REPÚBLICA DEL ECUADOR

INSTITUTO DE ALTOS ESTUDIOS NACIONALES
UNIVERSIDAD DE POSTGRADO DEL ESTADO

ESCUELA DE ESTUDIOS ESTRATÉGICOS Y SEGURIDAD
MAESTRÍA EN SEGURIDAD Y DEFENSA

LAS POLÍTICAS REGIONALES SOBRE ATAQUES INFORMÁTICOS Y SU INCIDENCIA EN LA VULNERABILIDAD DE LA DEFENSA DE LA UNASUR EN EL PERÍODO 2009-2013

Tesis de Grado para optar
al Título de Magíster en Seguridad y Defensa

AUTOR: DANIEL ACACIO QUINTERO RODRÍGUEZ
DIRECTOR: LESTER CABRERA TOLEDO

QUITO, JUNIO DE 2014

INSTITUTO DE ALTOS ESTUDIOS NACIONALES
SECRETARIA GENERAL

No. 043-2014

ACTA DE GRADO

En la ciudad de Quito, a los seis días del mes de junio, del año dos mil catorce, **DANIEL ACACIO QUINTERO RODRIGUEZ,** portador de la cédula de ciudadanía: V-14268417, **EGRESADO DEL PROGRAMA DE MAESTRÍA EN SEGURIDAD Y DEFENSA,** se presentó a la exposición y defensa oral de su Tesis, con el tema: **"LAS POLÍTICAS REGIONALES SOBRE ATAQUES INFORMÁTICOS Y SU INCIDENCIA EN LA VULNERABILIDAD DE LA DEFENSA DE LA UNASUR EN EL PERÍODO 2009-2013",** dando así cumplimiento al requisito, previo a la obtención del título de: **MAGÍSTER EN SEGURIDAD Y DEFENSA.**

Habiendo obtenido las siguientes notas:

Promedio Académico:	9.23
Tesis Escrita:	9.47
Grado Oral:	9.68
Nota Final Promedio:	9.46.

En consecuencia, **DANIEL ACACIO QUINTERO RODRIGUEZ,** ha obtenido el título mencionado.

Para constancia firman:

iaen Instituto de Altos Estudios Nacionales
La Universidad de Postgrado del Estado

De conformidad con la facultad prevista en el estatuto del IAEN, **CERTIFICO** que la presente es fiel copia del original

Fojas 01
Fecha 06/06/2014
Secretaria General

Mgs. Leonardo Jaramillo
PRESIDENTE DEL TRIBUNAL

Mgs. José Luis Castillo
MIEMBRO

Mgs. Lesly Muñoz
MIEMBRO

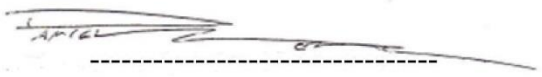
Ab. Anabela Vallejo V.
DELEGADA DE SECRETARÍA GENERAL

Av. Amazonas N37 - 271 y Villalengua (esq.) * Telf: 2464-201 / 2457-763 / 2260-002 / 2260-008 * Telefax: 2436-519 * Casilla 17-17-219
www.iaen.edu.ec RUC: 1768120520001 e-mail: infoiaen@ iaen.edu.ec

AUTORIA

Yo, Daniel Acacio Quintero Rodríguez, Cédula de Identidad venezolana número 14.268.417, declaro que las ideas, juicios, valoraciones, interpretaciones, consultas bibliográficas, definiciones y conceptualizaciones expuestas en el presente trabajo; así cómo, los procedimientos y herramientas utilizadas en la investigación, son de absoluta responsabilidad del autor de la Tesis.

Quito, junio, 2014



FIRMA DEL AUTOR

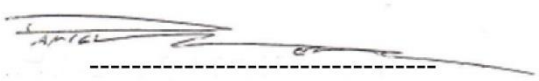
DANIEL ACACIO QUINTERO RODRÍGUEZ

CI.V: 14.268.417

AUTORIZACIÓN DE PUBLICACIÓN

Autorizo al Instituto de Altos Estudios Nacionales la publicación de esta Tesis, de su bibliografía y anexos, como artículo en publicaciones para lectura seleccionada o fuente de investigación, siempre dando a conocer el nombre del autor y respetando la propiedad intelectual del mismo.

Quito, junio, 2014



FIRMA DEL AUTOR

DANIEL ACACIO QUINTERO RODRÍGUEZ

CI.V: 14.268.417

RESUMEN

Los ataques informáticos (ciberataques) entendidos como acciones enmarcadas en una «*ciberguerra*» se han convertido en una amenaza importante para los Estados, organizaciones regionales y alianzas militares, ya que sus repercusiones van más allá del ámbito de la Defensa. En vista del rol importante en el sistema de integración a nivel regional, y el papel protagónico en el expectro mundial de la UNASUR, que avanza en la consecución de «*una identidad suramericana en materia de defensa*» (CDS, 2008), la dinámica geopolítica mundial representa una serie de desafíos estratégicos a los países componentes de la misma, que podrían convertirse en Estados vulnerables ante la amenaza de «*ciberataques*». Este estudio tomará como punto de partida la Declaración de Santiago de Chile en el año 2009 cuando se crea el Consejo de Defensa Suramericano (CDS), que definió cuatro ejes a desarrollar, teniendo especial interés para esta investigación: «las Políticas de Defensa; y la Industria y Tecnología de la Defensa» (CDS, 2010). La delimitación temporal concluye en el año 2013, en vista que en dicho período hay tres marcos referenciales; Primero: la propuesta primigenia sobre «*Defensa Cibernética*» enmarcada en el literal 1.f de los Planes de Acción 2012/2013 del Consejo de Defensa Sudamericano; Segundo: la decisión de creación del mega anillo de fibra óptica para la región sudamericana; y Tercero: el Pronunciamiento presidencial de Paramaribo y su propuesta sobre «*Defensa Cibernética*». La coherencia y pertinencia de este estudio dentro de la Maestría en Seguridad y Defensa, recae en la necesidad de analizar los aportes estratégicos, legales, normativos, y teóricos impulsados desde el «CDS» para erigir una visión sudamericana que contrarreste ataques cibernéticos que vulneren la Defensa Regional.

Descriptores: ciberataques, ciberguerra, Defensa, Unasur, estrategia, Consejo de Defensa Suramericano, amenaza, vulnerabilidad, identidad, y política de Defensa.

DEDICATORIA

- A la República Bolivariana de Venezuela por brindarme la oportunidad de cursar estudios superiores y por confiarme la digna tarea de representar a nuestra Patria.

- A la República del Ecuador y su Pueblo que supo darme cobijo en su seno como un hijo durante este periplo de más de dos años.

- A todos quienes partieron a la inmortalidad en estos últimos años y que son ejemplo perenne que nos animan a seguir adelante con principios y dignidad.

- A mis seres queridos Francisca (Abuela), Ramona (Madre), Acacio (Padre), Nathalie y David (hermanos), y demás familiares y amigos que contribuyeron con su apoyo incondicional y aliento permanente a la consecución de esta meta.

- A Luz mi Esposa y Víctor mi Hijo que con su amor infinito, entrega desinteresada y sacrificio personal fueron el pilar fundamental para sustentar anímicamente este emprendimiento.

AGRADECIMIENTO

- A la Fundación Gran Mariscal de Ayacucho (FUNDAYACUCHO) que colaboró y apoyó institucionalmente nuestras actividades y realizó un seguimiento constante para garantizar las mejores condiciones durante nuestra estadía en tierra ecuatoriana.
- Al personal docente, administrativo, y obrero del Instituto de Altos Estudios Nacionales del Ecuador (IAEN) que con su gentileza, hermandad y profesionalismo contribuyeron destacadamente en el período de formación que permanecimos en dicha casa de estudio.
- Al Centro Nacional de Desarrollo e Investigación en Tecnologías Libres (CENDITEL) ente adscrito al Ministerio del Poder Popular para Ciencia, Tecnología e Innovación de la República Bolivariana de Venezuela por apoyar mi postulación y brindarme la colaboración institucional para emprender este proceso formativo.
- A las diferentes instituciones como la Unión de Naciones Sudamericanas, el Centro de Estudios Estratégicos, y el Ministerio de Defensa Nacional del Ecuador, especialmente a Pablo Celi, Michelle Fiol, y el Doctor Pedro Sassone por tener la amabilidad de dedicar su tiempo y experiencia para enriquecer este trabajo.
- A las compañeras y compañeros de Maestría con quienes forjamos una gran amistad, especialmente a mis compatriotas Wilmer Herrera, Pedro Lanza, Magaly Villasmil, y José Ruíz que siempre tuvieron extendida su mano solidaria, y demostraron su profunda hermandad.
- Al Profesor Lester Cabrera que con su gran calidad profesional y personal supo orientar este emprendimiento investigativo de forma exitosa.

Índice

Contenido **pag.**

«[…] *Repito mi absoluto convencimiento de la identidad de causa en los americanos que poseídos únicamente del amor patrio deben pensar sólo en combatir los enemigos y en llevar adelante la marcha de la independencia*».
Quito 01 de febrero 1823

Antonio José Francisco de Sucre y Alcalá. Gran Mariscal de Ayacucho

INTRODUCCIÓN

Esta investigación buscará estudiar las políticas y estrategias conjuntas emprendidas durante el período 2009-2013 por la Unión de Naciones Suramericanas (UNASUR) para contrarrestar la amenaza de Ataques Informáticos (ciberataques) que pudieran vulnerar o afectar la Defensa Regional. La inquietud para desarrollar esta disertación se origina en la dimensión absoluta que las tecnologías han desplegado sobre los distintos sectores que componen la sociedad, como acota Caro (2013): «Al igual que la llamada telaraña mundial o *World Wide Web*, inventada sólo hace un par de décadas, ha ido evolucionando, también lo han hecho las amenazas a que se enfrenta» (Caro, 2013: 2). En este sentido, los análisis estratégicos siempre deben marchar en paralelo con las reconfiguraciones o surgimiento de las amenazas para poder delinear su proyección hacia la Defensa. Cuando Fred Cohen se aventuró a enunciar un rasgo desconocido de la computación como eran los virus, las concepciones militares arraigadas en 1984 no advirtieron inicialmente el impacto estratégico, precisando el investigador: «Definimos "virus" de computadora como un programa que puede 'infectar' a otros programas modificándolos para incluir una copia posiblemente evolucionada de sí mismo» (Cohen, 1987: 23). Estas apreciaciones de Cohen en su momento parecían limitarse a una caracterización técnica sobre asuntos informáticos civiles, pero la asimilación teórica fue lo que condujo a que en diferentes países se empezara a hablar de «*ciberamenazas*» y sobre el conjunto estratégico que es la «*ciberguerra*».

Si a la variable técnica precedentemente expuesta se añade la tendencia global a la que Sudamérica no escapó, donde la población y sus instituciones empezaron a interactuar estrechamente con sistemas cibernéticos, al punto que Castells (2004) describía esta relación como: «la extensión y el acrecentamiento del cuerpo y la mente de sujetos humanos en redes de interacción potenciadas por tecnologías microelectrónicas de comunicación operadas por software» (Castells, 2004: 7), entonces estamos en presencia de un campo de estudio, que

remite a dos hechos: primeramente desde mediados de los años ochenta del siglo pasado ya se había señalado con detalle la existencia de sistemas intrusivos como los «*virus informáticos*», y en segunda instancia el uso extensivo a lo interno de los Estados de estas redes informáticas desvela: una exposición tecnológica, junto a la potencialidad de una amenaza. Partiendo de esto, se evaluarán los planteamientos estratégicos desarrollados desde la UNASUR ante ataques informáticos, con el fin de bosquejar los elementos que contribuyen a la vulnerabilidad en materia de Defensa Regional, que no implica exclusivamente enunciados técnicos, ni precisiones operativas; por el contrario es ahí donde se profundizará teóricamente para definir los rasgos regionales con respecto al «*teatro de la guerra*» y las premisas políticas en el marco del Consejo de Defensa Sudamericano (CDS) que se hayan trazado para examinar escenarios informáticos, procurando comprender sobre que ámbito enfoca la UNASUR los temas cibernéticos: Seguridad o Defensa.

Es importante destacar que este proceso investigativo se fundamentará en un análisis estratégico, que extraerá los principios del pensamiento militar clásico, contemporáneo y moderno para establecer las redefiniciones que en los ámbitos de Defensa ha producido el ingrediente tecnológico, que se relaciona al panorama expuesto por los estrategas chinos Liang y Xiangsui: «Podemos anticipar que cada modificación importante o una extensión del espacio de batalla del futuro dependerá de si un determinado tipo de invención tecnológica, o un gran número de tecnologías en combinación, puede crear un nuevo espacio tecnológico» (Liang & Xiangsui, 1999: 42). Conforme a lo explicado, esta tesis puntualizará sobre ese contexto mundial en temas cibernéticos que muestra como un grupo de potencias militares y actores estatales han desarrollado teóricamente conceptos como: «*ciberguerra*», «*ciberestrategia*», «*ciberpoder*», que les han permitido desplegar capacidades superiores a la mayoría de los Estados, buscando establecer cuál es la apreciación regional que permita visualizar analíticamente estos escenarios y proponga alternativas estratégicas.

CAPÍTULO I

1. MARCO METODOLÓGICO

1.1. Aproximación al Tema

Ante lo diversificado e integral de la «*ciberamenaza*», las teorías y conceptos sobre la guerra que se venían pregonando durante años debieron pasar por una reingeniería profunda. El camino ascendente de los ataques cibernéticos desde 1980[1] en adelante condujo a una mirada acuciosa de los Estados, que lidiaban con hechos que no eran asimilados con facilidad. Muestra de ello es lo sucedido en 1988 cuando se: «creó en Bulgaria el Dark Avenger, el primer virus polimórfico y stealth (invisible) de la historia [...] varios antivirus detectaban el Dark Avenger, pero no podían descubrir los 512 bytes escritos aleatoriamente en el disco, ya que estos nunca eran los mismos por el hecho de tener una estructura polimórfica» (Campàs, 2007: 24-25). Este carácter polimórfico, virtual e inmaterial son una muestra de cómo los Estados se vieron en la necesidad de moldear nuevas concepciones de Defensa, tomando como referencia la tecnología y la asimetría para intentar adaptarse a la vorágine que representaban los nuevos desafíos cibernéticos que hacían complicado este abordaje, ya que gobiernos, estudiosos y militares no atinaban a ubicar estos temas entre la seguridad interna o bajo competencia de las Fuerzas Armadas. Derivándose lo previo entre otros motivos porque: «La entidad atacante puede ser un Estado o de un agente no estatal, […] si el atacante es una entidad no estatal, es poco probable que presente la mayoría de los casos un objetivo para el Estado que se defiende devolviendo el golpe en contra» (Libicki, 2009: 117). De esto último surge una constante asimétrica para hacer la valoración estratégica

[1] La literatura especializada en informática remontan los primeros virus computacionales al año 1981: Programa CLDNER autorreproduc. para Appel II, Programa parásito indetectable para Appel II (Vílchez, 2000: 110).

sobre las amenazas cibernéticas, que se ha afianzado en las temáticas de Defensa desde mediados del siglo XX, al respecto plantea Urzúa (2003) que:

> La estrategia asimétrica se organiza, piensa y aplica métodos, tecnologías, valores y perspectivas del tiempo, en forma totalmente diferentes a sus oponentes, con el propósito de maximizar sus propias ventajas, explotar las debilidades del adversario, quitarle la iniciativa y ganar libertad de acción (Urzúa, 2003: 215).

Esa asimetría que puede ser usada desde un sencillo dispositivo cibernético, expuso a serias vulneraciones a la Defensa de los Estados, contribuyendo a la constitución de oficinas civiles o comandos militares encauzados en proveerlos de sistemas y unidades informáticas de ataque y defensa, encaminándose los gobiernos a la instauración: «de medios de seguridad especializados en ciberdefensa para reducir las amenazas y las vulnerabilidades de los mismos, aunque siempre considerando que existe la posibilidad de que sean vulnerados» (Sánchez, 2013: 123).

En definitiva, los temas informáticos dejaron de ser abordados como excentricidades, ya que paulatinamente esta amenaza trascendió la afectación de individualidades, en vista que: «El ciberespacio está ligado prácticamente a todos los sectores de nuestra economía. Penetra en nuestro sistema de transporte, nuestro poder y las redes de energía, nuestros sistemas de emergencia, y nuestros programas militares» (Rosenzweig, 2013: 3).

En el ámbito económico los ciberataques han producido serios daños que tienden en algunos casos a la afectación de otros sectores indirectamente, apuntando García (2013) que los mismos tienen un: «impacto de 400.000 millones de dólares (305.000 millones de euros) en la economía mundial. Más que el tráfico de drogas» (García, 2013: 2). Como se puede apreciar el contexto de la «*ciberamenaza*» se fue engrandeciendo, hacia espacios estratégicos (políticos/económicos/energéticos), y su potencial bélico empezó a valorarse, advirtiendo Olson (2012) que es viable: «La idea de usar la guerra cibernética para atacar a un blanco

imprevisto, tales como los recursos estratégicos» (Olson, 2012: 70). De hecho, en el año 2007 expertos estadounidenses del Laboratorio Nacional de Idaho experimentaron con ataques informáticos sobre una planta de energía, arrojando el examen que: «El ataque puso al generador fuera de control y, finalmente provocó la autodestrucción, lo que fue alarmante para el gobierno federal y la industria eléctrica sobre lo que podría suceder si tal ataque se llevara a cabo a una escala mayor» (Harrison, 2012: 6). El ex secretario de Defensa estadounidense León Panetta, en el año 2012 señaló que la magnitud de la «*ciberamenaza*» representaba una preocupación creciente para la nación norteamericana, sugiriendo:

> Los escenarios más destructivos implican que actores cibernéticos lancen varios ataques a nuestra infraestructura crítica de una sola vez, en combinación con un ataque físico en nuestro país. Los atacantes también podrían tratar de desactivar o degradar los sistemas militares críticos y redes de comunicación. (U.S. Department of Defense, 2012).

Este discurso del alto funcionario norteamericano coloca al ciberespacio en la palestra de la lucha hegemónica por el poder, ya que han sido continuas las acusaciones mutuas por parte de las grandes potencias (China/Estados Unidos) sobre incursiones o sabotajes informáticos, al punto que el Diario Oficial del Ejército Popular de Liberación de China, ha hecho públicos serios cuestionamientos a las acusaciones de Washington, entre las que destaca las del investigador Wang Xinjun, quien expresó: «A pesar de que es de sentido común que no se puede determinar las fuentes de los ataques cibernéticos sólo a través de las direcciones IP, algunas personas en el Pentágono todavía prefieren creer que son de China, ya que siempre tienen un sentido de la rivalidad» (Chinese People's Liberation Army, 2013).

1.2. Planteamiento del Problema

El escenario internacional, tras el fin de la «Guerra Fría» ha desembocado en una multidimensionalidad de los conflictos bélicos: aspectos étnicos, religiosos, y tecnológicos

son facetas muchos más visibles del panorama que deben enfrentar los países en el siglo XXI. La dinámica global ha dado pie a un nuevo regionalismo que se afianza en diferentes partes del mundo como una respuesta al unilateralismo de los Estados Unidos. En Sudamérica, particularmente con la constitución de la UNASUR se ha dado el primer paso para un proceso de posicionamiento del subcontinente como un factor relevante en las relaciones internacionales mundiales, según Pereira de Lima (2010):

> Esta coordinación política está guiada por unos principios políticos del multilateralismo y el derecho internacional para así reforzar el papel de América del Sur como un actor global. La práctica del multilateralismo es un instrumento en la construcción de un nuevo orden internacional, más justo e igualitario, con reflejos en el ámbito social. (Pereira de Lima, 2010: 159).

No obstante, la avanzada bélica que vive el planeta en estos momentos, coloca a la UNASUR en su condición de actor político planetario como un blanco de posibles ataques o sabotajes tecnológicos. La reciente publicación por parte del Centro de Excelencia en Ciberdefensa Cooperativa de la Organización del Tratado del Atlántico Norte (OTAN) del llamado «*Manual de Tallínn*» (Tallinn Manual on the International Law Applicable to Cyber Warfare), elaborado por expertos mundiales con la finalidad de exponer los pormenores legales en materia de Derecho Internacional sobre la Ciberguerra, es una prueba fehaciente de los avances conceptuales en relación a la región. En el mismo sentido, el gobierno de Obama aprobó en el año 2012 la llamada «*Presidential Policy Directive 20*» que busca determinar los parámetros para que los órganos militares o de inteligencia ejecuten ciber-operaciones. La existencia de estos instrumentos que tienen trazas de extraterritorialidad, colocan a la comunidad internacional ante una disyuntiva amenazante, ya que:

> Las implicaciones de lo que está en juego - es decir, si un ciberataque dado podría ser considerado un acto de guerra - es inevitable de acuerdo en que la claridad y el rigor

> del concepto son fundamentales no sólo para la seguridad jurídica, como también para que los responsables políticos puedan elegir la opción más adecuada en caso de un ciberconflicto (Teixeira, 2012: 55).

En tal sentido, para comprender el fondo investigativo de este estudio, hay que llamar la atención del hecho que: «no se puede ser vulnerable si no se está amenazado y no existe una condición de amenaza para un elemento, sujeto o sistema si no está expuesto y es vulnerable a la acción potencial que representa dicha amenaza» (Cardona, 2001: 2). Un exiguo desarrollo de las políticas sudamericanas para contrarrestar la amenaza de ataques informáticos, con respecto a los avances estratégicos adelantados en instrumentos de corte teórico como el «Tallinn Manual» u operativos en el caso de la «Presidential Policy Directive 20» repercutirían en la vulnerabilidad de la región, ya que se vería seriamente afectada la Defensa de la UNASUR, al no tener planes para direccionar las acciones pertinentes ante eventos informáticos. Como complementa Sánchez (2013): «es necesario que, previamente, los gobiernos y los actores gubernamentales se hayan decantado por desarrollar planes de contingencia que sean adecuados y probados […] que debe depender directamente del departamento encargado de la seguridad cibernética» (Sánchez, 2013: 117). La concomitancia entre la Amenaza: «Ataque Informático» y la Vulnerabilidad: «Defensa de la UNASUR», ponen en evidencia una problemática estratégica que podría subvertir a la unidad subregional. Por lo tanto, los desarrollos de planes subcontinentales, deben trascender las medidas clásicas de Defensa, como apuntan Rantapelkonen, y Salminen (2013):

> La ciberestrategia común si los países no comparten un objetivo común, es difícil desarrollarla como actividad cibernética sostenible. Los desafíos cibernéticos no varían según el país y por lo tanto, hay una necesidad de una cooperación más amplia.

> Una posibilidad es el desarrollo de una ciberestrategia común. (Rantapelkonen & Salminen, 2013: 12).

El transitar hacia la consecución de una «*ciberestrategia*» sudamericana, requeriría adaptarse a la integralidad que representan los ataques cibernéticos, y determinar hasta qué punto se: «cuenta con infraestructura de información crítica, requerida para mantener la operación y gobernabilidad» (Cano, 2011: 5). Es por ello, que la finalidad de esta investigación es estudiar los procesos políticos y estratégicos que en la UNASUR se están desarrollando para afrontar este teatro bélico, así como las implicaciones de las políticas sudamericanas en este escenario «virtual», buscando establecer la vulnerabilidad de la Defensa Regional en el contexto de la UNASUR ante las «*ciberamenazas*».

1.2.1. Pregunta Central

¿Cuál es la relación entre las políticas regionales sobre ataques informáticos y la Defensa de la UNASUR?

1.2.2. Preguntas Complementarias

- ¿De qué manera los Ataques Informáticos representan una amenaza para la Defensa Regional de la UNASUR?

- ¿Cuáles son los planteamientos estratégicos desarrollados desde la UNASUR para contrarrestar ataques informáticos que vulneren la Defensa Regional?

- ¿Cuáles son las falencias en materia de Defensa Regional que influyen en la vulnerabilidad de la UNASUR ante la amenaza de ataques informáticos?

1.3. Justificación de la Investigación

La región sudamericana ha tenido fuertes lazos de dependencia tecnológica en la fase posterior a su independencia, acentuándose los mismos en el siglo XX, y parte del XXI,

generando la adquisición de tecnología civil y militar de fuentes externas y privativas una vulnerabilidad para la Defensa local y regional. Es de interés académico abordar en esta investigación las políticas regionales, que se están construyendo entre el conjunto de países de la UNASUR para definir la estrategia unificada ante la posibilidad de un escenario de «*ciberguerra*», que tiene una alta probabilidad como explica Rosenzweig (2013): «Cada minuto, se envían más de 168 millones de mensajes de correo electrónico. Eso es 88 billones de mensajes al año, y todos y cada uno de ellos es un vector de amenaza potencial y fuente de una intrusión de *malware*» (Rosenzweig, 2013: 24). Circunscribiendo la vista a Sudamérica, se podrían enunciar que estadísticas recientes, demuestran que el promedio de ataques informáticos en escenarios complejos superan los ciento de miles, como reportó el Consejo Nacional Electoral (CNE) del Ecuador, según su vicepresidente Raúl Salazar, la página web del organismo comicial recibió ochocientos mil (800.000) «intentos no permitidos de instrucción o penetración» (AVN, 2013) durante los comicios presidenciales, estando en presencia de un fenómeno social/tecnológico/político/militar que amerita ser estudiado para comprender la visión subcontinental que se tiene al respecto.

Si bien, actualmente los países integrantes de la UNASUR impulsan el desarrollo del anillo de fibra óptica con una extensión de 10 mil kilómetros para disminuir la vulnerabilidad con respecto al secreto de los datos oficiales y militares, aun son escasos los avances en política cibernética regional. Mientras la potencia hegemónica continental (EE.UU.), desde hace años diagramó cómo lograr el control del ciberespacio, al punto que define la superioridad ciberespacial como: «El grado de predominio en el ciberespacio por una fuerza que permite una conducción segura, confiable de las operaciones, relacionada con sus fuerzas de tierra, aire, mar y espaciales en un tiempo dado y en el marco de las operaciones sin la interferencia prohibitiva por un adversario» (Taylor & Carter, 2010: 13). Por ende, el estudio planteado ayudará entre otros aspectos, a conocer la amenaza de un ataque cibernético, junto

a las implicaciones para la Defensa Regional, y cuál es el papel que desarrolla el Consejo de Defensa de la UNASUR en temas cibernéticos (Ataque/Defensa), proporcionando información que será útil para gobiernos y ministerios de Defensa sobre las aportaciones y falencias en un área como la «ciberguerra». Por otra parte, la investigación contribuirá académicamente a contrastar desde una visión estratégica el contexto sudamericano, para arrojar aportes que sirvan para futuros debates sobre el tema en cuestión. Asimismo, dentro de las líneas de investigación estipuladas en la Maestría en Seguridad y Defensa por el IAEN, la presente tesis se enmarcará específicamente en la octava línea: «Estructura organizacionales para la Seguridad y la Defensa», pero teniendo un vínculo con la quinta: «Tecnología y escenarios estratégicos prospectivos». La investigación es viable, pues se dispondrán de entrevistas a personal de la UNASUR y otras instituciones, así como del apoyo de fuentes bibliográficas, hemerográficas, y electrónicas.

1.4. Hipótesis

Dentro de la construcción teórica y conceptual producto del proceso de investigación, el diseño de la hipótesis ha emanado de los enunciados propuestos en el planteamiento del problema que se nutre de la bibliografía consultada para erigir el marco teórico. La reflexión en torno a las disertaciones de académicos y estudiosos de la Estrategia nos presenta un crisol de propuestas y análisis que han decantado las variables que se contrastarán y estudiarán. En el armazón lógico que aquí se desarrolla, se ha seguido un hilo conductor que conecte la integralidad de ítems para que confluyan en la hipótesis. En tal sentido, se propone como hipótesis de investigación de este trabajo: **La carencia[2] de una política y estrategia**

[2] Se usa la acepción «carencia», según su definición "1.f. Falta o privación de algo" (RAE).

regional sobre ataques informáticos aumenta la vulnerabilidad[3] de la Defensa de la UNASUR.

1.5. Objetivos de la Investigación

En el entendido que esta investigación pretende estudiar las políticas regionales sobre ataques informáticos y su incidencia en la vulnerabilidad de la Defensa de la UNASUR en el período 2009-2013, tanto el objetivo general como los específicos estarán centrados en buscar las respuestas pertinentes que contribuyan a dilucidar los aspectos conceptuales, teóricos, y hechos relevantes que coadyuven a clarificar el «*iter*» investigativo que se transitará. Por tanto, en vista de lo complejo de la problemática que se intenta desarrollar, se toman los objetivos de investigación como «piedras angulares» que eviten distanciamientos del planteamiento del problema original y den congruencia a los tratamientos analíticos.

1.5.1. Objetivo General

Estudiar las políticas y estrategias de la Unión de Naciones Suramericanas (UNASUR) para contrarrestar la amenaza de Ataques Informáticos (ciberataques) que vulneren o afecten la Defensa Regional en el período 2009-2013.

1.5.2. Objetivos Específicos

- Determinar de qué manera los Ataques Informáticos representan una amenaza para la Defensa Regional de la UNASUR.
- Evaluar los planteamientos estratégicos desarrollados desde la UNASUR para contrarrestar ataques informáticos que vulneren la Defensa Regional.
- Analizar las vulnerabilidades en materia de Defensa Regional ante un Ataque

[3] Se usa la acepción «vulnerabilidad», según su definición "1. adj. Que puede ser herido o recibir lesión, física o moralmente." (RAE).

Informático (ciberataque) a la UNASUR.

1.6. Tipo de Investigación

Evidentemente las técnicas e instrumentos deben estar íntimamente ligadas a la teoría general, siendo el sustento teórico en esta tesis la Estrategia, que da una plenitud interpretativa, en razón que: «la estrategia limita con la política y con el gobierno, o, más bien, pasa a ser ambos a la vez, y, como hemos observado antes, éstos tienen más influencia sobre lo mucho o lo poco que ha de hacerse que sobre cómo ha de realizarse» (Clausewitz, 2002: 100). En concordancia con esto, se plantea un diseño de investigación integral que se apoyará en técnicas cualitativas: «que aluden a aquellas que nos permiten obtener datos que luego serán interpretados hermenéuticamente» (IAEN, 2012: 18). Precisamente una de las ventajas propias de este tipo de enfoques y técnicas estriba en que:

> [...] en el proceso de investigación cualitativa los investigadores pueden combinar distintas técnicas de recolección de información. Es más, para el investigador la posibilidad de disponer de diferentes tipos de datos, recogidos simultanemanete o en diferentes momentos, constituye un aporte significativo para el proceso de triangulación de fuentes (Yuni & Urbano, 2005: 171).

Esa triangulación contribuirá a la articulación de los enfoques exploratorios, correlacionales o explicativos, con el fin de especificar y analizar las políticas regionales sobre ataques informáticos, y su incidencia en la vulnerabilidad de la Defensa de la UNASUR. En una de las obras de mayor referencia metodológica que tiene como autores a Roberto Hernández, Carlos Fernández y Pilar Baptista titulada «Metodología de la Investigación» se hace una explicación de la aplicabilidad de los mismos y su mutuo enriquecimiento para un proceso investigativo:

> Las investigaciones que se están realizando en un campo de conocimiento específico pueden incluir los tipos de estudio en las distintas etapas de su

> desarrollo. Una investigación puede iniciarse como exploratoria, después ser descriptiva y correlacional, y terminar como explicativa (Hernández, Fernández & Baptista, 1997: 69).

Para la consecución de los objetivos investigativos debe existir una relación consistente entre metodología y la teoría, en vista que: «La metodología debe tener coherencia con los postulados teóricos escogidos, con el objeto de estudio y con parámetros éticos. Su aplicación se realiza a través de técnicas, las mismas que pueden combinarse y utilizarse según el modelo de investigación que se plantea» (IAEN, 2012: 18). Precisamente la metodología cualitativa y la Estrategia como enfoque teórico dan una globalidad analítica, que permitirá acoplar el conjunto de variables propias de los ataques informáticos, de hecho algunos estrategas coinciden en la importancia de esa visión ampliada o conjunta, como reflexionaba Mao Zedong: «Estudiar las leyes de la dirección de la guerra que rigen una situación de guerra en su conjunto, es tarea de la estrategia» (Mao, 1976: 198).

Se encaminará esta investigación al uso de técnicas e instrumentos que permitan componer un análisis estratégico, pero entendiendo que estos fundamentos generales no deben ser tomados como un grillete teórico o metodológico, ya que las amenazas cibernéticas o la ciberguerra carece de profundidad teórica en relación a otros estudios, es por ello que parte de esta investigación recaerá en la exploración temática, entendiendo que: «Los estudios exploratorios se efectúan, normalmente, cuando el objetivo es examinar un tema o problema de investigación poco estudiado o que no ha sido abordado antes» (Hernández, Fernández & Baptista, 1997: 70). Particularmente en Sudamérica los estudios estratégicos en ciberguerra cuentan con una mora investigativa, esto no es sólo falta de interés, sino que representan una dinámica compleja, como analiza Liang & Xiangsui: «Con respecto a la tecnología en sí, cada tecnología tiene aspectos específicos, que por lo tanto, significa que cada una tiene sus límites de tiempo. La que Ayer era "alta" es muy posiblemente que sea

"baja", mientras que lo "nuevo" de hoy en día, a su vez se convertirá mañana en "viejo"» (Liang & Xiangsui, 1999: 17). Por tanto, hacer un análisis sobre un campo que es cambiante constantemente y con características desconocidas ha disuadido a muchos de emprender mayores desarrollos.

No obstante, si bien esta trabajo tiene una estructura predominantemente exploratoria, también se aprecian semblantes propios de un emprendimiento descriptivo, concordando con la definición de Dankhe (1986): «Los estudios descriptivos buscan especificar las propiedades importantes de personas, grupos, -comunidades o cualquier otro fenómeno que sea sometido a análisis» (Dankhe, 1986 citado en Hernández, Fernández & Baptista, 1997: 71). Concretamente, desenvolverá este estudio una revisión general sobre las políticas de la UNASUR pero se centrará específicamente en las nociones que maneja el Consejo de Defensa Sudamericano (CDS) y el Centro de Estudios Estratégicos de Defensa (CEED) en políticas con relación a las amenazas cibernéticas, requiriendo apoyarse para esto en los elementos propios del método descriptivo para enlazarlo con la disertación estratégica del marco teórico.

Por otra parte, en la actualidad la obsolescencia tecnológica coloca en una posición vulnerable a las fuerzas de Defensa, en vista que las «*ciberamenazas*» evolucionan constantemente y esto presenta tres escenarios que afrontan los Estados: la adquisición de tecnología militar por parte de proveedores externos; la puesta en marcha de centros de investigación regionales que estén en capacidad de articular con la industria de Defensa; y finalmente el obviar la amenaza limitando la Defensa a la convencionalidad tradicional. Como se ha referido, además de explorar y describir se hace necesario el correlacionar la amenaza con la vulnerabilidad, que no radica enteramente en lo técnico sino en lo político y estratégico, siendo necesario complementar los dos enfoques anteriores con la técnica explicada a continuación: «La utilidad y el propósito principal de los estudios

correlacionales son saber cómo se puede comportar un concepto o variable conociendo el comportamiento de otra u otras variables relacionadas» (Hernández, Fernández & Baptista, 1997: 73).

Este engranaje tripartito permitirá conducir satisfactoriamente el diagnóstico estratégico, que llevará el debate entre pensadores actuales, funcionarios regionales, y estrategas clásicos, que lejos de contradictorio es enriquecedor remitiéndonos a Van Creveld (1983): «es un error creer que algo se puede aprender sólo de los casos cuyas circunstancias son más o menos similares, y que por ejemplo todo lo ocurrido antes de la invención de la máquina de vapor, del tiro rápido de rifle, automóviles, tanques, aviones, armas nucleares o de misiles balísticos por lo tanto, es irrelevante» (Van Creveld, 1983: 560). Es decir, las herramientas conceptuales propias de los estrategas no se desfasan, por el contrario pueden complementar investigaciones actuales sobre asuntos cibernéticos en donde el fondo teórico es aun insuficiente, especialmente en Sudamérica.

El tener un cuerpo lógico desde la perspectiva estratégica guía el diálogo no siempre armonioso entre lo que se enfoca teóricamente y lo que se recaba con los instrumentos, dando fortaleza al organismo investigativo, cuando Clausewitz advertía: «Afirmamos, en consecuencia, que la guerra no pertenece al terreno de las artes o de las ciencias, sino al de la vida social. Es un conflicto de grandes intereses, resuelto mediante derramamiento de sangre, y solamente en esto se diferencia de otros conflictos» (Clausewitz, 2002: 75), estaba reflejando que el hecho bélico es inmanente a lo social. Si no se liga uniformemente los tres enfoques metodológicos, con los escenarios político/estratégico en materia de Defensa sudamericana donde interviene la variable tecnológica, se desmembraría el cuerpo social figurado por Clausewitz. La ciberguerra no deja de ser social por su condición técnica, ya que en ella también pueden estar presentes los intereses y el derramamiento de sangre que avizoraba el prusiano en el siglo XIX.

El hacer investigaciones sociales partiendo de la Estrategia, constituye un reto metodológico, ya que representa para el investigador una construcción dinámica, que es compleja, y obliga a profundizar en fondos conceptuales, ya que: «Esta vez, la tecnología parece estar corriendo por delante del pensamiento militar. Si bien ningún pensador militar aún ha presentado un amplio concepto del campo de batalla, la tecnología está haciendo todo lo posible para ampliar el campo de batalla contemporáneo hasta un grado que es virtualmente infinito» (Liang & Xiangsui, 1999: 41), este razonamiento de los militares asiáticos es concluyente para percibir que se requiere de todo el entramado metodológico que se ha expuesto para canalizar la propuesta teórica estratégica.

1.6.1. Técnicas e Instrumento

Las técnicas e instrumentos que se utilizarán en la presente investigación serán las siguientes:

A) Entrevista: en esta tesis se emprenderán un conjunto de entrevistas que en concordancia con la metodología aquí expuesta se hará conforme a lo que se ha denominado en ciencias sociales la «entrevista cualitativa», en este sentido Tarrés (2001) orienta sobre los pormenores de la misma:

> La entrevista cualitativa proporciona una lectura de lo social a través de la reconstrucción del lenguaje, en el cual los entrevistados expresan los pensamientos, los deseos y el mismo inconsciente; es, por tanto, una técnica invaluable para el conocimiento de los hechos sociales, para el análisis de los procesos de integración cultural y para el estudio de los sucesos presentes en la formación de identidades. (Tarrés (ed.), 2001: 68).

La utilización de la entrevista tendrá como objetivos establecer una interacción activa con el experto consultado, que estará centrada en temáticas estratégicas como: Regionalismo, Política Sudamericana, Soberanía, Vulnerabilidad, Amenaza Informática, y Ciberguerra, a la luz del enfoque tecnológico en el contexto sudamericano, en el entendido que hay una

conjugación entre cada elemento, conforme lo describía Mao: «La relación entre el todo y la parte se refiere no sólo a la relación entre la estrategia y la campaña militar, sino también a la relación que hay entre la campaña militar y la táctica» (Mao, 1976: 199). Ese sentido de relacionamiento apuntado anteriormente es el que debe existir entre la teoría y la técnica, considerándose que dentro de la entrevista cualitativa es la tipología «semiestructurada» la más precisa para formular la guía de entrevista que se realizará a investigadores, académicos y personal de la UNASUR. Como aclara Bemard (1988): «Así en la entrevista semiestructurada, el entrevistador mantiene la conversación enfocada sobre un tema particular, y le proporciona al informante el espacio y la libertad suficientes para definir el contenido de la discusión» (Bemard, 1988: 204-207 citado en Tarrés (ed.), 2001: 76-77). Las entrevistas que se tienen planteadas realizar son las siguientes:

- Michelle Fiol (Asesora del Gabinete del Ministerio de Defensa Nacional del Ecuador)
- Pablo Celi (Subdirector del Centro de Estudios Estratégicos de Defensa de la UNASUR)
- Pedro Sassone (Representante diplomático de la República Bolivariana de Venezuela ante la Secretaría General de la UNASUR)

B) Análisis de documentos: esta investigación requerirá de un importante aporte documental, que deberá hacer revisión de oficios, directrices, propuestas y acuerdos emanados de la UNASUR, CDS y CEED, para comprender la dimensión de esta fuente hay que remitirse a lo expuesto por Erlandson (1993):

> Los documentos incluyen prácticamente cualquier cosa existente previa a y durante la investigación, incluyendo relatos históricos o periodísticos, obras de arte, fotografías, memoranda, registros de acreditación, transcripciones de televisión, periódicos, folletos, agendas y notas de reuniones, audio o videocintas, extractos presupuestarios

> o estados de cuentas, apuntes de estudiantes o profesores, discursos (Erlandson, 1993, 99, citado en Valles, 2000: 109)

Por tanto, se tiene previsto hacer una revisión de fuentes en la Secretaría General de la UNASUR y el CEED, orientándose este análisis documental en lo reseñado por Valles (2000): «Si la documentación disponible se ve afectada por circunstancias que hacen vislumbrar su falta de autenticidad, credibilidad y representatividad, parece claro que falla la base necesaria para la interpretación (o que la clase y alcance de ésta deberá adaptarse a las limitaciones advertidas)» (Valles, 2000: 136). Para evitar esta situación se acudirán a fuentes documentales oficiales de la institucionalidad sudamericana para soslayar desviaciones en la fase interpretativa.

C) Análisis Bibliográfico: finalmente esta investigación se sustentará sobre la base de literatura especializada que nutra académicamente la tesis y contribuya a la afinación teórica para la interpretación estratégica de rigor, que se llevará de la siguiente forma: «La búsqueda bibliográfica comienza por los temas más específicos vinculados a nuestros intereses. Si el número y contenido de los artículos seleccionados no es satisfactorio, entonces procedemos por aproximación. Esto consiste en definir la clase de proceso, evento, situación, poblaciones, cercanos o vinculados a nuestro tema de interés» (Sautu, Boniolo, Dalle & Elbert, 2005: 83-84). Esa aproximación que refieren los autores, se precisa en este trabajo debido a que la bibliografía sobre «ciberamenazas» y «ciberguerra» en castellano es sensiblemente escasa, debiendo afincarse esta investigación en la consulta de fuentes norteamericanas, europeas y asiáticas, ya que no son muy prolíficos los estudios regionales en el centro de debate que aquí se analiza.

CAPÍTULO II

2. MARCO TEÓRICO

Dentro de un estudio que busque realizar un análisis de la «*guerra informática*» y las «*amenazas cibernéticas*», es importante hacer una construcción teórica sobre el pensamiento que desde el siglo XIX al XXI ha moldeado las propuestas de estrategia militar. A lo largo del tiempo la guerra ha tenido un importante papel en los hechos socio-políticos, configurando y delimitando el comportamiento de los pueblos, naciones, y Estados. La estrategia militar resulta tan antigua como el hecho mismo de la guerra, y desde esa época se puede citar una larga lista de estrategas militares clásicos como Sun Tzu, Alejandro, Julio César, Belisario, Maquiavelo, Suvórov, Bonaparte, Bolívar, von Moltke, entre muchos otros que enfrentaron y dirigieron contiendas por todo el mundo, y en diferentes condiciones.

Precisamente, es la coyuntura que encara cada pensador la que nutre el dibujo estratégico con elementos políticos, culturales, ideológicos, étnicos, y tecnológicos, evidenciándose que la guerra es un acontecimiento cíclico y recurrente en la sociedad. En este contexto, la estrategia militar no ha sido ajena a la afectación de las corrientes de pensamiento, pero hay una naturaleza lógica, que es su centro de determinación de objetivos, que en rasgos generales se mantiene con el transcurrir de los años, al respecto sugiere Van Creveld (1991) que:

> […] la guerra ya no es simplemente una cuestión de que un luchador lance al otro fuera del ring. Desde Moltke a Liddell Hart, el objetivo de la estrategia ha sido todo lo contrario: es decir, de flanquear al enemigo, rodearlo, interrumpirlo, privarle de suministros y hacerle rendirse sin tener que luchar por el terreno donde se encontraba. (Van Creveld, 1991: 423).

Este «*objetivo estratégico*» descrito por Van Creveld se amolda en general a muchos de los desarrollos del pensamiento militar de los tres últimos siglos, pero es preciso iniciar un

exhaustivo examen que permita visualizar los elementos coincidentes con una estrategia «*cibernética*». El establecer puntos de partida en análisis sociales suele estar cubierto bajo una estela de «*arbitrariedad*», ya que se precisa instaurar una línea temporal analítica de arranque, y es así que en la presente investigación se tomará como referente inicial a Carl von Clausewitz, que no deja de ser un pensador que polariza entre quienes defienden sus axiomas y los que en cambio los desdeñan como anacrónicos, pero como destaca Baquer (1989):

> Clausewitz sigue de actualidad, incluso para quienes le combaten con ardor. De las enseñanzas de Clausewitz han hecho uso muy distinto los militares del Occidente (y del Oriente) europeo, los dirigentes de las grandes potencias y los cabecillas del Tercer Mundo. Clausewitz sigue siendo el frontón donde se estrellan encontradas opiniones. (Baquer, 1989: 226).

La amplia estructura estratégica «*clausewitziana*» se ha aglutinado en torno a la definición de «*Guerra Absoluta*», originariamente el autor alemán despliega sus ideas en los siguientes términos: «Si la política es grande y poderosa, igualmente lo será la guerra, y esto puede ser llevado al nivel en que la guerra alcanza su forma absoluta» (Clausewitz, 2002: 163). La «*piedra angular*» de la visión «*absoluta*» está erigida sobre una noción que sustentó la doctrina militar a escala mundial: la «*trinidad*», que asocia el conflicto físico con los distintos escalafones de la sociedad, como una manera de canalizar la violencia instintiva con un raciocinio político, al exponer que:

> Esta trinidad está integrada tanto por el odio, la enemistad y la violencia primigenia de su esencia, elementos que deben ser considerados como un ciego impulso natural […] El primero de estos tres aspectos interesa especialmente al pueblo; el segundo, al comandante en jefe y a su ejército, y el tercero, solamente al gobierno. (Clausewitz, 2002: 21).

Es bastante riguroso el análisis del nativo del reino de Prusia, al dejar sentado sobre la trinidad que: «Una teoría que rehuyera tomar en cuenta cualquiera de ellas o fijara una relación arbitraria entre ellas incurriría en tal contradicción con la realidad que por este solo hecho debería ser considerada como nula» (Clausewitz, 2002: 21). La conjugación trinitaria de elementos traza un actuar «*íntegro*», para evitar una descoordinación que pudiera desencadenar una implosión antes del inicio incluso del «*duelo*», explica sobre esa argumentación Girard (2010):

> Clausewitz intenta, sí, convencernos de que todavía estamos en la época de los conflictos clásicos entre estados. Es el efecto que él da por descontado al intentar disimular el duelo por detrás de una definición racional de la guerra. Así, el gobernante "(re)tendría" al estratega, quien a su vez "(re)tendría" las pasiones populares. (Girard, 2010: 91).

En tal sentido, el entramado compuesto por «*Pueblo*», «*Ejército*» y «*Gobierno*» plantean un proceder afinado para emprender el «*encuentro*» contra su par antagónico, debiendo maniobrar conforme al «*principio de polaridad*», que retoma del teórico prusiano el escritor Rozitchner (1980), expresando que: «Lo que es más para uno, es menos para el otro: la suma total siempre será cero. Este principio de polaridad nos proporciona una apariencia de la verdadera razón, pues supone la identidad entre los objetos de la relación» (Rozitchner, 1980: 344). Por tanto, ante esa identidad, se deben impedir flancos débiles que puedan ser aprovechados por el enemigo, siendo preciso el concebir la guerra orgánicamente: «del cual no pueden separarse los miembros individuales, y en el cual, por consiguiente, toda actividad individual fluye dentro del todo y tiene también su origen en la idea de este todo» (Clausewitz, 2002: 164), esa es la esencia «*absoluta*» de la guerra.

Cuando se entrecruzan estos elementos tripartitos se constituye un andamiaje que intenta articular y hacer transitar ordenadamente «*El Duelo*», «*El Encuentro*», y «*El*

Combate», buscando dirigir «*absolutamente*» el acto de la guerra, para que la violencia no se desborde opacando los objetivos políticos perseguidos, destacando Clausewitz que: «la guerra no constituye simplemente un acto político, sino un verdadero instrumento político, una continuación de la actividad política, una realización de ésta por otros medios» (Clausewitz, 2002: 19). En «*Vom Kriege*» la dimensión que imprime el pensador prusiano denota lo indisoluble entre el acto de la guerra y la direccionalidad política, que asume el campo bélico como un modo para conquistar sus fines, pudiendo percibirse la conciliación de un impulso violento con los objetivos políticos, comprendiendo Clausewitz lo «*holístico*» de la guerra.

La lectura profunda de este pensador militar tiene la particularidad de mostrar y dirigir las conclusiones de maneras muy diferentes según el «*ojo acucioso*» de quien las analiza, particularmente la extensión y profundidad de la «*Guerra Absoluta*» tuvo en Vladimir Ilyich Lenin, un continuador de los enunciados de Clausewitz, surgiendo del cotejo de los conceptos manejados por ambos estrategas un conjunto de paralelismos teóricos, en palabras del líder soviético: «Toda guerra es la continuación de la política con otros medios» (Lenin, 1973: 5). Esta vinculación entre la política y la guerra la compartían el nativo del Óblast de Uliánovsk y el prusiano, que concebían una supeditación de la guerra a los fines del Estado.

A diferencia del elemento «*político*» concordante en Clausewitz y Lenin, sus razonamientos contrastan teóricamente con el estratega de origen «*tudesco*» Erich Ludendorff, quien bosquejaba una contrapropuesta precisada como «*Guerra Total*», que sometía lo político a lo militar, arguyendo que: «Habiendo cambiado el carácter de la guerra y el de la política, las relaciones entre la política y la estrategia militar deben modificarse. Todas las teorías de von Clausewitz deben ser remplazadas […] Por ello es que la política debe servir a la guerra» (Ludendorff, 1964: 21-22). Aunque en algunas ocasiones, se han

usado erróneamente los términos «*Absoluta*» y «*Total*» como sinónimos, claramente los dos teóricos tenían una percepción disímil de la guerra, en palabras de Honig (2012):

> Las diferencias sugieren que Ludendorff y Clausewitz eligieron sus términos con cuidado y, a pesar de que eran hijos de su tiempo en el sentido de que interactúan estrechamente con los ambientes militares, políticos, teóricos y prácticos de la época, trataron de capturar algo distinto y especialmente apropiado para abordar eficazmente los desafíos militares de su tiempo. (Honig, 2012: 30).

Esta polarización conceptual, ha marcado a grandes rasgos el desarrollo estratégico del siglo XX y XXI, ya que ambos modelos perviven en la actualidad. Cuando en el siglo XIX Clausewitz disertaba que la estrategia: «es el uso del encuentro para alcanzar el objetivo de la guerra. Por lo tanto, debe imprimir un propósito a toda la acción militar, propósito que debe concordar con el objetivo de la guerra» (Clausewitz, 2002: 99), él estaba inoculando un sentido político al «*objetivo*» que debía tener una relación jerárquica sobre la «*acción*» militar en sí misma.

Era incisivo Clausewitz sobre la relevancia no sólo de la victoria militar, que podría terminar desvirtuando el «*objetivo*», orientando que: «Después de ganar una batalla, cuantos más éxitos pueda incluir la estrategia, mediante sus combinaciones, en los resultados obtenidos, tanto más podrá elevarse de los escombros que ha provocado la lucha» (Clausewitz, 2002: 144). Particularmente la percepción de «*combinación*» compatibiliza y viabiliza ese relacionamiento estratégico que se pretende realizar entre la «*Guerra Absoluta*» y la «*Guerra Cibernética*».

Pero el conjugar principios propuestos por Clausewitz a un contexto bélico en donde el factor informático es determinante, entraña la adecuación del análisis, en vista que: «el advenimiento de la guerra informática es probablemente una de las mayores razones detrás del cambio histórico en curso, constituyendo una distancia entre la gran guerra de los

principales estados hacia el mundo no-trinitario del conflicto futuro» (Van Creveld, 2008: 12). Al respecto conviene decir que las guerras han tomado un rumbo que supera en algunos aspectos la trinidad «*clausewitziana*», por ello la reflexión de Van Creveld sobre un futuro bélico «*no trinitario*», pero no hay que descartar el pensamiento visionario del prusiano, que aún está vigente en un extenso conjunto de conceptos, propuestas y teorías.

Justamente, entre la amplia teoría del autor teutón, se extraerán tres aportes que podrían encajar en el nuevo escenario de conflicto informático: «*la Cosa Real*», el «*Teatro de la Guerra*», y la «*Eficacia Estratégica*». Con respecto a «*la Cosa Real*» bosquejaba Clausewitz una disertación sobre lo «*inmaterial*» y su proyección a lo «*real*», indicando que: «la mera posibilidad de un encuentro ha producido consecuencias y, por consiguiente, ha accedido a la categoría de cosa real» (Clausewitz, 2002: 103). Extrapolando lo anterior, las redes virtuales diversificaron el espacio/tiempo de la guerra, ya que la variable «*cibernética*» no es palpable físicamente en primera instancia, pero sus consecuencias lo configuran como una «*Cosa Real*» al tener la capacidad de infringir daños de igual o más magnitud que un armamento convencional.

Para ilustrar la materialización de la «*Cosa Real*» en la «*guerra cibernética*», se pueden citar dos ejemplos de cómo acciones virtuales afectaron sistemas de defensa de algunas naciones. En primera instancia, en el año 2009 aeronaves de combate francesas fueron infectados por el virus «*Conficker*», viéndose imposibilitadas de iniciar vuelo: «[…] el 15 y 16 de enero los aviones Rafale de la Marina fueron "clavados en el suelo", porque no fueron capaces de "bajar sus planes de vuelo"» (The Telegraph, 2009). Por otra parte, ese mismo año aviones no tripulados «*Drones*» de la Fuerza Aérea estadounidense recibieron incursiones «*cibernéticas*» a través de un programa ruso denominado «*Skygrabber*» que tiene un valor de menos de treinta dólares, que permitió a grupos iraquíes extraer información y videos de la aeronave, como refleja un reporte de lo acontecido: «El Pentágono había sido

consciente del problema desde hace muchos años, pero había asumido que los insurgentes no tenían los conocimientos técnicos para interceptar la fuentes de información (feeds)» (The Guardian, 2009). En tal sentido, el accionar de un dispositivo informático que es imperceptible se trasformó en «*Cosa Real*» al momento que tuvo una afectación sobre estos sistemas militares.

En el caso del «*Teatro de la Guerra*», es presentado en una lógica defensiva por Clausewitz que indica: «Cuanto más grande es el campo de operaciones que ha de atravesar, más se debilitará el ejército atacante» (Clausewitz, 2002: 145). Lo anterior, se puede readaptar a la «*guerra cibernética*» pero invirtiendo la debilidad del atacante hacia el defensor, en donde el «*campo de operaciones*» se expande en lo ilimitado del espacio informático, quedando los Estados u organizaciones regionales en una posición vulnerable ante el agresor que aprovecha las variables amplitud/espacio para diversificar los ataques a la «*infraestructura crítica*»[4]que abarca:

> […] sistemas agrícolas y alimentarios, la base industrial de defensa, sistemas de energía, la salud pública y los centros de salud, los monumentos nacionales y los íconos, los sistemas bancarios y financieros, sistemas de agua potable, instalaciones químicas, instalaciones comerciales, presas, servicios de emergencia, sistemas de energía nuclear, sistemas de tecnología de la información, sistemas de telecomunicaciones, los servicios postales, el transporte marítimo, los sistemas de transporte, y las instalaciones del gobierno. (O'Rourke, 2007: 22).

En cuanto a la «*Eficacia Estratégica*», indicaba primeramente Clausewitz tres principios conducentes: «1. La ventaja del terreno; 2. La sorpresa, ya sea en forma de un verdadero

[4] Se entiende por Infraestructura Crítica: «Las infraestructuras estratégicas (es decir, aquellas que proporcionan servicios esenciales) cuyo funcionamiento es indispensable y no permite soluciones alternativas, por lo que su perturbación o destrucción tendría un grave impacto sobre los servicios esenciales» (CNPIC, 2010).

ataque o por la disposición inesperada, en ciertos puntos, de fuerzas superiores; 3. El ataque desde varios lados (tres, como en la táctica)» (Clausewitz, 2002: 144). Estos enunciados teóricos se pueden enlazar a un hecho práctico de la «*guerra informática*», como es el caso del sistema de vigilancia extensiva manejado por EE.UU, denominado «*X-Keyscore*»[5], que es reseñado de la siguiente manera:

> El sistema informático XKeyscore es algo así como una navaja suiza de análisis de datos para los servicios de inteligencia. Por un lado, está la parte delantera, se pueden analizar las enormes cantidades de datos con los funcionarios de inteligencia. En segundo lugar, es un sistema de servidores Linux distribuido a nivel mundial. Más de 700 de estos equipos en 150 localidades estaban conectados en 2008 al XKeyscore y dibujaban el tráfico de Internet en las respectivas regiones. (Der Spiegel, 2013).

Lo indicado en la referencia anterior fue evidenciado en el informe filtrado de la National Security Agency (NSA) identificado como «NSA/CSSM 1-52», que revela precisamente la existencia de una cantidad superior a los setecientos servidores ubicados a nivel mundial para interceptar información «*Metadatos*», dándoles una «*ventaja del terreno*» en la «*guerra informática*». Asimismo, aprovechan la fortaleza generada por el sistema «*X-Keyscore*» para hacer uso de «*La sorpresa*», incursionando en sistemas informáticos de otras naciones, valiéndose de las vulnerabilidades detectadas. Finalmente, el «*ataque desde varios lados*» puede ser emprendido cibernéticamente, ya que el sistema «*X-Keyscore*» se apoya de servidores diseminados a escala planetaria para perpetrar operaciones desde diferentes lugares.

En consonancia con la «*Guerra Absoluta*» destacada por Clausewitz, y en la búsqueda de configurar elementos tendientes a vislumbrar una estrategia «*cibernética*», se inserta

[5] Observar el **ANEXO «A».**

teóricamente a otro estudioso militar que contribuyó al desarrollo del pensamiento castrense en el siglo XX, como lo fue Basil Liddell Hart, que añadió el concepto de «*Aproximación Indirecta*», presentándolo análogamente como un arte marcial: «que hace dar al adversario un paso en falso, de manera que, como en el jiu-jitsu, su propio esfuerzo contribuya a derribarlo» (Liddell Hart, 1946: 198). Hay que referir que el autor anglosajón, al igual que Clausewitz hace un planteamiento de la estrategia militar desde la política para ver la justa medida de ellas en la guerra, manifestando que desde Napoleón se había iniciado un proceso creciente de dominio exclusivo de la estrategia por parte de los militares, desvirtuándose los objetivos de la misma, expone Larson (1980) citando a Liddell Hart:

> Por lo tanto, se define la estrategia como "la distribución y transmisión de medios militares para cumplir con las necesidades de la política", por lo que es claramente más dependiente de las decisiones políticas, mientras que, según explicó, dejando su ejecución en manos de los militares". (Larson, 1980: 70-71).

Esa concepción política sobre la guerra era trazada por Liddell Hart en base a un escenario bélico que daba preponderancia a la «*simetría actoral*» del Estado, que fue característica de las concepciones estratégicas del siglo XX. Empero, es preciso señalar que hubo otras estructuraciones del comportamiento bélico como las de Lenin, que desestatizó la guerra y puso en la palestra la confrontación: Proletario/Burguesía, sobre esto opina Rubio (1966): «Fue Lenin quien franqueó la etapa definitiva, sustituyendo en sus reflexiones la lucha de Estados por la lucha de clases -necesariamente revolucionaria en la óptica marxista» (Rubio, 1966: 119). Aunque en relación al marxismo un teórico como Liddell Hart pudiera parecer «*estatizador actoral*», en sus análisis sobre los objetivos de la guerra dedica espacio a otros factores sociales como el «*Pueblo*», advirtiendo que: «Así, cuanto más igualados se hallen los dos bandos, más juicioso será evitar las violencias extremas, que tenderían a consolidar a las tropas y al pueblo enemigo en torno de sus dirigentes» (Liddell Hart, 1946: 221).

Por otra parte, resalta el británico que la conducción del ataque se debe concentrar en primera instancia contra el adversario con menos potencial, con la finalidad de dosificar las fuerzas y preparar la contienda contra el enemigo de más cuidado, aclarando: «Pero en realidad ha de ampliarse esta palabra en el sentido de «concentración de la fuerza contra la debilidad» (Liddell Hart, 1946: 226). Con respecto a lo anteriormente referido, se pueden encontrar diferencias y concurrencias relevantes con otro estratega como Ludendorff, que contrariamente a Liddell Hart sugería el sometimiento del contrincante de más cuidado, pero coincidiendo en la precepción de afincarse sobre la debilidad, en este sentido opinó el militar alemán:

> El arte del comando de la guerra consiste no solamente en repartir las fuerzas y concentrarlas en un punto del cual partirá el ataque contra los puntos débiles del enemigo, ataque que decidirá la victoria; antes de preparar esta concentración hará falta que todas las tropas movilizadas puedan ser agrupadas desde un principio contra el enemigo considerado más peligroso. (Ludendorff, 1964: 131-132).

Esta percepción de la guerra fue ampliamente difundida en los planes militares alemanes (Plan Schlieffen) previos a la Primera Guerra Mundial para afrontar una guerra internacional, donde preveían atacar duramente a Francia hasta vencerla, para enfrentar posteriormente a Rusia. La discrepancia de Ludendorff y Liddell Hart estriba en que este último planteaba la caída del más débil y el subsecuente direccionamiento de las fuerzas hacia el contendor simétrico, enfocándose en reducir la capacidad de las contrapartes de soportar los embates de la guerra. Además establecía que la concentración de acciones sobre el área menos fortalecida, debía contribuir igualmente a la afectación de otros objetivos, reseñando: «Y de ello se sigue otro axioma: que para asegurar el logro de un objetivo hay que tener varios objetivos alternativos. Un ataque dirigido sobre un punto ha de amenazar y poder divergir hacia otros» (Liddell Hart, 1946: 300).

Las máximas que desarrolla este intelectual castrense son considerablemente importantes para los estudios estratégicos en «*ciberguerra*», partiendo del hecho que en la guerra sea física o virtual: «el objeto fundamental puede sintetizarse diciendo que es el de asegurar la continuación de su política frente a la decisión de una potencia opuesta que trata de perseguir una política contraria» (Liddell Hart, 1946: 299). Esa diatriba política con consecuencias militares es central en los argumentos de Liddell Hart, pero además es reconocido por las puntualizaciones no sólo de la «*aproximación indirecta*», sino en un extenso abanico estratégico, destacando Atkinson (1966) que: «la mayor fama de Liddell Hart reposará sobre sus ideas en dos áreas importantes: (1) Los aspectos tecnológicos de la guerra, y (2) el conflicto psico-social» (Atkinson, 1966: 162). Esas dos áreas podrían considerarse como parte de la tipología informática de la guerra, siendo oportuno y coherente hacer uso de las mismas, específicamente en puntos como: «*Combinación*», «*Efecto Moral*» y «*Objetivo Económico*».

La «*guerra cibernética*» es un complemento de la confrontación física, siendo su «*Combinación*» propia de las circunstancias del duelo que se libra, esa diversificación se debe a que: «En lugar de dar un énfasis excesivo a un medio que las circunstancias pueden hacer ineficaz, es más juicioso escoger y combinar los que entre todos ellos sean más apropiados, los que penetren más efectivamente y conserven mejor el esfuerzo» (Liddell Hart, 1946: 299). La «*Combinación*» de medios es un fundamento de la «*guerra informática*» desde finales del siglo XX cuando antes de iniciarse los bombardeos, se ponía en acción una avanzada de ataques «*cibernéticos*», siendo una estrategia innovadora que se materializó en la Primera Invasión a Irak, que contó: «con las armas de la nueva era –virus, gusanos, caballos de Troya electrónicos– utilizando redes informáticas que nos conectan a todos» (Adams, 1999: 114).

En relación al llamado «*Efecto Moral*», este era descrito por Liddell Hart, como un acicate: «al ejercerse sobre un pueblo agotado por el hambre y sin esperanza alguna de victoria» (Liddell Hart, 1946: 288). Para una sociedad moderna habituada al uso extensivo de tecnologías computacionales, el enfrentar un sabotaje económico, acompañado de una interrupción periódica o total del acceso a redes telefónicas, de internet, o medios de comunicación, significa un golpe psicológico que afectaría sensiblemente la moral, generando una presión inusitada al gobierno agraviado. El llamado «*Efecto Moral*» está íntimamente ligado a la exposición que sobre los «*objetivos económicos*» persigue la aproximación indirecta, relatando el historiador inglés que:

> Ha consistido normalmente en un movimiento militar logístico dirigido contra un objetivo económico: "la fuente de aprovisionamientos del ejército o del país enemigos. A veces, no obstante, ha tenido un objetivo puramente psicológico […] cualquiera que sea su forma, el efecto a buscar es la dislocación del enemigo; este es el verdadero signo distintivo de la aproximación indirecta. (Liddell Hart, 1946: 198).

Esa dislocación no deja de ser una de las finalidades de la «*guerra cibernética*», que puede apuntar en primera instancia al sabotaje de los centros tecnológicos vinculados a las finanzas y economía, siendo un posible objetivo, el crear caos financiero en una fase previa a las acciones militares convencionales, o conforme remarca Liddell Hart para sembrar desconcierto psicológico, como sucedió en los ataques recibidos por Georgia en el año 2008, cuando fue seriamente afectada su «*infraestructura crítica*» por ataques que presumiblemente venían de su vecino ruso, aconteciendo que:

> El 19 de julio de 2008, una empresa de seguridad de Internet informó de un ataque distribuido de denegación de servicio (DDoS) contra sitios Web de Georgia […] Los analistas señalaron que los ataques DDoS adicionales parecían coincidir con el movimiento de las tropas rusas en Osetia del Sur en respuesta a Operaciones militares

> georgianas lanzadas un día antes en la región. Para el 10 de Agosto los ataques DDoS habían desactivado varias Webs gubernamentales dejando otros sitios georgianos inactivos. (Korns & Kastenberg, 2009: 60).

Estos ataques cumplieron a cabalidad el axioma propuesto por Liddell Hart, sumiendo en un desconcierto a la nación caucásica, como anticipo a la intervención del 58° Ejército ruso en apoyo a las fuerzas de paz asentadas en Osetia del Sur, desencadenándose la Batalla de Tsjinval.

Una vez desplegados un conjunto de categorías estratégicas de la «*aproximación indirecta*» acuñada por Liddell Hart, se precisa traer a colación las ideas militares que adelantó el líder chino Mao Zedong, quien se destacó por erigir al unísono, una estructura militar y política en medio de un escenario de conflicto marcado primero por la Guerra Civil contra el Kuomintang, y posteriormente contra el ejército imperial japonés, todo lo anterior con la particularidad geográfica de un gigante continental con una vasta población.

Las dificultades y contradicciones enfrentadas en los conflictos chinos sucedidos en los primeros cincuenta años del siglo XX fueron asumidos por Mao bajo la premisa de la «*evolución estratégica*», explicando que: «primero fue el paso de la guerra de guerrillas a la guerra regular en la guerra civil. El segundo fue el paso de la guerra regular en la guerra civil a la guerra de guerrillas […] Y el tercero será el paso de la guerra de guerrillas a la guerra regular» (Mao, 1976: 236). El adaptarse y evitar un estancamiento estratégico que afectará la lucha armada, fue una constante china para asumir la guerra polifacéticamente, con la finalidad de perturbar al contendiente. Junto a la «*evolución estratégica*», el maoísmo exponía las llamadas «*etapas estratégicas*» para estructurar el teatro de guerra oriental, contextualizadas como «*defensiva*», «*equilibrio*» y «*contraofensiva*», reflexionando Katzenbach y Hanrahan (1955) que:

> La primera de las tres etapas es aquella en la que el enemigo está a la ofensiva estratégica y la que Mao llama la "defensiva estratégica". La segunda es una fase de estancamiento en la que los comunistas se preparan para tomar la iniciativa. En la tercera etapa se produce un cambio a la ofensiva estratégica por parte de los comunistas, lo que obliga al enemigo a la defensiva estratégica, y, finalmente, con la guerra total. (Katzenbach & Hanrahan, 1955: 330).

Este armazón llamado «*Guerra de Resistencia*», con su combinación político/militar, supuso un desafío para el adversario, que no encontraba períodos para consolidar las conquistas territoriales, al tener un clima hostil marcado por incursiones guerrilleras o ataques convencionales de las tropas regulares chinas, que se intercalaban para desconcertar la vanguardia o retaguardia enemiga según los fines que se perseguían. Como acota Fuller (1958) en un estudio sobre el pensamiento militar maoísta, y su comprensión del enemigo y movilidad en el campo de batalla, espetó:

> Mao había combinado la vieja guerra de guerrilla partisana con conceptos modernos de la guerra psicológica y total. "Sobre las unidades guerrilleras," Mao dijo, "por lo general crecen de la nada y se amplían de una pequeña fuerza a una grande, deberían no sólo preservarse sino también ampliar sus fuerzas." Este es el núcleo de la estrategia de Mao de la guerra de guerrillas. (Fuller, 1958: 140).

El estadista asiático indicaba que: «En lo que respecta a la Guerra de Resistencia en su conjunto, la guerra regular juega el papel principal, y la guerra de guerrillas, el auxiliar, porque únicamente la guerra regular puede decidir el desenlace de la Guerra de Resistencia» (Mao, 1976: 237). Aquí se visibiliza un punto de coincidencia entre Mao y Liddell Hart, ya que ambos plantean la necesidad de evitar una confrontación directa, pero son igualmente conscientes de que la regularidad de la guerra es determinante, y tendrá un papel crucial en el devenir del conflicto. Sin embargo, lo primordial de la «*Guerra Regular*» no significaba una aminoración de la «*Guerra de Guerrillas*», aclarando Mao que:

> La guerra de guerrillas desempeña un importante papel estratégico en toda la guerra. Si no hacemos la guerra de guerrillas, si no nos preocupamos de la organización de unidades y ejércitos guerrilleros, así como del estudio y la dirección de la guerra de guerrillas, tampoco podremos derrotar al Japón. (Mao, 1976: 238).

Ese factor central recaía en evitar que la retaguardia japonesa se consolidara, incursionando las guerrillas chinas en las posiciones del enemigo, ocasionado un desequilibrio en sus defensas, debiendo los nipones luchar en dos frentes, ya que la contraofensiva regular golpeaba recurrentemente articulada con la insurgencia. Aquí se vuelven a cruzar los caminos conceptuales de Mao y Liddell Hart, que concordaban en la caza del contrincante con estratagemas, como el mecanismo indirecto más plausible, aclarando el teórico británico: «Sí no puede ser así o si falla de esta manera, se deberá elegir otra forma de aproximación indirecta que aspire a lograr una decisión eventual minando la fuerza y la voluntad del adversario. Todo es preferible a la aproximación directa» (Liddell Hart, 1946: 266).

Es interesante como a pesar de la distancia temporal y territorial del pensamiento de Clausewitz y Mao, el prusiano asomó tempranamente una modalidad de guerra que en términos contemporáneos podría ser enmarcada en una percepción «*asimétrica*», muy cercana a la puesta en marcha en China por los maoístas, reflexionando sobre cómo más allá de los ejércitos regulares, en un momento dado la pequeña guerra defensiva (ejército del pueblo) puede ser definitoria, acota Aron (1973) referenciado en Clausewitz:

> La guerra popular solamente constituye en su sistema una modalidad de la pequeña guerra, la guerra que hacen destacamentos de una fuerza no mayor a los 200 o 300 hombres. Para que la guerra popular por sí sola pueda obligar al invasor a que evacúe el país –escribe– hay que suponer espacios tan vastos como los de Rusia y una extrema desproporción entre la fuerza del ejército conquistador y las dimensiones del terreno. (Aron, 1973: 20).

Esto último extraído del pensamiento «*clausewitziano*» es precisamente lo acontecido con los japoneses en la Segunda Guerra Mundial en el frente chino, que confrontaban con la inmensidad territorial de China, y además las tropas imperiales niponas representaban un numero significativamente inferior con relación a los millones de pobladores chinos que eran organizados para la resistencia por los militantes comunistas.

Otro elemento del «*maoísmo*» que retrotrae el análisis al «*Efecto Moral*» de Liddell Hart por sus rasgos similares, es como los chinos promovieron en su lucha interna y de liberación contra los japoneses, la estrategia de afectar paralelamente al enemigo física y mentalmente, para desencadenar un desmoronamiento total, como lo explica Mack (1975): «Si se destruye la "voluntad" de la fuente de alimentación externa para continuar la lucha, entonces su capacidad militar-no importa cuán poderosa sea, es totalmente irrelevante» (Mack, 1975: 178-179). El escenario de la «*Guerra de Resistencia*» estaba configurado para aglutinar «*tiempo*» y «*estancamiento*» que daban lugar a la frustración del adversario. Es así que el «*tiempo*» fue una variable intensamente examinada por las fuerzas chinas en la «*Guerra de Resistencia*», que fusionaban una paciencia milenaria con una movilidad inusitada, como esboza Joxe (1968): «El factor tiempo no es de misma naturaleza […] Clausewitz piensa después de las batallas napoleónicas, Mao durante una guerra prolongada y popular, dentro de un campo de batalla que no varía en función de los progresos de la física aplicada» (Joxe, 1968: 285).

Partiendo de la «*Línea Estratégica Militar*» explicada por Mao Zedong donde exhibía dieciocho puntos favorables sobre el cambio en la guerra, específicamente en los numerales «1» y «15», se pueden arrojar algunas conclusiones estratégicas sobre la «*ciberguerra*». Anteriormente se reflejó algunos pormenores del programa informático «*X-Keyscore*» utilizado por la National Security Agency (NSA) estadounidense, pero en este ejercicio analítico del pensamiento «*maoísta*» contrastaremos sus elementos estratégicos con otro

sistema conocido en la comunidad de inteligencia como «*Prism*»[6], en el siguiente reporte se ofrecen detalles del mismo:

> La Agencia de Seguridad Nacional y el FBI están recurriendo directamente a los servidores centrales de nueve de las principales compañías estadounidenses de Internet, para la extracción de audio y video chats, fotografías, correos electrónicos, documentos y registros de conexión que permiten a los analistas rastrear objetivos extranjeros, de acuerdo con documento altamente secreto obtenido por el diario The Washington Post. (The Washington Post, 2013).

El sistema «*Prism*» demuestra los abismos tecnológicos que separan a las naciones en la lucha en el «*ciberespacio*», pero la consideración de las desventajas propias remite al punto primero de las líneas estratégicas del «*maoísmo*», que ahondan en la determinación de los planes conducentes a la: «reducción del territorio ocupado por las fuerzas enemigas» (Mao, 1976: 239). Así como la estrategia china planeaba un asecho constante de la retaguardia japonesa para evitar que sus posiciones se fortalecieran, esta misma razón aplica en la «*guerra cibernética*», particularmente el terreno computacional debe ser resguardado con un control soberano sobre la información, datos, y comunicaciones estratégicas que no sean proclives de intervenciones. Al lograr una capacidad para contrarrestar ataques y responder ofensivamente en resguardo de la «*infraestructura crítica*», se estaría reduciendo el «*campo de acción del enemigo*».

Las delaciones que colocaron en conocimiento público la existencia y uso del «*Prism*» desnudaron inmediatamente dos problemas para los países que estaban siendo afectados por este novedoso sistema informático: la «*vulnerabilidad en defensa*», y la «*incapacidad de enfrentar una amenaza*». La evolución de la amenaza de «*probable*» a «*posible*» y finalmente

[6] Observar el **ANEXO «B».**

«*materializable*», hace que sea inaplazable la aplicación del apartado quince que refiere: «adaptación a las condiciones en que el enemigo es fuerte y nosotros débiles, a fin de sufrir menos pérdidas y alcanzar más victorias» (Mao, 1976: 240). Las vulnerabilidades informáticas pasan por una cadena de aspectos: políticos, estratégicos, tácticos, técnicos. En tanto no se consideren los «*ciberataques*» como una amenaza a la Defensa, difícilmente se tomaran las decisiones estratégicas dirigidas a la adaptación de las condiciones con relación al adversario. Para ello, se requiere analizar estratégicamente al «*ciberespacio*» como un área en donde se debaten intereses, se generan conflictos, proyectan amenazas y desnudan vulnerabilidades, partiendo de estos hechos se pueden establecer los parámetros que están estrechamente asociados con la tecnología como medio para alcanzar los fines políticos de un Estado.

El análisis que se ha venido realizando demuestra lo dinámico que es el proceso estratégico en la guerra, pero particularmente la transición entre los siglos XX y XXI ha producido una readaptación del «*teatro de la guerra*», revelando un nuevo panorama bélico mucho más difuso e ininteligible, que se deriva según Cordesman y Yarosh (2012) porque: «la eficacia del poder militar ha disminuido en relación con los nuevos medios infinitos de coaccionar a los enemigos. Como dicen, el entorno externo cambiante y dinámico hacia los estados-nación de hoy en día hace "obsoleta la idea de la guerra de confinamiento con el dominio militar"» (Cordesman & Yarosh, 2012: 35).

El escenario detallado por Cordesman y Yarosh concuerda con la propuesta estratégica militar impulsada por los militares chinos Qiao Liang y Wang Xiangsui, que establece una reingeniería del clásico concepto de enfrentamiento entre ejércitos, y daños por medios militares, que pasó de ser la totalidad a una parte de la guerra, dejando un arsenal de medios no militares a la disposición para ocasionar la mayor cantidad de daño al contrincante, exponiendo:

> Sí reconocemos que los nuevos principios de la guerra ya no son "uso de la fuerza armada para obligar al enemigo a someterse a la voluntad de uno", sino que se "utilizan todos los medios, incluida la fuerza armada o fuerzas no armadas, militares y no militares, y medios letales y no letales para obligar al enemigo a aceptar sus intereses" Esto representa el cambio. (Liang & Xiangsui, 1999: 7).

La esencia de esta nueva forma y fondo bélico multidimensional con respecto a la «*Guerra Absoluta*», la «*Guerra de Aproximación Indirecta*», y la «*Guerra de Resistencia*», tiende a deslindarse en lo que se refiere a la convencionalidad bélica, pero encuentra especial asidero en la irregularidad del «*maoísmo*». La «*Guerra Irrestricta*» según los militares asiáticos debe su denominación a que:

> […] Este tipo de guerra establece que todos los medios estarán en disposición, considerando que será omnipresente, y el campo de batalla estará en todas partes. Esto significa que todas las armas y la tecnología se pueden superponer a voluntad, por tanto, todos los límites que se encuentran entre los dos mundos de la guerra y la no guerra, de los militares y no militares, serán totalmente destruidos. (Liang & Xiangsui, 1999: 12).

Pero, es importante poner atención que la «*Guerra Irrestricta*» descolló la mera propuesta teórica, y se ha ido adoptando paulatinamente por parte de las Fuerzas Armadas chinas, que entiende que los conflictos bélicos del siglo XXI estarán marcados por infinidad de factores que escapan al simple dominio de lo militar, refiriendo Chansoria (2012):

> Como consecuencias de esta estrategia, ha fluido la idea, y el ejército de China se ha concentrado en el desarrollo de una amplia gama de capacidades materiales y no materiales que harían posible "derrotar lo superior con lo inferior" […] De acuerdo con el EPL, los cambios se centran principalmente en la transformación de las fuerzas armadas de una "fuerza cerrada" a una "potencia informática de la era moderna"

> hábilmente resaltada oficialmente en el Libro Blanco 2008 de la Defensa Nacional china. (Chansoria, 2012: 111).

Lo preliminar muestra una guerra que se ha desbordado completamente de todos los parámetros de control establecidos, y da pie a la utilización de cualquier medio para alcanzar los objetivos planteados, como diserta Manwaring (2007): «Mediante el uso de todo el espectro de los componentes multidimensionales de la guerra indirecta y totalmente libre, el protagonista puede producir lo que Qiao y Wang llaman una "mezcla cóctel" de manera poco convencional y un medio de hacer frente a un oponente más fuerte» (Manwaring, 2007: 25).

Si se hace un paralelismo entre la «*Guerra de Resistencia*» de Mao Zedong y la «*Guerra Popular*» de Vo Nguyen Giap con la variante «*Irrestricta*», ciertamente tienen puntos de coincidencia, especialmente en lo que respecta a la adopción de medidas integrales para causar el mayor daño al enemigo con la menor exposición, graduando fuerzas y prolongando la lucha para debilitar las posiciones del adversario, combinándose ejércitos regulares con tácticas guerrilleras, para acosar a las tropas enemigas en sus posiciones (frente, flancos, bloque, y retaguardia). Otro punto concurrente, es que así como la estrategia maoísta o vietnamita se contraponían a la antítesis propuesta por japoneses, franceses o estadounidenses, la «*Guerra Irrestricta*» confronta la nueva estrategia militar de los Estados Unidos que se ha delineado conforme a una: «*visión ampliada de dominio*» que intenta incidir en diferentes ámbitos del sistema internacional, al plantear una seguridad extraterritorial sin límites aparentes, en el entendido que: «Este tipo de "visión ampliada de dominio" es una premisa para la supervivencia y el desarrollo de las naciones soberanas modernas, así como por su esfuerzo para tener influencia en el mundo» (Liang & Xiangsui, 1999: 118). Pero este dominio, parte de un conjunto de futuros escenarios de intervención o combate a nivel mundial, presentando opciones militares o no, conforme a una variedad de factores: «Los estadounidenses han resumido las cuatro formas principales que la lucha en la

guerra tomará en el futuro como son: 1) la guerra de información, 2) la guerra de precisión, 3) las operaciones conjuntas, y 4) las operaciones militares distintas de la guerra (MOOTW)» (Liang & Xiangsui, 1999: 48).

La respuesta estratégica china ha sido el construir escenarios múltiples que contrarresten estas formas de hacer la guerra, bajo un esquema estratégico que abunde sobre las llamadas nuevas amenazas, para resguardarse defensivamente, y además determinar las vulnerabilidades del enemigo para dirigir todos los medios posibles en su contra para ocasionar un impacto que melle su resistencia al verse imposibilitado de escudarse ante tantas vías de ataque, reflexionando los teóricos asiáticos que: «Las nuevas amenazas requieren nuevas visiones de la seguridad nacional, y nuevos puntos de vista de seguridad y luego exigen soldados que primero expandan sus campos de visión antes de la ampliación de sus victorias» (Liang & Xiangsui, 1999: 129).

Dentro del campo «*cibernético*», son sustancialmente ricas las disertaciones de Liang y Xiangsui, que afinan fórmulas militares que escapan a la rigidez del pensamiento estratégico conservador, confluyendo los mismos que: «El que quiere ganar las guerras de hoy, o las de mañana, para obtener la victoria con firmeza en sus manos, debe "combinar" todos los recursos de la guerra que tiene a su disposición y usarlos como medios para proseguir la guerra» (Liang & Xiangsui, 1999: 181). La combinación como estrategia no es nueva, pero tiene su particularidad «*irrestricta*» en los nuevos «*blancos*» de ataques, como manipulaciones financieras a través de capitales buitres que inicien un colapso económico, mientras que en paralelo se:

> Lleva a cabo un ataque contra el enemigo para que la red eléctrica civil, el tráfico de envío de red, la red de transacciones financieras, la red de comunicaciones telefónicas y la red de medios de comunicación sean totalmente paralizadas, esto hará que la

> nación enemiga caiga en pánico social, disturbios callejeros, y una crisis política. (Liang & Xiangsui, 1999: 147).

Asimismo, cuatro definiciones de los pensadores chinos son destacables para enmarcarlas en la «*guerra cibernética*»: «*Dominio*», «*Medios*», «*Omnidireccionalidad*», y «*Asimetría*». En los conflictos «*irrestrictos*» se expone el «*Dominio*» en términos de: «un concepto derivado de la noción de territorio y se utiliza para delimitar el alcance de las actividades humanas. Visto en este sentido, un dominio de la guerra es una delimitación del ámbito de lo que abarca la guerra» (Liang & Xiangsui, 1999: 188). En el siglo XXI, entre el espectro de dominios como los diplomáticos, económicos, culturales, religiosos, o psicológicos, particularmente es el militar, el que más ha ampliado su abanico, como expone Van Creveld (2008) se están visualizando una variedad de conflictos bélicos que hace solo algunos años eran inexistentes: «[…] guerra popular, guerra del medio ambiente, guerra asimétrica, guerra de infraestructura, guerra no letal, guerra de áreas grises, guerra informal, guerra de la información (estratégica y táctica), guerra en red, ciberguerra, guerra comunicacional, guerra neocortical y guerra postmoderna» (Van Creveld, 2008: 9). La «*guerra cibernética*», dentro del ámbito de la guerra es un complemento a la estrategia bélica de un Estado u organización supraestatal, ya que su capacidad destructiva al poder infringir severos daños al conjunto de actividades vitales de una nación, puede crear un efecto en cadena sobre otros ámbitos que harán sucumbir diferentes dominios.

Los «*ciberataques*» propiamente no son un «*Dominio*», aunque están insertos en uno (Militar) según lo expuesto anteriormente, pero claramente entra en la categoría de «*Medios*», clarifican los autores asiáticos:

> De esto podemos ver que el concepto de medios abarca mucho territorio, en numerosos niveles, con la superposición de funciones, por lo que no es un concepto fácil de entender. Sólo ampliando nuestro campo de visión y la comprensión de los

> medios, y de captar el principio de que no hay nada que no pueda ser considerado un medio. (Liang & Xiangsui, 1999: 193).

El carácter irrestricto asoma el potencial de los ataques informáticos dentro de los «*medios*», para ocasionar un desbalance en el enemigo y afectarlo en puntos claves, alivianando el uso de sistemas de armamento clásicos o tropas, destacando Echevarría (2010) sobre lo expuesto por los oficiales chinos que: «Se hace hincapié en el logro de una mayor actuación conjunta para lanzar ataques enfocados contra objetivos presumiblemente "asimétricos", es decir, el principal "sistema de combate del adversario", para erosionar la cohesión de formas inesperadas» (Echevarría, 2010: 21).

Por otra parte, en las reflexiones estratégicas de Liang y Xiangsui, surge otro complemento nada descartable, como es la «*Omnidireccionalidad*», que comprende: «[…] observar el campo de batalla o un campo de batalla potencial, el diseño de planes, empleando medidas, y la combinación de la utilización de todos los recursos de guerra que puedan ser movilizados, para tener un campo de visión sin puntos ciegos, un concepto sin trabas ante los obstáculos, y una orientación sin ángulos ciegos» (Liang & Xiangsui, 1999: 207). La «*Omnidireccionalidad*» convierte la virtualidad de las redes informáticas en un campo de batalla más, siendo posible hacer un análisis de estrategia militar, que establezca: «*Enemigo*» y «*Terreno*», conduciendo los «*medios*» informáticos que forman parte del «*dominio*» de la ciberguerra para dejar desprovisto de capacidad de defensa al «*cibercontendor*». Finalmente, y que se presenta como relevante en la «*Guerra Irrestricta*», se enuncia una noción que permite concebir en detalle los nuevos conflictos bélicos: «*La Asimetría*», que es explicada en los términos sucesivos:

> Su punto esencial consiste en seguir la línea de pensamiento frente al equilibrio simétrico, y desarrollar la acción de combate sobre aquella línea. La disposición de fuerza, el empleo, la selección de los ejes principales de combate, el centro de

> gravedad para el ataque, y la asignación de armas, en todas estas cosas se debe considerar dos vías, el efecto de los factores asimétricos y el uso de la asimetría como una medida para lograr el objetivo. (Liang & Xiangsui, 1999: 211-212).

Lo esgrimido precedentemente por Liang y Xiangsui es concurrente con la apreciación «*asimétrica*» de la «*Guerra Popular*» de Vo Nguyen Giap, que maniató a las fuerzas militares norteamericanas en la Guerra de Vietnam, que a pesar de tener un potencial en tropas, poder de fuego y equipamiento muy superior, sucumbieron ante el empantanamiento que planteaba la variación del «*centro de gravedad*», refiriendo Giap sobre las fuerzas invasoras que: «Sus tropas se hunden en el océano de la guerra del pueblo, en una guerra sin frente ni retaguardia, en la que el frente se encuentra en todas partes y en ninguna» (Giap, 1975: 41).

Una importante proyección de la «*guerra informática*» es que un ataque efectuado por un adversario «*asimétrico*» puede afectar duramente a un contrincante de mucho más peso y poder militar, por tanto, los «*ciberataques*» cumplen con la «*bidireccionalidad*» de los conflictos bélicos irrestrictos, al asumir con disciplina la concepción de asimetría para la determinación del ataque, y segundo llevar a cabo la acción a pesar de la inferioridad ante el poderío que se enfrenta. La relevancia que apuntala el pensamiento militar chino del carácter «*asimétrico*» de los medios «*cibernéticos*» es reseñada por Bunker (2007):

> Se presta gran atención a los terroristas, hackers y otras organizaciones no gubernamentales y de cómo pueden participar en la nueva forma de hacer la guerra que se está desarrollando. Los autores sostienen que los militares de EE.UU. simplemente no ven la amenaza que estos grupos representan. Los métodos utilizados por estos grupos aportan lecciones importantes para China. (Bunker, 2007: 116).

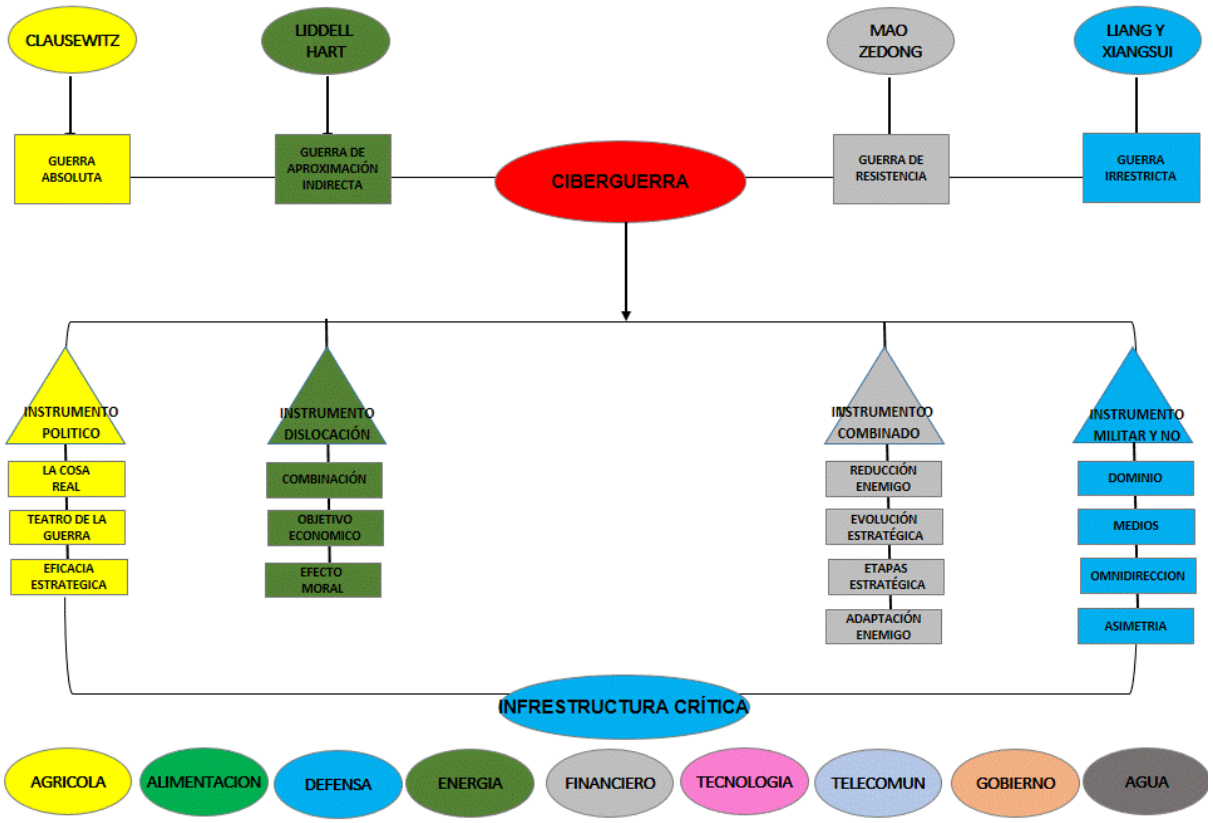
Esas lecciones aprendidas por las fuerzas armadas chinas y plasmadas estratégicamente por Liang y Xiangsui contienen un elemento transversal que es lograr un nivel de independencia

en la tecnología de defensa, para propiciar que sus adversarios no tengan claro cuáles son sus fortalezas o debilidades, diseminando sus fuerzas para generar imprevisibilidad, concordando esto con las reflexiones de Van Creveld (1991), quien sugiere: «Por lo tanto, la concentración en realidad consiste en la dispersión, mientras que la dispersión consiste en la concentración, la victoria va para el que mantiene el control y evita la confusión, cambiar rápidamente de una a otra» (Van Creveld, 1991: 121).

Una característica estructural de la «*guerra cibernética*» es la dispersión de los atacantes, siendo difícil su ubicación para neutralizarlos, en ese sentido, se debe procurar que el adversario desconozca la ubicación de las fuerzas informáticas que podrían atacar, defenderse o contraatacar, debiendo además descentralizarse y desmilitarizarse las posibles respuestas, ya que el carácter asimétrico del ataque informático es una fortaleza que hay que aprovechar.

El presente marco teórico que se ha apoyado en estrategas militares buscaba hacer un diálogo académico entre preceptos clásicos y contemporáneos del pensamiento militar, proyectándolo a la «*ciberguerra*», con la finalidad de percibir las confluencias y aplicabilidades de los principios y máximas que han sustentado durante siglos los planes y acciones bélicas, conjugándolas con precisiones tecnológicas de la coyuntura informática que caracteriza a la sociedad actual. A continuación se expone un cuadro explicativo, donde se puntualiza los elementos esenciales de cada intelectual de la guerra, y cuáles son esos fundamentos que tienen concomitancia para el teatro de la guerra cibernético, para ser direccionados contra una infraestructura crítica.

Esquema del Vínculo entre el pensamiento Estratégico y la Ciberguerra



CUADRO ELABORADO POR EL AUTOR DE LA PRESENTE TESIS DE INVESTIGACIÓN

CAPÍTULO III

3. ORÍGENES Y DESARROLLO ESTRATÉGICO DE LA CIBERGUERRA

3.1 La Cibernética y el Ciberespacio

Hace casi quinientos años (1532) en el tratado conocido como «*Dell 'arte della guerra*» Maquiavelo reflexionaba que: «Lo que favorece al enemigo nos perjudica a nosotros, y lo que nos favorece a nosotros perjudica al enemigo». Con el razonamiento anterior se quiere reflejar que en temas estratégicos las propuestas teóricas encuentran paralelismos entre el pasado y el presente, la misma faceta de pensamiento maquiavélico consigue asidero en el uso de ataques informáticos enmarcados en una «*Ciberguerra*». El componente tecnológico es un factor que ha incidido históricamente en la transformación del ámbito bélico, por ello como refleja Bacallao (2011): «el desarrollo de las artes guerreristas ha estado estrechamente ligado a la invención de nuevos instrumentos técnicos, y entre ellos, un lugar crecientemente especial – tan o más que el que ocupan los artefactos de matar–, han tenido las tecnologías comunicativas» (Bacallao, 2011: 57).

Para comprender el fondo conceptual de la «*Ciberguerra*», es importante entender semánticamente su significado compuesto, para visualizar concretamente que contiene y que descarta esta novedosa perspectiva bélica. Primeramente, hay que indagar sobre el término «*cibernética*», el Diccionario de la Lengua Española en su vigésima segunda edición del año 2001 expone que el origen etimológico de la palabra se vincula al término griego «κυβερνητική» (arte de gobernar una nave), pero el significado más básico referenciado en el mismo texto alude al: «Estudio de las analogías entre los sistemas de control y comunicación de los seres vivos y los de las máquinas; y en particular, el de las aplicaciones de los mecanismos de regulación biológica a la tecnología» (RAE, 2001).

Esta reseña general, conduce a escrutar sobre los pensadores que originaron esta corriente, estando los antecedentes en la primeras décadas del siglo XX, cuando escritores como Norbert Wiener fueron precursores de los estudios que inquirían explicar los relacionamientos y diferenciaciones entre seres vivientes y estructuras creadas artificialmente por el hombre, sugiriendo que la finalidad de la «*cibernética*» es el desarrollo de «[…] un lenguaje y técnicas que nos permitan de hecho atacar el problema del control y la comunicación en general, pero también para encontrar un buen repertorio de ideas y técnicas para clasificar a sus manifestaciones particulares en conceptos determinados» (Wiener, 1988: 17). Hay que destacar que Wiener tuvo sus primeras incursiones teóricas de la mano de Arturo Rosenblueth Stearns, siendo este estudioso de origen azteca uno de los estructuradores de los basamentos cibernéticos, destacándose: «La influencia enorme para la formación de ideas de Wiener acerca del problema de la interacción "hombre-máquina"» (Burtseva, Tyrsa, Ríos & Flores, 2013: 48). Fue así, que se colocaron los cimientos de lo que sería la «*cibernética*», que examinaba los ámbitos de control y comunicación tanto en la interrelación humana, animal y de las máquinas.

Estas pinceladas iniciales del pensamiento «*cibernético*» que emprendía explicaciones biológicas y físicas, posteriormente tuvieron en Ross Ashby uno de los artífices de las reflexiones actuales, pre visualizando en su obra «*An Introduction to Cybernetics*» lo vasto y conexo del tema, apuntando que esta rama de pensamiento tendería a desvelar «[…] una gran cantidad de paralelismos interesantes y sugerentes entre la máquina, el cerebro y la sociedad. Y puede proporcionar un lenguaje común por el que los descubrimientos en una rama con facilidad se puede hacer uso en otras» (Ashby, 1957: 4).

Esos tres factores de estudio (máquina/cerebro/sociedad) coinciden en una interoperabilidad que funge como eje transversal, conllevando a la generación de toda una nueva gama de procesos, relaciones, y lenguajes sociales. El pasar de los años fueron

ampliando el margen de aplicación, convirtiendo la «*cibernética*» en un campo multidisciplinario, destacando al respecto Heylighen y Joslyn (2001) que: «[...] la amplia filosofía cibernética de que los sistemas se definen por sus relaciones abstractas, funciones y flujos de información, en lugar de su material concreto o componentes, está empezando a impregnar la cultura popular, aunque de una manera todavía superficial [...]» (Heylighen & Joslyn, 2001: 5). De alguna manera, esa impregnación cultural que expresan los anteriores autores se fue imbuyendo en una ampliación «*ininteligible*», ligada al modismo propio de los años ochenta donde el uso extensivo del vocablo «*ciber*» tendió a identificar actividades o enfoques muy diversos. Pero es importante clarificar que para el interés académico de esta investigación, el contenido que es útil y se quiere referenciar, está ligado a esa conectividad y radialidad de la información propia de los medios computacionales que se asumen como células de un sistema virtual, que como propone Von Foerster (2003) «[…] la cibernética surge cuando los efectores (digamos, un motor, una máquina, nuestros músculos, etc) están conectados a un órgano sensorial que a su vez trabaja con sus señales sobre los efectores. Es esta organización circular la que establece los sistemas cibernéticos […]» (Von Foerster, 2003: 287).

La complejidad que encarnan todos aquellos vocablos que anteponen el prefijo «*ciber*» se manifiesta en el uso de la palabra «*ciberespacio*», que contradictoriamente no se vincula inicialmente a las teorías de control o sistemas que moldearon la «*cibernética*» disciplinariamente, sino que varios autores lo remontan al año 1984 en la obra literaria de William Gibson, quien describe el «*ciberespacio*» en uno de sus pasajes ficticios como: «Una alucinación consensual experimentada diariamente por billones de legítimos operadores, en todas las naciones, por niños a quienes se enseña altos conceptos matemáticos... Una representación gráfica de la información abstraída de los bancos de todos los ordenadores del sistema humano. Una complejidad inimaginable» (Gibson, 1984: 26). A pesar de lo

novelesco de esta propuesta, lo expuesto por Gibson da un abreboca de lo que ciertamente unas décadas después sería el escenario digital interconectado, que reúne concordancias con lo sugerido en su obra «*Neuromante*».

Entrando en un campo más teórico, Cicognani (1998) intenta irrumpir en las profundidades terminológicas para proponer que «[...] en el término ciber+espacio, espacio asume el significado de materia física, mientras que ciber le da las características inmateriales» (Cicognani, 1998: 20). Unificar lo físico y virtual, no ha sido sencillo, y ha necesitado un hondo ejercicio analítico, para ampliar y derrumbar viejos paradigmas que hacían imperioso lo material para asumirlo como real. Este intenso debate [7] sobre el «*ciberespacio*» ha conducido a reflexiones como las de Post (2013) quien indica: «[…] la pregunta "¿el ciberespacio realmente es un 'lugar'?"- es curiosa. Es como preguntar si la vida en la tierra es "idéntica a" o "diferente a" la vida en el océano. La respuesta es que se trata, simultáneamente, de ambas» (Post, 2013: 10). Pero, incluso asumiendo una postura de reconocimiento del espacio cibernético, las diferentes corrientes de pensamiento vuelven a recaer en otra bifurcación analítica, que consiste en abstraer el «*ciberespacio*» de lo social y centrarse en explicaciones «*instrumentalistas*», que si bien son importantes, terminan por ser incompletas, encontrándose explanaciones sistemáticas como las de Folsom (2007) que la detalla: «[...] como una red conmutada incorporada para mover tráfico de datos, más caracterizada por diversos grados de acceso, navegación, actividad-informática, e incremento (de la confianza)» (Folsom, 2007: 80).

[7] De hecho, las interpretaciones teóricas del «ciberespacio» cuentan con dos grandes vertientes conocidas como los «*Excepcionalistas*» (The Exceptionalists) y los «*No Exceptionalistas*» (The Unexceptionalists), estando los primeros enmarcados en el establecimiento de regulaciones e interpretaciones que asuman la especificidad que personifica el «ciberespacio». Mientras que los segundos, pregonan que la legislación existente en el «*espacio cinético*» se puede proyectar en el «ciberespacio».

En contraparte, resaltan las definiciones tendientes a abordar este espacio virtual estrechándolo con lo humano, ya que las conceptualizaciones, usos, aportes, no pueden deslindarse de su esencia social, y el «*ciberespacio*» en definitiva es una creación antrópica, como destaca Anders (2001): «Podemos caracterizar el ciberespacio como la referencia espacial utilizada en los medios de comunicación electrónicos, pero que plantea nuestra necesidad de definir el propio espacio, por lo que experimentamos como el espacio es en realidad el producto de procesos mentales complejos» (Anders, 2001: 409).

Lo manifestado por Peter Anders sobre esa construcción mental compleja indica que patrones conductuales generadores de la guerra cinética se pueden materializar en la virtualidad, quedando claro para algunas naciones las posibilidades bélicas de este nuevo espacio, generando una atención inmediata dentro de sus mandos militares, que perciben las potencialidades estratégicas y tácticas, en relación a esto espeta Flores (2012) que: «[...] una definición aprobada respecto a ciberespacio, habría consenso respecto a que las acciones de guerra relacionadas al mismo impactan en los ámbitos terrestres (tierra y mar) y aeroespacial, e interactúan con éstos en forma sinérgica» (Flores, 2012: 18). En esa misma línea de pensamiento, el Departamento de Defensa estadounidense, dedicó tiempo y espacio en sus investigaciones para dejar plasmado en su «*Diccionario Militar*» una definición que orientaría las operaciones armadas en el «*ciberespacio*», exponiéndolo como: «Un dominio mundial en el entorno informático consistente en una red interdependiente de infraestructuras de tecnologías de la información, incluida Internet, redes de telecomunicaciones, sistemas informáticos, procesadores y controladores embebidos» (Department of Defense Dictionary of Military and Associated, 2011: 92). Lo expresado precedentemente muestra como el «*ciberespacio*» pasó de una creación literaria a una dimensión técnica que trascendió paulatinamente las redes para convertirse en un novedoso proceso social que ha entrado en la órbita de estudio de organismos castrenses de potencias hegemónicas como campo de lucha,

que empezaron a llenar los vacíos en las estrategias militares que surgían de este fenómeno.

3.2 La Ciberguerra y sus armas como factores para la reconfiguración estratégica

Una vez esbozada la connotación de «*cibernética*» y «*ciberespacio*», es preciso adentrarse en su vinculación con la guerra, que ha pasado por un proceso acumulativo de conceptualizaciones de investigadores que han intentado dar la justa medida a esta novedosa forma bélica, aconteciendo lo que Fritz (2013) denotaba: «Con el crecimiento de la guerra cibernética como un campo de estudio, la cantidad de terminología cibernética relacionada también ha crecido» (Fritz, 2013: 2). Esta multiplicidad de interpretaciones y la necesidad de tomar medidas cibernéticas en materia de Defensa enfrentó a muchos estrategas y gobernantes a tener que asumir una delimitación entre el antiguo y nuevo campo de batalla que era inadvertido en el pasado, tal como los exponen Winterfeld y Andress (2012): «La diferencia principal entre Cinético (el verdadero mundo) y el No - Cinético (el mundo virtual) es la metodología de guerra, las armas contra programas de software que ellos usan» (Winterfeld & Andress, 2012: 3). La materialización de la batalla en este nuevo «*Teatro de la Guerra*» generó inmediatamente un controvertido giro que pasaba de la convencionalidad militar entre Estados que es perfectamente detectable y suele tener una respuesta recíproca en poder de fuego, a un escenario centrado en la virtualidad informática, donde los límites y acciones se hacen dudosos, aunque la capacidad de infringir daño puede ser la misma.

Sobre esta cuestión McGraw (2013) exhibe: «La ciberguerra requiere un consecuente impacto en el mundo físico, o lo que los expertos militares llaman un efecto "cinético" […] Para calificar como una guerra cibernética, los medios pueden ser virtuales, pero el impacto debe ser físico» (McGraw, 2013: 111-112). Por tanto, hay confluencias en la guerra informática y física, siendo las más palpables: el uso de la fuerza, y por otra parte, el fin político que persigue el ataque, que son los baluartes para establecer la identidad (Intelectual/Material) del «*cibercontendor*», reflejando Kostyuk y Alí (2013): «Tanto la

guerra tradicional y la guerra cibernética son similares en que su objetivo común es lograr una ventaja frente a un Estado-nación, competir o tratar de impedir que dicho Estado-nación alcance una ventaja» (Kostyuk & Alí, 2013: 241).

Es así que varios teóricos han pretendido acoplar en un esquema articulado las diferentes variables intervinientes en la «*ciberguerra*», con la finalidad de hacer más digerible la propuesta, explicando Lewis (2010) que la guerra convencional consistiría en la utilización de componentes militares con la finalidad que un país destruya o averíe las capacidades de un adversario, mientras que: «La Ciberguerra implicaría un esfuerzo por parte de otra nación o de un grupo por motivos políticos a utilizar ciberataques para alcanzar fines políticos» (Lewis, 2010: 1). Lo expuesto por Lewis es concordante con los principios «*clausewitzanos*» que supeditan lo militar a lo político, siendo la «*ciberguerra*» un medio y no un fin en sí mismo. En gran medida, lo esgrimido en las líneas previas, coincide con lo agregado por Flores (2012) que hace un vuelco actoral, indicando que la guerra cibernética es: «la figura de un Estado o grupo de Estados que atacan la estructura funcional y/o decisional de otro u otros Estados, empleando el ciberespacio (normalmente junto al empleo de capacidades cinéticas tradicionales)» (Flores, 2012: 25). Se revela que la divergencia entre Lewis y Flores recae en que éste último da una vinculación estatal al ataque, circunscribiendo el episodio bélico al accionar entre los actores tradicionales. Esta perspectiva, ejemplifica lo controvertido y dinámico de la variable cibernética en la guerra, ya que hay quienes parten para su definición de la relación simétrica, mientras que otros autores amplían el espectro del contrincante informático hacia individualidades o grupos asimétricos.

Una propuesta enfocada en parámetros técnicos, la aborda Swanson (2010) que apoyándose en varios estudiosos de asuntos informáticos expresa que la guerra cibernética consiste en: «[…] la última forma de la guerra de información, y puede incluir ataques a redes informáticas (CNA), que consisten en "operaciones para interrumpir, denegar,

deteriorar o borrar información albergada en ordenadores o redes informáticas, o los ordenadores y las propias redes"» (Swanson, 2010: 308). No es menor, el hecho que en esta conceptualización se identifique la «*ciberguerra*» como un subconjunto de la «*guerra de información*»[8], siendo esto un indicio del rico crisol de disertaciones que existen sobre el tema. Complementando la tecnificación abordada por varios diseños investigativos, algunos académicos ya han detectado diferenciaciones necesarias sobre aspectos que aparentan similitud, pero internalizan cuestiones diferentes, los autores Arquilla y Ronfeldt (1997) intentan desmarcar la «*ciberguerra*» y la «*guerra en red*», en relación a la primera analizan lo siguiente: «Ciberguerra se refiere a la conducción, y la preparación para llevar a cabo, las operaciones militares de acuerdo a los principios relacionados con la información. Significa romper si no la destrucción de la información y sistemas de comunicación [del adversario]» (Arquilla & Ronfeldt, 1997: 30). Es decir, la acción cibernética no sólo se compone de una operatividad militar que claramente persigue la inutilización o neutralización de las fuerzas informáticas rivales, sino que hay una fase estratégica previa donde se afianzan los planes y se prepara su ejecución.

Por otra parte, los mismos analistas contraponen el término «*guerra en red*» (*netwar*) que no tiene una finalidad militar necesariamente y los ataques no están plenamente relacionados al direccionamiento de un adversario estatal, indicando que esta forma bélica abarca acciones de: «[…] diplomacia pública, propaganda y campañas psicológicas, subversión política y cultural, el engaño o interferencia con los medios locales, la infiltración

[8] «En última instancia, la guerra de información es sobre el uso de información para tomar decisiones y tratando de influir, negar o alterar información que se utiliza en los procesos de toma de decisiones del adversario» (Williams, 2010: 38).

de las redes informáticas y bases de datos, y los esfuerzos para promover disidencia o movimientos de oposición a través de redes informáticas» (Arquilla & Ronfeldt, 1997: 28). De cada una de las facetas discurridas, se observa como las referencias intelectuales sobre la «*ciberguerra*» son variables y se van matizando según las perspectivas políticas que persiguen los Estados, pero está claramente demostrado que es un campo de estudio que se desarrolla pujantemente, y requiere esfuerzos investigativos para mejorar su comprensión.

En los planteamientos de los autores anteriores, la diferencia clave radica en lo actoral (Actores: Estatales o No), pero en general concuerdan que la «*ciberguerra*» conlleva «*ciberataques*» dirigidos contra la «*infraestructura crítica*» de otro Estado. Por tanto, el ataque cibernético amerita de mecanismos o armas para ocasionarle un daño que destruya o incapacite la capacidad de Defensa (Cinética o No Cinética) del contrincante, expone Trendle (2002): «[…] la ciberguerra ha introducido una serie de nuevas armas, tales como virus, gusanos y caballos de Troya, que puede causar estragos en los sistemas informáticos» (Trendle, 2002: 7). Pero es importante evitar confundir que cualquier uso de tecnología militar sea una «*ciberguerra*», ya que aunque en la actualidad se desarrollan a nivel mundial conflictos armados convencionales con el uso de armamento tradicional optimizado con dispositivos tecnológicos para mejorar su rendimiento, en esos casos no se puede calificar estos como «*ciberarmas*». En palabras de Piris (2003) en los conflictos informáticos se: «emplean armas cibernéticas: virus, ataques electrónicos a los servidores informáticos, perturbación de las bases de datos, interferencias o contaminación de programas y dispositivos, saturación de sus posibilidades de conexión, penetración en redes protegidas que controlan elementos vitales y otras acciones» (Piris, 2003: 69).

Previo a detallar algunas de estas armas cibernéticas, es relevante dedicar un espacio de análisis a los escenarios para hacer uso de estas, coincidiendo varios especialistas en que técnicamente algunos desarrollos para la «*ciberguerra*» independientemente del nombre dado

en cada país, podrían encontrar similitudes concretas en su forma de aplicación, comparativamente planteamientos estadounidenses, ingleses, y chinos, por citar a algunas potencias militares con capacidad cibernética, tienen planes operativos que podrían enmarcarse en las llamadas «*Operaciones de la Red Informática*» (CNO), como lo expresa, Rathmell (2003) quien aporta:

> CNO son un subconjunto de un conjunto más amplio de actividades maliciosas mediadas por computadoras. De acuerdo con el proyecto de doctrina militar británica, CNO comprende: Red de Explotación Informática (CNE), a saber: "la capacidad de tener acceso a la información alojada en los sistemas de información y la posibilidad de hacer uso del propio sistema"; Ataque de Red de Computadoras (CNA), a saber: "el uso de nuevos enfoques para entrar en las redes informáticas y atacar a los datos, los procesos o el hardware"; y la Red Informática de Defensa (CND), que es "protección contra el enemigo del CNA y CNE e incorpora enfoques de hardware y software junto a enfoques basados en la gente." A su vez, CNO es uno de los elementos de las Operaciones de Información (IO). (Rathmell, 2003: 215).

Tanto el «*CNO*» que aglutina a «*CNE*», «*CNA*», y «*CND*» comprenden en general las modalidades de accionar en el campo cibernético, y se puede detectar un «*isomorfismo*» práctico en el desempeño de las «*ciberoperaciones*», más allá del enunciado que quiera dar cada Fuerza Armada. La referencia de Andrew Rathmell en su parte final vincula a las «*CNO*» como un componente de las denominadas «*Operaciones de Información*» (*IO*), que los autores Rob Sentse y Arno Storm apoyándose en documentación militar británica, explican como: «Una función militar para proporcionar asesoramiento y coordinación de las actividades de información militar con el fin de crear efectos deseados en la voluntad, la comprensión y la capacidad de las audiencias […]» (Sentse & Storm, 2010: 7). Lo previo,

coloca a las «*ciberarmas*» utilizadas en las «IO» como medios[9] de un amplio arsenal de posibilidades que se combinan para lograr los objetivos en una confrontación bélica.

Una vez expuestos los «*Teatros de Operaciones*» en donde se podrían utilizar las armas cibernéticas, se pasa a revisar sucintamente el potencial de las mismas, resaltando su carácter inadvertido, que no debe ser confundido con inocuidad, ya que la propagación sigilosa es una poderosa forma de causar severos daños al enemigo, pudiéndose a grandes rasgos denominarse estas armas informáticas como «*malware*», que abarcaría los «*virus*», «*gusanos*», «*caballos de Troya*», «*rootkit*», y «*bombas lógicas*». Previo al inicio del análisis de estos mecanismos informáticos, es preciso dejar sentado que el «*medio*» por sí sólo no define el derrotero de una guerra, y que el instrumento técnico debe estar siempre supeditado a la proyección estratégica que se le quiera dar, reflexionando sobre esto Gordon (2008): «El Malware es incapaz de destruir edificios, derribar gobiernos, o tomar decisiones tácticas. En ambos casos, el patógeno puede ser capaz de desestabilizar el medio ambiente específico y permitir un ataque complementario para tener éxito» (Gordon, 2008: 1).

El término «*malware*» aglutina un amplio conjunto de armas informáticas utilizadas para efectuar diferentes tipos de incursiones o infringir daños variables a la «*infraestructura crítica*» de un Estado, describiendo Waters, Ball, y Dudgeon (2008) este mecanismo digital como: «El software malicioso diseñado para llevar a cabo acciones molestas o dañinas. El

[9] Según la Directiva del Departamento de Defensa estadounidense Nº O-3600.1 del 14 de agosto del 2006, y que fue hecha pública conforme a la «Freedom of Information Act» el 09 de mayo de 2008, las «IO» comprenden «El empleo integrado de las capacidades básicas de la guerra electrónica (EW), Operaciones de la Red Informática (CNO), las operaciones psicológicas (PSYOP), engaño militar (MILDEC) y de Operaciones de Seguridad (OPSEC)» (Department of Defense, 2006: 1)

malware a menudo se disfraza como programas útiles o se incrusta en programas útiles para que los usuarios sean inducidos a la activación de ellos» (Waters, Ball & Dudgeon, 2008: 48). Teniendo una concepción general sobre el «*malware*», se precisa abordar una de las herramientas más publicitadas, y que suelen ser ampliamente combatidas, los llamados «*virus*», que consiste en: «[…] un conjunto viral que contiene exactamente un programa, que simplemente se reproduce a sí mismo. Conjuntos más grandes representan los virus polimórficos, que tienen un número de diferentes formas posibles, todo lo cual eventualmente reproduce todos los demás» (Chess & White, 2000: 1). Una analogía algo cruda, pero pertinente para comparar la propagación del virus informático, es la funcionalidad dada al virus biológico por los colonos ingleses, que entregaban frazadas infectadas con viruela a los indígenas norteamericanos para erradicarlos durante las luchas acontecidas en el establecimiento de sus colonias, es así como un «*ciberadversario*» lentamente contamina los sistemas computacionales vitales de su contrincante hasta inutilizarlos.

En esa misma secuencia descriptiva sobre las armas cibernéticas entran los denominados «*gusanos*», que suelen tener menos seguimiento con relación a los «*virus*», configurando una peligrosidad exponencial ante el desconocimiento o subestimación que los rodea, detallándolos los expertos de la siguiente manera: «Un gusano informático es un programa que se auto-propaga a través de una red que explota fallos en las política de seguridad o en los servicios de uso común» (Weaver, Paxson, Staniford & Cunningham, 2003: 11). Por otra parte, están los frecuentemente nombrados «*caballos de Troya*», que al igual que el legendario equino de madera descrito por Homero y Virgilio, asume la sorpresa y el engaño para irrumpir en un sistema informático, es así que: «[…] un caballo de Troya se instala en el ordenador del usuario sin su conocimiento. Ese pequeño programa entonces se ejecuta en segundo plano, sin el conocimiento del usuario, y en el silencio espera para tomar acción» (Kang, 2005: 1554). En la cadena destructiva de las armas cibernéticas que se viene

siguiendo, se presenta un programa seriamente amenazante el «*rootkit*», que según alertan Wang y Dasgupta (2007): «Entre los malwares, los rootkits son la amenaza más peligrosa. Ellos son particularmente difíciles de detectar y prevenir, ya que son internos a los sistemas operativos y se esconden por parchear el kernel» (Wang & Dasgupta, 2007: 1). Finalmente, pero no menos letales están las «*bombas lógicas*», que son las más referenciadas entre la literatura militar, al temerse que sean una de las posibles «*ciberarmas*» a utilizar contra la infraestructuras crítica, ya que permanecen inactivas en el tiempo, esperando ser activadas ante una coyuntura bélica que lo amerite, disertando Klimburg (2011): «[…] Estos archivos ocultos o paquetes de software son relativamente pequeños y, ya que no necesitan comunicarse, son extremadamente difíciles de localizar. Una vez activadas, las bombas lógicas pueden ser enormemente destructivas» (Klimburg, 2011: 42).

Ahora bien, más allá de las apreciaciones teóricas expuestas primariamente, se pueden citar algunos casos puntuales del uso de estas armas cibernéticas (malware), y su potencial destructivo. A pesar que no suele relacionarse las confrontaciones informáticas con la «*Guerra Fría*» uno de los primeros usos de una «*ciberarma*» se registró cuando en el año 1982 la Agencia Central de Inteligencia (CIA) colocó una «*bomba lógica*» en un software canadiense que había sido sustraído por agentes soviéticos para ser utilizado en instalaciones gasíferas en la Unión Soviética (URSS), como detalla Hamilton (2009):

> Una vez instalado en el oleoducto trans-Siberiano, el controlador corrió una prueba de medidores de presión en la tubería durante el cual la bomba lógica restableció esos medidores de gas al doble de presión en la tubería. La explosión resultante era, hasta ese momento, la explosión no nuclear más grande alguna vez fotografiada desde el espacio. (Hamilton, 2009:15)

El remontarnos a los años ochenta del siglo XX nos demuestra la vieja data de las armas cibernéticas, pero casi tres décadas después entre los años 2009 y 2010, salió a la palestra

pública las implicaciones de un ataque cibernético orquestado de nuevo por los estadounidenses, pero en este caso su objetivo era la República Islámica de Irán, que tuvo una afectación por un «*malware*» en sus instalaciones de Bushehr, siendo calificado por algunos analistas técnicos de «*gusanos*» y otros lo enmarcan dentro de los «troyanos», sobre esto explica Joyanes (2010) que el «*Stuxnet*» es un software dañino: «[…] del tipo troyano muy avanzado, que aprovecha la vulnerabilidad MS10-0466 […] y que se utiliza en infraestructuras críticas tales como el control de oleoductos, plataformas petroleras, centrales eléctricas, centrales nucleares y otras instalaciones industriales con el objetivo de sabotearlos» (Joyanes, 2010: 26). Lo antepuesto, realza la importancia de deslastrar la «*ciberguerra*» y sus armas de la connotación futurista, fantástica o ficticia y comprender que es una realidad concreta, y que la parálisis estratégica sólo contribuye en el acrecentamiento de las amenazas para un Estado.

Tanto la «*ciberguerra*» como sus armas incursionaron intempestivamente, requiriendo en el mundo militar una acelerada restructuración estratégica ante la nueva realidad derivada de los sistemas tecnológicos, apunta Sierra (2002): «[…] la guerra informacional representa un replanteamiento de raíz de la acción bélica, la estrategia y sistema de mando, control e inteligencia, así como de la táctica y la organización militar, cada vez más dependientes del dominio y capacidad de destrucción informativa […]» (Sierra, 2002: 2). Destaca en este razonamiento como la red informática definió los parámetros de las acciones militares futuras, ya que contradictoriamente muchas de las tecnologías de la información pasaron del campo castrense al civil, y esta transferencia se hizo en el entendido de su condición neutra. No obstante, la organización militar y la estrategia de la «*ciberguerra*» han dejado seriamente cuestionado el principio de «*neutralidad de la red*», el cual se fundamenta en que: «Internet debe permanecer sin cambios para garantizar que sus contenidos no serán objeto de manipulación por aquellos que gocen de los privilegios suficientes para alterarlos» (Soler &

Hernández, 2010: 331). Cabe señalar que el debate sobre la «*neutralidad de la red*» es un ideal más que una realidad, pues los campos de batalla computacionales dejaron de ser simulaciones, y son sustento de grandes inversiones por parte del «*Complejo Militar Industrial*» que construye nuevos armamentos al unísono de la diversificación del posible «*cibercontrincante*». En retrospectiva, una percepción estatal de neutralidad cibernética puede configurar una debilidad a ser aprovechada estratégicamente por los oponentes para planificar escenarios de ataque, en palabras de LibiCki (2012): «Los estados pueden atacarse unos a otros de muchas maneras sin que la víctima sepa exactamente quién lo hizo o incluso qué se hizo» (LibiCki, 2012: 19).

Los enfoques de diversos análisis mundiales dan luces de lo importante que es la materialización de una estrategia en el área cibernética, como detalla Ferrero (2013): «Algunas naciones, entre ellas China, Rusia, Corea del norte e Israel, disponen de unidades especializadas con capacidad de llevar a cabo ciberataques, por lo que es necesario disponer de una capacidad de defensa ciberespacial que garantice una protección […]» (Ferrero, 2013: 87). Sin embargo, lo vertiginoso del escenario informático ha engendrado una tendencia mundial hacia la militarización a ultranza del «*ciberespacio*», asumiéndose estrategias controladoras y restrictivas, como las emanadas de centros hegemónicos, pero como apunta Kiravuo (2013): «la estrategia de defensa nacional no exige necesariamente que se trate como parte de la defensa bajo el régimen militar. Esta defensa cibernética puede ser considerada como parte de la defensa civil, en lugar de la defensa militar» (Kiravuo, 2013: 90). Empero, un escenario necesario para el «*ciberteatro*» de la guerra actual, pasa por no desligar totalmente a las instancias civiles y militares, para propiciar una respuesta integral en un conflicto informático. Es decir, el debate sobre el carácter militar o civil que se debe imprimir a la «*ciberestrategia*» no puede empantanar la adopción de la misma, ya que la mutación del campo de batalla del siglo XXI hace impostergable la implementación de medidas para

asumir un ataque informático que ponga en peligro la integridad del conjunto nacional o supraestatal, referenciando Sanz y Fojón (2011): «los adversarios, en cualquiera de sus formas (naciones, grupos criminales o terroristas, facciones extremistas, etc.) tienen acceso y pueden utilizar las mismas tecnologías de un modo completamente innovador y singular» (Sanz & Fojón, 2011: 43).

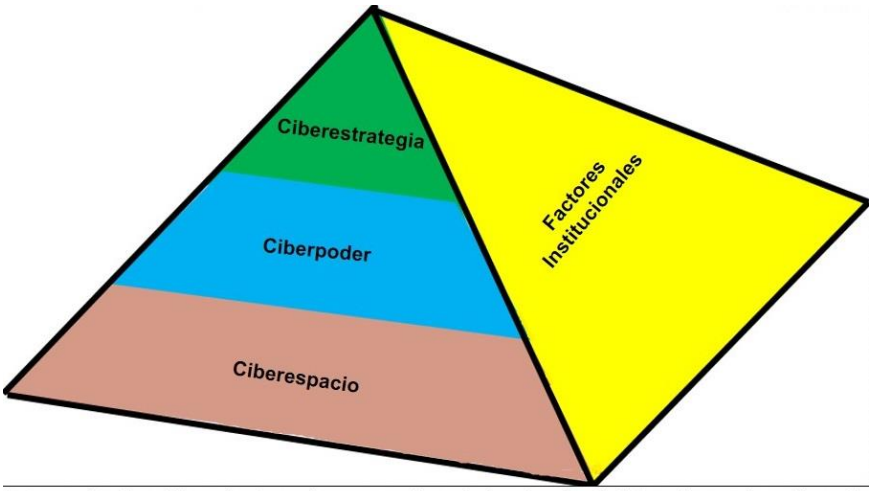
Dentro de esas concepciones sobre establecer una estrategia para enfrentar acciones enmarcadas en una «*ciberguerra*» puntualiza Rattray (2001) que hay cuatro condiciones estratégicas favorables, sobre las que se debe sostener un conflicto bélico: «1. Libertad de acción Ofensiva; 2. Vulnerabilidad significativa para atacar; 3. Mínima perspectiva de represalia y escalada; 4. Capacidad para identificar y seleccionar el centro de gravedad del adversario» (Rattray, 2001: 4). Esta propuesta no es lejana a algunos de los planteamientos estratégicos de Clausewitz, Ludendorff, Lenin, Liddell Hart, Mao Zedong, pero el hilo conductor para enhebrar la visión tradicional con la «*ciberguerra*» recae en complementarlo con cinco elementos propiciadores de una «*capacidad tecnológica*» para sustentar una «*ciberestrategia*»: «1. Entorno institucional propicio; 2. Motivación de la demanda; 3. Iniciativa de gestión; 4. Conocimientos tecnológicos; 5. capacidad de aprendizaje» (Rattray, 2001: 4). Por tanto, como se ha reiterado en varios pasajes de esta investigación, lo «*monolítico*» de la conducción ofensiva, defensiva, o contraofensiva de la «*ciberguerra*» sólo es posible a partir de plasmar una propuesta que amalgame: La «*Estrategia*» y la «*Capacidad Tecnológica*», en búsqueda de superar el reiterado desbalance estratégico/táctico, vinculado a decisiones apresuradas de gobiernos o altos mandos militares que pretenden minimizar las vulnerabilidades con la adquisición de soluciones técnicas (software o hardware), pero sin la debida proyección y planificación que se logra bajo un direccionamiento que se enmarque en lo que Rantapelkonen, y Salminen (2013) aclaraban:

> La ciberdirección requiere algo más que hablar; también requiere declaraciones conjuntas, planes e implementación de acciones conjuntas. El fomento de la comprensión compartida de los dirigentes debe promoverse. Se debe tomar una iniciativa para promover el discurso cibernético. (Rantapelkonen & Salminen, 2013: 11).

En los estudios estratégicos ha surgido un concepto que hace acompañamiento teórico a la «*ciberestrategia*» como es el «*ciberpoder*», ambas definiciones se interrelacionan y despejan algunas dudas sobre el carácter con que se asume el «*ciberespacio*» por los actores. Particularmente el autor Starr (2009) clarifica el fondo de dichos presupuestos, sobre el «*ciberpoder*» afirma que: «Es la capacidad de utilizar el ciberespacio para crear ventajas y eventos de influencia en los otros entornos operativos y a través de los instrumentos de poder» (Czosseck & Geers (Eds.), 2009: 22). Interpretando lo expuesto, se distingue que se inclina hacia la dominación del «ciberespacio»; mientras que la «*ciberestrategia*» representaría: «el desarrollo y el empleo de las capacidades para operar en el ciberespacio, integrado y coordinado con los otros dominios operacionales, para establecer o apoyar el logro de los objetivos a través de los elementos del poder nacional» (Czosseck & Geers (Eds.), 2009: 22). Es decir, la estrategia cibernética sería el emprendimiento de planes y acciones por un Estado en el «*ciberespacio*» conforme a sus fines políticos, pero no necesariamente contiene un germen dominador.

Finalmente, y que es relevante referenciarlo, Stuart H. Starr se empeña en dar la justa dimensión a los conceptos, en la medida que es necesario establecer las prioridades del personal que se amerita para consolidarlos, señalando que en el «ciberespacio» se enfoca hacia lo técnico (físicos, ingenieros eléctricos, informáticos, de sistemas). En tanto, que el «ciberpoder» precisa de personal que apuntalé planes de dominación (política, diplomática, informática, militar, y económica). Y en la cúspide de la pirámide está la «*ciberestrategia*»

que en palabras de Starr (2009): «[…] hay una necesidad de expertos interdisciplinarios que sean capaces de hacer frente a toda la gama de cuestiones políticas, militares, económicas, sociales, informáticas y de infraestructura […]» (Czosseck & Geers (Eds.), 2009: 23-24).



Este cuadro fue elaborado tomando como referencia la obra de Christian Czosseck, y Kenneth Geers (Eds.). (2009). The Virtual Battlefield: Perspectives on Cyber Warfare (Vol. 3). Ios Press. p.p. 23-24.

Lo enunciado pone en evidencia lo holístico que debe ser la estructuración de una «*ciberestrategia*», que debe cumplir con una cadena lógica, donde lo estratégico oriente lo táctico, y no a la inversa, siendo Kiravuo (2013) bastante puntual al respecto: «La credibilidad de la defensa cibernética no se basa en la cantidad de servidores, firewalls o técnicos, ya que el atacante puede seleccionar el punto de ataque» (Kiravuo, 2013: 90). Por tanto, la «*ciberguerra*» debe ser un eje clave, a ser tomado en cuenta en una estrategia global de Defensa, ya que: «A pesar de su capacidad demostrada para producir efectos cinéticos, la verdadera importancia de la guerra cibernética radica en su aplicación estratégica» (Olson, 2012: 67).

3.3 Elementos Normativos y Principios de la Ciberguerra

La confrontación entre Estados ha sido una constante generadora de conflictos durante toda la historia, el control de lo que llamaba Sun Tzu «*terreno de confluencia de caminos*», que se podría traducir en la «*ciberguerra*» como la supremacía sobre el oponente en el campo informático, es fuente de discordia entre los hegemónes mundiales en la actualidad. Acota

desde la perspectiva politológica Colom (2009) que las luchas entre potencias: «También verá disputada su hegemonía en áreas puntuales como el espacio, el ciberespacio o la información» (Colom, 2009: 2). Los teóricos estadounidenses de hecho, promueven la militarización de las redes de información, previendo que su control será una determinante estratégica para el accionar táctico en un conflicto futuro, Bodine y Mills (2011) indican que el ciberespacio: «definitivamente es un ámbito por el cual luchar […] el ciberespacio es análogo a otros ámbitos bélicos; por ende, podemos aplicar lecciones del espacio y de las operaciones aéreas al ciberespacio» (Bodine & Mills, 2011: 11).

De lo preliminar, se desprende que un ataque informático puede constituir un «*Acto de Guerra*», ya que el uso de un medio computacional puede ocasionar serios daños a la «*infraestructura crítica*» de una nación, razona Stone (2013): «Por otra parte, la influencia de la mediación de la tecnología significa que los pequeños actos de fuerza - como tocar un teclado - pueden dar lugar a una gran cantidad de violencia, mortal o no» (Stone, 2013: 107). La gran disyuntiva es el ligar la trilogía atacante-arma-objetivo que en el mundo «*cinético*» es menos difusa, Rid (2012) reflexiona sobre el «*Acto de Guerra*» o «*Acto de Fuerza*» tradicional, que puede comprender: «[…] descargas de artillería, un avión de ataque no tripulado, los dispositivos explosivos improvisados colocados a un lado de un camino, incluso un terrorista suicida en una plaza pública […] Un acto de guerra cibernética sería un juego completamente diferente» (Rid, 2012: 9).

El análisis de Rid que intenta afincar la condición de letalidad para configurar un «*Acto de Guerra*», muestra lo confuso que es aplicar esa visualización al atacante y acto hostil digital, y que la proporcionalidad en la respuesta es aún más entramada, ya que confundir un hecho individual con un acto de otro Estado puede ser el desencadenante de una guerra «*cinética*». Con respecto a esto último, varios estudiosos militares advierten de la relativa libertad de acción cibernética con que cuentan algunas fuerzas militares, siendo esto

un peligro al poder ocasionar un «*Acto de Guerra Informático*» que no esté autorizado por las jerarquías políticas. Haciendo una comparación sobre los protocolos para el uso de armamento nuclear en la «*Guerra Fría*» que estaban estrictamente delimitados, destaca Junio (2013) la disparidad en el proceder del uso de «*ciberarmas*» al desvirtuarse su letalidad: «[…] vienen a ser percibidas ampliamente (como potestativas), siendo razonable concluir que el umbral para su uso será más bajo que otros tipos de armas - incluso si el costo de los ataques cibernéticos es mayor» (Junio, 2013: 130).

Como se evidencia de lo anteriormente citado, hay dificultades internas y externas para encaminar una perspectiva dilucidante sobre el «*Acto de Guerra Informático*». En este orden de ideas, Beidleman (2009) intenta mostrar esa tenue línea entre la guerra y un ataque que no debe escalar en un conflicto de mayor gravedad, aclarando que más allá del «*ciberataque*» y su carácter intrínsecamente hostil: «[…] en el ciberespacio, no todos los ataques cibernéticos equivalen a un ataque armado […] En algún lugar a lo largo de este espectro de los conflictos en el ciberespacio, el ataque cibernético cruza el umbral y se convierte en un ataque armado» (Beidleman, 2009: 12). Esta ilustración teórica, aflora lo dubitativo que es canalizar los factores de reconocimiento del «*Acto de Guerra Informático*», siendo ilusorio asegurar que hay un consenso mundial sobre la temática, particularmente porque la brecha tecnológica entre las naciones que tienen mayor desarrollo cibernético, y los países que arrastran problemas sociales estructurales más graves, colocan el debate en diferentes ámbitos de prioridad, dando una ventaja injusta a quienes accionan irrestrictamente en el «*ciberespacio*» al poseer un monopolio tecnológico.

Por si fuera poco, otra dificultad para detectar la autoría de un «*Acto de Guerra Informático*» recae en la multiplicación de grupos o individualidades que bien sean a «*motu proprio*» o bajo el patrocinio de algún Estado, pueden causar severos daños a la infraestructura de una nación con un sutil mecanismo cibernético. Estos actores no

gubernamentales, irregulares, o asimétricos son una variable que expone a los Estados a agresiones informáticas, siendo referidos por Sánchez (2010): «[…] Actualmente, existen alrededor de 10.000 sitios web dedicados a la divulgación de material violento y terrorista, lo que indica un crecimiento de la presencia de estos grupos en el ciberespacio» (Sánchez, 2010: 203). Lo ininteligible del contendor que atacará, bien sea en busca de posicionar sus luchas ante la comunidad internacional o hacer visible sus exigencias (Políticas, religiosas, ideológicas, reivindicativas, económicas), hacen dificultoso el rastrear el origen de un ataque cibernético, debiendo el Estado o entidad vulnerada dar una respuesta en una fracción de tiempo, y discerniendo si se dirigirá hacia un actor estatal o no estatal, ejemplifica Goldsmith (2010): «Es muy difícil, y muy intensivo en recursos, y a veces imposible, trazar con mucha certeza el origen del equipo de un ataque cibernético profesional o de explotación cibernética, es aún más difícil de hacerlo en tiempo real o incluso en el corto plazo» (Goldsmith, 2013: 4).

Precisamente, el mundo de posibilidades que significa el «*ciberespacio*» para ejercer acciones lesivas contra gobiernos, instituciones o personas, es enfocado por Denning (2000) que discurre: «Para un terrorista, tendría algunas ventajas sobre los métodos físicos. Podría llevarse a cabo de forma remota y de forma anónima, y no requeriría la manipulación de explosivos o una misión suicida» (Denning, 2000: 75). En el análisis precedente y el debate teórico entre autores, se exteriorizan elementos que colocan lejano el establecimiento del «*Acto de Guerra Informático*» bajo un consenso mundial, entre otros elementos por: Indefinición del atacante (Estatal/No estatal); Carencia de parámetros para diferenciar medios (Ciberguerra, Ciberterrorismo, Ciberespionaje, Guerra en Red (Netwar)); y superposición de normas internas y externas (Seguridad/Defensa), como acota Brenner (2007) una secuela del «*isomorfismo*» de la soberanía/territorio: «[…] es que las amenazas para el orden social son fácilmente identificables como internas (crimen / terrorismo) o externas (guerra). La

comunicación mediada por ordenador erosiona la validez de este árbol de decisión binario haciendo territorio cada vez más irrelevante […]» (Brenner, 2007: 382).

El que se haya ido desdibujando la territorialidad estatal, se refleja en la dinámica actual de la política internacional, que dista notablemente de la apreciación que planteaba Mearsheimer (2005) en donde un marco de reconocimiento mutuo entre Estados, concebía una institucionalización con normativas explicitas o implícitas, que entre otras áreas regían el accionar en la guerra o el conflicto: «Estas reglas son negociadas por los estados, y de acuerdo con muchos de los teóricos importantes, implican la aceptación mutua de las normas más altas, que son las normas de comportamiento definidas en términos de derechos y obligaciones» (Mearsheimer, 2005: 8). El último conflicto referencial a gran escala que fue la «*Guerra Fría*» tuvo en la estrategia de «*Destrucción Mutua Asegurada*» un acuerdo no escrito de definición de pasos para evitar una operación militar que conllevará a una confrontación letal, pero en el «*teatro de operaciones informático*» las formas para regular el proceder de la guerra computacional no existen a escala global. El escenario cibernético conforme pasan los años hace impostergable el establecimiento de normas que sienten las bases de un derecho internacional sobre la materia, que permita fijar límites a los Estados, así como lo hicieron en su momento las convenciones sobre la guerra de Ginebra, en palabras de Janczewski y Colarik (2008): «Por lo tanto, hay una necesidad urgente de una legislación global para el manejo de la guerra cibernética y el ciberterrorismo […] Al abordar el acecho cibernético, nuevas e innovadoras legislaciones, e investigaciones de tecnologías y contramedidas seguramente serán obligatorias» (Janczewski & Colarik, 2008: 223).

Ese debate necesario sobre la «*ciberguerra*» debería partir de la Organización de las Naciones Unidas (ONU) que es la instancia internacional que puede generar parámetros mundiales para delimitar el accionar bélico en el «*ciberespacio*», el propio texto fundacional recoge principios jurídicos que son aplicables a la lucha virtual que está empezando a

prevalecer entre los países, estableciendo el artículo segundo de la Carta de las Naciones Unidas (1945), en su cuarto numeral que: «Los Miembros de la Organización, en sus relaciones internacionales, se abstendrán de recurrir a la amenaza o al uso de la fuerza contra la integridad territorial o la independencia política de cualquier Estado, o en cualquier otra forma incompatible con los Propósitos de las Naciones Unidas» (ONU, 1945: 3).

Sin embargo, para el momento de adopción de este instrumento no se avizoraba lo poco convencional que sería el panorama bélico medio siglo después, al respecto Hoisington (2009) indica: «Con el fin de definir la guerra cibernética efectivamente, la comunidad internacional debe llegar a un consenso sobre el significado de este tipo de actividades dentro de la penumbra de la Carta, en particular el artículo 2 (4) la regulación del uso de la fuerza […]» (Hoisington, 2009: 446). Pero, los debates y discusiones diplomáticas para construir un basamento jurídico conjunto sobre la «*ciberguerra*» son meras proyecciones, constituyendo excepciones las acciones de organismos militares como la OTAN y naciones que individualmente han emprendido su regulación (EE.UU., Rusia, o China), por tanto, como argumenta Banks (2013): «Desarrollar un entendimiento consensuado sobre el derecho internacional de la ciberguerra es complicado por unos atributos singulares del ámbito cibernético. Señalar la intencionalidad de un ataque e incluso la identificación de las amenazas puede ser muy difícil» (Banks, 2013: 162).

Los menudos intentos por promover una legislación mundial han sido relegados paulatinamente por las instancias militares dominantes, que han llevado la delantera con respecto al análisis de las normativas internacionales para contribuir a construir una doctrina y estrategia cibernética, en el caso estadounidense Hughes (2010) señala que el año 2009 el Comité de Guerra de la Información ofensiva del Consejo de Investigación Nacional de EE.UU. (NRC) desarrolló un informe sobre la temática, expresando que: «[…]la Carta de las Naciones Unidas-incluyendo tanto las leyes que rigen la legalidad de ir a la guerra (jus ad

bellum) y la ley que rige el comportamiento durante guerra (jus in bello) se aplican a los ciber-ataques» (Hughes, 2010: 534). Proyectar los basamentos legales de la guerra cinética a la informática es enmarañado, ya que la determinación de la naturaleza jurídica de una norma trasciende el mero reacomodo, pero la propuesta de la «*NRC*» asume una reingeniería legal que es necesaria. En relación a ese debate del contexto cibernético de la guerra, Schmitt (2012) remarca que los «*ciberataques*» enmarcados en operaciones militares deben cumplir las máximas de una acción convencional, aclarando que el comportamiento debe ajustarse a: «[…] el jus ad bellum principio de proporcionalidad, permitiendo sólo el grado de fuerza que se requiere para una defensa eficaz. El uso de la Ciberfuerza en frente de un ataque armado debe cumplir además los requisitos relacionados de inminencia y la inmediatez […]» (Schmitt, 2012: 286).

En el mismo sentido que las disertaciones sobre el «*Acto de Guerra Informático*» buscan un fundamento válido para iniciar un conflicto como condición «*sine qua non*» para los Estados, el desarrollo de la doctrina jurídica y militar debe procurar el despejar las incertidumbres sobre la interpretación de una «*Causa Justa*» para declarar una «*ciberguerra*», reflexiona interrogativamente sobre casos ambiguos para determinar la justicia de la causalidad en la guerra cibernética Eberle (2013) exponiendo:

> Sin embargo, algunos ataques cibernéticos destruyen la propiedad sin matar o mutilar a nadie […] Naturalmente, esto plantea la pregunta: ¿es la destrucción de la propiedad siempre una causa justa para la guerra? Si es así, ¿cuándo la destrucción de la propiedad proporciona una causa justa para la guerra? […] Así que tal vez, como una cuestión de derecho, la destrucción de la propiedad no letal puede dar en el blanco con el permiso de usar la violencia militar. (Eberle, 2013: 61).

No sólo estas interrogantes, sino muchas más están sin respuesta en el «*Derecho Internacional*» que no logra dar cuenta de la naturaleza jurídica de la «*ciberguerra*», y los

órganos multilaterales tienen repuestas «*tibias*» o hacen caso omiso al vacío legal que va a ocasionar graves conflictos en el corto y mediano plazo.

Las «lagunas» normativas sobre la «*ciberguerra*» han desembocado en la estructuración de medidas «*supralegales*» por parte de naciones o instancia de Defensa multinacionales, que ante el letargo o despreocupación de la comunidad internacional han generado un conjunto de doctrinas tendientes a establecer los parámetros para intervenir militarmente en el «*ciberespacio*». Hay dos ejemplos palpables sobre este tipo de instrumentos, uno sería el llamado «*Manual de Tallínn*» (Tallinn Manual on the International Law Applicable to Cyber Warfare), elaborado por un conjunto de expertos a pedido del Centro de Excelencia en Ciberdefensa Cooperativa de la Organización del Tratado del Atlántico Norte (OTAN) en el año 2013; y por otra parte, la «*Presidential Policy Directive 20*» (PPD-20) que fue emitida por el gobierno de Obama y que data del 2012, que representan antecedentes en lo jurídico, estratégico y operativo de la «*ciberguerra*», pero además, muestran un horizonte de los peligros que se avecinan relacionados con la unilateralidad y extraterritorialidad.

En relación al «*Manual de Tallínn*», esta interesante propuesta jurídica hace un amplio desarrollo de términos basados en el «*jus ad bellum*» y «*jus in bello*», relacionándolos con preceptos legales de uso clásico como la soberanía, jurisdicción, territorialidad, y la responsabilidad del Estado, en un entorno cibernético. En la «*Regla 1*», numeral primero, el referido texto manifiesta sobre la «*cibersoberania*» que: «Esta regla hace hincapié en el hecho de que, aunque ningún Estado podrá reivindicar su soberanía sobre el ciberespacio *per se*, los Estados pueden ejercer prerrogativas soberanas sobre cualquier ciberinfraestructura situada en su territorio, así como las actividades relacionadas con esa ciberinfraestructura» (Schmitt (ed.), 2013: 25). De forma discreta, hay un contenido intrínseco de extraterritorialidad basado en el dominio tecnológico, es decir, evidentemente el

«*ciberespacio*» es una amplia red interconectada que no se circunscribe a un territorio específico, pero el perfilar normativamente que se podrá ejercer soberanamente acciones sobre una «*ciberinfraestructura*» que probablemente tendrá raíces en diferentes naciones, deja abierta la posibilidad de legitimar operaciones sobre plataformas tecnológicas de otros Estados. Esto último, es aún más palpable, cuando en la misma propuesta legal, se enfatiza lo maleable que puede ser la identificación de jurisdicción en relación al espacio cibernético, tomando como basamento la determinación de la territorialidad esbozada en 1994 por la Procuraduría General de Justicia del Tribunal Europeo:

> […] (i) la territorialidad subjetiva, la que permite al Estado hacer frente a actuaciones que se han originado dentro de su territorio, a pesar de que se completaron en el extranjero, (ii) la territorialidad objetiva, que, por el contrario, permite a un Estado hacer frente a actuaciones que se han originado en el extranjero, pero que se han completado, al menos en parte, dentro de su propio territorio (Schmitt (ed.), 2013: 29).

Esta dualidad en la jurisprudencia se afinca aún más en el aspecto «*cibernético*», ya que la intervención de la virtualidad hace que se tienda a sobreponer una concepción extraterritorial que se encuentra circunscrita a la objetividad o subjetividad territorial. Como se analiza en el numeral nueve de la «*Regla 2*» del «*Manual de Tallínn*» un ataque cibernético puede ser efectuado contra un Estado desde un país extranjero, por un actor no estatal que detente una nacionalidad distinta al lugar desde donde se perpetró. Conllevando esto a que hayan distintas competencias en la jurisdicción para intervenir, en vista que podrían alegar interés: el Estado agraviado por el ataque, el Estado desde donde se generó la acción enemistosa, o el Estado que identifica al actor atacante como ciudadano de su país.

En la «*Regla 6*» que versa sobre la responsabilidad del Estado, en su numeral tercero destaca que la ilicitud del ataque cibernético puede fundamentarse en una transgresión a lo

estipulado en la Carta de las Naciones Unidas: «[…] (por ejemplo, un uso de la fuerza cometida a través de medios cibernéticos, Regla 10) o una violación de un derecho de las obligaciones del conflicto armado (por ejemplo, un ataque cibernético contra bienes de carácter civil, artículo 37) atribuible al Estado en cuestión» (Schmitt (ed.), 2013: 35-36). De hecho, el determinar la ilegalidad de las acciones atribuibles a un Estado es sumamente enmarañado para la mayoría de las naciones, que no cuentan con medios informáticos para detectar incursiones ilegales o ataques contra su «*infraestructura crítica*». Como se ejemplifica en ese mismo numeral tercero, mientras un buque de guerra este de «*paso inocente*» tiene prohibido el emprendimiento de «*ciberoperaciones*» contra la nación costera, pero cabría la pregunta ¿Puede un Estado con escasos recursos informáticos detectar que está siendo víctima de una incursión cibernética? La respuesta seguramente será negativa. Por tanto, la extraterritorialidad se afianza en el subdesarrollo tecnológico imperante en el mundo, que sólo cuenta con una decena de naciones con capacidad para realizar este tipo de operaciones y detectarlas.

En el estricto ámbito de la «*ciberguerra*» el precitado manual adapta un conjunto de conceptos propios del «*Derecho Internacional*» tradicional para describir una coyuntura en donde se lleven a cabo «*ciberoperaciones*» y sus fundamentos jurídicos, como son las limitaciones geográficas, la participación en los conflictos armados, el ataque cibernético, y el principio de distinción. En el caso de las denominadas «*Limitaciones Geográficas*» se quiere dar un carácter espacial que se asimile a las guerras convencionales, para de alguna manera establecer cuáles son las fronteras que abarca una «*ciberoperación*», refiere el manual en la «*Regla 21*», numeral primero que pueden emprenderse: «[…] en o con efectos en todo el territorio de las partes en el conflicto, las aguas o espacio aéreo internacionales, y, con sujeción a ciertas limitaciones, el espacio exterior. Las operaciones cibernéticas generalmente están prohibidas en otro lugar» (Schmitt (ed.), 2013: 71). Aunque al final de

este artículo se advierten las excepciones o prohibiciones, la permisividad de las acciones cibernéticas queda ampliamente aceptada en el propio manual en prácticamente cualquier espacio que involucre a los beligerantes en un conflicto.

Más adelante en el Capítulo IV donde se estudia la «*Conducción de las hostilidades*», en la «*Regla 26*» dedicada a las fuerzas castrenses intervinientes en operaciones cibernéticas, formula la normativa que sí los integrantes de un componente militar en conflicto: «[…] en el curso de operaciones cibernéticas, no cumplen con los requisitos del estatuto de combatiente, pierden su derecho a la inmunidad de combatiente y de prisionero de estado de guerra» (Schmitt (ed.), 2013: 84). Es decir, independientemente de lo poco ortodoxo del combatiente cibernético, este debe ajustarse a las reglas establecidas por la comunidad internacional, obrando dentro de los límites bélicos para optar al estatus legal que le corresponda.

El Protocolo Adicional a los Convenios de Ginebra, aprobado el 8 de junio de 1977 instituye en su artículo 49 lo que en «*Derecho Internacional*» debe considerarse como ataque, estableciéndose que son: «los actos de violencia contra el adversario, sean ofensivos o defensivos» (Protocolo Adicional a los Convenios de Ginebra, 1977: 20), tomando esta estructura es que el «*Manual de Tallínn*» edifica la conceptualización de ataque cibernético, detallando que: «Un ataque cibernético es una operación cibernética, ya sea ofensiva o defensiva, es decir que supone razonablemente que cause lesiones o la muerte a personas o daños o destrucción de objetos» (Schmitt (ed.), 2013: 92). Es precisa la definición al asomar la letalidad que puede internalizar un «*ciberataque*», siendo particularmente ilustrativa esta regla, que despeja dudas sobre la afectación de lo «*virtual*» en lo «*cinético*», que trasciende el mero daño material, y puede suprimir la vida humana.

El documento preparado para el Centro de Excelencia en Ciberdefensa Cooperativa de la OTAN, establece que la destrucción física o informática debe responder a normativas internacionales como la «*Declaración de San Petersburgo*», celebrada entre noviembre y

diciembre de 1868, que intentaba humanizar la guerra para deslindarse de la aniquilación, indicando: «Que la única finalidad legítima que los Estados deben proponerse durante la guerra es el debilitamiento de las fuerzas militares del enemigo» (Declaración de San Petersburgo, 1868: 1). En concordancia con lo expresado en 1868, los estudiosos del derecho internacional y los diferentes expertos que intervinieron en la elaboración del manual coinciden en fundamentar ese lindero bélico con el «*Principio de Distinción*», que tiene como finalidad hacer una clara diferenciación entre la población civil y las fuerzas militares que se enfrentan en una guerra, estando crucialmente relacionado este fundamento jurídico a las «*ciberoperaciones*» que no deben transgredir este límite, en el entendido que al establecer como objetivo a: «[…] civiles o bienes de carácter civil (o de otras personas y objetos protegidos) se eleva a la categoría de un ataque, estando prohibida por el principio de distinción y de las normas del derecho de los conflictos armados que se derivan de este principio» (Schmitt (ed.), 2013: 96). No obstante, lo explicado sobre el «*Principio de Distinción*» queda reducido a lo eminentemente teórico, ya que al contrastarlo con el proceder bélico en este siglo XXI queda claramente expuesto que la población civil ha sido objeto de afectaciones directas de la guerra convencional y cibernética.

En este examen del «*Manual de Tallínn*» se han tomado algunas de las noventa y cinco (95) reglas de la propuesta teórica, que deja visiblemente establecido el avance normativo por parte de organizaciones militar y tecnológicamente dominantes como la OTAN, siendo particularmente alarmante el hecho que sean exiguas las estrategias y políticas de otras naciones, quedando seriamente comprometida su espacio cibernético. Tomado como referencia final la «*Regla 94*» relacionada a la «*Respuesta de las partes en conflicto a Violaciones*» que detalla: «Si un Estado neutral no puede anular el ejercicio de los derechos de los beligerantes en su territorio, la parte agraviada en conflicto podrá tomar las medidas, incluso por ciberoperaciones, ya que son necesarias para contrarrestar ese comportamiento»

(Schmitt (ed.), 2013: 207). Si bien, los expertos matizan la intervención en un tercero haciendo énfasis en la necesidad de medir la neutralidad, gravedad, o amenaza, pareciera que el «*garantísmo*» de la propuesta legal se va diluyendo por la preeminencia de los objetivos militares de la alianza atlántica.

Contradictoriamente a los alegatos jurídicos desarrollados por el conjunto de expertos en el ensayo teórico que originó el «*Manual de Tallínn*», en las normativas establecidas por el gobierno norteamericano sobre «*ciberoperaciones*» como la llamada «*Presidential Policy Directive 20*» (PPD-20), no se hacen tantas consideraciones sobre la legalidad internacional de intervenir en espacios fuera de la jurisdicción de su país, centrándose en el reconocimiento del fuero de: « […] la Constitución de los EE.UU. y otras leyes y políticas aplicables de los Estados Unidos, incluidas las órdenes presidenciales y directivas» (PPD-20, 2012: 11). En ese entorno, lo que eran visos de extraterritorialidad en parte del articulado del documento trabajado para el Centro de Excelencia en Ciberdefensa Cooperativa de la OTAN, es plenamente visible en la doctrina surgida en el gobierno de Obama, que hace del espacio cibernético un «*teatro de la guerra*». Mientras que la generalidad de los Estados apenas inician procesos para establecer leyes o manuales sobre asuntos informáticos, los estadounidenses llevan la delantera en atender estos requerimientos para preparar el terreno ante una «*ciberguerra*», conteniendo la normativa referenciada reglas que desarrollan en parte o se complementan con todo un entramado legal especializado que también reglamenta asuntos cibernéticos en diferentes entornos con un alcance interno y externo:

> NSPD-54/ Directiva Presidencial de Seguridad Interna (HSPD)-23 sobre "Política de Ciberseguridad" del 8 de enero de 2008; la Directiva de Seguridad Nacional (NSD)-42 sobre "Política Nacional para el Resguardo de la Seguridad Nacional de las Telecomunicaciones y Sistemas de Información" del 5 de julio de 1990 y la PPD-8 sobre "Preparación Nacional" del 30 de marzo de 2011. (PPD-20, 2012: 1).

En el contenido de la «PPD-20» se hace una clara identificación del «*Objeto y ámbito de aplicación*» de esta política, que enfatiza la importancia de regular las operaciones que se realicen en el espectro de las redes informáticas, estableciendo la importancia para los EE.UU. del: «[…] desarrollo y mantenimiento del uso del ciberespacio como una parte integral de las capacidades nacionales estadounidenses para reunir información y para disuadir, negar, o vencer a cualquier enemigo que busque perjudicar los intereses nacionales norteamericanos en la paz, la crisis o la guerra» (PPD-20, 2012: 4). Nótese que las acciones sobre el «*ciberespacio*» no se ciñen a la guerra, quedando legalizado el proceder de las agencias militares o civiles para hacer cumplir la «PPD-20» si perciben peligros a los intereses de su país, incluyendo operaciones en tiempos de paz o en una coyuntura de crisis.

En el contenido de la directiva, se detallan aspectos que ciertamente reflejan el futuro de la guerra, precisando tres acciones que son la columna vertebral de la «PPD-20», como son las llamadas «*Operaciones Defensivas de Efectos Cibernéticos*» (DCEO), las «*Operaciones Ofensivas de Efectos Cibernéticos*» (OCEO), y las «*Ciberacciones de Emergencia*». En relación a las «*Operaciones Defensivas de Efectos Cibernéticos*» (DCEO), este texto señala que estas se circunscriben a las direccionadas por la administración estadounidense: «[…] destinadas a permitir o producir efectos cibernéticos fuera de las Redes del Gobierno de los Estados Unidos con el propósito de defender o protegerlo contra amenazas inminentes, o ataques en curso, o actividades cibernéticas maliciosas contra los intereses nacionales norteamericanos dentro o fuera del ciberespacio» (PPD-20, 2012: 3). Si se analiza a fondo el «*DCEO*», se pueden encontrar aspectos preocupantes sobre lo ilimitado del carácter de la operación, que puede ampliarse más allá de redes que territorialmente se ubiquen en Estados Unidos, dejando además nítidamente fijado que podrán hacer uso de medios cibernéticos defensivos ante acciones que estén o no vinculadas a vulneraciones informáticas.

En la estrategia militar, siempre se preparan escenarios defensivos y ofensivos, es así que los estadounidenses plantean también las «*Operaciones Ofensivas de Efectos Cibernéticos*» (OCEO), que abarcan acciones, programas y actividades autorizadas por las instancias competentes del gobierno norteamericano, indicándose que las: «OCEO pueden ofrecer capacidades únicas y no convencionales para hacer avanzar los objetivos nacionales de los Estados Unidos en todo el mundo, con poca o ninguna advertencia al adversario u objetivo y con los efectos potenciales que van desde lo sutil a lo severamente perjudicial» (PPD-20, 2012: 8). Aunque la «PPD-20» es reiterativa sobre el apego de sus operaciones al derecho estadounidense y a ciertos principios de las normas internacionales, se palpa una anteposición de sus «*objetivos nacionales*» en desmedro de la soberanía nacional de otros países, reflejando la explicación del «*OCEO*» una discrecionalidad legal de los gobiernos norteamericanos para la aplicación de «*ciberoperaciones*», que sin tapujos son reseñadas en relación a su carácter inadvertido o por lo altamente dañinos para el contrincante.

Esta facultad potestativa para impulsar operaciones cibernéticas independientemente del otro Estado donde ocurrirán queda asentada en la premisa que refiere que el primer mandatario de los EE.UU. previa sugerencia de la comisión de diputados competente en la materia, o de sus directores en asuntos de seguridad decidirá lo ineludible de: «[…] una excepción a la obtención de consentimiento, teniendo en cuenta los intereses nacionales generales de los Estados Unidos y que las acciones cumplan con un alto umbral de necesidad y los resultados puedan ser eficaces en relación con los riesgos creados por esa excepción» (PPD-20, 2012: 7). No obstante, si las autoridades en aplicación de la «PPD-20» se decantan por el consentimiento de otra nación, esto queda estrictamente limitado a que: «La información revelada a otros países en el curso de búsqueda de consentimiento deberá ser coherente con los requerimientos de seguridad operacional y la protección de las fuentes de inteligencia, métodos y actividades» (PPD-20, 2012: 6-7), siendo seriamente limitada las

eventuales explicaciones pre y post operativas de la «*cibercontienda*».

Finalmente, en el entendido que las eventualidades del escenario bélico actual pueden entrañar situaciones que escapen a la mera planificación ofensiva/defensiva, expone la «PPD-20» las medidas urgentes que deben emprender el conjunto de órganos del gobierno norteamericano para ejecutar «*Ciberacciones de Emergencia*», que prevenga o enfrenten la inminencia de una amenaza: «[…] contra los intereses nacionales de los Estados Unidos desde dentro o fuera del ciberespacio y en circunstancias que en el momento no permiten obtener la previa aprobación presidencial de la medida, requiriéndose dicha autorización de otro modo» (PPD-20, 2012: 3-4). Lo apremiante de la coyuntura cibernética hace de las «Ciberacciones de Emergencia» una medida que potencialmente puede generar un amplio margen de daños colaterales, ya que al ser emprendido unilateralmente por un alto mando militar quien consideró que su accionar debía ser inmediato, deja en un segundo plano la cadena de mando político que reside en el presidente estadounidense, pudiendo desencadenar la acción no cinética (Ciberguerra) en una respuesta cinética (Guerra Convencional).

CAPÍTULO IV

4. POLÍTICA SUDAMERICANA SOBRE CIBERDEFENSA

4.1. El Regionalismo y la conformación del Consejo de Defensa Suramericano (CDS) en el marco de la Unión de Naciones Suramericanas (UNASUR)

Durante el período comprendido entre el inicio del siglo XX y la década de los noventa del mismo, las formas de «*regionalización*» en Sudamérica fueron acompañantes de los modelos económicos nacionales o supranacionales, con un limitado espacio de maniobra en ámbitos estratégicos (políticos, sociales, ambientales o tecnológicos). Los tenues esfuerzos por apuntalar una integración encontraron serios problemas en hacer confluir las dinámicas estatales de los países del norte y sur del subcontinente. Las experiencias sudamericanas respondían a la realidad del momento en el sistema internacional, que se ilustra al analizar teóricamente dos enfoques: el «*régimen internacional*» y el «*régimen de comercio internacional*», con respecto al primero señala Ruggie (1998): «Los regímenes internacionales son comúnmente definidos como instituciones sociales en torno a las cuales las expectativas de los estados convergen en diversas temáticas» (Ruggie, 1998: 177). Dentro de ese conjunto de temáticas fue la basada en un relacionamiento o intercambio economicista la que preponderó en la centuria pasada en la región, donde el factor social no era céntrico sino periférico, ajustándose este escenario a la caracterización que Keohane (1998) hacia del «*régimen de comercio internacional*» referenciándose en la experiencia del General Agreement on Tariffs and Trade (GATT), refiriendo:

> El régimen de comercio internacional, por ejemplo, no tenía reglas formales o fuertes, gestión integrada y centralizada, sino que proporcionan un conjunto de instituciones interrelacionadas, incluyendo reuniones regulares de las partes contratantes del GATT, los acuerdos formales de resolución de conflictos, y la delegación de tareas técnicas a una secretaría, que desarrolló gradualmente un cuerpo de jurisprudencia y procedimientos. (Keohane, 1998: 85).

Por tanto, la organicidad de estos regímenes responden a criterios arancelarios, impositivos, aduanales, que resaltan el fondo comercial omnipresente con preeminencia del intercambio económico, que prioriza los beneficios empresariales a las necesidades sociales. La institucionalidad sudamericana que precedió a la UNASUR (Unión de Naciones Suramericanas), es decir la CAN (Comunidad Andina de Naciones) y MERCOSUR (Mercado Común del Sur) se manejaron dentro de un ámbito que disminuía lo político al mínimo, obviaba lo estratégico, descartaba lo social, y maximizaba lo comercial, pudiendo calificase en estricto apego al concepto de «*regímenes de comercio internacional*». Además, lo preliminar se encuadraría en una «*regionalización*» más que un «*regionalismo*», que los teóricos Bernal-Meza, y Masera (2008) intentan deslindar, ya que los conceptos suelen ser usados como pares:

> Si la regionalización es el proceso mediante el cual se conforman áreas regionales de comercio en la economía mundial, el regionalismo es tanto el sistema de ideas que actúa como teoría de la diversificación de los espacios de integración en el escenario internacional, como el criterio normativo que permite la formulación de políticas orientadas a la construcción de esquemas institucionales regionales. (Bernal-Meza, 1999: 2).

Sólo hasta iniciado el nuevo milenio la subregión empezó a establecer procesos que trascendían la «*regionalización*» circunscrita a un «*régimen de comercio internacional*», unificándose esfuerzos para construir un «*regionalismo sudamericano*» que tuviera un perfilamiento político estratégico, conforme lo plasma Bonilla (2010) quien expresa: «El nuevo regionalismo sudamericano parecería entender al comercio como un instrumento de integración política, y no como el objetivo final de la misma» (Bonilla, 2010: 25).

Dentro de esta nueva concepción subregional, los primeros antecedentes directos de un proceso de «*regionalismo*» se remonta al año 2000, cuando desde Brasil se convocó a

todos los presidentes de Sudamérica a una cumbre que tenía como finalidad la conformación de la «*Iniciativa para la Integración de la Infraestructura Regional Suramericana (IIRSA)*». No obstante, la infraestructura fue sólo una de las temáticas, y se dejó señalado en el «*Comunicado de Brasilia*» en su numeral octavo que los Jefes de Estado: «Manifestaron la convicción de que el refuerzo de la concertación suramericana en temas específicos de interés común constituirá un aporte constructivo al compromiso con los ideales y principios que han orientado su proceso de integración» (Comunicado de Brasilia, 2000: 2). Fue así que se transitó paulatinamente hacia la constitución de la Comunidad Sudamericana de Naciones (CSAN), que tuvo en la III Cumbre Presidencial Sudamericana celebrada en Perú en 2004 un avance significativo, quedando establecida en la declaración final la voluntad colectiva de los mandatarios asistentes para crear una institucionalidad en la región, acordándose que: «La Comunidad Sudamericana de Naciones establecerá e implementará progresivamente sus niveles y ámbitos de acción conjunta, promoviendo la convergencia y sobre la base de la institucionalidad existente, evitando la duplicación y superposición de esfuerzos y sin que implique nuevos gastos financieros» (CSAN, 2004: 3). La experiencia de la «CSAN» sirvió de fase previa para la maduración del proceso de integración, lográndose establecer algunas convergencias de agendas y planteamientos regionales sobre problemas compartidos. No obstante, la dinámica de interacción marcaba la necesidad de trascender esta iniciativa, desembocando en que: «La CSAN fue reemplazada por la Unión de Naciones Suramericanas en abril de 2007, en la primera Cumbre energética sudamericana realizada en Venezuela» (Baroni & Rubiolo, 2010: 137). Ratificándose esta decisión en la reunión con carácter extraordinario citada en Brasilia en el año 2008, donde finalmente se estableció el Tratado Constitutivo, que dejaba expresamente señalado en su artículo segundo:

> La Unión de Naciones Suramericanas tiene como objetivo construir, de manera participativa y consensuada, un espacio de integración y unión en lo cultural, social,

> económico y político entre sus pueblos, otorgando prioridad al diálogo político, las políticas sociales, la educación, la energía, la infraestructura, el financiamiento y el medio ambiente, entre otros, con miras a eliminar la desigualdad socioeconómica, lograr la inclusión social y la participación ciudadana, fortalecer la democracia y reducir las asimetrías en el marco del fortalecimiento de la soberanía e independencia de los Estados. (UNASUR, 2008: 2).

Dentro de esta nueva lógica establecida en la UNASUR, empezaron a surgir un conjunto de desafíos derivados de la extensa agenda y la diversidad de percepciones para el abordaje institucional, pero particularmente llama la atención el devenir estratégico regional, que va más allá del análisis meramente político, como Bizzozero (2011) puntualiza: «En particular, se fueron esbozando, a partir de los cambios de gobierno que se produjeron en los países de la región: una modificación de las prioridades, centrándolas en lo político y social; una vinculación del regionalismo con el debate estratégico sobre el orden internacional y su estructura» (Bizzozero, 2011: 36).

El reencuentro entre muchos Estados en un espacio político como la UNASUR, tras décadas de acumulación de un «*sentimiento hostil*» [10] azuzado por viejos diferendos limítrofes, significó un avance regional especialmente para debatir temas de Defensa que siempre habían estado ocultos o secretos. Esta variación re direccionó la «*polaridad*» fuertemente arraigada en la realidad regional, como ilustra Menezes (2010) se propició una variación notable de los patrones de «*amistad/enemistad*» sudamericanos, aclarando:

[10] En su momento Clausewitz ilustró cómo el sentimiento hostil puede ser un factor desencadenante del conflicto: «En dos naciones y estados pueden producirse tales tensiones y tal cúmulo de sentimientos hostiles que un motivo para la guerra, insignificante en sí mismo, puede originar, no obstante, un efecto totalmente desproporcionado con su naturaleza, como es el de una verdadera explosión» (Clausewitz, 2002: 13).

> Argumentamos que una de las contribuciones esenciales, sino la más importante del regionalismo en lo que respecta al cambio en la polarización sudamericana, fue haber funcionado como un catalizador de los emprendimientos cooperativos e integracionales, expandiéndose hacia toda la región a la luz de la Unasur. (Menezes, 2010: 52).

El desarrollo de la iniciativa regional tuvo en 2008 un punto de inflexión, cuando en el encuentro con carácter extraordinario celebrado en Brasil específicamente en Salvador de Bahía, los primeros mandatarios asistentes consensuaron la institución del Consejo de Defensa Suramericano (CDS), estipulándose lo siguiente: «Créase el Consejo de Defensa Suramericano como una instancia de consulta, cooperación y coordinación en materia de Defensa en armonía con las disposiciones del Tratado Constitutivo de UNASUR en sus Artículos 3° letra s, 5° y 6°» (CDS, 2008: 2). Posteriormente en Chile, el año siguiente se efectúa el primer encuentro de ministros del área de Defensa subregional, que hace un pronunciamiento sobre el recién creado «CDS», expresando que: «ACUERDAN impulsar el Consejo de Defensa Suramericano en el marco de la UNASUR a través de la ejecución del Plan de Acción 2009-2010, que desarrolla cuatro ejes o lineamientos que, a su vez, contienen una serie de iniciativas específicas» (CDS, 2009: 1). Los ejes estructurales en que las delegaciones concordaron eran: «*Políticas de Defensa*», «*Cooperación Militar, Acciones Humanitarias y Operaciones de Paz*», «*Industria y Tecnología de la Defensa*», y «*Formación y Capacitación*». La estructura funcional del «CDS» quedó formada por las distintas instancias ministeriales en Defensa de Sudamérica, que serían coordinadas por la cartera viceministerial de los países componentes, como detalla Moreira (2008): «El CDS contará también con una instancia ejecutiva, integrada por las Viceministras y los Viceministros de Defensa. La Presidencia del CDS se quedará a cargo del Ministro de Defensa del país que ocupa, de forma temporaria, la Presidencia de la UNASUR» (Moreira, 2008: 13).

Pero la materialización y operativización del «CDS» con la puesta en marcha del primer «*Plan de Acción*» desencadenó un intenso debate académico, teórico y estratégico sobre la finalidad de este espacio sudamericano en «*Defensa*», refiriendo Martínez (2008) que: «El proyecto de CDS tiene poco que ver con la OTAN. En ningún caso está prevista una cláusula de seguridad mutua. Tampoco el modelo europeo de la PESD es su homónimo» (Martínez, 2008: 2). Es decir, la propuesta del «CDS» no contemplaba un nuevo Tratado Interamericano de Asistencia Recíproca (TIAR) a escala subregional, sino que se circunscribe a un ente: «tendiente a convertir a Sudamérica en una verdadera zona de paz, en la que las partes puedan informarse realmente sobre en qué y cuánto se está gastando en materia de Defensa, evitando la confusión entre procesos de modernización y carreras armamentísticas» (Comini, 2010: 19-20).

4.2 La conceptualización de Defensa y Seguridad en la UNASUR como elementos para la construcción de la Identidad Regional

La conceptualización de la «*Defensa*» en el entorno sudamericano ha pasado por un proceso de consulta y adecuación, para intentar acoplarse a la multiplicidad de visiones que tienen los países componentes de la misma. En primera instancia una de las problemáticas surge del hecho que para varias naciones de la UNASUR la Seguridad y Defensa tienen una línea muy tenue, que hace difícil diferenciar claramente algunas competencias. Por tanto, el Centro de Estudios Estratégicos de Defensa (CEED) de la UNASUR en el «*Informe Preliminar del CEED al Consejo de Defensa Suramericano acerca de los Términos de Referencia para los Conceptos Seguridad y Defensa en la Región Suramericana*» efectuó las siguientes recomendaciones en cuanto a la «*seguridad pública*»:

> Sistematizar las coincidencias y diferencias entre los países de la región respecto de la seguridad pública en su relación con la Defensa, fundamentalmente las referidas a las condiciones de participación subsidiaria de las Fuerzas Armadas en tareas de

> seguridad pública o interior, a fin de coadyuvar a una definición más rigurosa de este campo de la seguridad, en su dimensión política e institucional, para efectos de la cooperación regional y la eventual homologación de modelos de organización y gestión. (CEED, 2011: 6).

Lo indicado precedentemente expone las diferencias de forma y fondo para coincidir inicialmente en estas definiciones, específicamente por una realidad que vive actualmente la región, que es descrita por Pión-Berlín: «Mientras que las instituciones regionales empujan a los militares de regreso a los cuarteles, los problemas internos los reinstalan en la arena económica y social» (Pion-Berlín, 2008: 55). Además la internacionalización de problemas como el tráfico ilícito de drogas o el crimen organizado ha hecho que los delitos trasciendan de lo local a lo regional, contribuyendo a hacer aún más complicados los consensos. En el mismo informe citado precedentemente, el «CEED» efectúa una recomendación en lo atinente a la conformación de un «*sistema de defensa subregional*»:

> Avanzar en la caracterización de riesgos y amenazas, evaluando sus impactos regionales, con el objeto de diferenciar y jerarquizar los distintos niveles y espacios de cooperación en seguridad y defensa entre los países de la región, la posible formulación de estrategias comunes y acciones concertadas en cada uno de los campos y la determinación de sus órganos ejecutores. (CEED, 2011: 12).

Estas recomendaciones que se remonta al 2011, tuvieron una evolución teórica, en vista que para el año 2012 el «CEED» presentó al «CDS» un nuevo informe titulado «*Avance a diciembre de 2012 sobre Conceptos e Institucionalidad de Seguridad y Defensa, Amenazas, Factores de Riesgo y Desafíos del Consejo Sudamericano de Defensa*», que mostraba concreciones notables como «*Seguridad Regional*» y «*Defensa Regional*», sobre el primer concepto se expone: «La seguridad regional se aborda desde una visión cooperativa,

basada en la confianza y la concurrencia de intereses para la conformación de una comunidad de seguridad sudamericana» (CEED, 2012: 8).

En el postulado estratégico regional esbozado por el «CEED», llama la atención el uso del término «*comunidad de seguridad sudamericana*», que se relaciona con las propuestas «*securitizadoras*» de la Escuela de Copenhague, específicamente a los llamados «*Complejo Regionales de Seguridad (CRS)*», desde esa perspectiva Menezes Teixeira (2010) reflexiona: «una comunidad de seguridad está caracterizada por una situación en la cual el recurso de la fuerza para la resolución de problemas entre los miembros no es una opción, imperando la ausencia de conflicto armado entre éstos, como demuestra la Europa Occidental contemporánea» (Menezes, 2010: 47). De alguna manera, la coyuntura regional actual pone en un plano temporal lejano la conformación de una «*comunidad de seguridad*», ya que las relaciones nacionales guardan cierta animosidad, adaptándose a lo descrito por Hobsbawm: «no ha logrado traer paz, sino a lo sumo una ausencia prolongada de enfrentamientos» (Hobsbawm, 2002). En tal sentido, a pesar de los avances presentados en el proceso de integración, Sudamérica se encuadraría en un «*régimen de seguridad*», que según Cogollos (2011) referenciado en Barry Buzan explica de la siguiente manera: «[…] en donde los Estados todavía se tratan entre sí como amenazas potenciales, pero han realizado acuerdos para reducir el dilema de seguridad entre ellos» (Cogollos, 2011: 5).

El conflicto sucedido tras el bombardeo de fuerzas colombianas a Sucumbíos en el año 2008, generó una tensión creciente en la región que produjo movilización de tropas por parte de Ecuador y Venezuela hacia sus fronteras con Colombia, lo que demuestra que ciertamente el proceso de maduración se acerca más a lo que se puntualiza como un «*régimen de seguridad*», debiendo clarificar y solucionar los estados sudamericanos un conjunto de temas para hacer realidad la «*comunidad de seguridad*».

Por otra parte, es reiterativo tanto el «CDS» como el «CEED» sobre la importancia de encaminar los esfuerzos a la consecución de una «*identidad suramericana en defensa*», que en su momento era manifestada por Nelson Jobim, Ministro de Defensa de Brasil, en los términos sucesivos:

> Estoy convencido que llegó la hora de que profundicemos nuestra identidad sudamericana también en el campo de la defensa. [...] Debemos articular una nueva visión de defensa en la región fundada en valores y principios comunes, como el respeto a la soberanía, a la autodeterminación, a la integridad territorial de los Estados y a la no intervención en los asuntos internos. (Saint-Pierre & Castro, 2008: 1).

Ese mismo criterio fue el plasmado en el «*Estatuto para el Consejo de Defensa Suramericano*», que dejó establecido en su artículo cuarto, literal «*b*» entre sus objetivos el: «Construir una identidad suramericana en materia de defensa, que tome en cuenta las características subregionales y nacionales y que contribuya al fortalecimiento de la unidad de América Latina y el Caribe» (CDS, 2008: 4). En los análisis estratégicos del «CEED», se ahonda sobre la «*identidad suramericana en defensa*» que es exhibida como aquellos conceptos que se asemejan y enriquecen entre sí en la diversidad regional, destacando: «Esta perspectiva estratégica suramericana se sustenta en definiciones comunes de seguridad y defensa que orientan la cooperación y complementariedad en estos campos, en base al diálogo y aproximación de las políticas nacionales» (CEED, 2012: 8). La «*identidad suramericana en defensa*» es un factor central para erigir la «*comunidad de seguridad sudamericana*», pero ello pasa por manejar un lenguaje en común en lo que respecta a las amenazas, según lo plantea Wendt (2005) y Hopf (1999) citados por Obando (2012):

> En cuanto a la creación de comunidades de seguridad, estas nuevas amenazas supondrían, además, nuevos mecanismos institucionales para afrontarlas. Nos referimos al rol de la comunidad internacional comprometida e interpelada por las

> nuevas normas constitutivas, como el principio de responsabilidad de proteger, la creación de una identidad colectiva inspirada en la protección de las personas y en la solución pacífica de las controversias con todo lo que conlleva la creación de regímenes internacionales específicos, en tanto que se constituyen en factores o mecanismos de socialización de ideas. (Wendt (2005) y Hopf (1999) citado en Obando, 2012: 196).

Es decir, la percepción de las amenazas conlleva a un abordaje en conjunto, ya que las afectaciones son «*multiestatales*», siendo el aislamiento en temas de Seguridad y Defensa contraproducentes para los actores regionales, en este sentido añade Menezes (2010): «No pudiendo ser resueltas de forma unilateral, las nuevas amenazas proporcionan el contexto para la cooperación en seguridad, entendiéndolas como un bien público regional» (Menezes, 2010: 47).

La comprensión de la «*amenaza*» es primordial para desplegar la concepción de «*Defensa Regional*», que en Sudamérica esta intrínsecamente ligada a la apreciación de «*Seguridad Regional*», exponiéndose desde el «CEED» que: «La Defensa Regional se entiende como la serie de medidas, acciones, métodos o sistemas, que los Estados Naciones de la Región Suramericana, asumen y coordinan en forma de cooperación e interrelación, para alcanzar y mantener las condiciones de seguridad regional» (CEED, 2012: 9). Desde la visión del «CEED» la «*Defensa Regional*» debe propender al alcance y mantenimiento de la «*Seguridad Regional*», y esta confluencia es recurrente teóricamente con la reflexión de Saint-Pierre (2008):

> En principio, el término "seguridad" indica un estado o sensación que produce la percepción de ausencia de amenazas que coloque en riesgo la existencia, la propiedad, los intereses, los valores o el particular modo de ser de quien percibe. […] La actividad, que en última instancia es la garantía de aquélla, normalmente es referida con el nombre de "Defensa". (Saint-Pierre, 2008: 59)

Es importante aclarar que la vinculación de la «*Seguridad Regional*» y la «*Defensa Regional*», no debe confundirse con la indefinición local de algunos Estados en donde se asumen maniqueamente la «*Seguridad Pública/Defensa Nacional*», de hecho el «CEED» recomendó al «CDS» la necesidad de creación del «*Consejo Suramericano de Seguridad Pública*» para deslindar el debate entre dos temáticas que tienen puntos de confluencia pero ameritan tratamientos estratégicos diferentes en su fondo.

El análisis del proceso de constitución del «CDS», y las concepciones que sobre la «*Seguridad Regional*», «*Defensa Regional*», «*Comunidad de Seguridad*» e «*Identidad en Defensa*» se manejan dentro de la UNASUR buscan determinar cuál es la apreciación de «*amenaza*». Partiendo de esto es preciso traer a colación la propuesta que se maneja en la UNASUR, que es precisada desde la «*Seguridad Regional*»:

> En relación con la Seguridad Regional, distintos tipos de riesgos o amenazas de alcance transnacional o transfronterizo, en dependencia de su impacto regional, tienen diferente relevancia, correspondiendo su enfrentamiento a instancias de cooperación de defensa o de seguridad pública, según su naturaleza, mediante el empleo de los medios, instrumentos y mecanismos institucionales competentes para su tratamiento. (CEED, 2012: 13).

De lo expresado en la cita precedente, se pueden extraer varias ideas importantes, primeramente se reconoce el carácter «*transnacional*» o «*transfronterizo*» de las amenazas, en el entendido que el grupo o individualidad que incurre en un acto antijurídico contra la legislación de un actor integrante de la unidad regional, puede ser concebido como un factor desestabilizador que afecte paralelamente la Seguridad y Defensa interna de un país, pudiendo menoscabar la «*Seguridad Regional*» por su connotación expansiva. Asimismo, se reconoce la variabilidad propia de las amenazas que socaban la institucionalidad, pudiendo ser contrarrestada individual o conjuntamente por organismos castrenses o de seguridad

ciudadana. En relación a la «*Defensa Regional*», la propuesta emanada del «CEED» tiende a ser más amplia en cuanto a las puntualizaciones de las amenazas, expresando lo sucesivo:

> En relación con la Defensa Regional, las amenazas que, eventualmente puedan comprometerla, tienen relación con intereses y actores extra regionales que atenten contra la soberanía, la integridad de territorio, población y recursos, la estabilidad institucional del estado y la seguridad de la región como zona de paz. (CEED, 2012: 14).

En esta caracterización resalta el uso del adverbio «*eventualmente*», que según la edición vigesimosegunda del Diccionario de la Lengua Española define esta palabra como: «Incierta o casualmente» (RAE), dejando este término un matiz estratégico claroscuro en la conceptualización de las amenazas en el ámbito de la Defensa. Empero, hay un reconocimiento por parte del «CEED» que las amenazas a la «Defensa Regional» están estrechamente relacionadas a «*intereses y actores extra regionales*» en aspectos amplios como la «*Agresión armada externa*», la «*Ocupación territorial*», y los «*Conflictos bélicos*», pero resultan enunciaciones generales, comparativamente en la «*seguridad regional*» son claramente expuestas un conjunto de amenazas como: «narcotráfico, el terrorismo, el tráfico de personas y órganos, el lavado de dinero, los delitos informáticos, el tráfico de bienes y recursos ambientales, el secuestro, y acciones provenientes de grupos armados fuera de la ley» (CEED, 2012: 14).

4.3 Las consideraciones estratégicas de la UNASUR sobre la amenaza de ataques informáticos

Las propuestas que involucren asuntos relacionados a temas «*informáticos*» o «*cibernéticos*» en las políticas o estrategias de la UNASUR han sido especialmente reflejadas en el entorno de la «*Seguridad*», con menor medida en «*Defensa*» y sin mención alguna como «*ciberguerra*». Sin embargo, independientemente de la nomenclatura con que esta se maneje,

lo que precisa más atención es sí verdaderamente está siendo objeto de análisis desde una visión estratégica regional, como agregan Rantapelkonen y Kantola (2013): «Por lo tanto, la pregunta no es si se trata de que la ciberguerra es ofensiva y/o defensiva. Es más bien la forma de satisfacer el fenómeno de la "ciberguerra" y la manera de soportar los problemas que surgen en el contexto del ciberespacio cuando no necesariamente definirla como una guerra» (Rantapelkonen & Kantola, 2013: 33). Es decir, no por colocar el prefijo «*ciber*» a la «*guerra*» se tiene por antonomasia una política sobre la misma. Pero, sí se precisan definiciones cónsonas y no meramente enunciativas para el abordaje estratégico de los ataques informáticos en el ámbito de la Defensa. Precisamente, dentro del proceso institucional de la «UNASUR» y el «CDS» se ha dado un progreso que tiene tres puntos de marcada importancia: los «*Planes de Acción 2012/2013*», la decisión de creación del «*Mega Anillo de Fibra Óptica*», y el pronunciamiento en 2013 en la cumbre de la Paramaribo.

En primera instancia, los asuntos «*cibernéticos*» pasaron a ser parte de la matriz de análisis del «CDS» por primera vez en su «*Plan de Acción 2012*», donde se deja establecido en su punto «*1.f*» lo siguiente: «Conformación de un Grupo de Trabajo para evaluar la factibilidad de establecer políticas y mecanismos regionales para hacer frente a las amenazas cibernéticas o informáticas en el ámbito de la defensa» (CDS, 2012: 1). En el documento se asigna la responsabilidad directa a la delegación peruana, y como corresponsables a Venezuela y Uruguay. Esta misma línea se mantuvo en el «*Plan de Acción 2013*», que igualmente en su punto «*1.f*» reitera: «Mantener el grupo de trabajo para establecer una política y mecanismos regionales para hacer frente a las amenazas cibernéticas e informáticas en el ámbito de la defensa» (CDS, 2013: 1). La responsabilidad continúa sobre la representación del Perú, con la variable que a los venezolanos y uruguayos se agregan los colombianos y brasileños como corresponsables. En el desarrollo del punto «*1.f*» entre 2012 y 2013 las naciones sudamericanas han efectuado un sólo encuentro enmarcado directamente

en los ataques informáticos como asunto de Defensa, al respecto Pablo Celi quien funge como Subdirector del Centro de Estudios Estratégicos de Defensa de la UNASUR, en entrevista realizada para esta investigación explica:

> A esto podríamos añadir una última iniciativa que fue incorporada a raíz de los fenómenos de tipo internacional que despertaron el interés por la noción de ciberdefensa, y respecto a lo cual Unasur ha hecho hasta hoy un encuentro que se realizó en Lima para discutir cuales serían las líneas de trabajo en este campo. No existe todavía una definición conjunta, existe un planteamiento de abrir una línea de definiciones que está en una fase yo diría bastante previa. (P. Celi, entrevista personal, 07 de noviembre de 2013).

Entre las apreciaciones del documento propuesto por la delegación peruana en 2013, y que se titula: «*Establecer una política y mecanismos regionales para hacer frente a las amenazas cibernéticas o informáticas en el ámbito de la defensa*», se presentan tres objetivos que abarcan temas técnicos, formativos, y legislativos que deberían emprenderse. El marco general del primer objetivo propone la conformación de un Equipo de Respuesta a Incidentes Teleinformáticos de las FFAA y que se interrelacioné con una coordinación de Respuesta a Emergencias Teleinformática de la Administración Pública de los CERT de cada país. Esto resulta una propuesta coherente, pero siempre y cuando responda a un direccionamiento estratégico que deje claro la finalidad de estos equipos técnicos, sobre la estructuración de estos centros de respuesta diserta Kärkkäinen, (2013):

> La cuestión más concreta de la estrategia es el establecimiento de un cibercentro nacional. El centro cibernético mantendrá conocimiento de la situación, mejorará la coordinación entre los actores, acelerará la toma de decisiones y el desarrollo de habilidades relacionadas con la seguridad cibernética. Esto permite mejorar la sensibilidad estratégica, el uso flexible de los recursos y la coherencia de la gestión. (Kärkkäinen, 2013: 97).

Nótese que Anssi Kärkkäinen no prioriza una respuesta técnica, sino que la supedita a la toma de decisiones que debe ajustarse a la «*sensibilidad estratégica*». En cuanto al segundo objetivo contenido en el papel de trabajo sudamericano, este tiene un fin formativo, buscando propender a una capacitación técnica del personal encargado para apuntalar sus capacidades en «*ciberseguridad*» y «*ciberdefensa*». Este segundo apartado está correctamente orientado, ya que es importante y vital, la formación técnica de personal para contar con la pericia para desarrollar potencialidades «*cibernéticas*», como delibera Grant (2009): «La tarea de hacer frente a los ataques del ciberespacio nunca termina. Como resultado de ello, la misión de defensa cibernética es menos acerca de cómo detener los ataques cibernéticos que de la configuración y el entrenamiento de las fuerzas militares nacionales para que sean capaces de luchar a través de ellos» (Grant, 2009: 26). Pero esta capacitación debería ser antecedida por una clara concepción estratégica, que prefigure si este personal sudamericano será instruido para «*ciberseguridad*», «*ciberdefensa*» o «*ciberguerra*».

Finalmente, se expone en el último objetivo del texto sobre «*ciberdefensa*» regional, la necesidad de adecuación legislativa de los países miembros para lograr normativas que permitan prevenir y combatir legalmente asuntos relacionados a «*seguridad*» y «*defensa*» en el plano «*cibernético*». Empero, la adecuación legislativa de cada país representa un desafío a muy largo alcance, ya que se entra en una dinámica local que dilataría una propuesta regional, que es necesaria desarrollarse en un mediano plazo. Esto no quiere decir que las discusiones en un plano subcontinental estarían carentes de «*baches interpretativos*», ya que como demarca Tuukkanen (2013):

> Teniendo en cuenta el carácter novedoso de las tecnologías, los académicos y los gobiernos todavía no están seguros si la interpretación tradicional del derecho internacional consuetudinario daría los resultados deseados. Por lo tanto, podemos esperar que los académicos y los gobiernos continúen con sus esfuerzos para

> establecer interpretaciones estabilizadas y compartidas de las normas jurídicas internacionales y el comportamiento respectivo en el ciberespacio. (Tuukkanen, 2013: 42).

A grandes rasgos, esos son los cimientos que fundamentan este documento que tiene elementos importantes y necesarios, pero no se plasma un tratamiento estratégico sudamericano de las amenazas cibernéticas en un contexto de «*ciberguerra*», precisándose un bosquejo que refleje capacidades regionales y se exterioricen las inferioridades tecnológicas, para determinar esa «*base objetiva*» que es propiciadora de iniciativas estratégicas, sobre esto reflexionó hondamente Mao: «La iniciativa es inseparable de la superioridad en la capacidad bélica, en tanto que la pasividad es inseparable de la inferioridad en ese terreno. Tal superioridad o inferioridad constituyen, respectivamente, la base objetiva para la iniciativa o la pasividad» (Mao, 1976: 167). Varios de los análisis estratégicos de mayor profundidad sobre «*ciberestrategia*» lo han desarrollado diferentes autores nórdicos, que estudian la integración de los espacios regionales en el «*ciberespacio*», y que presentan elementos teóricos que pueden servir para complementar algunos puntos del documento expuesto al grupo de trabajo del «CDS», asomando Kiravuo y Särelä (2013) algunos principios básicos:

> Aprender las capacidades de las armas cibernéticas. Crear un liderazgo para el ciber-comando que entiende estas capacidades. Comunicar estas capacidades a otras ramas de la comunidad militar y de inteligencia. Asegurarse que el conocimiento suficiente esté disponible para la planificación de las operaciones militares. El conocimiento de las capacidades cibernéticas debería estar disponible a los planificadores para que las operaciones cibernéticas se puedan utilizar en apoyo o sustitución de las operaciones convencionales. (Kiravuo & Särelä, 2013: 229).

Lo expresado por Kiravuo y Särelä contiene trazas necesarias para erigir una «*base objetiva*» pertinente para una «*ciberestrategia*», que requiere la articulación de «*Aprendizaje*»,

«*Liderazgo*», «*Comunicación*», «*Acceso al Conocimiento*», «*Planificación*» e «*Interoperabilidad*». Ciertamente el documento presentado en Lima es una primera propuesta que pasará por una metamorfosis conforme se hagan aportes de otras delegaciones, pero es la percepción de esta investigación que hay aspectos «*ciberestratégicos*» transversales que van desde definir «*acto de guerra informático*», pasando por la caracterización de posibles atacantes, junto a la determinación de cuantos sistemas pertenecientes a la «infraestructura crítica» de la región están vinculados a sistemas privativos, así como el establecimiento de las potencialidades de fuerzas extra regionales con respecto a nuestras carencias, que son pertinentes y previas a iniciativas técnicas u operativas como un «*Equipo de Respuesta a Incidentes Teleinformáticos*» vinculados a una «*coordinación de Respuesta a Emergencias Teleinformática de la Administración Pública de los CERT*».

Dentro de esa misma perspectiva de asumir decisiones sobre temáticas relacionadas a asuntos cibernéticos, en mayo de 2013 se materializa una respuesta ejecutiva de los gobiernos sudamericanos, que puede considerarse el punto de partida de la mayor orientación política en la materia asumida por la UNASUR, cuando la totalidad de representantes de las carteras ministeriales de ciencia, tecnología y comunicaciones sudamericanas acordaron la creación del «*Mega Anillo de Fibra Óptica*», sobre esto Pablo Celi acota:

> Hay un aspecto en el cual se va a reflejar más una visión política del tema que será el sistema de administración de esto y el sistema jurídico, la base normativa a través de la cual se oriente la ejecución del proyecto, son dos cosas que van no necesariamente una delante de la otra, pueden ir en paralelo, yo creo que con los últimos acontecimientos esta segunda parte va a tener un mayor énfasis en la definición de políticas, mientras el aspecto técnico va avanzando para que el proyecto sea factible en el tiempo. (P. Celi, entrevista personal, 07 de noviembre de 2013).

Las reflexiones del subdirector del «CEED» exponen una dimensión política y jurídica que trasciende el simple aspecto técnico y muestra la iniciativa del «*Mega Anillo de Fibra Óptica*» como un determinante estratégico para la región. La importancia de este proyecto está íntimamente ligado a salvaguardar un activo estratégico, ya que las infraestructuras críticas en Sudamérica están interrelacionadas directa o indirectamente con plataformas informáticas extraregionales, como refleja Raúl Zibechi (2011):

> Un mail enviado entre dos ciudades limítrofes de Brasil y Perú, por ejemplo entre Rio Branco, capital de Acre, y Puerto Maldonado, va hasta Brasilia, sale por Fortaleza en cable submarino, ingresa a Estados Unidos por Miami, llega a California para descender por el Pacífico hasta Lima y seguir viaje hasta Puerto Maldonado, a escasos 300 kilómetros de donde partió. (La Jornada, 2011)

Lo previo demuestra cómo se vinculan vulnerabilidades propias de la «*dependencia tecnología*», y la gravedad del hecho que un actor ajeno a la realidad sudamericana pueda acceder, interrumpir, manipular, afectar o espiar los sistemas informáticos. El factor «*cibernético*» se ha expandido de tal manera que no puede ser desvinculado de otras «*amenazas*», destaca Huopio (2013): «En la actualidad, no existe una amenaza cibernética separada […] Por lo tanto, las amenazas cibernéticas deben considerarse como un elemento de amenaza horizontal en relación con prácticamente todos los escenarios de amenaza» (Huopio, 2013: 127).

Lo referido sobre la vulnerabilidad que significa la «*dependencia tecnología*» y como estimula una amenaza, queda evidenciado para el caso sudamericano en el sistema de vigilancia extensiva manejado por EE.UU, Gran Bretaña, Australia, Nueva Zelanda y Canadá, denominado «*Echelon*», que venía funcionado desde los años 1960 como herramienta de intercepción en la «*Guerra Fría*», pero conforme las redes informáticas

empezaron a tener preeminencia en las comunicaciones se perfeccionó en la sustracción de información para establecer debilidades de otras naciones:

> El sistema de espionaje consiste en un sistema de seguimiento de comunicaciones por medio de "sniffers" (rastreadores) y su posterior filtrado. Se identifican palabras clave que están determinadas y alimentadas al mismo tiempo mediante grandes bases de datos que se denominan "diccionarios". Mediante programas de reconocimiento de voz basados en inteligencia artificial se filtran hasta 3.000 millones de mensajes por hora. (Le Monde Diplomatique, 2013: 30).

El «*Echelon*» permite a estas naciones, la dominación basada en la tecnología, ya que se sirve de una gran cantidad de sistemas informáticos, siendo la Isla de Ascensión[11] ubicada en pleno océano Atlántico entre el continente africano y Sudamérica una de las bases de operaciones para controlar parte del subcontinente:

> La Isla de la Ascensión es de sólo 91 kilómetros cuadrados, y es irrelevante si no estuviera en una posición estratégica a medio camino de los continentes de África y América del Sur [...] su superficie alberga potentes estaciones de intercepción de señales (Singint), que destacan como enormes bolas blancas. Integran un sistema de inteligencia avanzada que monitoriza en tiempo real a todas las comunicaciones de Brasil, Argentina, Uruguay, Colombia y Venezuela, y son parte de un proyecto conocido como Echelon. (Istoe, 2013).

Por tanto, la incidencia intrusiva de sistemas como el «*Echelon*» que están al servicio de intereses externos y lesionan la soberanía de la región, demuestra la trascendencia del «*Mega Anillo de Fibra Óptica*», que no recae sólo en la infraestructura, sino en la potencialidad para preparar estrategias colaborativas que permitan afrontar un eventual escenario de

[11] Observar el **ANEXO «C».**

«*ciberguerra*», conforme a esto aporta Pedro Sassone Representante de Venezuela ante la Secretaria General de la UNASUR:

> El proceso de construcción del anillo de fibra óptica, es la concreción de la profundización de las políticas de cooperación, no es solamente aprender lo que se tiene, es que se definen mecanismos comunes y estructuras tecnológicas comunes para el dominio de la información y para el intercambio de la información. (P. Sassone, entrevista personal, 18 de diciembre de 2013).

En este sentido, el «*dominio*» del «*ciberespacio*» no parte desde un sentido restrictivo o conculcador, sino del resguardo de un ámbito de la soberanía que debe estar bajo la tutela regional. Y esa presencia subcontinental que se debe tener en el «*ciberespacio*», tiene sus orígenes en que la tecnología es una herramienta que puede amoldarse a cualquier funcionalidad, siendo igualmente provechosa como destructiva, esto lo fundamentan Liang y Xiangsui:

> […] mientras que la revolución de la tecnología militar ha permitido que uno sea capaz de seleccionar las medidas dentro de un rango más amplio, también se ha hecho para que uno se vea amenazado por estas medidas dentro de la misma gama (esto se debe a que el acaparamiento de un tipo de tecnología es mucho más difícil que inventar un tipo de tecnología). Estas amenazas nunca habian sido como hoy, porque las medidas son diversas e infinitamente cambiante, y esto realmente le da a uno la sensación de ver al enemigo detrás de cada árbol. (Liang y Xiangsui, 1999: 115-116).

La VII Reunión Ordinaria del Consejo de Jefas y Jefes de Estado y de Gobierno de la Unión de Naciones Suramericanas, mantuvo una postura cónsona con las gestiones ministeriales acordadas en el Consejo Suramericano de Infraestructura y Planeamiento (Cosiplan) y las entrelazó con los ejes del «CDS», procediendo a instruir:

> Al Consejo de Defensa Suramericano (CDS) y al COSIPLAN, evaluar la cooperación con otros consejos ministeriales competentes y avanzar en sus respectivos proyectos sobre defensa cibernética y la interconexión de las redes de fibra óptica de nuestros países, con el objetivo de tornar nuestras telecomunicaciones más seguras, fortalecer el desarrollo de tecnologías regionales y promover la inclusión digital. (UNASUR, 2013: 8).

En referencia a la instrucción efectuada por los primeros mandatarios, es importante destacar la integralidad dada al direccionamiento para la «*defensa cibernética*», instándose en la declaración final de la cumbre a la cooperación entre los consejos de la UNASUR para no divorciar lo estratégico, lo político, y lo operativo, que coincide con lo esbozado por Kärkkäinen (2013): «No es simplemente una cuestión de protección y defensa de la información ya que toda la infraestructura de procesamiento de la información mantiene los ecosistemas económicos, políticos y sociales en marcha» (Kärkkäinen, 2013: 105). La congregación de iniciativas para la «*Defensa Cibernética*» puede ampliar el horizonte estratégico, para evitar restricciones propias del «*tecnicismo*», y generar una retroalimentación entre los consejos, como acota Michelle Fiol asesora de la Ministra de la Defensa del Ecuador:

> La instrucción que se le está dando al CDS y al COSIPLAN para que se cree un grupo de trabajo que nos permita hacer propuestas de proyectos conjuntos con respecto a la seguridad informática, y que tiene relación justamente con este anillo de fibra óptica, no es un trabajo aislado, al saber que es también un tema de Defensa, tenemos que integrar un poco la visión y los proyectos, porque no podemos trabajar tanto como un tema de Seguridad y Defensa que como un tema tecnológico, creo que van de la mano. (M. Fiol, entrevista personal, 04 de octubre de 2013).

La evolución conceptual en la UNASUR sobre los «*ataques informáticos*» demuestra un paulatino avance, tomando conciencia que es un asunto diferente de los «*delitos*

informáticos» que entran en la competencia de la «*seguridad interna*» de los Estados o en el caso regional del Consejo Suramericano de Seguridad (CSS). Esta discusión que se ha ido profundizando en el «*CDS*», parte de la comprensión que los «*ataques informáticos*» tiene elementos característicos para percibirlos dentro de las amenazas en materia de Defensa, entre otros motivos por lo que aporta Palokangas (2013): «Es típico de los ataques cibernéticos que los efectos indirectos causados suelen ser más importantes que los efectos directos. Los efectos son generalmente muy difíciles de estimar. Su diseño y puesta en práctica requiere una cantidad significativa de conocimiento humano y de inversión» (Palokangas, 2013: 146). Una demostración que en el plano sudamericano la apreciación de «*ciberamenaza*» ha ido afianzándose, radica no sólo en las decisiones políticas, sino en las opiniones de reconocidos estudiosos regionales, en este caso Pablo Celi indica:

> Sin duda con todas esas características esta constituye una amenaza que afecta a una dimensión muy importante de la integridad de los Estados que es la información estratégica con la cual se procesan sus políticas. En este sentido, hay un interés en la región por desarrollar mecanismos primero de análisis de determinación del alcance del fenómeno y a partir de ello mecanismos que nos permitan adoptar decisiones tanto en el plano político como en el plano técnico, como en el plano operacional para asegurar los sistemas de información de los países. (P. Celi, entrevista personal, 07 de noviembre de 2013).

Una organización supraestatal como la UNASUR amerita dinamizar la delimitación de las posibles amenazas en el entorno tecnológico, entendiendo que las mismas tienen una «*virtualidad*» e «*inmaterialidad*» que se tergiversa como «*ficticia*». Además de suponer una preocupación, las amenazas pueden ser un catalizador para acelerar la apreciación colectiva, que la afectación de un miembro puede repercutir sobre la totalidad de la región, siendo un paso para aglutinar y consensuar medidas, en este sentido Michelle Fiol señala:

> Partiendo de las amenazas y riesgos uno puede ir construyendo tal vez una Defensa común, pero estamos en esa discusión, es un proceso, la Comunidad Europea se ha demorado sesenta años en definir lo que es su política exterior de Defensa, es un proceso complejo, y llegar a homologar conceptos nos va a tomar tiempo. (M. Fiol, entrevista personal, 04 de octubre de 2013).

El peligro de la amenaza siempre ha sido una variable tomada en cuenta por los teóricos militares, pero es importante el manejarla para desarrollar fortalezas y no para consumirse en el desasosiego de la impotencia, refería Clausewitz: «El peligro domina al jefe no sólo porque lo amenaza a él personalmente, sino también mediante la amenaza a todos aquellos que se hallan bajo sus órdenes; no sólo en el momento en que se hace presente en realidad, sino por medio de la imaginación en todos los momentos relacionados con el presente» (Clausewitz, 2002: 21). Si el conjunto regional se encuentra ante una amenaza, hay que evitar que el peligro sea el profundizador de un temor paralizante, debiendo encaminarse la UNASUR hacia una homologación que fortalezca la colectividad de naciones, que puede partir de circunscribir el «*espacio cibernético*» como un «*interés regional*», apuntando Celi sobre este concepto: «surge del reconocimiento de que existen factores de riesgo y amenazas que implican al conjunto de países de la región, y que existen también un conjunto de recursos, de potenciales, de capacidades, que en la región demandan un tratamiento colectivo» (P. Celi, entrevista personal, 07 de noviembre de 2013). El «*interés regional*» es una noción que es relevante para vincularla a la compresión de la amenaza, ya que genera un foco de atención sobre un aspecto puntual que amerita la protección para evitar la masificación de la afectación, como refiere Sassone:

> Es un concepto abarcante, cuando uno analiza el Interés Regional toca las diferentes materias, de la definición que el concepto de Interés Regional sintetiza también se incorpora el Interés Nacional […] Podemos estar en presencia de un concepto matriz

> ordenador de las diferentes políticas en el caso concreto evidentemente en Defensa que ahí nació el concepto. (P. Sassone, entrevista personal, 18 de diciembre de 2013).

Si se concreta la concepción sudamericana del «*espacio cibernético*» como un «*interés regional*» se podría apuntalar la adopción de medidas que primeramente deberían estar centradas en el desarrollo de «*soberanía tecnológica*» pensando en la «*disuasión*» como un pilar estratégico de Defensa para el subcontinente. Esta «*disuasión*» es un camino complejo, ya que como establece Limnéll (2013): «La disuasión depende de una comunicación efectiva entre el Estado y la entidad que desea disuadir. Hay que convencer a los demás de que si atacan, uno tiene la capacidad de hacer algo al respecto. Este es también el caso en el dominio cibernético» (Limnéll, 2013: 202). Es decir, la «*ciberdefensa*» o «*ciberguerra*» deben estar pensadas como un medio «*disuasivo*» para garantizar un fin que es el «*ciberespacio sudamericano*» como «*interés regional*». Para Clausewitz la «*disuasión*» era un punto focal de la guerra, exponiendo que el hecho militar normalmente viene acompañado de una postura que exterioriza fortaleza ante el adversario, con la finalidad de advertirle lo contraproducente que sería iniciar un conflicto, especificando: «A menudo la guerra no es más que una neutralidad armada o una actitud amenazadora destinada a entablar unas negociaciones, o un intento moderado de ganar alguna ventaja y esperar luego el resultado» (Clausewitz, 2002: 134). Esta actitud asentada por el prusiano se logra con un desarrollo del pensamiento estratégico en Defensa, como reflexionaba Alfredo Fortí, Director del «CEED» en la Conferencia Suramericana «Visiones Hacia una Estrategia Suramericana para el Aprovechamiento de los Recursos Naturales», celebrada en Caracas: «la disuasión "hacia fuera", implica que nuestras capacidades regionales en materia de defensa y militar deben concentrarse y fundirse en una sola cuando de lo que se trata es proteger al interés regional que representan los recursos naturales suramericanos frente al eventual accionar de

terceros estados» (Forti, 2013: 17). Tomando las reflexiones de Forti, el delegado venezolano ante la Secretaria General de UNASUR disertaba:

> Él decía: «cooperación hacia dentro, disuasión hacia afuera», eso toca la respuesta de la necesidad de dar respuesta frente al problema de la guerra cibernética por ejemplo. Es decir, que la cooperación hacia dentro es la profundización del proceso de confianza, que va desde el intercambio de lo que tengo, desde aprender lo que tengo, desde la definición de políticas comunes, y la definición de sistemas de alianzas, todo eso son las dinámicas de la profundización de la cooperación. (P. Sassone, entrevista personal, 18 de diciembre de 2013).

Por ende, como refieren tanto Sassone como Forti la «*disuasión*» es una postura que requiere la cooperación de todos los componentes de la unidad, y en temas tan puntuales como la «*ciberguerra*» debe haber un acompañamiento «*monolítico*» de toda la institucionalidad. Un ejemplo orientador de la disuasión estratégica configurada en «*poder*», se percibe en los embates sorteados por la Unión Soviética, que asumió una unidad inquebrantable para mostrarse fuerte y retraer los planes enemigos que continuamente conspiraban contra el Estado soviético, expresando Lenin: «Y todo intento de guerra contra nosotros significará, para los Estados que se enzarcen en este conflicto, agravar las condiciones que habrían podido tener sin la guerra y antes de la guerra, en comparación con las que obtendrán como resultado de ella y después de ella» (Lenin, 1973: 124). El mensaje político leninista surtió un efecto de frenado ante las pretensiones de conflicto de otros Estados, y años después ese mismo análisis fue emprendido por el General André Beaufre, que coincidía que las dudas que se siembran en la contraparte por el temor a ser sorprendidas, generan un freno psicológico, reseñaba el francés sobre la «*disuasión*» que: « […] se trata de influir directamente sobre la voluntad del adversario sin pasar por el intermediario de una prueba de fuerza» (Beaufre, 1977: 65). Pero la «*disuasión*» amerita una

interoperabilidad defensiva/ofensiva para lograr la credibilidad disuasiva, es decir: «si los adversarios saben que la infraestructura digital es resistente; que hay una detección de amenazas creíbles por el sistema de prevención, y que hay una capacidad para llevar a cabo contraataques, la disuasión es mucho más creíble» (Limnéll, 2013: 205).

En la declaración de Santiago en 2009, se estableció entre uno de los cuatro ejes del CDS la «*Industria y Tecnología de la Defensa*», reseñando dicho apartado: «Elaborar un diagnóstico de la industria de Defensa de los países miembros identificando capacidades y áreas de asociación estratégicas, para promover la complementariedad, la investigación y la transferencia tecnológica» (UNASUR. 2009: 2). Esto debe ser concebido como un factor importante para encaminar al subcontinente a una «*soberanía tecnológica*» que contribuya a la perspectiva previamente enunciada por Forti de: «*cooperación hacia dentro, disuasión hacia afuera*», estando ajustado esto a los razonamientos manifestados por Fiol:

> Pero la voluntad es generar capacidades regionales para poder abastecernos de lo que existe ya en la región, evidentemente la tecnología europea o norteamericana está mucho más avanzada, entonces vamos a seguir dependiendo de eso mientras no exista una trasferencia tecnológica y convenios de cofabricación que impliquen esta trasferencia tecnológica. (M. Fiol, entrevista personal, 04 de octubre de 2013).

Empero, la transferencia tecnológica por sí misma no tiene un valor agregado, esto recae en percibir su fondo estratégico y comprender qué se quiere lograr con el conocimiento trasferido. Es decir, la «*Industria y Tecnología de la Defensa*» puede representar el punto de partida de un vasto proyecto regional que permita hacer creíble una postura disuasiva en relación a actores extra regionales, acota García Covarrubias (2001):

> La gran razón es que la Disuasión como actitud o modelo político estratégico es "voluntarista", esto significa que es una actitud decidida, responsable, planeada y

> organizada de un país, por lo tanto no es ni aleatoria, ni casual. Es fundamental entender que habrá, entonces, una disuasión natural o latente que se lleva a cabo básicamente en el nivel político-estratégico y una Disuasión manifiesta con la combinación de los dos niveles. (García, 2001: 74).

El superar esa «aleatoriedad» y «casualidad» propia de la improvisación, pasa por un planteamiento coherente de las líneas de pensamiento político-estratégico que contraponga una disuasión real con relación a una amenaza no convencional, que se enmarca en una variable tecnológica que amplia las asimetrías, y refuerza la dominación sobre quien carece de los medios para producirla, detallando este escenario Heickerö (2013):

> En una perspectiva de futuro, la guerra de información es una parte integral de cada conflicto militar y político importante, y el ciberespacio es a la vez su propia dimensión y una parte coordinada de los otros espacios físicos, como la Tierra, Mar, Aire y Espacio. La guerra de información se lleva a cabo en todo el espectro entero de la zona de combate, en todos los niveles: estratégico, operacional y táctico con diferentes énfasis principales durante las diferentes fases. Un conflicto puede estar en marcha y decidido en el ámbito digital, sin medios cinéticos que tengan que ser utilizados. (Heickerö, 2013: 124).

Este entorno es un reto, ya que la «*Industria y Tecnología de la Defensa*» deben diversificarse para ajustarse a la necesidad de «*software*» y «*hardware*» que amerite la Defensa del «*ciberespacio sudamericano*», siendo ineludible reconfigurar la visión de ciencia y la tecnología regional, que responde a patrones de dominación, apuntando Sassone que:

> Tenemos que reconstruir una nueva concepción de la ciencia y la tecnología, para poder dar en los puntos que se necesitan en términos de convertirnos en Centro de Poder, y Región Poder, no se trata justamente de copiar, de adaptar modelos tecnológicos, porque al final nos quedaríamos con la esencia del modelo, con el

> núcleo central del modelo, no van a transferir lo que para ellos es el núcleo esencial de su dominio de poder. (P. Sassone, entrevista personal, 18 de diciembre de 2013).

Cuando el diplomático venezolano expresa que ciertamente una potencia militar difícilmente trasferirá el «*núcleo esencial de su dominio de poder*», está mostrando una realidad que era en su momento disertada por Clausewitz: «Por lo tanto, si hemos de obligar por medio de la acción militar al oponente a cumplir con nuestra voluntad, tenemos o bien que desarmarlo de hecho, o bien colocarlo en tal posición que se sienta amenazado por la posibilidad de que lo logremos» (Clausewitz, 2002: 9).

El ajuste estratégico disuasivo para la región que se ha venido explorando, debe estar acompañado de una adecuación del abordaje de los asuntos cibernéticos que han tendido mundialmente a la «*militarización*». Los diferentes eventos históricos que durante el siglo XX enfrentaron en Sudamérica a las Fuerzas Armadas con amplios sectores sociales, creó un recelo natural entre militares y civiles, que tiene que ser superado y comprender que el abordaje de asuntos cibernéticos amerita ser nutrido por ambos, aporta sobre esto Mørkestøl (2013) que:

> Con los años, hemos visto cómo los sectores civiles y militares de todo el mundo están en la mira de los actores en el ciberespacio que buscan interrumpir, negar, engañar, degradar, destruir o de cualquier otra manera afectar las redes de ordenadores y otras infraestructuras de comunicación (incluyendo SCADAs etcétera). En la medida que las víctimas de estas transgresiones pueden ser tanto civiles como militares, las medidas de respuesta deben aplicarse en estos dos sectores. (Mørkestøl, 2013: 109).

Es un hecho claro que esta problemática debe contar con un direccionamiento compartido entre civiles y militares, siendo preciso no desvirtuar esta visión en Sudamérica, ya que una

parte importante de la «*infraestructura crítica*» se encuentra en instituciones públicas y privadas de carácter civil, aporta Fiol al respecto:

> La ciberdefensa y la ciberguerra de todas maneras se están desarrollando desde el ámbito militar pero con criterio y con direccionamientos que tienen que venir desde el ámbito civil de la conducción política en estos temas, creemos que debe haber participación tanto civil como militar para definir las amenazas, para saber qué lineamientos se deben establecer y la parte operativa que es para nosotros la parte militar, asesorarnos con ellos para que puedan definir qué es la ciberdefensa, la ciberguerra, qué elementos o qué instrumentos técnicos vamos a necesitar para poder desarrollar capacidades. (M. Fiol, entrevista personal, 04 de octubre de 2013).

Por otra parte, entrando en el ámbito de la conceptualización de la «*ciberdefensa*» que se propone desde la institucionalidad subregional, es significativo hacer algunas apreciaciones teóricas sobre las connotaciones estratégicas «*defensiva*» y «*ofensiva*» para comprender los «*ataques cibernéticos*» en toda su dimensión. El asimilar sí la «*ciberdefensa*» es el concepto más adecuado y el que permite ampliar el campo de visión estratégico es un tema para la discusión regional, corresponde al «CDS» reflejar cuál es el fondo terminológico del uso de «*ciberdefensa*», para dejar establecido el alcance en relación a definiciones estratégicas como la «*ciberguerra*» o la «*ciberseguridad*». Pensadores militares desde el siglo XIX han sido propiciadores de enconadas reyertas intelectuales para deslindar las apreciaciones de defensa y ofensiva, el propio Clausewitz llamaba la atención de las diferenciaciones que deben ser estudiadas en su justa medida:

> Si sólo existiera una forma de guerra, digamos la que corresponde al ataque del enemigo, no habría defensa; ello es tanto como decir que si hubiera de distinguirse al ataque de la defensa sólo por el motivo positivo que el uno posee y del que la otra carece, si los métodos de lucha fueran siempre invariablemente los mismos, en tal empeño, cualquier ventaja de un bando tendría que representar una

> desventaja equivalente para el otro, existiendo entonces una verdadera polaridad. Pero la acción militar adopta dos formas distintas, la de ataque y la de defensa, que son muy diferentes y de fuerza desigual (Clausewitz, 2002: 16).

No es menor esta discusión, que puede contribuir a centrar y precisar las «*amenazas cibernéticas*» subregionales, pero de no dirigirse correctamente podría caer en un marasmo propio de generalidades, que serían una impronta sudamericana que ensancharía las vulnerabilidades. El propio Mao aleccionaba que las dimensiones de la «*defensa*» y el «*ataque*», deben ser correctamente asumidas por las particularidades que limitan y potencian su accionar, detallando:

> El ataque es el medio principal para destruir las fuerzas enemigas, pero no se puede prescindir de la defensa. El ataque se realiza con el objetivo inmediato de aniquilar las fuerzas del enemigo, pero al mismo tiempo para conservar las fuerzas propias, porque si uno no aniquila al enemigo, será aniquilado. La defensa tiene como objetivo inmediato conservar las fuerzas propias, pero al mismo tiempo es un medio de complementar el ataque o de prepararse para pasar a él. (Mao, 1976: 160).

En el momento que la VII Reunión Ordinaria del Consejo de Jefas y Jefes de Estado y de Gobierno de la Unión de Naciones Suramericanas hizo uso del término «*Defensa Cibernética*», las diferentes instancias como el «CDS», el «CEED» y las delegaciones que tienen la responsabilidad y corresponsabilidad deben concretar qué incluye y excluye este concepto, y tomar la bidimensionalidad que acusa Clausewitz y Mao, y que complementa Basil Liddell Hart:

> Una verdad más profunda a la que no llegaron plenamente Foch ni los otros discípulos de Clausewitz, es la de que en la guerra todo problema, como todo principio, es necesariamente dual. Tiene dos caras, como una moneda, y de aquí la necesidad de llegar a una componenda bien calculada como medio de conciliación. Esto es consecuencia inevitable del hecho de ser la guerra un juego entre dos bandos e

> imponer por lo tanto la necesidad de guardarse a la vez que se ataca. (Liddell Hart, 1946: 212).

En su momento Kärkkäinen presentaba una enunciación que da un justo equilibrio entre «*defensiva*» y «*ofensiva*», destacando que: «La defensa cibernética es una capacidad operativa en el ciberespacio y, por tanto, similar a las capacidades del Ejército, la Fuerza Aérea y la Armada. La defensa cibernética consiste en las capacidades defensivas, ofensivas y de inteligencia» (Kärkkäinen, 2013: 98). Pero como se contrastó entre varios teóricos militares no todas las percepciones suelen ser tan inclusivas. La aclaratoria de los límites conceptuales de la «*Defensa Cibernética*» contribuirá a que las líneas políticas «*macro*» que se han definido desde los presidentes de la UNASUR, y en donde se han dado pasos importantes en aspectos técnicos como el «*Mega Anillo de Fibra Óptica*», tiendan a la concreción sobre la visión de «*ciberguerra*» que aún son pocas.

CAPÍTULO V

5. CONCLUSIONES

En la presente tesis se buscaba analizar la relación entre las políticas regionales sobre ataques informáticos y la Defensa de la UNASUR, lográndose extraer información esclarecedora producto de la revisión de documentos del «CDS» y el «CEED», así como de las entrevistas con especialistas, que han permitido observar en su justa medida la evolución que la temática de las «*ciberamenazas*» han tenido en Sudamérica. Cuando de la cumbre de Paramaribo surgió la orden ejecutiva de iniciar un trabajo colaborativo entre los consejos de la UNASUR para atender la «*ciberdefensa*», esto significó un paso notable dentro de la institucionalidad subcontinental que vinculó una decisión política con una interacción estratégico/técnica. Pero, del análisis de la documentación de los diferentes entes regionales donde se ha tocado la materia surge la duda sobre la connotación de «*ciberdefensa*», que no es la enunciación más abarcante, siendo esto expuesto en las diferentes interpretaciones teóricas de estrategas que han mostrado el carácter «*bidimensionalidad*» (ataque y defensa) de la guerra, surgiendo la interrogante sobre cuál sería el ámbito para discutir la «*ciberguerra*» y la «*ciberestrategia*». Es la apreciación que se concluye de esta investigación que al estar presente la amenaza cibernética, y que la misma es tratada hondamente desde lo estratégico y táctico por las naciones u organizaciones militares con mayor poderío militar (EE.UU., China, la OTAN), se debe sincerar en la UNASUR y particularmente en el «CDS» el tratamiento como «*ciberguerra*». Son suficientemente precisas las intenciones de potencias militares en el «*ciberespacio*» como para tener una posición dubitativa, que pretenda dar meras respuestas políticas o diplomáticas ante un frente de batalla que aunque virtual es real.

En cuanto a los planteamientos estratégicos desarrollados desde la UNASUR, para contrarrestar ataques informáticos que vulneren la Defensa Regional, estos son aun limitados, entre otros motivos por la tendencia a la minimización de la discusión sobre la amenaza

informática por subestimación o desconocimiento. La amenaza «*cibernética*» es transversal a los cuatro ejes que plantea el «CDS» tocando: «*Políticas de Defensa*», «*Cooperación Militar*», «*Industria y Tecnología de la Defensa*», y «*Formación y Capacitación*», ya que la variable tecnológica está enraizada prácticamente en todos los entramados de un Estado u organismo. Tomando como referencia estos «ejes», se pueden hacer una serie de conclusiones, primeramente en las «*Políticas de Defensa*» se vislumbran pinceladas en los «*Planes de Acción 2012/2013*», que arrojó una propuesta inicial presentada por la delegación peruana que mostraba elementos generales y que deben ser profundizados estratégicamente. Si se pretende crear un grupo de trabajo para establecer políticas y estrategias, las definiciones claves como «*ciberpoder*», «*acto de guerra cibernético*», o «*ciberguerra*» deben estar presentes. La mayoría de los estrategas militares coinciden en que la acción militar está supeditada a la política, debiéndose delimitar desde los niveles ejecutivos con precisión las líneas generales sobre «*Defensa Cibernética*» antes de entrar en detalles de «*operativización*» como proponer la estructuración de una coordinación de Respuesta a Emergencias Teleinformática de la Administración Pública de los CERT, para evitar la anteposición de disposiciones técnicas a las visiones estratégicas. Por tanto, la UNASUR se encuentra en una fase inicial de articulación política para atender la amenaza de ataques informáticos, con planteamientos estratégicos en una etapa previa de concreción y definición.

Sobre la manera en que los Ataques Informáticos representan una amenaza para la Defensa Regional de la UNASUR, se puede establecer que más allá del daño puntual (cinético) que puede ocasionar un Ataque Informático, la amenaza se afinca en las vulnerabilidades vinculadas a la falta de clarificación de las líneas generales que ocasiona un desbarajuste en la cadena lógica de desarrollo que debería ser política+estrategia+táctica+técnica/formativa. Los dos eslabones iniciales que es la decisión política para desplegar la propuesta estratégica han quedado circunscrita a generalidades que

no proporcionan las nociones, enunciaciones, y medidas regionales que se deben emprender en teatros bélicos de «*ciberguerra*», propiciando esto una debilidad estratégica que acarrea consecuencias en niveles tácticos como la «*Cooperación Militar*». En esta «*secuencia de efecto*» la desorientación inicial incide en el eslabón técnico que está representado por la «*Industria y Tecnología de la Defensa*» que debería programarse para el desarrollo de software y hardware sudamericano que pueda contribuir a la protección de la «*infraestructura crítica*» regional y potenciar capacidades militares. Así como se propone la construcción de un avión de entrenamiento el «*UNASUR-1*» entre los distintos integrantes de la unión, es preponderante que haya una sustitución de tecnología extra regional a mediano y largo plazo al menos en el medio cibernético, ya que la reproducción o mera transferencia no libera de la dependencia. Es de hacer notar que la «*Formación y Capacitación*» deben fundamentarse en la correcta percepción de tres áreas fundamentales como son la «*ciberestrategia*», «*ciberpoder*» y «*ciberespacio*», siendo los dos primeros los encargados de prefigurar el plano político/estratégico, mientras que la última se adentra sólo en el aspecto técnico. Las vulnerabilidades reflejadas se ensanchan principalmente por razones internas a la región, aunque ciertamente hay incursiones externas que contribuyen al estancamiento, debiendo procurarse que cada eslabón se comporte en consonancia con el otro, para dentro de esa lógica pensar la «*ciberguerra*» como un ente articulador de todo, que podría tener dos objetivos: el «*Interés Regional*», y la «*Disuasión*».

En relación a las falencias en materia de Defensa Regional que influyen en la vulnerabilidad de la UNASUR ante la amenaza de ataques informáticos, se puede apreciar desde un enfoque estratégico que el «*ciberespacio*» sudamericano debería ser concebido como un «*Interés Regional*» ameritando un tratamiento que exteriorice su importancia, como se ha reiterado en esta investigación la «*infraestructura crítica*» está vinculada a sistemas de defensa, finanzas, energía (Hidroeléctricas, Complejos Petroleros), servicios públicos,

telecomunicaciones, entre otros, siendo imprescindible que se atienda este espacio informático como un «*Interés Regional*». Si se lograra esta perspectiva integraríamos dos visiones que son necesarias para comprender la «*ciberguerra*» que serían: la «*amenaza*» (ataques cibernéticos) y por otro lado el «*Interés Regional*» (ciberespacio), teniéndose el acto de agresión, y el bien protegido claramente visualizados, quedando por reflejar la respuesta sudamericana ante la vulneración.

Otra falencia se vincula a los fuertes lazos de dependencia tecnológica con relación a empresas y naciones ajenas a la región, quedando afirmada esa vulnerabilidad en las acciones de espionaje e intercepción informática que han sido reveladas desde diferentes fuentes, lo que deja claro que la «*amenaza*» es cierta, pero además la facilidad que han tenido potencias mundiales para inmiscuirse en los sistemas informáticos del subcontinente refleja que en caso de querer ejercer acciones enmarcadas en una «*ciberguerra*» tendrían una resistencia insignificante.

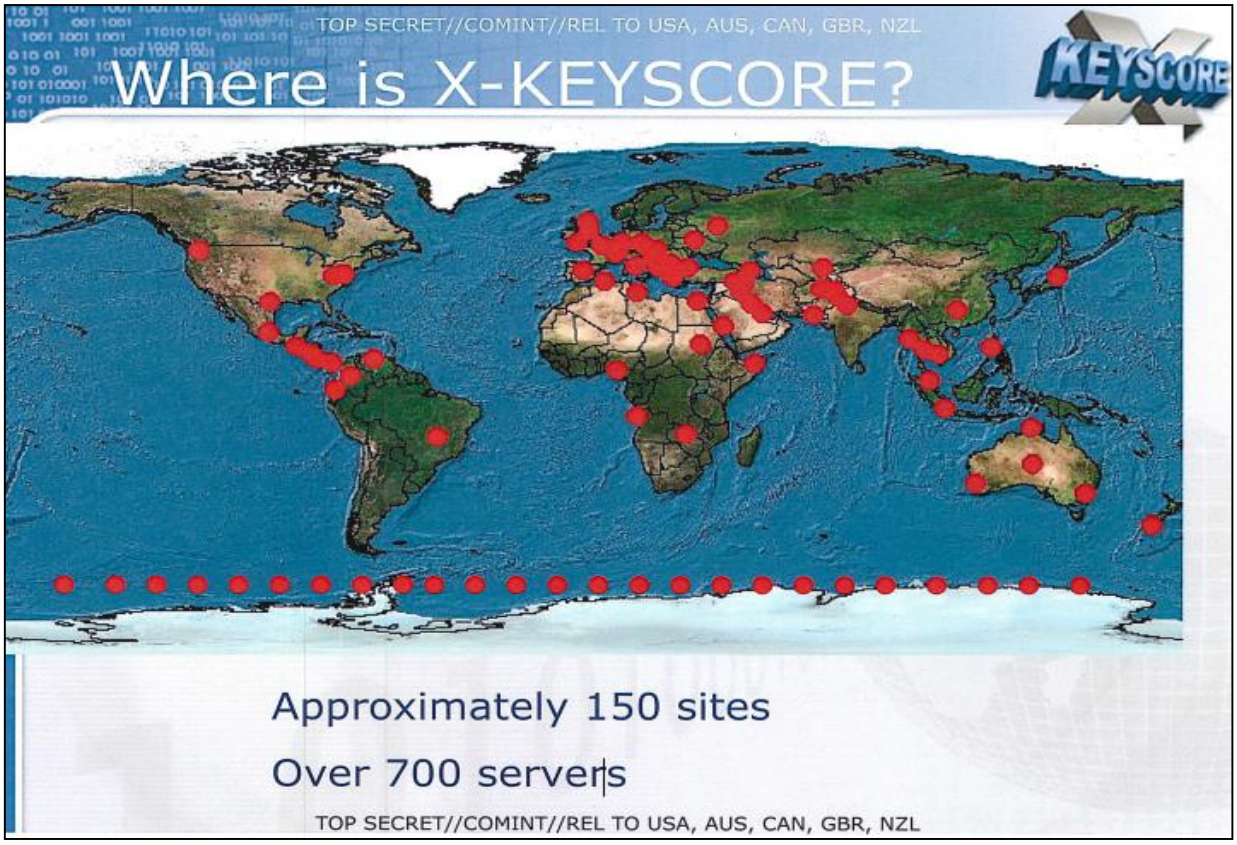
Por último, existe una falencia disuasiva, que como se ha denotado en el presente estudio tiene un efecto psicológico sobre posibles adversarios o atacantes, pero comprende la credibilidad del actor que intenta mostrar una fortaleza, y en Sudamérica el tratamiento a los fenómenos cibernéticos es muy reciente, no contándose con estrategias, infraestructura, ni operatividad para emprender conjuntamente acciones en un escenario de «*ciberguerra*». Las delaciones que demostraron las «*ciberincursiones*» sobre la región sólo han generado pronunciamientos políticos para iniciar tenues exploraciones sobre la temática, pero la actualidad muestra a la región como un campo desprotegido que sabe que tiene una amenaza pero atiende lentamente sus vulnerabilidades.

El desarrollar la presente tesis apoyado en un marco teórico estratégico permitió darle una perspectiva desde el pensamiento militar a una temática que a nivel sudamericano ha sido poco estudiada tanto en instituciones castrenses como civiles, pero se precisaba este aporte

para visibilizar cómo la tecnología se ha rebosado hacia todos los ámbitos sociales, teniendo particular incidencia en la guerra. Además hacer un estudio desde la visión civil sobre un asunto de Defensa logró matizar la disertación sobre las amenazas informáticas que erróneamente en algunas naciones ha pasado a estar bajo un tutelaje absolutamente militar, siendo necesaria la apreciación conjunta de esta situación. La formación de un investigador social no está inicialmente configurada para comprender a fondo el pensamiento militar, pero el ser un observante no perteneciente a una institución de la Fuerza Armada ha permitido asimilar particularidades como la sobrestimación de la convencionalidad y la reducción a la mínima expresión de los aspectos relacionados a la ciberguerra, percepción muy ligada a un pensamiento clásico de la confrontación bélica en Sudamérica. Todo este aprendizaje teórico de los principios generadores de la estrategia han contribuido a fundamentar la hipótesis que dio pie a esta investigación: **La carencia de una política y estrategia regional sobre ataques informáticos aumenta la vulnerabilidad de la Defensa de la UNASUR.** Como se ha documentado y expuesto, se están apenas dando los primeros avances regionales para entablar discusiones sobre «*Defensa Cibernética*», por tanto la primera variable de la hipótesis ha sido confirmada, ya que no hay todavía una política sudamericana sobre ataques informáticos. Por otro lado, la ratificación de la certeza de la primera variable tiene concomitancia sobre la segunda, que se relaciona al aumento de la vulnerabilidad, y que se hace evidente, ya que al no tener una profundidad en los direccionamientos políticos y estratégicos esto desequilibra los planos: tácticos, técnicos y formativos, confirmándose afirmativamente el segundo apartado hipotético. Es decir la hipótesis como conjunto ha sido comprobada con elementos teóricos, metodológicos, documentales y analíticos, que dan cuenta del cumplimento a cabalidad del objetivo central propuesto en esta tesis.

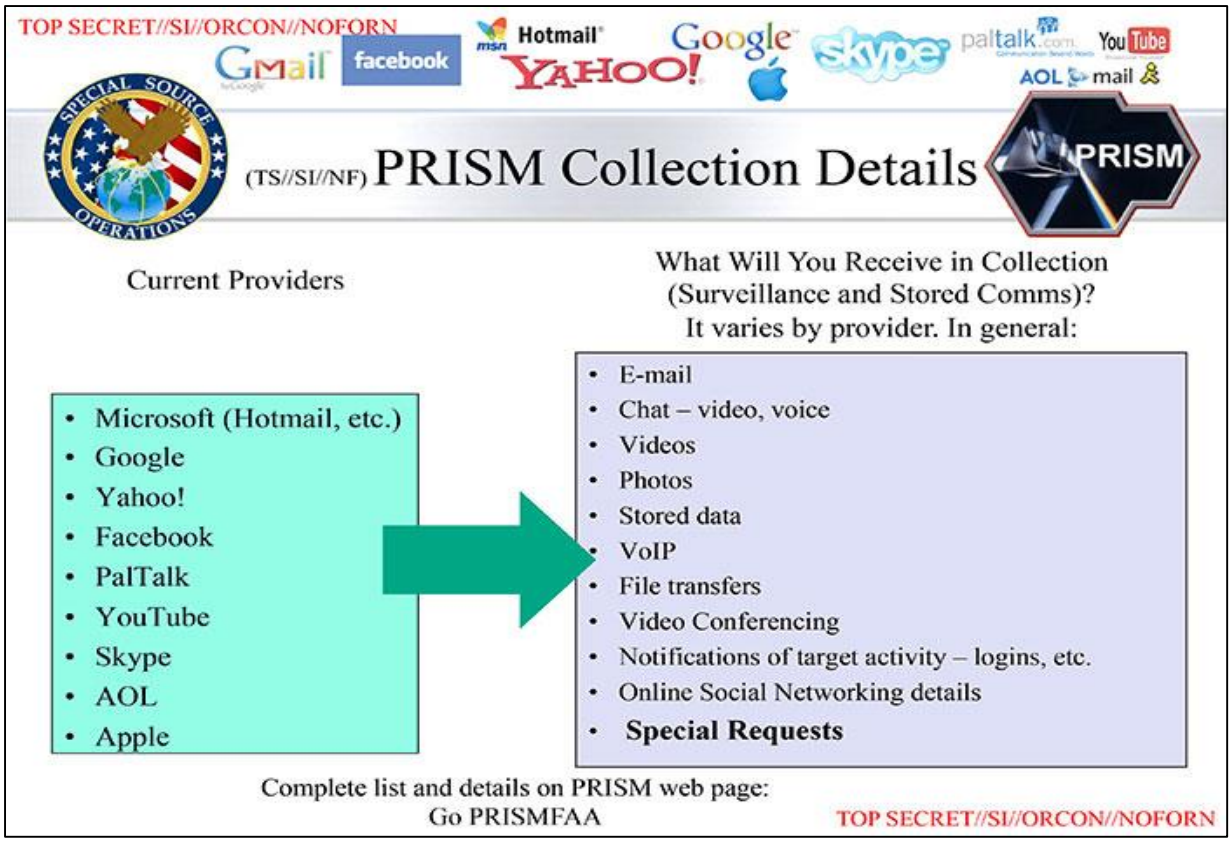
6. ANEXOS

ANEXO «A»



Fuente: The Guardian **(2008).**

ANEXO «B»



Fuente: The Washington Post **(2013).**

ANEXO «C»

Fuente: Istoe **(2013).**

7. CITAS EN SU IDIOMA ORIGINAL

CAPÍTULO I

«We define a computer 'virus' as a program that can 'infect' other programs by modifying them to include a possibly evolved copy of itself» (Cohen, 1987: 23).

«We can anticipate that every major alteration or extension of the battlespace of the future will depend on whether a certain kind of technological invention, or a number of technologies in combination, can create a brand new technological space» (Liang & Xiangsui, 1999: 42).

«crear a Bulgària el Dark Avenger, el primer virus polimòrfic i stealth (invisible) de la historia (…) diversos antivirus detectaven el Dark Avenger, però no podien descobrir els 512 bytes escrits aleatòriament al disc, ja que aquests mai eren els mateixos pel fet de tenir una estructura polimòrfica» (Campàs, 2007: 24-25).

«The attacking entity can be a state or a nonstate actor […] if the attacker is a nonstate entity, it is unlikely to present much of a target for the defending state to hit back against» (Libicki, 2009: 117).

«Cyberspace is bound up in virtually every sector of our economy. It pervades our transportation system, our power and energy grids, our emergency systems, and our military programs» (Rosenzweig, 2013: 3)

«The attack sent the generator out of control and ultimately caused in to self-destruct, alarming the federal government and electrical industry about what might happen if such an attack were carried out on a larger scale» (Harrison, 2012: 6).

«The most destructive scenarios involve cyber actors launching several attacks on our critical infrastructure at one time, in combination with a physical attack on our country. Attackers could also seek to disable or degrade critical military systems and communication networks» (U.S. Department of Defense, 2012).

«Although it is common sense that you cannot determine sources of cyber attacks only through IP addresses, some people in the Pentagon still prefer believing they are from China as they always bear a sense of rivalry» (Chinese People's Liberation Army, 2013).

«pelas implicações do que está em jogo – nomeadamente saber se um determinado ciberataque poderá ser considerado um ato de guerra –, é inevitável concordar-se que a clareza e o rigor do conceito são fundamentais não só para a segurança jurídica, como, também, para os decisores políticos poderem escolher a opção mais adequada em caso de um ciberconflito» (Teixeira, 2012: 55).

«Common cyber strategy If the countries do not share a common goal, it is difficult to develop sustainable cyber activity. Cyber challenges are not country specific and therefore, there is a need for wider cooperation. One possibility is to develop a common cyber strategy» (Rantapelkonen, y Salminen, 2013: 12).

«And, with the growth of information also comes a growing threat to our security. Every minute, more than 168 million e-mail messages are sent. That’s 88 quadrillion messages every year, and each and every one of them is a potential threat vector and source of a malware intrusion» (Rosenzweig, 2013: 24).

«the degree of dominance in cyberspace by one force that permits the secure, reliable conduct of operations of that force, and its related land, air, sea and space forces at a given time and sphere of operations without prohibitive interference by an adversary» (Taylor, y Carter, 2010: 13).

«With regard to technology itself, each technology has specific aspects, which therefore means that each has its time limits. Yesterday's "high" is very possibly today's "low," while today's "new" will in turn become tomorrow's "old."» (Liang & Xiangsui, 1999: 17).

«it is a mistake to believe that something can be learnt only from cases whose circumstances are more or less similar, and that everything that took place before e.g the invention of the steam engine, quick-firing rifle, automobile, tank, aircraft, nuclear arms, or ballistic missile is therefore irrelevant» (Van Creveld, 1983: 560).

«This time, technology is again running ahead of the military thinking. While no military thinker has yet put forth an extremely wide-ranging concept of the battlefield, technology is doing its utmost to extend the contemporary battlefield to a degree that is virtually infinite» (Liang & Xiangsui, 1999: 41).

CAPÍTULO II

«[...] war is no longer simply a question of one wrestler throwing the other out of the ring. From Moltke to Liddell Hart, the goal of strategy has been just the opposite: namely, to outflank the enemy, encircle him, cut him off, deprive him of supplies and make him surrender without actually having to fight for the ground on which he stood» (Van Creveld, 1991: 423).

«The differences suggest that Ludendorff and Clausewitz chose their terms with care and, although they were children of their time in the sense that they closely interacted with the intellectual and practical military and political environments of their day, they tried to capture something distinct and uniquely appropriate to addressing effectively the military challenges of their time» (Honig, 2012: 30)

«In this way, the advent of information warfare is probably one more reason behind the ongoing historical shift away form major war between major states towards the non-trinitarian world of future conflict» (Van Creveld, 2002: 12).

«[…] the 15 and 16 January the Navy's Rafale aircraft were "nailed to the ground" because they were unable to "download their flight plans"» (The Telegraph, 2009).

«The Pentagon had been aware of the problem for many years, but had assumed the insurgents would not have the technical knowledge to intercept the feeds» (The Guardian, 2009).

«[…] agriculture and food systems, the defense-industrial base, energy systems, public health and health care facilities, national monuments and icons, banking and finance systems, drinking water systems, chemical facilities, commercial facilities, dams, emergency services, nuclear power systems, information technology systems, telecommunications systems, postal and shipping services, transportation systems, and government facilities» (O'Rourke, 2007: 22).

«Das Computersystem XKeyscore ist für die Geheimdienste so etwas wie ein Schweizer Taschenmesser der Datenauswertung. Auf der einen Seite ist es das Frontend, mit dem Geheimdienstmitarbeiter die enormen Datenmengen auswerten können. Zum anderen ist es ein System weltweit verteilter Linux-Server. Mehr als 700 solcher Rechner an 150 Standorten waren 2008 an XKeyscore angeschlossen und zeichnen in den jeweiligen Regionen Internet-Datenverkehr auf» (Der Spiegel, 2013).

«Hence, he defined strategy as "the distribution and transmission of military means to fulfill the needs of policy," making it more clearly dependent upon political decisions while, as he explained, leaving its execution in the hands of the military"» (Larson, 1980: 70-71).

«that Liddell Hart's greatest fame will rest on his ideas in two significant areas: (1) The technological aspects of warfare. (2) Psycho-political conflict» (Atkinson, 1966: 162).

«On 19 July 2008 an Internet security firm reported a distributed denial of service (DDoS) cyber attack against Web sites in the country of Georgia. Analysts noted that these additional DDoS attacks appeared to coincide with the movement of Russian troops into South Ossetia in response to Georgian military operations launched a day earlier in the region. By 10

August the DDoS attacks had rendered most Georgian governmental Web sites inoperative"» (Korns & Kastenberg, 2009: 60).

«The first of the three stages is one in which the enemy is on the strategic offensive, and Mao is on what he calls the "strategic defensive". The second is a stalemate stage in which the Communists prepare to seize the initiative .In the third stage there is a shift to the strategic offensive on the Communists' part, forcing the enemy onto the strategic defensive, and eventually out of the war altogether"» (Katzenbach & Hanrahan, 1955: 330).

«Mao combined the old guerrilla-partisan warfare with modern concepts of psychological and total war." Since the guerrilla units," Mao said, "generally grow out of nothing and expand from a small force to a big one, they should not only preserve themselves but also expand their forces." This is the core of Mao's strategy of guerrilla warfare» (Fuller, 1958: 140).

«If the external power's "will" to continue the struggle is destroyed, then its military capability-no matter how powerful-is totally irrelevant» (Mack, 1975: 178-179).

«The National Security Agency and the FBI are tapping directly into the central servers of nine leading U.S. Internet companies, extracting audio and video chats, photographs, e-mails, documents, and connection logs that enable analysts to track foreign targets, according to a top-secret document obtained by The Washington Post» (The Washington Post, 2013).

«the effectiveness of military power has declined relative to the new, infinite means of coercing one's enemies. As they argue, the dynamically changing external environment facing nation-states today makes "obsolete the idea of confining warfare to the military domain"» (Cordesman & Yarosh, 2012: 35).

«If we acknowledge that the new principles of war are no longer "using armed force to compel the enemy to submit to one's will," but rather are "using all means, including armed

force or nonarmed force, military and non-military, and lethal and non-lethal means to compel the enemy to accept one's interests." This represents change» (Liang & Xiangsui, 1999: 7).

«[…] this kind of war means that all means will be in readiness, that information will be omnipresent, and the battlefield will be everywhere. It means that all weapons and technology can be superimposed at will, it means that all the boundaries lying between the two worlds of war and non-war, of military and non-military, will be totally destroyed» (Liang & Xiangsui, 1999:12).

«As a fallout of this strategy and a consequently flowing thought, China's military has been concentrating on developing a wide range of material and non-material capabilities that would make possible "defeating the superior with the inferior" […] According to the PLA, the changes primarily focus upon transforming the military from a 'closed force' into a 'modern information-age power,' deftly highlighted in China's official 2008 White Paper on National Defence» (Chansoria, 2012: 111).

«By using the full spectrum of the multidimensional components of indirect and unrestricted—total—war, a protagonist can produce what Qiao and Wang call a “Cocktail Mixture” of unconventional ways and means of confronting a stronger opponent» (Manwaring, 2007: 25).

«This type of "extended domain view" is a premise for the survival and development of modern sovereign nations as well as for their striving to have influence in the world» (Liang & Xiangsui, 1999: 118).

«The Americans have summed up the four main forms that warfighting will take in the future as: 1) Information warfare; 2) Precision warfare; 3) Joint operations; and 4) Military operations other than war (MOOTW)» (Liang & Xiangsui, 1999: 48).

«The new threats require new national security views, and new security views then necessitate soldiers who first expand their fields of vision prior to expanding their victories» (Liang & Xiangsui, 1999: 129).

«He who wants to win today's wars, or those of tomorrow, to have victory firmly in his grasp, must "combine" all of the resources of war which he has at his disposal and use them as means to prosecute the war» (Liang & Xiangsui, 1999: 181).

«carrying out a network attack against the enemy so that the civilian electricity network, traffic dispatching network, financial transaction network, telephone communications network, and mass media network are completely paralyzed, this will cause the enemy nation to fall into social panic, street riots, and a political crisis» (Liang & Xiangsui, 1999: 147).

«"Domain" is a concept derived from the concept of territory and used to delineate the scope of human activities. Seen in this sense, a domain of warfare is a demarcation of the scope of what is encompassed by warfare» (Liang & Xiangsui, 1999: 188).

«[…] population war, environmental war, asymmetrical war, infrastructure war, non-lethal war, gray area war, informal war, information war (strategic and tactical), netwar, cyberwar, mediawar, neocortical war and postmodern war» (Van Creveld, 2002: 9).

«From this we can see that the concept of means covers a lot of territory, on numerous levels, with overlapping functions, and thus it is not an easy concept to grasp. Only by expanding our field of vision and our understanding of means, and grasping the principle that there is nothing which cannot be considered a means» (Liang & Xiangsui, 1999: 193).

«Emphasis is on achieving greater jointness to launch focused attacks against purportedly “asymmetric” targets, namely, the principal “combat system of the opponent,” so as to erode its cohesion in unexpected ways» (Echevarría, 2010: 21).

«[…] observing the battlefield or a potential battlefield, designing plans, employing measures, and combining the use of all war resources which can be mobilized, to have a field of vision with no blind spots, a concept unhindered by obstacles, and an orientation with no blind angles» (Liang & Xiangsui, 1999: 207).

«As a principle is an important fulcrum for tipping the normal rules in beyond-limits ideology. Its essential point is to follow the train of thought opposite to the balance of symmetry, and develop combat action on that line. From force disposition and employment, selection of the main combat axis and the center of gravity for the attack, all the way to the allocation of weapons, in all these things give two-way consideration to the effect of asymmetrical factors, and use asymmetry as a measure to accomplish the objective» (Liang y Xiangsui, 1999, p.p. 211, 212).

«Great attention is paid to terrorists, hackers, and other non-state organizations and how they engage in the new form of warfare which has developed. The authors argue that the US military simply does not see the threat these groups represent. The methods used by these groups provide important lessons for China» (Bunker, 2007: 116).

«Thus concentration actually consists of dispersion, whereas dispersion consists of concentration, victory going to him who, retaining control and avoiding confusion, switches rapidly from one to the other» (Van Creveld, 1991: 121).

CAPÍTULO III

«[…] a language and techniques that will enable us indeed to attack the problem of control and communication in general, but also to find the proper repertory of ideas and techniques to classify their particular manifestations under certain concepts» (Wiener, 1988: 17).

«[…] great number of interesting and suggestive parallelisms between machine and brain and society. And it can provide the common language by which discoveries in one branch can readily be made use of in the others» (Ashby, 1957: 4).

«[…] the broad cybernetic philosophy that systems are defined by their abstract relations, functions, and information flows, rather than by their concrete material or components, is starting to pervade popular culture, albeit it in a still shallow manner […]» (Heylighen & Joslyn, 2001: 5).

«[…] cybernetics arises when effectors (say, a motor, an engine, our muscles, etc.) are connected to a sensory organ which in turn acts with its signals upon the effectors. It is this circular organization which sets cybernetic systems […]» (Von on Foerster, 2003: 287).

«[…] in the term cyber+space, space assumes the meaning of physical matter, whereas cyber gives it the immaterial characteristic. The term 'cyber' comes from 'cybernetics', which means 'leading, piloting'» (Cicognani, 1998: 20).

«[…] the question "is cyberspace really a 'place'?" – a curious one. It's like asking whether life on land is "identical to" or "different from" life in the ocean. The answer is that it is, simultaneously, both» (Post, 2013: 10).

«[…] as an embodied switched network for moving information traffic, further characterized by varying degrees of access, navigation, information-activity, augmentation (and trust)» (Folsom, 2007: 80).

«We may characterize cyberspace as the spatial reference used in electronic media, but that begs our need to define space itself, for what we experience as space is actually the product of complex mental processes» (Anders, 2001: 409).

«cyberspace — A global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the Internet,

telecommunications networks, computer systems, and embedded processors and controllers» (Department of Defense Dictionary of Military and Associated, 2011: 92).

«With the growth in cyber warfare as a field of study, the amount of cyber related terminology has also grown» (Fritz, 2013: 2).

«The major difference between Kinetic (real world) and Nom – Kinetic (virtual world) warfare methodology is the weapons vs. software programs they use» (Winterfeld & Andress, 2012: 3).

«Cyber war requires a consequential impact in the physical world, or what military experts call a 'kinetic' effect […] In the end, war is the application of force to achieve a desired end. To qualify as cyber war, the means may be virtual but the impact should be physical» (McGraw, 2013: 111-112).

«Both traditional war and cyberwarfare are similar in that their common aim is to achieve an advantage over a competing nation-state or try to prevent said nation-state from achieving an advantage» (Kostyuk & Alí, 2013: 241).

«[…] force to attack another nation and damage or destroy its capability and will to resist. Cyber war would involve an effort by another nation or a politically motivated group to use cyber attacks to attain political ends» (Lewis, 2010: 1).

«[…] the latest form of information warfare, and can include computer network attacks (CNA), which consist of "operations to disrupt, deny, degrade, or destroy information resident in computers or computer networks, or the computers and networks themselves."» (Swanson, 2010: 308).

«Cyberwar refers to conducting, and preparing to conduct, military operations according to information-related principles. It means disrupting if not destroying the information and communications systems» (Arquilla & Ronfeldt, 1997: 30).

«[…] public diplomacy measures, propaganda and psychological campaigns, political and cultural subversion, deception of or interference with local media, infiltration of computer networks and databases, and efforts to promote a dissident or opposition movements across computer networks» (Arquilla & Ronfeldt, 1997: 28).

«Ultimately, information warfare is about using information to make decisions and for the adversary, trying to influence, deny, or disrupt information used in decision making processes» (Williams, 2010: 38)

«[…] cyberwar has introduced a host of new weapons such as viruses, worms and trojan horses, which can wreak havoc on computer systems» (Trendle, 2002: 7).

«CNO are a subset of a broader set of malicious computer mediated activities. According to draft British military doctrine, CNO comprises: Computer Network Exploitation (CNE), namely: "the ability to gain access to information hosted on information systems and the ability to make use of the system itself;" Computer Network Attack (CNA), namely: the "use of novel approaches to enter computer networks and attack the data, the processes or the hardware;" and Computer Network Defense (CND), which is "protection against the enemy's CNA and CNE and incorporates hardware and software approaches alongside people-based approaches." In turn, CNO are one element of Information Operations (IO)» (Rathmell, 2003: 215).

«A military function to provide advice and coordination of military information activities in order to create desired effects on the will, understanding and capability of audiences (...)» (Sentse & Storm, 2010: 7).

«Malware is incapable of destroying buildings, overthrowing governments, or making tactical decisions. In both cases, the pathogen may be capable of destabilizing the targeted environment and allow for a complementary attack to succeed» (Gordon, 2008:1).

«The integrated employment of the core capabilities of Electronic Warfare (EW), Computer Network Operations (CNO), Psychological Operations (PSYOP), Military Deception (MILDEC), and Operations Security (OPSEC)» (Department of Defense, 2006: 1)

«Malicious software designed to carry out annoying or harmful actions. Malware often masquerades as useful programs or is embedded into useful programs so that users are induced into activating them» (Waters, 2008: 48).

«[...] is a viral set that contains exactly one program, where that program simply produces itself. Larger sets represent polymorphic viruses, which have a number of different possible forms, all of which eventually produce all the others» (Chess & White, 2000: 1)

«A computer worm is a program that self-propagates across a network exploiting security or policy flaws in widely-used services (...) As such, viruses tend to propagate more slowly» (Weaver, Paxson, Staniford & Cunningham, 2003: 11).

«[...] a Trojan Horse installs itself on a user's computer without her awareness. That small program then runs in the background, without the user's knowledge, and silently waits to take action» (Kang, 2005: 1554).

«Amongst malware, rootkits are the most dangerous threat. They are particularly difficult to detect and prevent, because they are internal to the operating systems and hide by patching the kernel» (Wang & Dasgupta, 2007: 1).

«These hidden files or software packages are relatively small and, as they do not need to communicate, are extremely difficult to locate. Once triggered, the logic bombs can be massively destructive» (Klimburg, 2011: 42).

«Once installed on the trans-Siberian pipeline, the controller ran a test of the pipeline's pressure gauges during which the logic bomb reset those gauges to double gas pressure in the

pipeline. The resulting explosion was, up to that time, the largest non-nuclear explosion ever photographed from space» (Hamilton, 2009:15).

«the national defense strategy does not necessarily require this part of defense to be under the military. This cyber defense may be considered part of civil defense, instead of military defense» (Kiravuo, 2013: 90).

«1. Offensive freedom of action; 2. Significant vulnerability to attack; 3. Minimal prospects for retaliation and escalation, 4. Ability to identify amd target an adversary's center gravity» (Rattray, 2001: 4).

«1. Supportive institutional enviroment; 2. Demand-pull motivation; 3. Management initiative; 4. Technological expertise; 5. Learning ability» (Rattray, 2001: 4).

«The leadership of cyber requires more than just talk; it also requires joint statements, plans, their implementation and joint action. The fostering of shared understanding of leaders should be encouraged. An initiative should be taken to promote cyber discourse. Leadership skills can be created together in the Nordic countries» (Rantapelkonen & Salminen, 2013: 11)

«It is the ability to use cyberspace to create advantages and influence events in the other operational environments and across the instruments of power» (Czosseck & Geers (Eds.), 2009: 22).

«the development and employment of capabilities to operate in cyberspace, integrated and coordinated with the other operational domains, to achieve or support the achievement of objectives across the elements of national power» (Czosseck & Geers (Eds.), 2009: 22).

«[...] there is a need for interdisciplinary experts who are able to deal with the full range of political, military, economic, social, informational, and infrastructure (PMESII) (...)» (Czosseck & Geers (Eds.), 2009: 25-26).

«Credibility of cyber defense is not based on the amount of servers, firewalls or technicians, as the attacker can select the point of attack» (Kiravuo, 2013: 90).

«Moreover, the mediating influence of technology means that small acts of force – such as tapping a keyboard – can result in large amounts of violence, lethal or otherwise» (Stone, 2012: 107).

«[...] artillery barrages, a drone-strike, improvised explosive devices placed by the side of a road, even a suicide bomber in a public square [...] An act of cyber war would be an entirely different game» (Rid, 2011: 9).

«[...] comes to be widely perceived (as would prefer), it is reasonable to conclude that the threshold for their use will be lower than other kinds of weapons – even if the cost of cyber attacks is greate» (Junio, 2013: 130).

«While cyber attacks are hostile acts in cyberspace, not all cyber attacks equate to armed attack (...) Somewhere along this spectrum of conflict in cyberspace, cyber attack crosses the threshold and becomes an armed attack» (Beidleman, 2009: 12).

«It is very difficult, and very resource-intensive, and sometimes impossible, to trace with much certainty the computer origin of a professional cyber attack or cyber exploitation; it is even harder to do so in real time or even in the short-term» (Goldsmith, 2013: 4).

«For a terrorist, it would have some advantages over physical methods. It could be conducted remotely and anonymously, and it would not require the handling of explosives or a suicide mission» (Denning, 2000: 75).

«[...] is that threats to social order are easily identifiable as being either internal (crime/terrorism) or external (war). Computer-mediated communication erodes the validity of this binary decision tree by making territory increasingly irrelevant [...]» (Brenner, 2007: 382).

«These rules are negotiated by states, and according to many prominent theorists, they entail the mutual acceptance of higher norms, which are standards of behavior defined in terms of rights and obligations» (Mearsheimer, 2005: 8).

«Therefore, there is an urgent need to make global legislation for handling cyberwarfare and cyberterrorism. […] In addressing cyber stalking, new and innovative legislations, technologies, and investigative countermeasures will almost certainly be mandatory» (Janczewski y Colarik, 2008: 223).

«In order to define cyberwarfare effectively, the international community must come to some consensus on the meaning of such activities within the penumbra of the Charter, specifically article 2(4) regulating the use of force […]» (Hoisington, 2009: 446).

«Developing a consensus understanding of the international law of cyber war is complicated by a few unique attributes of the cyber domain. Prompt attribution of an attack and even threat identification can be very difficult» (Banks, 2013: 162).

«[…] the Charter of the United Nations—including both law governing the legality of going to war (jus ad bellum) and law governing behavior during war (jus in bello)—do apply to cyber-attack» (Hughes, 2010: 534).

«[…] the jus ad bellum principle of proportionality, allowing only that degree of force required for an effective defence. Cyber uses of force in the face of an armed attack must further meet the related requirements of imminency and immediacy […]» (Schmitt, 2012: 286).

«But some cyber-attacks destroy property without killing or maiming anyone (...) This naturally raises the question: is the destruction of property ever a just cause for war? If so, when does the destruction of property provide a just cause for war? (...) So perhaps, as a

matter of law, non-lethal property destruction can provide the target with permission to use military violence» (Eberle, 2013: 61).

«This Rule emphasizes the fact that although no State may claim sovereignty over cyberspace per se, States may exercise sovereign prerogatives over any cyber infrastructure located on their territory, as well as activities associated with that cyber infrastructure» (Schmitt (ed.), 2013: 25).

«[…] (i) subjective territoriality, which permits a State to deal with acts which originated within its territory, even though they were completed abroad, objective territoriality, which, conversely, permits a State to deal with acts which originated abroad but which were completed, at least in part, within its own territory» (Schmitt (ed.), 2013: 29).

«[…] (e.g., a use of force committed through cyber means, Rule 10) or a violation of a law of armed conflict obligations (e.g., a cyber attack against civilian objects, Rule 37) attributable to the State in question» (Schmitt (ed.), 2013: 35-36).

«[…] on, or with effects in the entire territory of the parties to the conflict, international waters or airspace, and, subject to certain limitations, outer space. Cyber operations are generally prohibited elsewhere» (Schmitt (ed.), 2013: 71).

«[…] in the course of cyber operations, fail to comply with the requirements of combatant status lose their entitlement to combatant immunity and prisoner of war status» (Schmitt (ed.), 2013: 84).

«A cyber attack is a cyber operation, whether offensive or defensive, that is reasonably expected to cause injury or death to persons or damage or destruction to objects» (Schmitt (ed.), 2013: 92).

«[…] civilians or civilian objects (or other protected persons and objects) rises to the level of an attack is it prohibited by the principle of distinction and those rules of the law of armed conflict that derive from the principle» (Schmitt (ed.), 2013: 96).

«If a neutral State fails to terminate the exercise of belligerent rights on its territory, the aggrieved party to the conflict may take such steps, including by cyber operations, as are necessary to counter that conduct» (Schmitt (ed.), 2013: 207).

«[…] with the U.S. Constitution and other applicable laws and policies of the United States, including Presidential orders and directives» (PPD-20, 2012: 11).

«NSPD-54/Homeland Security Presidential Directive (HSPD)-23 on "Cybersecurity Policy" of January 8, 2008; National Security Directive (NSD)-42 on "National Policy for the Security of National Security Telecommunications and Information Systems" of July 5, 1990; and PPD-8 on "National Preparedness" of March 30, 2011» (PPD-20, 2012: 1).

«[…] developing and maintaining use of cyberspace as an integral part of U.S. national capabilities to collect intelligence and to deter, deny, or defeat any adversary that seeks to harm U.S. national interests in peace, crisis, or war» (PPD-20, 2012: 4).

«[…] are intended to enable or produce cyber effects outside United States Government networks for the purpose of defending or protecting against imminent threats or ongoing attacks or malicious cyber activity against U.S. national interests from inside or outside cyberspace» (PPD-20, 2012: 3).

«OCEO can offer unique and unconventional capabilities to advance U.S. national objectives around the world with little or no warning to the adversary or target and with potential effects ranging from subtle to severely damaging» (PPD-20, 2012: 8).

«[…] exception to obtaining consent is necessary, takes into account overall U.S. national interests and equities, and meets a high threshold of need and effective outcomes relative to the risks created by such an exception» (PPD-20, 2012: 7).

«The information revealed to other countries in the course of seeking consent shall be consistent with operational security requirements and the protection of intelligence sources, methods, and activities» (PPD-20, 2012: 6-7).

«[…] against U.S. national interests from inside or outside cyberspace and under circumstances that at the time do not permit obtaining prior Presidential approval to the extent that such approval would otherwise be required» (PPD-20, 2012: 3-4).

CAPÍTULO IV

«The international trade regime, for example, did not have strong formal rules or integrated, centralized management; rather, it provided a set of interlocking institutions, including regular meetings of the GATT contracting parties, formal dispute settlement arrangements, and delegation of technical tasks to a secretariat, which gradually developed a body of case law and practice» (Keohane, 1998: 85).

«Therefore, the question is not whether cyberwar is about offense and/or defense. It is rather how to meet the phenomenon of "cyberwar" and how to endure problems that arise in the context of cyberspace when not necessarily defining them as a war» (Rantapelkonen & Kantola, 2013: 33)

«The most concrete issue of the strategy is the establishment of a national cyber centre. The cyber centre will maintain situational awareness, improve coordination between actors, accelerate decision making, and develop cyber security related skills. This enables improved strategic sensitivity, flexible resource usage and consistency of management» (Kärkkäinen, 2013: 97)

«The task of coping with cyberspace attacks never ends. As a result, the cyber defense mission is less about stopping cyber-attacks than it is about configuring and training national military forces to be able to fight through them» (Grant, 2009: 26).

«In view of the novel character of technologies, scholars and governments are yet unsure whether the traditional interpretation of customary international law would yield desired results. Therefore, we can expect that scholars and governments continue their efforts to establish stabilised and shared interpretations of international legal norms and the respective behaviour in cyberspace» (Tuukkanen, 2013: 42)

«Learn the capabilities of cyber weapons. Create a cyber-command leadership that understands these capabilities. Communicate these capabilities to other branches in the military and intelligence community. Make sure that enough knowledge is available for military operations planning. Knowledge of cyber capabilities should be available to the planners so that cyber operations can be used to support or replace conventional operations» (Kiravuo & Särelä, 2013: 229).

«Currently, there is no separate cyber threat […] Therefore, cyber threats should be viewed as a horizontal threat element relating to practically all threat scenarios» (Huopio, 2013: 127).

«A ilha de Ascensão tem apenas 91 quilômetros quadrados e seria irrelevante se não estivesse numa posição estratégica, a meio caminho dos continentes africano e sul-americano (...) sua superfície abriga poderosas estações de interceptação de sinais (Singint), que se erguem como imensas bolas brancas. Elas integram um avançado sistema de inteligência que monitora em tempo real todas as comunicações de Brasil, Argentina, Uruguai, Colômbia e Venezuela e fazem parte de um projeto conhecido como Echelon» (Istoe, 2013).

«[…] while the revolution of military technology has allowed one to be able to select measures within a larger range, it has also made it so that one is threatened by these measures within the same range (this is because the monopolizing of one type of technology is far more difficult than inventing a type of technology). These threats have never been like they are today because the measures are diverse and infinitely changing, and this really gives one a feeling of seeing the enemy behind every tree» (Liang y Xiangsui, 1999: 115-116).

«It is not merely a question of protecting and defending information since the entire information processing infrastructure keeps the economic, political and social ecosystems running» (Kärkkäinen, 2013: 105)

«It is typical of cyber attacks that the caused indirect effects are usually more important than the direct effects. The effects are generally very difficult to estimate. Particularly, targeted intelligent cyber attacks are often complicated. Their design and implementation requires a significant amount of human knowledge and capital» (Palokangas, 2013: 146).

«Deterrence depends upon effective communication between the state and the entity it wishes to deter. One has to convince the others that if they attack, one has the capability and the capacity to do something about it. This is also the case in the cyber domain» (Limnéll, 2013: 202).

«However, if the adversaries know that the digital infrastructure is resilient; that there is a credible threat detection and prevention system; and that there is a capability to conduct counterattacks, the deterrence is much more credible» (Limnéll, 2013: 205).

«In a future perspective, information warfare is an integrated part of every major military and political conflict, and cyberspace is both its own dimension and a co-ordinated part of the other physical arenas, such as Land, Sea, Air and Space. Information warfare takes place all

over the whole spectrum of the combat zone, at all levels: strategic, operational and tactical with different main emphases during different phases. A conflict can be both started and decided in the digital sphere, without kinetic means having to be used. Means for information warfare, both offensive and defensive, can be used individually or in combination with other weapons systems» (Heickerö, 2013: 124).

«Over the years, we have seen how both civilian and military sectors worldwide are being targeted by actors in cyberspace seeking to disrupt, deny, deceive, degrade, destroy or in any other way affect computer networks and other communication infrastructure (including SCADAs etcetera). As the victims of such offences may be both civilian and military, response measures need to be implemented in both of these sectors» (Mørkestøl, 2013: 109).

«Cyber defence is an operational capability in cyberspace and hence similar to the capabilities of the Army, Air Force and Navy. Cyber defence consists of defensive, offensive and intelligence capabilities» (Kärkkäinen, 2013: 98)

8. BIBLIOGRAFÍA

- Adams, James (1999). La Próxima Guerra Mundial. Ediciones Granica S.A. Argentina. p. 114.
- Anders, Peter (2001). Anthropic cyberspace: Defining electronic space from first principles. Leonardo, vol. 34, no 5. p. 409.
- Arquilla, John; y Ronfeldt, David (1997). Cyberwar Is Coming. Naval Postgraduate School Monterey Ca Graduate School Of Operational And Information Sciences. p. 28, 30.
- Aron, Raymond (1973). Clausewitz y la guerra popular. Diálogos: Artes, Letras, Ciencias humanas, Vol. 9, No. 2 (50) (marzo-abril 1973), El Colegio de México. p. 20.
- Ashby, Ross (1957). An introduction to cybernetics. London: Chapman & Hall Ltd. p. 4.
- Atkinson, James (1966). Liddell Hart and Warfare of the Future. Military Affairs, Vol. 29, No. 4 (Winter, 1965-1966). p.162.
- AVN (2013). CNE de Ecuador aborta intento de sabotaje electrónico. Recuperado: http://www.avn.info.ve/contenido/p%C3%A1gina-web-del-cne-ecuador-ha-recibido-800000-intentos-ataques
- Bacallao Pino, Lázaro (2011). La comunicación de la guerra/la guerra de la comunicación: disturbios y convergencia. Revista Punto Cero, Universidad de la Habana. p. 57.
- Banks, William (2013). The Role of Counterterrorism Law in Shaping Ad Bellum Norms for Cyber War. Available at SSRN 2160078. p.p. 161, 162.
- Baquer, Miguel Alonso (1989). Actualidad del pensamiento de Clausewitz. Política Exterior, Vol. 3, No. 13. Estudios de Política Exterior S. A. p. 226.
- Baroni, Paola; y Rubiolo (2010). UNASUR: alternativa de integración frente a desafíos internacionales emergentes/UNASUR: an alternative for integration in the face of emerging international challenges. Estudios Internacionales, 2010, p. 129-151. p. 137.
- Beidleman, Scott (2009). Defining and Deterring Cyber War. Army War Coll Carlisle Barracks PA. p. 12.

- Bernal-Meza, Raúl (1999). Mercosur ¿Regionalismo o globalización? Tres aspectos para la decisión de políticas. Revista Realidad Económica Buenos Aires (Argentina), núm. 165 -1 julio al 15 agosto de 1999. p.2.
- Beaufre, André (1977). Introducción a la Estrategia. Editorial Rioplatense. p. 65.
- Biblioteca Ayacucho (1993). Documentos Selectos: Antonio José de Sucre. Fundacion Biblioteca Ayacucho. p. 41.
- Bizzozero, Lincoln (2011). América Latina a inicios de la segunda década del siglo XXI: entre el regionalismo estratégico y la regionalización fragmentada. Rev. Bras. Polít. Int. 54 (1): 29-43 [2011]. p. 36.
- Bodine Birdwell, M. y Mills, Robert (2011). La Conducción de la Guerra en el Ciberespacio Desarrollando la Presentación de la Fuerza y el Mando y Control. p. 11.
- Bonilla, Adrián (2010). Un nuevo regionalismo sudamericano Presentación del dossier. Íconos. Revista de Ciencias Sociales. Num. 38, Quito, septiembre 2010, pp. 23-28. Facultad Latinoamericana de Ciencias Sociales-Sede Académica de Ecuador. ISSN: 1390-1249. p.p 24, 25, 27, 28.
- Bunker, Robert (2007). Unrestricted warfare: Review essay I. Small Wars & Insurgencies, 11(1), 114-121. p. 116.
- Burtseva, Larisa; Tyrsa, Valentyn; Ríos, Brenda Leticia Flores (2013). Norbert Wiener: Padre de la cibernética. Revista UABC, vol. 4, no 54. p. 48.
- Brenner, Susan (2007). "At light speed": Attribution and response to cybercrime/terrorism/warfare. The Journal of Criminal Law and Criminology. p. 382.
- Campàs, Joan (2007). Els Hackers. Editorial UOC. Barcelona. p.p. 24-25.
- Cano, Jeimy (2011). Ciberseguridad y ciberdefensa: dos tendencias emergentes en un contexto global. Sistemas Nº 119, Abril-Junio 2011. p.5.
- Caro, Mª José (2013). La Nueva Dimensión de la Amenaza Global: La Amenaza Cibernética. Instituto Español de Estudios Estratégicos. Documento de Análisis 40/2013. p.2.
- Cardona, Omar (2001). La Necesidad de Repensar de Manera Holistica. Los Conceptos de Vulnerabilidad y Riesgo. Artículo y ponencia para International Work-Conference onVulnerability in Disaster Theory and Practice, 29 y 30 de Junio de 2001,

Disaster Studies of Wageningen University and Research Centre, Wageningen, Holanda. p. 2.

- Castells, Manuel (2004). The Network Society. A Cross-cultural Perspective. Cheltenham, Northampton: Edward Elgar. VAN DIJK, J. (2008). The Network Society. Segunda edición. London: Sage Publications. p.7.
- CEED (2011). Anexo 4. Informe Preliminar del CEED al Consejo de Defensa Suramericano Acerca de los Términos de Referencia para los Conceptos Seguridad y Defensa en la Región Suramericana. p.p. 6, 12.
- CEED (2012). Informe de Avance a diciembre de 2012 sobre Conceptos e Institucionalidad de Seguridad y Defensa, Amenazas, Factores de Riesgo y Desafíos del Consejo Sudamericano de Defensa. p.p. 8, 9, 13, 14.
- Celi, Pablo (2013). Entrevista personal realizada el 07 de noviembre de 2013 al Subdirector del Centro de Estudios Estratégicos de Defensa de la UNASUR.
- Centro Nacional para la Protección de las Infraestructuras Críticas (2010). ¿Qué es una Infraestructura Crítica? Recuperado: www.cnpic-es.es/Preguntas_Frecuentes/Que_es_una_Infraestructura_Critica/index.html
- Cicognani, Anna (1998). On the linguistic nature of cyberspace and virtual communities. Virtual reality, 1998, vol. 3, no 1. p. 20.
- Cogollos, Sofía (2011). UNASUR: una respuesta transnacional a los nuevos retos de la seguridad en Suramérica. Centro Argentino de Estudios Internacionales (CAEI). Working paper nº 49, Programa Integración Regional. p. 5.
- Cohen, Fred (1987). Computer Viruses Theory and Experiments. Dept of Computer Science onri Electric Engineering, Lehigh University, Bethiehern. p. 23.
- Colom, Guillem (2009). El nuevo concepto estadounidense para el empleo de la fuerza militar. Área: Seguridad y Defensa - ARI No 70/2009, Fecha: 23/04/2009, Real Instituto El Cano. p. 2.
- Consejo de Defensa Sudamericano (2013). Propuesta de la delegación Peruana. Establecer una política y mecanismos regionales para hacer frente a las amenazas cibernéticas o informáticas en el ámbito de la defensa. Consejo de Defensa Suramericano.

- Consejo de Defensa Sudamericano (2013). Plan de Acción 2013 – CDS. p. 1.
- Consejo de Defensa Sudamericano (2012). Plan de Acción 2012 – CDS. p. 1.
- Consejo de Defensa Sudamericano (2010). DECLARACION DE GUAYAQUIL 6 y 7 de mayo de 2010. Consejo de Defensa Suramericano. Recuperado: http://www.unasursg.org/uploads/ca/bd/cabda918bf3492200fdf08a6221fc1fd/Declaracio%CC%81n-de-Guayaquil-Guayaquil-Ecuador-6-mayo-2010..pdf
- Consejo de Defensa Sudamericano (2008). Objetivos Consejo de Defensa Suramericano UNASUR. Consejo de Defensa Suramericano. Recuperado: www.unasursg.org/inicio/organizacion/consejos/cds
- Comini, Nicolás (2010). El rol del Consejo de Defensa de la UNASUR en los últimos conflictos regionales. Nueva Sociedad, 2010, no 230. p.p. 19-20.
- Comunidad Sudamericana de Naciones (2004). Declaración del Cusco III Cumbre Presidencial Sudamericana. p.3
- Cordesman, Anthony H; y Yarosh, Nicholas (2012). Chinese Military Modernization and Force Development: A Western Perspective. CSIS. p. 35.
- Chansoria, Monika (2012). Defying Borders in Future Conflict in East Asia: Chinese Capabilities in The Realm of Information Warfare and Cyber Space. The Journal of East Asian Affairs. p. 111.
- Chess, David; y White, Steve (2000). An undetectable computer virus. En Proceedings of Virus Bulletin Conference. p. 1.
- Chinese People's Liberation Army (2013). Pentagon's cyberattack accusations irresponsible: expert. Recuperado: http://eng.chinamil.com.cn/news-channels/pla-daily-commentary/2013-05/08/content_5333521.htm
- Czosseck, Christian y Geers Kenneth (Eds.). (2009). The Virtual Battlefield: Perspectives on Cyber Warfare (Vol. 3). Ios Press. . Stuart H. Starr Towards an Evolving Theory of Cyberpower. p.p. 22, 23, 24.
- Clausewitz, Carl Von (2002). De La Guerra. Editorial Librodot. p.p. 9, 13, 16, 19, 20, 21, 75, 99, 100, 103, 134, 144, 145, 163, 164.
- Declaración de San Petersburgo (1868). Declaración de San Petersburgo De 1868 Con el Objeto de Prohibir el Uso de Determinados Proyectiles en Tiempo de Guerra. p. 1.

- Dantas, Claudio; y Jeronimo, Josie (2013). Como eles espionam. Istoe. Recuperado: http://www.istoe.com.br/reportagens/paginar/323087_COMO+ELES+ESPIONAM/12
- Denning, Dorothy (2000). Cyberterrorism: Testimony before the Special Oversight Panel on Terrorism Committee on Armed Services US House of Representatives (Vol. 23). Washington, May. 1. p. 75.
- Department of Defense (2006). DOD Directive Number O-3600.1 "Information Operations" August 14, 2006. 01. (Freedom of Information Act" 09 may 2008). p. 1.
- Eberle, Christopher (2013). Just War and Cyberwar. Journal of Military Ethics, vol. 12, no 1. p. 61.
- Echevarría, Antulio (2010). Preparing for One War and Getting Another?. Strategic Studies Institute. p. 21.
- El País (2013). Unasur creará un mega anillo de fibra óptica. Recuperado: www.elpaisonline.com/index.php/agenciaplus/item/89224-unasur-creara-un-mega-anillo-de-fibra-optica
- Ferrero, Julio (2013). La Ciberguerra. Génesis y Evolución. Revista General de Marina, Año 2013. Enero-Febrero. Tomo 264. p. 87.
- Fiol, Michelle (2013). Entrevista personal realizada el 04 de octubre a la Asesora Gabinete del Ministerio de Defensa Nacional del Ecuador.
- Folsom, Thomas (2007). Defining Cyberspace (Finding Real Virtue in the Place of Virtual Reality). Tulane Journal of Technology & Intellectual Property, 2007, vol. 9. p. 80.
- Forti, Alfredo (2013). El papel de la Defensa en una Estrategia Suramericana para el Aprovechamiento de los Recursos Naturales. Conferencia Suramericana "Visiones Hacia Una Estrategia Suramericana Para El Aprovechamiento de Los Recursos Naturales". p. 74.
- Fuller, Francis (1958). Mao Tse-Tung: Military Thinker. Military Affairs, Vol. 22, No. 3 (Autumn, 1958), Society for Military History. p. 140.
- Flores, Héctor (2012). Los Ámbitos no Terrestres en la Guerra Futura: Ciberespacio. Centro Superior de Estudios de la Defensa Nacional Monografías del Ceseden, Nº 128, Marzo, 2012. p.p. 18, 25.

- Fritz, Jason (2013). The Semantics of Cyber Warfare 网络战的语义. p. 2.
- García, Miguel (2013). Peligro: ciberataques a empresas. Diario El País. Recuperado: http://economia.elpais.com/economia/2013/03/01/actualidad/1362156981_076595.html p. 2.
- García, Jaime (2001). La Disuasión Convencional. Military Review: Marzo-Abril 2001. ". p. 17.
- Gellman Barton, y Poitras Laura (2013). U.S., British intelligence mining data from nine U.S. Internet companies in broad secret program. The Washington Post. Recuperado: http://www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet-companies-in-broad-secret-rogram/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_story.html
- Giap, Vo (1975). Armar a las masas revolucionarias, construir el ejército popular. Editorial de Ciencias Sociales. p. 41.
- Gibson, William (1984). Neuromante. Minotauro. p. 26.
- Girard, René (2010). Clausewitz en los extremos. Katz Editores. p. 91.
- Goldsmith, Jack (2010). The New Vulnerability (How Cyber Changes the Laws of War). The New Republic. p. 4.
- Gordon, Jason (2008). Cyber Weaponization: Analysis of Internet Arms Development. Computer Security Conference, Myrtle Beach, South Carolina. p. 1.
- Grant, Rebecca (2009). The Cyber Menace. Air Force Magazine, vol. 92, p. 26.
- Greenwald, Glenn y MacAskill, Ewen (2013). Boundless Informant: the NSA's secret tool to track global surveillance data The Guardian. The Guardian. Recuperado: http://www.theguardian.com/world/2013/jun/08/nsa-boundless-informant-global-datamining
- Hamilton, Booz (2009). Software Survivability: Where Safety and Security Converge. p. 15.
- Harrison, Heather (2012). Cyber Warfare and the Laws of War. Cambridge University Press. p. 6.
- Heickerö, Roland (2013). Cyber Security in Sweden from the Past to the Future. The Fog of Cyber Defence. Eds. Jari Rantapelkonen & Mirva Salminen. National Defence

University. Department of Leadership and Military Pedagogy, Publication Series 2, Article Collection nº 10, Helsinki 2013. p. 124.

- Hernández, Roberto; Fernández-Collado, Carlos; Baptista, Lucio (1997). Metodología de la investigación segunda edición. McGRAW - HILL INTERAMERICANA DE MÉXICO, S.A. de C.V. p.p. 69, 70, 71, 73, 81-82.
- Heylighen, Francis; Joslyn, Cliff (2001). Cybernetics and second order cybernetics. Encyclopedia of physical science & technology, 2001, vol. 4. p. 5.
- Hobsbawn, Eric (2002). La guerra y la paz en el siglo XX. Recuperado: www.jornada.unam.mx/2002/03/24/021a1mun.php?origen=opinion.html
- Hoisington, Matthew (2009). Cyberwarfare and the Use of Force Giving Rise to the Right of Self-Defense. Boston College International and Comparative Law Review, 2009, vol. 32. p. 446.
- Honig, Jan (2012). The Idea of Total War: From Clausewitz to Ludendorff. In The Pacific War as Total War. National Institute for Defence Studies. p. 30.
- Hughes, Rex (2010). A treaty for cyberspace. International Affairs, vol. 86, no 2. p. 534.
- Huopio, Simo (2013). A Rugged Nation. The Fog of Cyber Defence. Eds. Jari Rantapelkonen & Mirva Salminen. National Defence University. Department of Leadership and Military Pedagogy, Publication Series 2, Article Collection nº 10, Helsinki 2013. p. 127.
- Instructivo para la Elaboración de Proyecto de Tesis, Tesis y Trabajos Académicos (2012). Editorial IAEN. p. 18.
- Janczewski, Lech; y Colarik, Andrew (Eds.). (2008). Cyber warfare and cyber terrorism. IGI Global. 1. p. 223.
- Joyanes, Luis (2010). Introducción. Estado del arte de la Ciberseguridad. En Cuadernos de Estrategia, Ciberseguridad. Retos y amenazas a la seguridad nacional en el ciberespacio, nº 149, diciembre. p. 26.
- Joxe, Alain (1968). Doctrina estratégica y guerra de intervención. Estudios Internacionales, Año 2, No. 2 (6) (julio-septiembre 1968). p. 285.
- Junio, Timothy (2013). How Probable is Cyber War? Bringing IR Theory Back In to

the Cyber Conflict Debate. Journal of Strategic Studies, 2013, vol. 36, no 1. p. 130.

- Kang, Jerry (2005). Trojan horses of race. Harvard Law Review, 2005. p. 1554.
- Kärkkäinen, Anssi (2013). The Origins and the Future of Cyber Security in the Finnish Defence Forces. The Fog of Cyber Defence. Eds. Jari Rantapelkonen & Mirva Salminen. National Defence University. Department of Leadership and Military Pedagogy, Publication Series 2, Article Collection nº 10, Helsinki 2013. p.p. 97, 98, 105.
- Katzenbach, Edward; y Hanrahan, Gene (1955). The Revolutionary Strategy of Mao Tse-Tung. Political Science Quarterly, Vol. 70, No. 3 (Sep., 1955), The Academy of Political Science. p. 330.
- Keohane, Robert O (1998). "International Institutions": Can Interdepende Work?. En Foreign Policy, primavera 110. p. 85.
- Kiravuo, Timo (2013). Offensive Cyber-capabilities against. Critical Infrastructure. Cyber Warfare. Editor Jouko Vankka. National Defence University. Department of Military Technology, Series 1, No. 34, Helsinki 2013. p.p. 90, 91.
- Kiravuo, Timo; y Särelä, Mikko (2013). The Care and Maintenance of Cyberweapons. The Fog of Cyber Defence. Eds. Jari Rantapelkonen & Mirva Salminen. National Defence University. Department of Leadership and Military Pedagogy, Publication Series 2, Article Collection nº 10, Helsinki 2013. p. 229.
- Korns, Stephen y Kastenberg, Joshua (2009). Georgia's Cyber Left Hook. Parameters, 38(4). p. 60.
- Kostyuk, Nadiya; Alí, Marielle (2013). The Cyber Dogs of War: Joint Efforts of Future World Leaders in The Prevention of Cyberwarfare. En The Second International Conference on Cyber Security, Cyber Peacefare and Digital Forensic (CyberSec2013). The Society of Digital Information and Wireless Communication. p. 241.
- Klimburg, Alexander (2011). Mobilising cyber power. Survival, , vol. 53, no 1. p. 42.
- Kremp, Von Matthias (2013). Internetüberwachung: All das können XKeyscore, Tempora und Prism. Der Spiegel. Recuperado: http://www.spiegel.de/netzwelt/netzpolitik/internetueberwachung-so-maechtig-sind-xkeyscore-tempora-und-prism-a-914300.html

- Larson, Robert (1980). B. H. Liddell Hart: Apostle of Limited War. Military Affairs, Vol. 44, No. 2 (Apr., 1980), Society for Military History. p.p. 70-71.
- Lenin, Vladímir (1973). Obras, Tomo V (1913-1916). Edición: Progreso, Moscú 1973. p.p. 124.
- Lenin, Vladímir (1973). Obras, Tomo XII (1921-1923). Edición: Progreso, Moscú 1973. p.p. 5.
- Lewis, James Andrew (2010). The cyber war has not begun. Center for Strategic and International Studies. p.1.
- Liang, Qiao y Xiangsui, Wang (1999). Unrestricted Warfare. Beijing: PLA Literature and Arts Publishing House, February 1999. p.p. 7, 12, 17, 41, 42, 48, 115, 116, 118, 129, 147, 181, 188, 189, 193, 207, 211, 212.
- Libicki, Martin (2009). Cyberdeterrence and Cyberwar. Rand Corporation. p.117.
- LibiCki, Martin (2012). El Espectro de una Guerra no Evidente. Air & Space Power Journal. p. 19.
- Liddell Hart, Basil (1946). La Estrategia de Aproximación Indirecta. Atalaya: Iberia-Joaquín Gil, Editores, S. A. p.p. 198, 205, 212, 221, 226, 266, 288, 299, 300.
- Limnéll, Jarno (2013). Offensive Cyber Capabilities are Needed Because of Deterrence. The Fog of Cyber Defence. Eds. Jari Rantapelkonen & Mirva Salminen. National Defence University. Department of Leadership and Military Pedagogy, Publication Series 2, Article Collection nº 10, Helsinki 2013. p.p. 202, 205.
- Ludendorff, Erich (1964). La Guerra Total. Ediciones Pleamar / Buenos. p.p. 21, 22, 131, 132.
- MacAskill, Even (2009). US drones hacked by Iraqi insurgents. The Guardian. Recuperado: http://www.theguardian.com/world/2009/dec/17/skygrabber-american-drones-hacked
- Mack JR, Andrew (1975). Why Big Nations Lose Small Wars: The Politics of Asymmetric Conflict. World Politics, Vol. 27, No. 2 (Jan., 1975). p.p. 178, 179.
- Maldonado, Carlos (2013). La red Echelon: el control de internet y de todas las comunicaciones. Le Monde diplomatique | el Dipló 124 | julio 2013. p. 30.
- Manwaring, Max (2007). Latin America's New Security Reality: Irregular Asymmetric Conflict and Hugo Chavez. StrategicStudiesInstitute. p. 25.

- Martínez, Rafael (2008). El Consejo Sudamericano de Defensa:¿ realidad o ficción?. CIDOB. p. 2.
- Mearsheimer, John (2005). The False Promise of International Institutions. En Paul F Diehl. The Politics of Global Governance Innternational organization. p. 8.
- Menezes, Augusto (2010). Regionalismo y seguridad sudamericana: ¿son relevantes el Mercosur y la Unasur? Íconos. Revista de Ciencias Sociales. Num. 38, Quito, septiembre 2010, p.p. 41-53, © Facultad Latinoamericana de Ciencias Sociales-Sede Académica de Ecuador. ISSN: 1390-1249. p.p. 47, 52.
- Moreira, Ángela. Consejo Sudamericano de Defensa: Hacia una integración regional en defensa. RESDAL, Documento de debate, Buenos Aires, 2008. p. 1-20. p. 13.
- Mørkestøl, Kristin (2013). Norwegian Cyber Security: How to Build a Resilient Cyber Society in a Small Nation. The Fog of Cyber Defence. Eds. Jari Rantapelkonen & Mirva Salminen. National Defence University. Department of Leadership and Military Pedagogy, Publication Series 2, Article Collection nº 10, Helsinki 2013. p. 109.
- McGraw, Gary (2013). Cyber War is Inevitable (Unless We Build Security In). Journal of Strategic Studies, 2013, vol. 36, no 1. p.p. 111-112.
- NATO Cooperative Cyber Defence Centre of Excellence Tallinn, Estonia (General Editor Michael N. Schmitt) (2013). The Tallinn Manual on the International Law Applicable to Cyber Warfare. Recuperado: www.ccdcoe.org/249.html Schmitt (ed.), 2013. p.p. 25, 29, 35, 36, 71, 84, 92, 96, 207.
- NSA (2008). Informe Desclasificado: X-KEYSCORE. NSA/CSSM 1-52. The Guardian. Recuperado: http://www.theguardian.com/world/interactive/2013/jul/31/nsa-xkeyscore-program-full-presentation
- Olson, Soren (2012). El boxeo con un contrincante imaginario. La guerra cibernética y el ataque económico estratégico. Military Review, Noviembre-Diciembre 2012. p.p. 67, 70.
- Organización de las Naciones Unidas (1945). Carta de las Naciones Unidas. Entrada en vigor: 24 de octubre de 1945, de conformidad con el artículo 110. p. 3.

- O'Rourke, Thomas (2007). Critical infrastructure, interdependencies, and resilience. Bridge-Washington-National Academy Of Engineering-, 2007, vol. 37, no 1, p. 22.
- Palokangas, Tero (2013). Cyberwar: Another Revolution in Military Affairs?. The Fog of Cyber Defence. Eds. Jari Rantapelkonen & Mirva Salminen. National Defence University. Department of Leadership and Military Pedagogy, Publication Series 2, Article Collection nº 10, Helsinki 2013. p. 146.
- Pereira de Lima, Maria Christiane (2010). La aportación de la UNASUR para el surgimiento de América del Sur como actor global de relevancia en el escenario internacional, (2004-2008). Tesis Doctoral. Universidad Complutense de Madrid, Servicio de Publicaciones. p. 159.
- Pion-Berlin, David (2008). Militares y democracia en el nuevo siglo. Cuatro descubrimientos inesperados y una conclusión sorprendente. Revista NUEVA SOCIEDAD N o 213, enero-febrero de 2008. p. 55.
- Piris, Alberto (2003). Guerras y ejércitos en el siglo XXI. El mundo a la deriva: crisis y pugnas de poder. Anuario 2011-2012. CEIPAZ, (Centro de Educación e Investigación para la Paz) de la Fundación Cultura de Paz. p. 69.
- Post, David G (2013). Against'Against Cyberanarchy'. Berkeley Technology Law Journal, 2002, vol. 17 (Version 1.0 Draft 12/10/13). p. 10.
- Presidential Policy Directive 20: [Classified] (2012). Recuperado: https://www.hsdl.org/?abstract&did=725668 p.p. 1, 3, 4, 6, 7, 8, 11.
- Protocolo Adicional a los Convenios de Ginebra (1977). Aprobado el 8 de junio de 1977 por la Conferencia Diplomática sobre la Reafirmación y el Desarrollo Internacional Humanitario Aplicable en los Conflictos Armados. Entrada en vigor: 7 de diciembre de 1978 de acuerdo con el artículo 95. p. 20.
- Rantapelkonen, Jari; y Salminen, Mirva (2013). The Fog of Cyber Defence. Eds. Jari Rantapelkonen & Mirva Salminen. National Defence University. Department of Leadership and Military Pedagogy, Publication Series 2, Article Collection nº 10, Helsinki 2013. p. 10, 11, 13.
- Rantapelkonen, Jari; y Harry Kantola (2013). Insights into Cyberspace, Cyber Security, and Cyberwar in the Nordic Countries. The Fog of Cyber Defence. Eds. Jari Rantapelkonen & Mirva Salminen. National Defence University. Department of

Leadership and Military Pedagogy, Publication Series 2, Article Collection nº 10, Helsinki 2013. p. 33.

- Rathmell, Andrew (2003). Controlling computer network operations. Studies in Conflict and Terrorism, 2003, vol. 26, no 3. p. 215.
- Rattray, Gregory (2001). Strategic warfare in cyberspace. MIT Press. 1. p. 4.
- Real Academia de la Lengua Española (2001). Diccionario de la Lengua Española (DRAE). Vigésima Segunda Edición. Recuperado: http://lema.rae.es/drae/?val=cibern%C3%A9tica
- Reunión de Presidentes de América del Sur (2000). Comunicado de Brasilia. Recuperado: http://www.sre.gob.mx/images/stories/dgomra/com_brasilia.pdf p.2.
- Rid, Thomas (2012). Cyber war will not take place. Journal of Strategic Studies, 2012, vol. 35, no 1. p. 9.
- Rubio, Leandro (1966). En torno a la guerra revolucionaria. Revista española de la opinión pública, No. 5 (Jul. - Sep., 1966). p. 119.
- Rosenzweig, Paul (2013). Cyber Warfare: How Conflicts In Cyberspace Are Challenging America and Changing The World. ABC-CLIO, LLC. p.p 3, 24.
- Rozitchner, León (1980). Clausewitz y Freud: Del duelo a la guerra. Revista Mexicana de Sociologia, 1980, p. 323-373. p. 344.
- Ruggie, John (1998). Epistemología, ontología y el estudio de los regímenes internacionales. Relaciones Internacionales, núm. 12, octubre de 2009. Revista académica cuatrimestral de publicación electrónica, Grupo de Estudios de Relaciones Internacionales (GERI), Universidad Autónoma de Madrid, España. Recuperado: www.relacionesinternacionales.info. p.177.
- Santana, Cristian Ovando (2012). La Seguridad Internacional en la Proyección de Chile Hacia el Cono Sur. Revista - Bogotá (Colombia) Vol. 7 No 2 - julio - diciembre 2012. p. 196.
- Saint-Pierre, Héctor (2008). Defensa y seguridad. RESDAL. Atlas Comparativo de la Defensa em América Latina. Buenos Aires, 2008. p. 59.
- Saint-Pierre, Héctor; Castro, Gustavo. El Consejo Sudamericano de Defensa. Boletín RESDAL, 2008, vol. 6, no 29. p. 1.

- Sassone, Pedro (2013). Entrevista personal realizada el 18 de diciembre de 2013 al Representante diplomático de la República Bolivariana de Venezuela ante la Secretaría General de la UNASUR.
- Sautu, Ruth; Boniolo, Paula; Dalle, Pablo; Elbert, Rodolfo (2005). Manual de metodología: construcción del marco teórico, formulación de los objetivos y elección de la metodología. Buenos Aires: Clacso, 2005. p.p. 83-84.
- Sánchez, Gema (2013). El ciberespionaje. No. 13. Nueva Época. Marzo-Mayo, 2013. p.p. 117, 123.
- Sánchez, Gema (2010). La nueva estrategia comunicativa de los grupos terroristas. Revista Enfoques • Vol. VIII • No12 • 2010. p. 203.
- Sanz, Ángel, y Fojón, Enrique (2011). Ciberespacio: La Nueva Dimensión del Entorno Operativo. Centro Superior de Estudios de la Defensa Nacional Monografías del CESEDEN, Nº 44, septiembre, Marzo, 2011. p. 43.
- Sentse, Rob; y Storm, Arno (2010). The Battle for the Information Domain. IO Journal, vol. 1, no 4, p. 7.
- Sierra, Francisco (2002). Guerra informacional y sociedad-red. La potencia inmaterial de los ejércitos. Revista Signo y Pensamiento, Vol 21, No 40. p. 2.
- Soler, Rafael; y Hernández, Rodolfo (2011). Cap V: La propiedad intelectual, ¿una amenaza para la neutralidad de la red? Cotino, Lorenzo. Libertades de expresión e información en Internet y las redes sociales: ejercicio, amenazas y garantías. Valencia: Servei de Publicacions de la Universitat de València. p. 331.
- Schmitt, Michael (2012). "Attack" as a term of art in international law: The cyber operations context. En Cyber Conflict (CYCON), 2012 4th International Conference on. IEEE, 2012. p. 286.
- Stone, John (2013). Cyber War Will Take Place!. Journal of Strategic Studies, 2013, vol. 36, no 1. p. 107.
- Swanson, Lesley (2010). Era of Cyber Warfare: Applying International Humanitarian Law to the 2008 Russian-Georgian Cyber Conflict, The. Loy. LA Int'l & Comp. L. Rev., vol. 32. p. 308.
- Tarrés, María Luisa (ed.) (2001). Observar, escuchar y comprender: Sobre la tradición

cualitativa en la investigación social. FLACSO Mexico, 2001. p.p. 68, 76-77.

- Taylor, Fred; y Carter, Jerry (2010). Cyberspace Superiority Considerations. Conflict and Cooperation in Cyberspace: The Challenge to National Security in Cyberspace. Editores: Yannakogeorgos, Panayotis; y Lowther, Adam Taylor y Francis Group, CRC Press. p. 13.
- Teixeira, José (2012). A ciberguerra como nova dimensão dos conflitos do século xxi. Relações Internacionais, Março: 2012 33 [pp. 053-069]. p. 55.
- Tuukkanen, Topi (2013). Sovereignty in the Cyber Domain. The Fog of Cyber Defence. Eds. Jari Rantapelkonen & Mirva Salminen. National Defence University. Department of Leadership and Military Pedagogy, Publication Series 2, Article Collection nº 10, Helsinki 2013. p. 42.
- Trendle, Giles (2002). Cyberwar. The World Today, vol. 58, no 4. p. 7.
- Unasur (2013). VII Reunión Ordinaria del Consejo de Jefas y Jefes de Estado y de Gobierno de la Unión de Naciones Suramericanas Declaración de Paramaribo. p. 8.
- Unasur (2012). UNASUR debate cooperación regional en crimen trasnacional organizado y nuevas amenazas. BP. 0060. Bogotá, febrero 16 de 2012.
- Unasur (2009). Consejo de Defensa Suramericano. Recuperado: www.unasursg.org/inicio/organizacion/consejos/cds
- Unasur (2009). Declaración de Santiago de Chile. Primera Reunión del Consejo de Defensa Suramericano (CDS) de la Unión de Naciones Suramericanas (UNASUR). p.p. 1, 2.
- Unasur (2008). Estatuto del Consejo de Defensa Suramericano de la Unasur. III Reunión Ordinaria de Jefas y Jefes de Estado y de Gobierno. Recuperado: http://www.ceedcds.org.ar/Espanol/09-Downloads/ESTATUTO_CDS.pdf p. 4.
- Unasur (2008). Tratado Constitutivo de la Unión de Naciones Suramericanas. p.2
- Unasur (2008). Cúpula Extraordinária da União de Naçõ es Sul-Americanas (UNASUL) – Costa do Sauípe, Bahia, 16 de dezembro de 2008 – Declaração e Decisões I. Declaração do Conselho de Chef as e Chefes de Estado e de Governo. p. 2.
- Urzúa, Gustavo (2003). Las Amenazas Asimétricas como Nuevas Formas de

Conflicto en el Contexto Sudamericano. 2003. Seguridad y defensa en las Américas: La búsqueda de nuevos consensos. Santiago, Chile, FLACSO-Chile. Serie Libros FLACSO ISBN: 956-205-180-3. p. 215.

- U.S. Department of Defens (2012). Presenter: Secretary of Defense Leon E. Panetta. Recuperado: http://www.defense.gov/transcripts/transcript.aspx?transcriptid=5136
- U.S. Department of Defense (2011). Dictionary of Military and Associated Terms, Joint Publication 1-02, Nov. 8, 2010, as amended through Jan. 31, 2011. p. 92.
- Valles, Miguel (2000). Técnicas cualitativas de investigación social. Síntesis Sociológica Editorial. p.p. 109, 136.
- Van Creveld, Martin (1983). Thoughts on military history. Journal of Contemporary History, 18(4), 549-566. p. 560.
- Van Creveld, Martín (1991). The Transformation of War. The Free Press. A Division Macmillan, Inc. p. 121.
- Van Creveld, Martin (1991). The Clausewitzian Universe and the Law of War. Journal of Contemporary History, 26(3/4). p. 423.
- Van Creveld, Martín (2008). The Transformation of War Revisited. Revisited, Small Wars & Insurgencies. p.p. 9, 12.
- Vílchez, Lorenzo (2000). La construcción social del virus informático. SIGNO Y PENSAMIENTO N" 36 (XIX), Universidad Javeriana: Departamento de Comunicación, 2000. p.p. 103-110.
- Von Foerster, Heinz (2003). Cybernetics of cybernetics. En Understanding Understanding. Springer New York, 2003. p. 287.
- Wang, Lifu; Dasgupta, Partha (2007). Kernel and application integrity assurance: Ensuring freedom from rootkits and malware in a computer system. En Advanced Information Networking and Applications Workshops, AINAW'07. 21st International Conference on. IEEE, 2007. p. 1.
- Waters, Gary; Ball, Desmond; y Dudgeon, Ian (2008). Australia and cyber-warfare. ANU E Press, 2008. p. 48.
- Weaver, Nicholas; Paxson, Vern; Staniford, Stuart; y Cunningham, Robert (2003). A taxonomy of computer worms. In Proceedings of the 2003 ACM workshop on Rapid

malcode (pp. 11-18). ACM. p. 11.

- Wiener, Norbert (1988). Human use of human beings: Cybernetics and society. Da Capo Press. p. 17.
- Williams, Patricia AH (2010). Information Warfare: Time for a redefinition. 2010. p. 38.
- Willsher, Kim (2009) French fighter planes grounded by computer virus. The Telegraph. Recuperado: http://www.telegraph.co.uk/news/worldnews/europe/france/4547649/French-fighter-planes-grounded-by-computer-virus.html
- Winterfeld, Steve; y Andress, Jason (2012). The Basics of Cyber Warfare: Understanding the Fundamentals of Cyber Warfare in Theory and Practice. Elsevier Inc. p. 3.
- Yuni, José & Urbano, Claudio. (2005). Mapas y herramientas para conocer la escuela: Investigación etnográfica e investigación-acción. Editorial Brujas. p. 171.
- Zedong, Mao (1976). Problemas de la Guerra y de La Estrategia. Ediciones En Lenguas Extranjeras Pekín 1976. Primera Edición 1968 (3a Impresión 1976), Tomo II. p.p. 160, 167, 198, 199, 236, 237, 238, 239, 240.
- Zibechi, Raúl (2011). La silenciosa revolución suramericana. La Jornada. Recuperado: http://www.jornada.unam.mx/2011/12/02/politica/025a1pol