asignados a los ministerios de defensa, constantemente han ido reduciéndose, el porcentaje del producto interno bruto no pasa del 4% en el mejor de los casos. Esto influye a que solamente algunos países tengan la capacidad de desarrollar tecnología militar, los ejemplos son muy pocos, pero para tener un factor de comparación se traen a cuenta algunos países principalmente de Suramérica entre los que tenemos Argentina, Brasil, Colombia, Chile, Ecuador, y Venezuela, todos con el agravante de depender de otros países para desarrollar su tecnología especialmente en lo que se refiere a la materia prima. Obviamente no se puede hacer un factor de comparación con países como los Estados Unidos y Canadá, con el resto del hemisferio.

Al analizar los gastos militares y el porcentaje del PIB que no pasan del 4% de las respectivas naciones, se puede apreciar diferencias por la cantidad en los gastos militares, lo interesante de los datos observados es que la mayoría de países del hemisferio emplean el presupuesto para pago de salarios y muy pocos invierten en una tecnología que les proporcione una marcada superioridad con sus vecinos, principalmente porque no tienen los recursos necesarios para ello.

La tecnología contribuye a la disuasión en nuestro hemisferio, especialmente cuando se tienen los medios materiales y humanos. Se pudo visualizar como países como Ecuador y Colombia están trabajando en ese sentido, en las Ramas Aérea, Ejército y Naval. Ecuador posee una capacidad tecnológica limitada en lo que se refiere a la construcción de equipo para desarrollar guerra electrónica, maneja una empresa metalúrgica muy importante, dándole capacidad para autoabastecerse de munición sin depender tanto del extranjero. Esto aunado a la capacidad de producción petrolera le proporciona una ventaja bastante significativa o por lo menos de igualdad con sus vecinos.

Colombia también es un país que está aprovechando los recursos que está recibiendo para afrontar el conflicto armado que está desarrollando el Estado contra la organización terrorista de las Fuerzas Revolucionarias de Colombia (FARC), su inversión en la tecnología naval es muy importante con la construcción de medios navales (naves nodrizas), con capacidad de proporcionar abastecimiento logístico e incluso con capacidad ofensiva. La modificación de las aeronaves especialmente los helicópteros para traslado de tropa a helicópteros de combate le da una capacidad mayor para el apoyo aéreo a sus unidades de combate. También posee capacidad de producción de petróleo y un territorio rico en minerales, aunado a la experiencia de combate de sus fuerzas militares.

El desarrollo de la tecnología no solo está dirigido al desarrollo en el campo militar sino que actúan varios factores entre los que podemos mencionar:

- 1.- La seguridad en el ciberespacio centrada en la seguridad de las redes y en las medidas contra un ataque cibernético contra las instalaciones vitales del estado.

- 2.- La globalidad de los medios de comunicación, se orienta a desarrollar el poder sutil de los ideales americanos para atraer, influenciar y conducir a otros hacia esos intereses estratégicos.

## CAPITULO 3

### LOS AVANCES TECNOLOGICOS COMO AMENAZA A LA SEGURIDAD Y A LA DEFENSA NACIONAL.

#### 3.1 Experiencias de ataques con las nuevas tecnologías de informática.

La multinacional empresa de computadoras IBM menciona lo siguiente “El presente año será mucho peor que 2004 en el ámbito de la seguridad informática y los ataques de virus y gusanos”<sup>17</sup>. En este mismo artículo se anuncia una nueva amenaza en el informe, titulado “IBM Global Business Security Index Report”, se indica que las agendas portátiles (PDA) y teléfonos móviles se están convirtiendo en el nuevo blanco predilecto de los programadores de virus.

Lo anterior es una muestra de los peligros que se está teniendo con los avances de la tecnología, ahora no solo amenazan las PC y los sistemas de informática, que van desde el robo de información hasta el bloqueo total de los sistemas, sino también a los equipos electrónicos con tecnología de punta como los antes mencionados.

Existen antecedentes del empleo de la tecnología para la obtención de información de los sistemas informáticos que van desde la obtención de información hasta el bloqueo de los sistemas de gobiernos, de la empresa privada hasta las computadoras personales, la primera potencia mundial inclusive reaccionó ante la amenaza del terrorismo cibernético que puede parecer inofensiva, sin embargo en el año 2000 el Presidente de los Estados Unidos Bill Clinton<sup>18</sup>, ordenó la primera estrategia nacional para proteger las computadoras de la nación conectadas a la red contra los ataques deliberados, asignando \$2 mil millones de dólares para este presupuesto, esto con la intención de proteger las críticas infraestructuras gubernamentales, incluyendo iniciativas importantes como son los fondos para educación en la seguridad de información, y un programa para establecer la competencia y certificación de los actuales trabajadores de tecnología.

En Octubre del año 2001, el Presidente George W. Bush fijó a Richard Clarke como el primer Consejero de Seguridad del Ciberespacio dentro del Concilio Nacional de Seguridad. Richard Clarke que fue el primer coordinador nacional para la seguridad, protección de la infraestructura, y contraterrorismo en el 1998 se encarga de proteger las telecomunicaciones de la nación y la infraestructura contra un ataque terrorista.

---

<sup>17</sup> Diario tin.com, edición 1727 año 9 22 de Febrero 2005.

<sup>18</sup> Artículo tomado del Teklatino News Paper Advertising., Septiembre 16 de 2002.

Cuando Richard Clarke fue anunciado, él alertó a los norteamericanos haciendo ver la realidad de que la tecnología de información computarizada, desde las comunicaciones, servicios de emergencia y transportación hasta la entrega del agua y la electricidad. "Destruya las redes", dijo Clarke, "y usted cerrará América como nosotros la conocemos y como nosotros la vivimos y como nosotros la experimentamos todos los días." Al analizar esta declaración podemos ver que una economía tan importante como la norteamericana y de hecho del mundo depende de las redes electrónicas, un ejemplo de ello son los millones de mensajes y billones de dólares se transfieren vía las computadoras diariamente. Los adversarios y enemigos de América reconocen esta dependencia y están desarrollando armas para causar masiva ruptura y destrucción. Esta es una gran razón por la cual el gobierno norteamericano tiene que protegerse contra la vulnerabilidad tecnológica. Después de todo, el gobierno opera redes que son extremadamente importantes para el ejército y los funcionamientos políticos así como las comunicaciones.

El público y sector privado deben salvaguardarse contra virus que afectan y tienen la capacidad para deshabilitar la economía y la seguridad de la infraestructura corporal y gubernamental. Los últimos cuatro virus han causado más de \$12 mil millones en daños. Un virus incapacitó más de 350,000 servidores en particular. Basado en las investigaciones por la compañía Computer Economics, Inc., se estima que el impacto económico mundial de códigos malévolos (virus) fue de \$13.2 Mil millones de Dólares en el año 2001, los contribuidores más grandes fueron los virus, SirCam que ya ha costado \$1.15 mil millones, Código Rojo, \$2.62 mil millones y NIMDA, \$635 Millones.

Las bombas Lógicas, caballos troyanos, los gusanos electrónicos, los virus y otras herramientas de guerra de información son ahora el arsenal en un nuevo cálculo geopolítico con que los enemigos pueden asumir una superpotencia que ya no puede desafiarse con las armas convencionales. Ningún enemigo puede emparejar el ejército norteamericano, como quedó demostrado en la Guerra del Golfo, esto lleva a que el terrorismo cibernético se vuelva una alternativa creíble para los enemigos de los Estados Unidos. Otra experiencia que atenta contra la seguridad nacional de una nación es el Espionaje en la actualidad se estima que el 70 por ciento del valor medio de una corporación reside en la información que posee.

En 1999, las compañías del ranking Fortune 1000 reportaron un total de 45 billones de dólares en pérdidas debidas al espionaje corporativo (fuente: Trends in Proprietary Information Loss -

Tendencias en la pérdida de información confidencial, American Society for Industrial Security and Pricewaterhouse Coopers, 1999). Las tecnologías informáticas son claramente un caldo de cultivo para el robo de información confidencial o protegida utilizada por estos espías corporativos. Los directores de sistemas deben dedicar tiempo a proteger a la compañía, aplicando medidas de seguridad adecuadas para su red y estableciendo normas eficaces.

En la actualidad la empresa McAfee, ha detectado un nuevo peligro, alertó sobre la creciente amenaza de fraudes informáticos, este intento de fraude persigue que la víctima visite un enlace que simula un sitio Web oficial y realice transacciones que parecen ser legítimas. Para darles mayor credibilidad, los atacantes incluso copian imágenes, logotipos y texto de empresas genuinas para respaldar su oferta. Para ello, suelen enviar un correo electrónico al usuario como si fuera de un proveedor de servicios, solicitándole que visite dicho enlace fraudulento e ingrese sus datos confidenciales. En el mismo informe de tendencias de los ataques de fraude electrónico” de APWG (Anti-Phishing Working Group), sólo en enero de 2004 se reportaron 176 nuevos ataques de fraudes únicos, llegando a 5,7 por día. Esto equivale a un incremento de un 52% respecto de diciembre de 2003.

Por todo lo anterior se puede determinar como la mayoría de ataques de las nuevas tecnologías de informática van dirigidos hacia el sector financiero, sin embargo cada vez existe mayor certeza de la capacidad de los grupos terroristas como Al Qaeda de realizar acciones de ciberterrorismo como podemos apreciar en la siguiente declaración “Los terroristas han demostrado una gran creatividad en la elección de sus instrumentos y objetivos. Por tanto, sólo es cuestión de tiempo que tenga lugar un acto de ciberterrorismo, con esta contundencia se expresó ayer en Madrid Michele Markoff, del Consejo para la Protección de Infraestructuras Críticas del Departamento de Estado. Markoff invitó a España sumarse a la red mundial para la alerta y evaluación de la amenaza de ataques informáticos que ha puesto en marcha la Administración Bush, Washington cuenta ya con un centro nacional dependiente del FBI, que funciona 24 horas al día, pero son necesarios puntos de contacto similares alrededor del mundo”<sup>19</sup>. El objetivo es reducir los riesgos de un ataque a los programas de gestión de infraestructuras estratégicas, como electricidad agua, transportes, telecomunicaciones. O al menos minimizar sus efectos, mediante la alerta temprana cuando no pueda evitarse.

---

<sup>19</sup>Tomado del artículo “Estados Unidos teme un ataque Ciberterrorista” 20/09/2002, [cibernauta.com/ciberactual/...?articulo=3274.php](http://cibernauta.com/ciberactual/...?articulo=3274.php)

La alta funcionaria, invitada por el Círculo de Tecnologías para la Defensa y la Seguridad, subrayó que las medidas de protección adoptadas por EE UU no son suficientes, pues el creciente grado de interconexión de las infraestructuras mundiales de información sugiere que sólo estaremos tan seguros como el menos seguro de los países con los que estemos, siquiera remotamente, conectados.

España cuenta con un Centro de Alerta Temprana sobre Virus y Seguridad Informática, dependiente de Ciencia y Tecnología, pero lo que propone Washington es distinto, pues no responde tanto a la necesidad de prestar un servicio al usuario como de preservar la seguridad nacional.

Markoff explicó que ordenadores requisados en Afganistán han demostrado que Al Qaeda estaba investigando métodos para realizar ataques informáticos y buscando posibles objetivos en Estados Unidos, tras recordar un ataque perpetrado en 1998 por adolescentes contra sistemas de gestión y despliegue de las tropas norteamericanas.

La situación presentada en este artículo es muy importante, primero porque existen pruebas de que un ataque ciberterrorista puede materializarse y lo segundo porque la gran mayoría de los países no sólo del hemisferio sino del mundo buscan solamente la seguridad informática, como es el caso de España. Por supuesto que todo esto requiere de complejos sistemas de seguridad, que puede ser implementado, primero en base a una adecuada investigación informática y segundo que es lo más complicado una inversión económica muy alta. Los dos problemas son por demás complicados para los países en vías de desarrollo como los que componemos el hemisferio.

Sin embargo es importante resaltar que los Estados Unidos están conectados a través de los servidores a los países del hemisferio, por lo que debe ser importante que este país, efectúe las coordinaciones y apoyos necesarios con estos países para que estos no puedan servir involuntariamente como un puente para las organizaciones terroristas que como Al Qaeda le han declarado la guerra. De ahí que la integración, el acercamiento, la revisión de las tecnologías usadas por éstas naciones deberían ser una preocupación no sólo para ellos sino también para la primera potencia mundial, los Estados Unidos.

### **3.2 Las Empresas Transnacionales como nuevos actores al servicio de la tecnología.**

Las principales empresas en el mundo como MICROSOFT de Bill Gates, tienen el monopolio en el mundo de la Informática, sin embargo existen otras empresas que están teniendo un desempeño bastante positivo dentro del mercado, un ejemplo de ello es la fundación Mozilla<sup>20</sup>, la cual ya posee una cantidad de descargas de 25 millones en su navegador Firefox. Este navegador ya está, disponible en 28

---

<sup>20</sup> Tomado del diario TI.Com, edición 1728, 22 de Febrero de 2005.

idiomas, ha sido creado en la modalidad de trabajo voluntario y en el código abierto. El entusiasmo que genera Firefox queda de manifiesto además con la iniciativa de promoción “Spread Firefox” cuenta con 70.000 usuarios en todo el mundo.

Pero esta empresa es tan solo otra en este mercado, porque por ejemplo los servicios de comunicación MSN Hotmail<sup>21</sup>, con 7,5 millones de cuentas activas, y MSN Messenger, con más de 7 millones de internautas, han crecido cerca del 30% con respecto a enero de 2004. Dentro de este ascenso de la audiencia de la plataforma, destaca el crecimiento cercano al 30% de los servicios de comunicación online MSN Messenger y MSN Hotmail. El servicio de mensajería instantánea ha sido uno de los puntales del éxito del portal, que le ha llevado a superar la barrera de los 7 millones de usuarios a comienzos de este año. Así, 98 usuarios de mensajería instantánea de cada 100 utilizan el servicio de MSN, según datos de Nielsen//Net Ratings.

Pero, ¿porqué se resaltan estos datos como parte de éste trabajo?, principalmente para llamar la atención sobre las capacidades de una amenaza que es muy significativa en manos de grupos que buscan causar daños no solo a las instituciones financieras o comerciales, sino también a las gubernamentales, por esa razón Bill Gates a finales de los años 90 publicó el documento “La Tecnología gubernamental para el siglo XXI, el impacto de la era de la información en el gobierno y la sociedad”, en ella él advierte sobre las necesidades de los gobiernos de utilizar las innovaciones tecnológicas por medio de lo que se denomina “Sistema Nervioso Digital” (SND) amplía con mucha autoridad que “los países que cuentan con infraestructuras de tecnologías maduras y están reforzando para modernizar los existente pueden aprender de los mercados emergentes, que están implementando nuevas tecnologías como base de sus infraestructuras, a la vez que los mercados emergentes pueden aprender mucho de los mercados desarrollados, que ahora están enfocando el mejoramiento de los servicios existentes para los ciudadanos e incrementando la eficiencia de los organismos gubernamentales”.

El Sistema Nervioso Digital propuesto por Bill Gates, sirve para administrar la información de los gobiernos en sus operaciones internas, la coordinación de las compañías que hacen negocios con ellos, y la entrega de los servicios gubernamentales a la población. Hay que recordar que la Internet no solo es una amenaza por el empleo que el terrorismo, el crimen internacional o la delincuencia le pueden dar, sino también para mejorar las condiciones de vida, aprendizaje y de trabajo de los

---

<sup>21</sup> Tomado del diario TI.Com, edición 1728, 22 de Febrero de 2005.

ciudadanos, siempre y cuando los países hagan inversiones necesarias en su infraestructura. La agilización de la información para los ciudadanos, les permite además realizar operaciones en línea con los gobiernos y la información oportuna de todas partes del mundo, la información publicada para los mismos.

Si analizamos la propuesta de Bill Gates sobre el SDN, vemos que presenta argumentos muy importantes como: El uso masivo del Internet, la modernización gubernamental para el uso de modelo de modernas tecnologías, la transformación gubernamental para realizar el punto de contacto único para los ciudadanos, la inversión significativa en infraestructura de telecomunicaciones e interconexión general de la red, el uso de nuevas tecnologías para mejorar el sistema educativo en todos los niveles, aumentar las capacidades de los ciudadanos por medio de proyectos piloto, concesiones o inversiones e infraestructura y atraer inversiones de compañías de tecnología y fomentar el comercio electrónico, algunas veces con incentivos financieros pero con mayor frecuencia con proyectos corporativos que benefician a la comunidad y a las compañías de tecnología.

Toda la información anterior refleja la importancia del empleo de la tecnología en dos direcciones: para seguridad de la información manejada por los aparatos gubernamentales, como inversión extranjera y para beneficio de la población porque se transforma no sólo en una posibilidad de mejores servicios, sino también para incrementar las fuentes de trabajo tan necesarias en los países del hemisferio. La globalización exige muchos retos para los gobiernos del hemisferio, los cuales deben estar preparados para afrontar exigencias que este fenómeno les exige, entre los que se pueden mencionar los siguientes:

- a.- La protección a la propiedad intelectual.
- b.- La creación de iniciativas reglamentarias basadas en el mercado.
- c.- La protección de datos privados.
- d.- La codificación y seguridad de los datos
- e.- La reglamentación del contenido.

Estos son elementos que deben considerarse para enriquecer el sistema nervioso digital, de lo contrario los inversionistas tienen argumentos de peso para no invertir en determinados países, solamente al hablar de la propiedad intelectual, existe en el hemisferio una constante “la piratería, a la música y a las películas, especialmente en DVD”.

Este impacto en la actividad económica y social de las personas implica la utilización de nuevos mecanismos de comunicación según: comunicación, acceso remoto, transferencia de archivos y

comunicación para acceso de información. Por ejemplo las banca electrónica que es una base para que los usuarios efectúen las diferentes transacciones requieren de cierto grado de seguridad como lo demuestra MICROSOFT<sup>22</sup> “Compruebe que está realizando operaciones bancarias a través de un servidor con tecnologías de seguridad mejoradas y que, además, usa un explorador que admite cifrado de 128 bits. El cifrado traduce la información financiera en algo parecido a un código secreto que se transmite a través del Web. Los conceptos anteriores son una muestra de lo importante que son las empresas transnacionales como algunas de las mencionadas, quizás la más completa y que tiene el monopolio es MICROSOFT, ésta empresa no sólo presenta una serie de estrategias para contrarrestar las infecciones de virus sino también para los gobiernos y empresas, un ejemplo son el Programa Estratégico para Protección de Tecnología (Strategic Technology Protection Program.-STPP)<sup>23</sup>, un programa de dos fases que representa una movilización sin precedentes del personal y recursos de Microsoft para integrar producto, servicios y soporte. El programa tiene como objetivo ayudar a los clientes de Microsoft a estar y mantenerse seguros.

El hemisferio al igual que el resto del mundo tiene una dependencia de las multinacionales, en el área de la informática y de las comunicaciones, que también tienen empresas que tienen monopolios como; la HARRIS, MOTOROLA, ROHDE SCHWARZ, DATRON, pero cuál es en realidad de nuestro hemisferio en este ámbito, “el alto costo de los radios”, los cuales oscilan entre \$4,369.75 hasta los \$29,000.00 dólares. La experiencia demuestra que los equipos de comunicaciones son bastante onerosos, lo cual trae como consecuencia que los países que no cuentan con un presupuesto que les proporcione la disponibilidad para adquirir sistemas de comunicaciones con medios digitales, que ha países como los nuestros se les hace imposible adquirirlos sino es con un refuerzo al presupuesto por parte de los respectivos gobierno y posiblemente haciéndolo por fases, que pueden durar hasta 7 ó 8 años.

### **3.3 La era de la información y su impacto en los sistemas de seguridad, defensa e inteligencia.**

Las estructuras de defensa de los Estados del hemisferio se ven impactadas por los avances tecnológicos en el campo económico y político, en materia de conducción en su pensamiento, previsión y desarrollo de un conflicto. Esto da lugar a la guerra de la información un tema actual, que está ligado no sólo a la defensa, sino también a la seguridad nacional. Cuando hablamos de la guerra de la

---

<sup>22</sup> [WWW.MICROSOFT.COM](http://WWW.MICROSOFT.COM), (Seguridad, recursos de productos)

<sup>23</sup> Ídem al anterior.

información, tenemos que referirnos a los desafíos que ésta presenta, donde el procesamiento de la información se aceleró producto de los avances tecnológicos y en muchas ocasiones se escapa a los sistemas de inteligencia, como muy bien los expresa Bruce Berkowitz ex miembro del Comité de Inteligencia del Senado de los Estados Unidos, en su estudio “La inteligencia en la era de la información”<sup>24</sup>, Según éste estudio la comunidad de inteligencia necesita mayor flexibilidad, como en las instituciones privadas. El proceso de conformación de la información es de retroalimentación y no sólo en una vía, utilizando los modos de las empresas que dominan las nuevas tecnologías de la información, para alcanzar una mayor descentralización.

Los Organismos de Inteligencia tienen ante sí dos retos muy importantes; las fuentes de información y especialmente la capacitación del personal. Si hablamos de las fuentes de información es necesario revalorar la inteligencia de medios humanos y la búsqueda de nuevas fuentes de datos, como los que provienen de las señales, ambas son muy necesarias en la actualidad, porque pueden ayudarnos a descifrar la información que grupos terroristas, el crimen organizado, el narcotráfico, la delincuencia común o las amenazas tradicionales contra otros Estados nos pueden proporcionar.

En la actualidad hablamos de nuevas amenazas y estas requieren mayor atención porque pueden ser producto de señales, aquí adquiere un gran significado la guerra electrónica.

La información que de ahí se obtiene requiere de la inteligencia, ya que los datos obtenidos por medios técnicos pueden ser relativos a los sistemas electrónicos que se van a enfrentar, lo cual es una función propia de la guerra electrónica, esto da como resultado la necesidad de tener personal técnico y los recursos materiales para estar en capacidad de desarrollar las actividades de guerra electrónica, que se ejecutan pensando en buscar, interceptar, localizar, escuchar, analizar, identificar, registrar y evaluar las emisiones radioeléctricas del adversario, a fin de explotarlas en beneficio de las operaciones propias, esto relacionado con una Hipótesis Vecinal es muy difícil sin los recursos humanos y técnicos, por su alto costo, pero cuando hablamos de las amenazas antes mencionadas como el terrorismo, la situación se complica mucho más y un caso bastante palpable fue el 9/11, donde quedó claramente demostrado que esta situación ya no se trata de la guerra fría donde se contrarrestaba la amenaza con espías y satélites espías, además los actores y consumidores eran definidos; hoy en día la tecnología le proporciona a la inteligencia muchos objetivos, una información que llega a ser demasiada, para poder procesarla, presentando además diferentes niveles de confiabilidad.

---

<sup>24</sup> Berkowitz Bruce: “La inteligencia en la era de la información parcerias estratégicas 1, No 4 (Diciembre 1997)  
Tomado de la publicación de estudios estratégicos de la presidencia de la republica  
Secretaria de Asuntos Estratégicos de la Presidencia de la Republica del Brasil.

La falta de integración de los organismos de inteligencia es otra de las causas que evitan que el producto de la inteligencia sea oportuno y confiable, solamente para descifrar los idiomas empleados por los árabes, son ya un obstáculo que se maximiza con los códigos que pueden utilizar.

Muchos son los escritores que han sido exmiembros del Gobierno de los Estados Unidos o de las Fuerzas Armadas Inglesas que han llegado a la conclusión de que se tiene que reformular la inteligencia para la era de la información entre los que se encuentran Gregory F. Treverton, quien fue Vicepresidente del Consejo Nacional de Inteligencia de los Estados Unidos, investigador del Senado y luego presidente y Director de estudios de la RAND Corporation, publicó en el año 2001 “Reformulando la Inteligencia Nacional” para la era de la información (Reshaping National Intelligence for an Age Información). Por otra parte también el británico Michael Herman quien sirvió durante 35 años en el Cuartel General de Comunicaciones del Gobierno Británico y en el sistema de defensa de ese país y luego fue profesor en el King’s Collage y la Universidad de Oxford, hizo una publicación en el mismo año 2001, “Los servicios de Inteligencia en la Era de la Información”<sup>25</sup> Lo importante de esta obra estriba no solamente en la coincidencia que tiene con los conceptos presentados por el estadounidense Gregory F. Treverton, sino también porque en ella presenta un análisis de tres grandes temas que son los siguientes:

a.- La distinción entre la información general de los gobiernos y la inteligencia (la información gubernamental, de los medios masivos de comunicación, de la diplomacia, etc., frente a la inteligencia). Que es un tema muy amplio y que coincide con la información que se ha presentado cuando se habla de la gran cantidad de información disponible y aquí es donde entra precisamente la guerra de la información.

b.- El gerenciamiento de la inteligencia estratégica a nivel nacional (las fuentes de información que necesita un país, como organizarlos en un contexto internacional distinto donde los Estados Unidos ejerce un liderazgo y como se ubica la inteligencia británica en el seno de la NATO, así como la importancia de la centralización en los sistemas de inteligencia, de la inteligencia satelital y el necesario balance entre la colección y la reunión de información) y por último analiza los efectos internacionales de la inteligencia en el contexto de la política exterior (que hace la inteligencia para la seguridad internacional), proponiendo un desarrollo ético en la actividad de inteligencia en la era de la información. Lo más preocupante para nuestro hemisferio no es solamente que no tenemos los recursos materiales y humanos para enfrentar estos desafíos como la guerra de la información, sino también la

---

<sup>25</sup> “Intelligence Services in the Information Age” Frank Cass. P. London, 2001.

falta de organismos que sirvan como eje para que sus Fuerzas Armadas puedan manejar este tipo de amenazas, solamente Estados Unidos y Canadá por ejemplo son miembros de la OTAN, el resto de países son solo firmantes de un tratado como el TIAR que no tiene los mecanismos suficientes para proporcionar a nuestros Estados las herramientas para poder enfrentar con éxito las posibles amenazas que pueden ser obtenidas de los medios técnicos o de la Internet donde actualmente navegan millones, solamente en Argentina<sup>26</sup> un país que ha estado en una crisis económica muy profunda el acceso al Internet creció desde el año 2001 hasta el 2004 en un 72% de usuarios. Que pasa entonces con la capacidad de los países Latinoamericanos, Centroamericanos, México y el Caribe, para contrarrestar las amenazas que se materializan muchas veces por el Internet ¿Se tendrán los mecanismos u organismos?, no se tiene una información de estos países que se esté haciendo algo precisamente porque la red es libre.

### **3.4 El desarrollo tecnológico como posibilidad de cooperación, integración y estabilidad de la región.**

Cuando analizamos los efectos de los avances tecnológicos en el hemisferio, encontramos varios ejemplos de cómo se puede aprovechar sus ventajas para lograr su aprovechamiento en beneficio de sus respectivos países, los desastres naturales, la globalización, los tratados de libre comercio han llevado a los diferentes estados componentes de este hemisferio a lograr acuerdos regionales para poder acceder a los grandes mercados internacionales. Los Call Center son actualmente uno de los proyectos de muchos países para lograr alcanzar mayores niveles de desarrollo, para proporcionar mejores oportunidades de empleo para personas capacitadas y con dominio del Idioma Inglés, lo que ha obligado a muchos países a modificar sus sistemas educativos dando mayor énfasis a éste idioma y tomándolo como segunda lengua, empresas como DELL han intensificado sus operaciones en diferentes países de Latinoamérica como El Salvador, solicitando operadores con conocimiento del Idioma Inglés. “Este país sedujo y conquistó las miradas de los inversionistas que buscaron iniciar o expandir sus negocios en Centroamérica. Al menos, esa es la lectura que se desprende del más reciente informe sobre Inversión Extranjera Directa (IED) en Latinoamérica y el Caribe, realizado por la Comisión Económica para América Latina y El Caribe (CEPAL)<sup>27</sup>.

Al cierre de 2004, El Salvador reportó un ingreso de \$389 millones en IED, \$286 millones más que los captados en 2003. Se sitúa en una lista exclusiva de seis naciones que se destacaron por sobre el

---

<sup>26</sup> Tomado del Estudio del impacto de la Internet en la Agenda Publica,  
Del Doctor Eduardo L. D'alessio

<sup>27</sup> Documento Informativo de la Inversión extranjera en América Latina y el Caribe 2004, Marzo 2005, [www.eclac.cl/](http://www.eclac.cl/)

promedio latinoamericano, que alcanzó un crecimiento del 44%. La nómina está conformada por Trinidad y Tobago, Chile, Brasil, México y Colombia, además de El Salvador. Costa Rica, que por años se mantuvo arriba en las preferencias de los inversionistas, pasó de \$576.8 millones en 2003 a \$585 millones en 2004, un crecimiento de \$8.2 millones. Latinoamérica<sup>28</sup>, debe pasar rápido al aprovechamiento concreto de la atracción de inversiones, según comenta Michael Martimore, encargado de la investigación de CEPAL. “Es importante tratar de captar toda la inversión directa; pero no captar por captar, sino para producir cambios”, señala al agregar que la mejor manera es “atraer la inversión que busca eficiencia”. Este tipo de inversión está vinculada a los mercados tecnológicos, que supone mano de obra calificada, y por ende una necesidad como país de avanzar en la calificación del recurso humano. El país más beneficiado fue Brasil el cual está en la cima de las inversiones, Latinoamérica, en conjunto, captó más de \$56 mil millones en inversión extranjera.

Los inversionistas optaron por Brasil, fue el mayor receptor de Inversión Extranjera Directa, según el informe de la Comisión Económica para América Latina (CEPAL). Con un reporte de \$18,165 millones al cierre de 2004, contra \$10,143 captados en 2003, el país suramericano fue considerado el caso “exitoso” del estudio. “Hay que ver que ahora la mayor empresa cervecera en el mundo está en Brasil”, sostiene Michael Mortimore, encargado de realizar el informe. Mortimore hace referencia a la fusión entre la brasileña AmBev y la belga Interbrew, en una operación valorada en \$4,000 millones.

Cuando hablamos de desastres naturales podemos señalar ejemplos muy valiosos uno de los cuales es el de Chile. En todas las fases de un desastre natural tales como las tareas de prevención, la mitigación, la preparación y la alerta, requieren sistemas de comunicación muy costosos y de alta tecnología, los países identifican sus vulnerabilidades un ejemplo de ello también es el sistema nacional de alarma de maremotos de Chile (S.N.A.M.), SISTEMA NACIONAL DE ALARMA DE MAREMOTOS DE CHILE (S.N.A.M.); Chile, por su situación geo-tectónica en la Cuenca del Pacífico Sur Oriental, está incluido dentro de los países que con mayor frecuencia se ven afectados por Maremotos o tsunamis. Los efectos producidos por el terremoto del 22 de mayo de 1960 que destruyó CORRAL y CHILOE, pusieron en evidencia la necesidad de contar a nivel nacional con un Sistema Internacional de Alarma de Tsunami y proporcionar una alerta oportuna a los centros poblados del litoral e islas adyacentes del territorio nacional ante la ocurrencia de un sismo tsunamigénico. El

---

<sup>28</sup> Ídem al anterior.

Decreto Supremo N° 26 de fecha 11 de Enero de 1966 designó al Servicio Hidrográfico y Oceanográfico de la Armada (S.H.O.A.) como representante oficial de Chile ante el Sistema Internacional de Alarma de Tsunami del Pacífico, que tiene el centro de operaciones situado en el Pacific Tsunami Warning Center (P.T.W.C.), Honolulu, Hawaii, y creó el Sistema Nacional de Alarma de Maremotos de Chile (S.N.A.M.). Chile actualmente forma parte de éste Sistema Internacional e interactúa con el PTWC, para lo cual cuenta con una serie de elementos tecnológicos que le permiten monitorear principalmente la actividad sísmica y el nivel del mar en el sector de la cuenca del océano pacífico bajo su jurisdicción.<sup>29</sup>

Otro ejemplo importante de esto es el Plan Puebla-Panamá, que es una propuesta de los ocho países mesoamericanos para fortalecer la integración regional e impulsar los proyectos de desarrollo social y económico en los estados del Sur-Sureste de México y el Istmo Centroamericano. Participan en el PPP Belice, Costa Rica, El Salvador, Guatemala, Honduras, Nicaragua, Panamá, y los nueve estados del Sur-Sureste de México, Campeche, Chiapas, Guerrero, Oaxaca, Puebla, Quintana Roo, Tabasco, Veracruz y Yucatán. La región mesoamericana cubre más de un millón de kilómetros cuadrados y tiene unos 64 millones de habitantes. Aspectos como la situación ambiental tienen mucha importancia para la realización del PPP, entre las que podemos encontrar la preparación de la viabilidad ambiental y social del Proyecto del BID, Programa Vial del Plan Puebla Panamá para la competitividad y dejar sentadas las bases para tener Evaluaciones Ambientales y Sociales (EAS) homogéneas en toda la obra civil y actividad de mantenimiento bajo el Programa. Este Plan Puebla- Panamá<sup>30</sup>, presenta (8) ocho iniciativas que son la base fundamental del mismo entre las que encontramos las siguientes:

**a.- La Iniciativa de Transporte**, la cual consiste en crear una red internacional de Carreteras Mesoamericanas (RICAM), compuesta por dos corredores principales sobre el Pacífico y el Atlántico y Ramales y conexiones complementarias.

**b.- La Iniciativa Energética Mesoamericana**, ésta iniciativa tiene por objeto promover el [desarrollo económico](#) y social de los pueblos de mesoamérica, propiciando una mayor y mejor

---

<sup>29</sup> Tomado del Servicio Hidrográfico y Oceanográfico de la Armada de Chile.

<sup>30</sup> Plan Puebla-Panamá “Iniciativas mesoamericanas de proyectos 15 de Junio de 2001 ([www.iadb.org/ppp/project](http://www.iadb.org/ppp/project))

cobertura del [servicio](#) eléctrico y la conformación de mercados mesoamericanos para atraer la participación del sector privado.

**c.- Iniciativa Facilitación del Intercambio Comercial,** el objetivo de la iniciativa es contribuir a dinamizar el intercambio comercial en la región mesoamericana y aumentar los niveles de competitividad del sector productivo, mediante acciones conducentes a reducir los costos del comercio intra-regional, especialmente aquellos de naturaleza logística y financiera.

**d.- Iniciativa Desarrollo Humano,** el objetivo de esta iniciativa es generar en la Región mesoamericana, bajo un enfoque de integración regional, un entorno donde sea posible que las personas en cada etapa del ciclo de vida, desarrollen completamente sus potencialidades.

**e.- Iniciativa de Desarrollo Sostenible,** los países participantes del Plan Puebla Panamá han adoptado la Iniciativa Mesoamericana de Desarrollo Sostenible (IMDS) como el marco programático transversal para el Plan Puebla Panamá para asegurar que todos los proyectos, programas e iniciativas incorporen una adecuada gestión ambiental y promuevan la conservación y el manejo sustentable de los recursos naturales.

**f.- Iniciativa de Telecomunicaciones,** esta iniciativa busca promover una auténtica sociedad mesoamericana de información, mediante la conectividad y el aprovechamiento de las tecnologías de información y comunicaciones (TIC's) como herramientas modernas de desarrollo.

**g.- Iniciativa de Prevención de Desastres,** los objetivos generales de la iniciativa son:

Fortalecer y promover acciones y procesos de reducción del riesgo como elemento de la estrategia de desarrollo regional, y su incorporación explícita en todos los niveles de la planificación integral y sectorial, a escalas regional, nacional y local. Así como asegurar la incorporación de criterios de reducción de riesgo en las iniciativas y procesos del PPP.

**h.- Iniciativa Mesoamericana de Turismo.** El objetivo de esta iniciativa es promover en la región mesoamericana el turismo de bajo impacto que favorezca la integración y el desarrollo económico y social de los países, promueva la conservación y el manejo sostenible de los recursos naturales, disminuya la vulnerabilidad ante los desastres naturales, reconozca y respete la diversidad étnica y cultural e incluya la participación del sector, privado y de la sociedad civil.

## CAPITULO 4

### CONSECUENCIA DE LA TECNOLOGIA CONTRA LA SEGURIDAD Y LA DEFENSA NACIONAL EN LAS EXPRESIONES DEL PODER.

#### 4.1 La expresión económica.

Esta expresión es una de las más vulnerables, principalmente a los ataques cibernéticos, por la cantidad de información, operaciones, servicios bancarios, depósitos de los clientes del sistema, el espionaje industrial, robo de base de datos, robo de números de tarjetas de crédito, a los cuales pueden tener acceso, conociendo sus respectivos códigos, por esa razón, existe el 70% de los asaltos a los clientes de las Instituciones bancarias en algunos países especialmente en Centroamérica por personal de los mismos bancos para fines delincuenciales. Asimismo se debe considerar las diferentes herramientas que ya mencionamos en el Capítulo 3, especialmente el espionaje corporativo que hace mucho daño en la actualidad, existen casos en las instituciones bancarias de los países del hemisferio, por el robo de información de algunos proyectos financieros que son utilizados por otras Instituciones, lo que no se publica en los medios de comunicación por evitar que los clientes conozcan sus vulnerabilidades y se tenga un temor generalizado de efectuar sus respectivos depósitos. Lo que puede afectar el desarrollo interno de los diferentes países que componen el hemisferio y por la posible falta de credibilidad de los inversionistas extranjeros y las transnacionales, que pueden afectar el logro de los objetivos nacionales establecidos en las Cartas Magnas especialmente de los países de Latinoamérica.

Podemos hablar entonces de una amenaza proveniente de la cibernética y ya no sólo de una amenaza interna o externa, con el agravante de no poderla enmarcar en ninguna de las dos, por las características del espacio tan grande de la red. La facilidad que tienen las organizaciones terroristas, crimen organizado, narcotraficantes, para acceder a la tecnología de punta es muy alta, por lo que las posibilidades de acceder a la información confidencial que manejan los bancos sobre sus clientes se les facilita, los Hacker, los Cracker, los piratas informáticos, el espionaje corporativo, las bombas lógicas, son verdaderos peligros para las instituciones financieras y para las transnacionales, las empresas nacionales etc.

Algunos países del hemisferio por el contrario, como las Islas Caimán o Islas Canarias que además tienen otro ingrediente como lo es el secreto bancario, reciben muchas veces recursos producto del lavado de dinero, por la misma flexibilidad que tienen para recibir fondos, misma situación que presentan los bancos Suizos. Estos son factores que afectan directamente el desarrollo principalmente de los países latinoamericanos, que en muchas ocasiones no cuentan con las herramientas necesarias

para proteger la información que poseen de las empresas y las personas naturales que tienen sus depósitos bancarios.

En 1998, casi todas las 500 empresas que figuran en la famosa lista de la revista Fortune habían sido penetradas en alguna ocasión por delincuentes informáticos. El FBI estima que este tipo de delitos moviliza 10,000 millones de dólares anuales, y que solo el 17% de las compañías agredidas, estafadas o chantajeadas electrónicamente efectúan las respectivas denuncias<sup>31</sup>.

Otro factor que no es menos dañino es la piratería comercial principalmente a la industria cinematográfica y musical, esto aparentemente puede afectar a las grandes transnacionales de Hollywood en los Estados Unidos o a Sony Music, sin embargo cuando se interioriza en las consecuencias a los países del hemisferio, encontramos que estas industrias proporcionan empleos por la publicidad, turismo y el sector informal, los latinos no son la excepción, sino la principal fuente de vigencia de estos mercados, principalmente en países como México, Venezuela, Colombia, Argentina, Chile y los Estados Unidos.

#### **4.2 La expresión política.**

Esta expresión por los medios electrónicos existentes tiene una limitada seguridad se puede obtener información que se maneja en los Congresos sobre proyectos de interés nacional, tanto interna como externamente. Asimismo la gobernabilidad en muchas ocasiones puede ser afectada especialmente cuando se obtiene información herrada sobre niveles de corrupción orientadas hacia los gobiernos y especialmente contra los mandatarios, un ejemplo de ello es el constante ataque contra el presidente Toledo en Perú, el presidente Bolaños en Nicaragua, que en la mayoría de casos es provocada por la oposición interna de las diferentes naciones latinoamericanas.

Las tendencias políticas dentro del escenario nacional e internacional de un país, pueden traerle consecuencias negativas ante la opinión nacional e internacional a una nación, ya que diferentes tipos de información pueden ser enviada por Internet con el auxilio de las cámaras digitales o teléfonos celulares, en el momento en que suceden los hechos, entre los que se encuentran la corrupción, el crimen organizado, el narcotráfico y lavado de dinero, donde en muchas ocasiones han sido detectados funcionarios públicos, como miembros de éstas organizaciones. Lo que en determinado momento pueden dañar la imagen de un Estado y por consiguiente el estado de derecho. Ejemplos de este tipo de problemas han sido la caída del gobierno de Fujimori en el Perú, donde un personaje como Vladimiro Montesinos realizaba todo tipo de acciones encubiertas que al final afectaron directamente al

---

<sup>31</sup> Tomado del sitio [www.csis.org/tnt/rc/cyber.html](http://www.csis.org/tnt/rc/cyber.html), Centro Transnacional del recurso de las amenazas.

Presidente de la República y más recientemente el escándalo de las torturas contra los iraquíes, del Ejército Norteamericano, que ha puesto en entredicho la política norteamericana en el medio oriente.

La tecnología facilita la obtención de mucha información que antes la población de los países del hemisferio ignoraba, la era de la información proporciona herramientas como el Internet, al cual se tiene acceso hasta en los teléfonos celulares y agendas electrónicas.

Las variantes que pueden tener organizaciones terroristas como las Fuerzas Armadas Revolucionarias de Colombia (FARC), son muchas especialmente cuando hablamos de recursos económicos, ya que éste grupo maneja mucho dinero producto del narcotráfico, esto les facilita la obtención de medios electrónicos para obtener información de las operaciones de la fuerza pública Colombiana, lo cual obliga por ejemplo a esta nación a reforzar la seguridad de sus comunicaciones.

La corrupción que pueden tener las altas esferas políticas y militares de un Estado puede ser alta por las amenazas de estos grupos contra la familia de los funcionarios públicos y en otros casos por las grandes cantidades de dinero ofrecido a los mismos. Lo que pone en peligro la gobernabilidad de los estados, en los países del hemisferio. Asimismo los partidos políticos por lo general constantemente están tratando de sacar ventajas sobre los adversarios con información obtenida en muchas ocasiones producto de la obtención de información de los mismos integrantes de un partido político, toda la información obtenida puede ser efectuada con medios electrónicos, como lo decíamos antes los celulares, las agendas electrónicas, los Jump Drive, las cámaras digitales, han hecho que las grabadoras o las antiguas cámaras fotográficas pasen a un segundo plano y ahora la información se pase en tiempo real.

Las consecuencias políticas de las nuevas amenazas podrían conllevar a un debilitamiento del estado de derecho, a la vulnerabilidad y falta de credibilidad de las instituciones democráticas, a la ingobernabilidad, la degradación del clima de seguridad ciudadana y en general a la inestabilidad política, económica y social.

Los riesgos implícitos de la nueva situación hemisférica apuntan fundamentalmente a producir desestabilización en la gobernabilidad y estabilidad política de los estados, a la vez que una creciente sensación de inseguridad en las personas.

Ello, por cuanto las "nuevas amenazas a la seguridad", entre las que destacan las migraciones ilegales masivas; el narcotráfico, terrorismo, tráfico ilícito de armas, cibercrimen, la corrupción y sus vinculaciones con la delincuencia transnacional organizada; las enfermedades pandémicas; las

catástrofes y desastres naturales y el transporte de sustancias peligrosas, tienen consecuencias y alcances que escapan al control individual de los Estados.

Frente a ello, la cooperación interestatal es imprescindible para el desarrollo de instrumentos jurídicos apropiados a las nuevas amenazas a la seguridad hemisférica, el esfuerzo regional es necesario para hacer frente a estos peligros que afectan a todo el hemisferio. Sin embargo se puede observar muchos vacíos legales que favorecen a los diferentes actores fuera de la ley que se han mencionado. Lo que en muchos países han tenido reacciones hasta del mismo ejecutivo, como es el caso de Ecuador, donde existía una iniciativa de ley para readecuar el poder judicial a las nuevas amenazas, que al final terminaron con el gobierno del expresidente Lucio Gutiérrez.

### **4.3 La expresión psicosocial.**

En ésta expresión la amenaza más grande es la inseguridad pública, lo cual se convierte en amenaza cuando rebasa la capacidad de las instituciones responsables. Así mismo el incremento del tráfico y consumo de drogas, la escalada de hechos delictivos; especialmente el secuestro, perturban en el presente, la tranquilidad pública y crean un clima de desconfianza e inseguridad, lo cual obstaculiza el logro de los Objetivos Nacionales. Por lo que al conjugarse la informática y las comunicaciones en la tecnología encontramos una serie de medios que son de especial interés para el crimen organizado y que amenazan la estabilidad de la empresa privada y de la población en general.

Las coordinaciones que se hacen por los medios existentes en estas dos áreas están relacionadas con las áreas de la delincuencia, donde entran flagelos tales como el narcotráfico y los secuestros, existe mucha facilidad para que delincuentes bien equipados obtengan información clasificada del patrimonio de una empresa o una persona cuyos bienes provoquen secuestros o robos.

Las coordinaciones que hacen los delincuentes desde la prisión donde se encuentran es clara, muchas acciones delincuenciales se han ejecutado por cabecillas capturados, en algunos países de Centroamérica por ejemplo los grupos conocidos como “maras”, reciben instrucciones para recaudar dinero de manera ilícita, para el mantenimiento de estos grupos, pago de sobornos y pago de sicarios para asesinar hasta los mismo agentes penitenciarios, por los cabecillas capturados. Cuando las instituciones de seguridad pública obtienen los resultados de las investigaciones efectuadas, la mayoría de los resultados son los siguientes:

- a.- Empleo de teléfonos celulares y satelitales como en el caso de las FARC.
- b.- Utilización del Internet para seleccionar los procedimientos a utilizar en las acciones delincuenciales.

c.- Hasta la utilización de uno de los medios de comunicación más antiguos como el mensajero.

Como consecuencia de este tipo de acciones debidamente comprobadas, se han tenido que efectuar una serie de medidas adicionales en los penales o reclusorios a fin de evitar el acceso a los medios electrónicos antes mencionados, este tipo de regulaciones han tenido como consecuencias amotinamientos como en Guatemala, Honduras y El Salvador en Centroamérica.

#### **4.4 La expresión militar.**

En el ámbito militar las amenazas pueden desarrollarse con la obtención de información sobre las posibles alianzas con países vecinos ante un posible conflicto externo que amenace la soberanía y la integridad territorial de un Estado. Ante las situaciones planteadas en el capítulo 1 respecto a las capacidades limitadas de países subdesarrollados para proteger la información que se maneja en dependencias como: los Ministerios de Defensa, los Estados Mayores o las diferentes Unidades con el manejo de información clasificada, donde la contrainteligencia es una herramienta eficiente para la protección de documentos, instalaciones físicas y de comunicaciones. La mayoría de las instituciones armadas constantemente investigan a su personal y hace pruebas poligráficas, este tipo de procedimientos los realizan desde los Estados Unidos hasta los países suramericanos, por ser una autoprotección a la información confidencial que manejan. Sin embargo cuando apreciamos las acciones realizadas por Al Qaeda el 11 de Septiembre del 2001, nos damos cuenta que la obtención de inteligencia para detectar este tipo de operaciones requiere de un trabajo conjunto.

Cuando tocamos la defensa nacional las amenazas son más claras, sin embargo las herramientas actuales proporcionan la ventaja de poder enviar por correo electrónico diferentes tipos de documentos confidenciales de un país a otro, con accesorios como los teléfonos celulares de última generación que han evolucionado en los últimos 10 años de manera constante, con costos muy económicos y fáciles de adquirir, las agendas electrónicas y las cámaras fotográficas digitales, las cuales no se necesitan ni sacar de las instalaciones, basta con sacar la memoria que miden como máximo una pulgada y un grosor de 2 milímetros, los Jump Drive que pueden tener una capacidad de 500 Mhz y tienen también un tamaño muy fácil de ocultar. Aunque es un tema muy delicado siempre los orígenes están basados principalmente en la parte económica, la compra de voluntades del mismo personal que trabaja en las dependencias más sensitivas. Por eso cobra vigencia como se menciona anteriormente la contrainteligencia, la protección de los documentos con las contraseñas, son las soluciones más apropiadas para proteger la información valiosa que se maneja por ejemplo de operaciones militares

como lo es en el caso de Colombia, donde en la reciente visita efectuada por el Colegio Interamericano de Defensa, se pudo apreciar la cantidad de medidas de seguridad y el compartimentaje de la información que se maneja, para evitar que personal ajeno a las instituciones militares la obtenga y detecte la planificación de las operaciones militares a futuro y en desarrollo.

Sin embargo es importante mencionar que existen mecanismos como las conferencias y reuniones de los Altos Mandos de las Fuerzas Armadas de toda América, que ayudan a fortalecer la confianza mutua entre las instituciones armadas del continente y ayudan a determinar problemas que puedan ser afrontados en forma conjunta y coordinada, en virtud de que dichos problemas pudieran tener incidencias para la paz y la seguridad de los países y subregiones del hemisferio. Aspectos como la Seguridad Hemisférica, la Confianza Mutua, la Transparencia y la Defensa y Desarrollo Regional son ejemplos de los importantes temas que se discuten en estos foros y que proporcionan nuevas experiencias para las instituciones militares y de seguridad pública, para afrontar de una manera más eficiente las crecientes amenazas a la seguridad y la defensa nacional.

## **CAPITULO 5**

### **CONCLUSIONES**

1.- Se considera que el empleo de los medios electrónicos especialmente en el área de la informática y de las comunicaciones no solamente amenazan el campo militar, sino también los campos psicosocial, económico y político, lo que pone vulnerables a los países del hemisferio a los ataques del ciberterrorismo, por la falta de medios para contrarrestarlos.

2.- La política de defensa en los países del hemisferio, anteriormente no había sido considerada con la responsabilidad que actualmente se está haciendo, lo que no permitía establecer los conceptos de seguridad y defensa nacional, que sirvieran para obtener los argumentos de cara a la obtención de un mejor presupuesto para las carteras de la defensa nacional, actualmente los diferentes Estados han publicando o están en proceso de hacerlo, sus libros blancos de la defensa nacional, para concretar este esfuerzo, lo que fortalece la confianza mutua.

3.- En lo que respecta al desarrollo tecnológico existe una marcada brecha entre los Estados Unidos y Canadá, con el resto del hemisferio, producto de las grandes diferencias en las economías de estos países, la gran mayoría del hemisferio son países en vías de desarrollo, que no tienen dentro de sus prioridades, el desarrollo tecnológico, salvo ligeras excepciones como: Brasil, Chile, Argentina, Colombia y Ecuador, que hacen esfuerzos por superar estas deficiencias.

4.- El hemisferio casi en su totalidad requiere del fortalecimiento del poder u órgano judicial, para poder enfrentar las amenazas emergentes, proporcionando a las Fuerzas Armadas, la Seguridad Pública y los Organismos de Inteligencia de Estado, las leyes que respalden el accionar de las mismas, con su respaldo en la carta magna o leyes auxiliares de los diferentes países que lo componen.

5.- La globalización está incidiendo positivamente cuando se habla de los adelantos tecnológicos, por su aporte a los diferentes esfuerzos de integración y negativamente en lo que se refiere a las nuevas amenazas que utilizan la tecnología, para ejecutar acciones de terrorismo, crimen organizado, narcotráfico y delincuencia común, lo que obliga a las diferentes instituciones de los Estados a coadyuvar esfuerzos regionales para contrarrestar este flagelo.

6.- Actualmente las instituciones no están siendo fortalecidas con la adquisición de tecnología vigente. Por tener presupuestos que en su gran mayoría en un 80 ó 90%, sirven solamente para cubrir el pago de salarios, lo que limita en gran medida las capacidades de contrarrestar las vulnerabilidades, ni adquirir tecnología de punta, por lo que las instituciones deben establecer planes a largo plazo para adquisición de estos medios, como producto de un buen diagnóstico.

7.- La seguridad cibernética no había sido tocada por los países del hemisferio como una amenaza, sin embargo en la Conferencia Especial de Seguridad Hemisférica realizada en México, en octubre de 2003, inicio la concepción de un nuevo concepto de seguridad, definiendo el enfoque “multidimensional”, que dará un nuevo impulso en la búsqueda de soluciones a ésta vulnerabilidad.

8.- Es necesario reconocer que la Política de Defensa Nacional, es importante para los países que componen el Hemisferio, porque tienen como fundamento los Objetivos Nacionales y los principios estipulados en las respectivas Cartas Magnas, lo cual tiene relación con la posición de los Estados en su Política Exterior, basadas en la búsqueda de la solución pacífica de las controversias.

9.- Los adelantos tecnológicos en la aérea de la informática están dando pie a que sustituyan las tradicionales agresiones militares, por las agresiones cibernéticas, lo cual complicará y exacerbará las vulnerabilidades que se deben prevenir y combatir. Por lo que la inversión en la tecnología es una necesidad en los países del Hemisferio.

10.- Los pocos países que están desarrollando proyectos tecnológicos como Argentina, Brasil, Colombia, Chile y Ecuador, tienen como agravante la dependencia de otros países para desarrollar su tecnología especialmente en lo que se refiere a recursos humanos y materiales. Por lo que la inversión será mayor tanto por la especialización del personal como por la adquisición de la materia prima.

11.- Los adelantos tecnológicos pueden proporcionar capacidad de disuasión en el Hemisferio especialmente cuando se tienen recursos para ello, por ejemplo la capacidad de producir hidrocarburos, la capacidad nuclear, la tecnología metalúrgica, la modificación o construcción de medios aéreos o navales, equipos de guerra electrónica y la capacidad de producción de munición. Lo que puede proporcionar una ventaja significativa o de igualdad entre los países que lo tengan.

12.- Las Bombas Lógicas, los Caballos Troyanos, los Gusanos Electrónicos, los Virus, los Hacker y otras herramientas de la guerra de la información son ahora el arsenal en un nuevo cálculo geopolítico con que los enemigos pueden desafiar una superpotencia que no puede enfrentarse con armas convencionales. Lo que nos puede llevar a establecer la premisa de que a mayor tecnología puede existir un mayor terrorismo.

13.- Los diferentes países del Hemisferio tienen mucha dependencia de la tecnología que proporcionan las transnacionales, en el área de informática y las comunicaciones, el monopolio es una limitante para que estos Estados puedan desarrollar sus propios sistemas. Lo que puede ser resuelto en parte con los recursos económicos necesarios o con proyectos a largo plazo, enmarcados en fases.

14.- La guerra de la información presenta desafíos muy grandes para los organismos de inteligencia de estado, por el gran flujo de información que se obtiene por ejemplo de la Internet que sobrepasa la capacidad para procesarla y obtener un producto útil en la prevención de actos terroristas. Lo que obliga a estas instituciones a modernizarse e integrarse para disminuir su impacto.

15.- Los planes de desarrollo de los países del hemisferio son de suma importancia para poder mejorar la capacidad de desarrollo tecnológico, la iniciativa de telecomunicaciones del Plan Puebla-Panamá y el sistema de alerta temprana de Chile contra los Tsunamis son un ejemplo de ello.

16.- Se puede determinar cómo las crecientes amenazas a la seguridad y la defensa nacional son originadas principalmente por los medios electrónicos, con capacidad para la obtención de información sin ni siquiera ser percibidos por los organismos de inteligencia.

17.- Las leyes contra los diferentes delitos en muchos países del hemisferio son muy débiles y en muchas ocasiones, lejos de afectar a los delincuentes comunes, narcotraficantes o crimen organizado, los beneficia, por eso es que países como Colombia tienen que apoyarse en la extradición en el caso de los narcotraficantes para evitar que estos sean puestos en libertad por jueces que han sido amenazados o comprados.

18.- La tecnología definitivamente es muy amplia y puede ser aplicada de muchas formas, por ejemplo las pandemias, las armas de destrucción masiva, el terrorismo mismo con el empleo de dispositivos electrónicos, un ejemplo son los atentados de Madrid con el empleo de los teléfonos celulares por parte de los terroristas, obligan a los Estados del Hemisferio a considerar todas las variables y a fortalecer un sistema de inteligencia integrado por todos sus componentes.

## **BIBLIOGRAFIA**

### **REFERENCIAS BIBLIOGRAFICAS:**

- a.- Clovis Baptista secretario ejecutivo de la CITEL, consideraciones proporcionadas a las interrogantes efectuadas por correo electrónico dentro del proceso de investigación de la presente Monografía.
- b.- Panel No 2 de seguridad nacional, políticas de defensa y fuerzas armadas, de la OEA 20 de Mayo de 2002 ([www.libroblancoecuador.org/panel2p.pdf](http://www.libroblancoecuador.org/panel2p.pdf)).
- c.- Profesor Thomas Guedes Da Costa Universidad Nacional de Defensa, Washington, expositor del panel No 2, 20 de mayo de 2002. ([www.libroblancoecuador.org/panel2p.pdf](http://www.libroblancoecuador.org/panel2p.pdf)).
- d.- General de Brigada Víctor Zabala, Secretario general del consejo de seguridad nacional COSENA (Ecuador), [www.libroblancoecuador.org/panel2p.pdf](http://www.libroblancoecuador.org/panel2p.pdf), Definición publicada por la Agencia de Seguridad Nacional el 07 de Mayo de 2002, en el documentó" as Atended Through página 295".
- e.- Rodrigo Atria exjefe del comité asesor de la exministra de defensa de Chile, expositor del panel No 2, 20 de mayo de 2002. ([www.libroblancoecuador.org/panel2p.pdf](http://www.libroblancoecuador.org/panel2p.pdf)).
- f.- Tomado del estudio de Daniel Atahuichi Quispe "Los Libros Blancos de Defensa". Es investigador de la Universidad de la Cordillera, Bolivia. ([www.cda-acd.forces.gc.ca/.../publications/research/background/doc/Defence\\_White\\_Papers\\_in\\_Bolivia\\_s.pdf](http://www.cda-acd.forces.gc.ca/.../publications/research/background/doc/Defence_White_Papers_in_Bolivia_s.pdf)).
- g.- Tomado del Libro [Política de Defensa Nacional 1996](#) (Traducido por el Departamento de Traducciones de la OEA), pagina de la OEA, sobre el Fomento de la Confianza y la Seguridad) Numerales del 4.3 al 4.7.
- h.- Tomado de la Oficina de Ciencia y Tecnología de la OEA, infraestructura de redes (Cumbre de las Pericas, plan de acción, Miami 1994).
- i.- Citado por Arthur S. Degroat, Capt. USA and David C. Nilsen, "Information and Combat Power on the Force XXI Battlefield," Military Review 75, No 6 (November-December 1995) 56.
- j.- Agenda de la política exterior de los Estados Unidos de América -- noviembre de 1998, "La defensa de la nación ante un ataque cibernético: La seguridad informática en el mundo de hoy", por el Teniente General Kenneth A. Minihan, Director de la Agencia de Seguridad Nacional de Estados Unidos (NSA).
- k.- Publicación Electrónica del USIS, Vol. 3, No. 4, noviembre de 1998, ([www.usis.com/](http://www.usis.com/)).

- l.- [www.washingtonpost.com/wp-dyn/articles/A38110-2003Feb6.html](http://www.washingtonpost.com/wp-dyn/articles/A38110-2003Feb6.html).
- m.- Tomado de la página Tierra América Noticias, artículo del Sr. Mario Osava, del 20 de octubre 2004. ENERGIA-BRASIL: Lucha por ingresar al club nuclear.
- n.- Diario tin.com, edición 1727 año 9/ 22 de Febrero 2005.
- ñ.- El Teklatino News Paper Advertising., Septiembre 16 de 2002.
- o.- Artículo “Estados Unidos teme un ataque Ciberterrorista” 20/09/2002, [cibernauta.com/ciberactual/...?articulo=3274.php](http://cibernauta.com/ciberactual/...?articulo=3274.php).
- p.- Diario TI.Com, edición 1728, 22 de Febrero de 2005.
- q.- [WWW.MICROSOFT.COM](http://WWW.MICROSOFT.COM), (Seguridad, recursos de productos)
- r.- <sup>1</sup> Berkowitz Bruce:”La inteligencia en la era de la información parceiras estratégicas 1, No 4 (Diciembre 1997), Tomado de la publicación de estudios estratégicos de la presidencia de la republica  
Secretaria de Asuntos Estratégicos de la Presidencia de la Republica del Brasil.
- s.- “Intelligence Services in the Information Age” Frank Cass. P. London, 2001.
- t.- Tomado del Estudio del impacto de la Internet en la Agenda Publica,  
Del Doctor Eduardo L. D’allessio.
- u.- Documento Informativo de la Inversión extranjera en América Latina y el Caribe 2004, Marzo 2005, [www.eclac.cl/](http://www.eclac.cl/).
- v.- Tomado del Servicio Hidrográfico y Oceanográfico de la Armada de Chile.
- w.- Plan Puebla-Panamá “Iniciativas mesoamericanas de proyectos 15 de Junio de 2001 ([www.iadb.org/ppp/project](http://www.iadb.org/ppp/project)).
- x.- Centro Transnacional del recurso de las amenazas, sitio [www.csis.org/tnt/rc/cyber.html](http://www.csis.org/tnt/rc/cyber.html)

## GLOSARIO DE TERMINOS

- 1.- FMLN.: Frente Farabundo Martí para la Liberación Nacional.
- 2.- FARC.: Fuerzas Armadas Revolucionarias de Colombia.
- 3.- OEA.: Organización de Estados Americanos.
- 4.- ONU.: Organización de las Naciones Unidas.
- 5.- CEFAC: Conferencia de Fuerzas Armadas Centroamericanas.
- 6.- PDD: Directiva de Decisión Presidencial.
- 7.- NSA.; Agencia de Seguridad Nacional.
- 8.- CENSAT.: Centro Nacional Salud Ambiente y Trabajo.
- 9.- MERCOSUR.: Mercado Común del Sur.
10. - JSF: Joint Strike Fighter.
11. - PIB: Producto Interno Bruto.
- 12.- IBM.: Internacional Bussines Machine.
- 13.- PDA.: Personal Digital Assistant.
- 14.- PC.: Personal Computer.
- 15.- NIMDA.: Es virus muy dañino, se desconoce el significado de las siglas.
16. - APWG: Anti-Phishing Working Group.
17. - FBI: Buro Federal de Investigations.
18. - SDN: Sistema Nervioso Digital.
- 19.- OTAN.: Organización del Tratado del Atlántico Norte.
- 20.: NATO.: Organización del Tratado del Atlántico Norte.
- 21.- CEPAL.: Comisión Económica para América Latina.
- 22.- SNAM.; Sistema Nacional de Alarma de Maremotos de Chile.
- 23.- SHOA.: Servicio Hidrográfico y Oceanográfico de la Armada.
- 24.- PPP.: Plan Puebla Panamá.
- 25.- BID.: Banco Interamericano de Desarrollo.
- 26.- EAS.: Evaluaciones Ambientales Sociales.
- 27.- IMDS.: Iniciativa Mesoamericana de Desarrollo Sostenible.
- 28.- TIC.: Tecnología de información y Comunicaciones.