ESPECIALIZACION EN ESTRATEGIA OPERACIONAL Y PLANEAMIENTO MILITAR CONJUNTO

TRABAJO FINAL DE INVESTIGACION

TEMA:

OPERACIONES MILITARES Y REDES SOCIALES EN INTERNET.

TÍTULO:

"LAS VULNERABILIDADES DE LAS OPERACIONES MILITARES DERIVADAS DE LAS REDES SOCIALES EN INTERNET".

AUTOR: CAPITÁN DE CORBETA AUGUSTO SEBASTIÁN RIVOLTA

Año 2012

RESUMEN

Con la llegada de las redes sociales, favorecidas por los avances tecnológicos digitales, se ha producido un nuevo modo de interrelación entre individuos, sin que todavía se haya podido precisar el alcance de esta interacción.

Periódicamente surgen en internet nuevos espacios de intercambio, algunos para mero entretenimiento y otros con abundante información, que generalmente contienen una cuota de valorización, positiva o negativa, de acuerdo a la ideología del medio/actor que la provee.

La posibilidad que brinda éste escenario (que cambió el paradigma de la comunicación tradicional), es la de permitir llegar a los usuarios de las redes sociales en forma personalizada y brindan un retorno, feed back, que le permite saber al medio/actor que agrada o desagrada a los usuarios.

La dificultad para el usuario, radica en los inconvenientes que genera la jerarquización y veracidad de la información que llega a través de las redes, dado que los distintos actores operan de acuerdo a sus intereses sacando provecho de distinta índole. Estos beneficios se pueden traducir en intereses políticos, económicos y por qué no militares; todos ellos normalmente desarrollados bajo el anonimato.

Para una organización militar estos hechos no pueden pasar inadvertidos, ya que cada miembro de la fuerza se transforma en un potencial transmisor involuntario de información. Las redes sociales no son entes ajenos a nuestra cotidianeidad y representan una vulnerabilidad que utilizada por actores adecuados pueden hacer caer operaciones militares dentro de un teatro.

El objetivo de este trabajo es el de describir cómo las redes sociales en internet pueden afectar las operaciones militares y analizar cómo neutralizar sus efectos dentro de un Teatro de Operaciones.

Con ello, corroboraremos que las FFAA Argentinas deben prepararse para hacer frente a las vulnerabilidades que provoca el uso de la tecnología digital. Dentro de ellas, las redes sociales serán la fuente de mayor fuga de información.

Palabras claves: Redes Sociales, Medios de Comunicación Tradicional, Cambio de Paradigma, Potencialidad, Operaciones Militares.

TABLA DE CONTENIDOS

INTRODUCCIÓN

Existe consenso en las Ciencias Sociales en definir al hombre como un ser gregario por naturaleza. Tiene la necesidad de formar grupos sociales y su vocación histórica ha sido agruparse con fines específicos[1]. Con el advenimiento de las redes sociales, favorecidas por las nuevas tecnologías de la información y comunicación (NTIC), se ha generado un salto cualitativo y cuantitativo en la forma de interrelacionarse de los individuos.

Actualmente, las redes sociales en internet han cobrado una significación sin precedentes dentro de la cultura social. Como sostienen algunos investigadores, que abordaremos en los capítulos precedentes, las mencionadas redes, conforman el rol organizativo de acciones colectivas y a su vez son un altavoz omnidireccional de lo que está ocurriendo diariamente[2]. Producto de ellas la anarquía comunicacional, la dificultad para determinar la fuente, la jerarquía y veracidad de la información son una constante del nuevo paradigma.

El surgimiento de estas tecnologías disruptivas[3] provocan cambios trascendentes, ya que tienen la capacidad inherente de reescribir las reglas, cambiar estructuras, y alterar organizaciones, las tácticas y las estrategias. Hacen avanzar a la Humanidad.

Ejemplo del potencial de esta nueva forma comunicacional, se vio durante la revuelta de los países Árabes del norte de África. La revolución de los Jazmines[4], que sumió en un conflicto social a la nación de Túnez en diciembre de 2010, culminó con la destitución de su líder Zine El Abidine Ben Ali[5]. Unos meses de organización ciudadana en las redes sociales con la utilización de las (NTIC), fueron más efectivas que veintitrés años de protestas. Posteriormente los efectos en cascada fueron visibles en Egipto, Yemen, Argelia, Libia y Siria; que aun hoy aparecen en las primeras planas de los diarios más importantes del mundo.

---

[1] Ardrey, Robert. La evolución del hombre: la hipótesis del cazador *(*en línea). Disponible en http://en.scientificcommons.org /34184701. Página en castellano. Fecha de captura 09/05/12.

[2] La Sociedad de la Información en el Siglo XXI: Un requisito para el desarrollo, (en línea). Disponible en http://www.slideshare.net/isidreb/sociedad-de-la-informacin-en-el-siglo-xxi-reflexiones-y-conocimiento-compartido. Página en castellano. Fecha de captura 14/08/12

[3] Tecnología Disruptiva: Término que procede del inglés *disruptive* y que se utiliza para nombrar a aquello que produce una ruptura brusca. Por lo general el término se utiliza en un sentido simbólico, en referencia a algo que genera un cambio muy importante o determinante. En línea http://definicion.de/disruptivo. Fecha de captura el 08/07/2012.

[4] También conocida como "La Revolución Tunecina" a raíz de la crisis política de Tunez en 2010 y 2011.

[5] Dictador tunecino, presidente de la república desde 1987 - año en el que derrocó al presidente Bourguiba - hasta el 14 de enero de 2011, cuando se vio obligado a escapar del país por la rebelión de su pueblo.

Dentro de los conflictos mencionados, el papel más importante fue el desempeñado por las redes sociales en internet, que se han mostrado como un conductor de información on-line con un gran poder aglutinante de masas; reafirmando que las redes sociales influencian en la comprensión y percepción que tienen los sujetos que las integran[6].

Esto corrobora la existencia de una conciencia colectiva, que puede surgir naturalmente o ser inducida por actores que operan de acuerdo a sus intereses[7]; algunos personales, otros políticos, económicos y/o militares. Este escenario, se muestra como un ámbito propicio para llevar adelante operaciones de inteligencia, que afectan tanto al resguardo de información como en el desarrollo de operaciones militares.

Se sabe, el riego que implica para una institución militar que determinada información clasificada llegue a manos del oponente, sobre todo durante la ejecución de operaciones militares. Pero muy pocos integrantes de las fuerzas toman real conciencia del grado de exposición que tiene su computadora, con la información personal y profesional, cada vez que se conecta a la web.

Con nuestra investigación nos proponemos mostrar que el escenario cibernético no es un escenario de conflicto a futuro, sino un conflicto que está en pleno desarrollo. Se observa que no se están tomando las medidas necesarias para hacerle frente y tanto el personal como las instituciones de las Fuerzas Armadas Argentinas están expuestos y presentan vulnerabilidades, en el ámbito de la comunicación institucional y de la inteligencia militar.

Entre los problemas que se perciben y orientan el presente trabajo está el hecho que las redes sociales no son entes ajenos a nuestra cotidianeidad y su uso, representa una vulnerabilidad, que explotada por actores adecuados pueden hacer peligrar el éxito de operaciones militares.
Cada miembro de la fuerza, a raíz de su uso, se transforma en un potencial transmisor involuntario de información.

---

[6] El poder de la Comunicación. Disponible en, http://www.comunicacionclave.mx/CGI-BIN/index.php?option.com_content } &view=article&id=9:revolución-jasmin-como-destruir-un-imperio-en-treinta-dias&catid=6:noviembre 10&Itemid=3. Página en castellano. Fecha de captura 13/08/12.

[7] Periodismo ciudadano. evolución positiva de la comunicación. Disponible en, http://www.scribd.com/doc/74211965/ Página en castellano. Fecha de captura 12/07/12.

Por ello, dentro de las NTIC las redes sociales serán nuestro objeto de estudio, lo que nos lleva a formularnos la siguiente pregunta:

¿De qué manera las redes sociales en internet pueden afectar las operaciones militares y como se pueden neutralizar sus efectos dentro de un Teatro de Operaciones (TO)?

Para realizar el análisis situacional, dividiremos las dificultades englobándolas en tres aspectos, en función de los factores que afectan.

Por un lado, se buscará entender el fenómeno social y cultural que provocan la incorporación masiva de las NTIC y como afectan al personal militar. Por otro, describir el grado de vulnerabilidad que éstas provocan, derivadas de la utilización de redes sociales en interne; como afectan al manejo de la información y a las instituciones militares. Por último identificar los problemas y las posibles soluciones que permitan reducir el impacto en el tratamiento mediático de los conflictos armados.

El trabajo estará estructurado en capítulos. En ellos se realizará una descripción del comportamiento social derivado de las redes sociales, del escenario y finalizaremos con un análisis de la situación; a fin de llegar a las conclusiones que nos permitirán proponer posibles soluciones.

Éste desarrollo nos permitirá comprender y analizar qué debilidades y fortalezas, propone este escenario virtual, qué consecuencias tiene en el real y cómo afecta al ámbito que se vincula con lo militar.

Siendo los objetivos específicos:

- ✓ Describir la nueva cultura digital, generada a partir del advenimiento de la tecnología afín y la importancia de entenderla.

- ✓ Identificar las nuevas tecnologías de la información que han intervenido en los últimos conflictos armados (Irak, Kosovo, Lituania, Egipto, etc.).

- ✓ Identificar las reglas o normas implementadas por las otras fuerzas armadas que permitan hacer frente a las vulnerabilidades provocadas por el uso de la tecnología digital.

La hipótesis que guía la investigación es:

Las FFAA Argentinas deben prepararse para hacer frente a las vulnerabilidades que provoca el uso de la tecnología digital. Dentro de ellas las redes sociales serán la fuente de mayor fuga de información.

La metodología adoptada para el desarrollo del presente trabajo ha sido del tipo descriptivo. Así mismo se relevarán fuentes primarias y secundarias de la bibliografía referida al tema que nos compete (redes sociales, conflictos armados durante el siglo XXI y normas de seguridad informática, etc.). Además se abordaran libros, publicaciones y revistas técnicas y especializadas, así como artículos e informes elegidos a partir de una investigación de material disponible en Internet, bibliotecas nacionales y en el Archivo de la Escuela de Guerra Conjunta.

CAPÍTULO I

EL COMPORTAMIENTO CULTURAL DERIVADO DE LAS REDES SOCIALES.

El tema que trata el presente Capítulo, se encuentra en constante evolución, producto del avance tecnológico y del comportamiento social del hombre. En fusión del momento histórico tecnológico en que se vive, los pensadores han ido madurando y evolucionando en su pensamiento. Para éste caso particular, tratando de pronosticar y anticipar el impacto social y cultural que provocan las NTIC.

Para el hombre, desde el comienzo de la escritura, su mayor fuente de conocimiento eran los textos impresos y con la aparición de internet esto ha cambiado radicalmente. En la búsqueda de encontrar parámetros que permitan analizar este complejo escenario, se realizará la descripción de las consecuencias a nivel cultural que generan las NTIC. Por otro lado, se describirá el comportamiento, las motivaciones, creencias y razones de los individuos que forman parte de la sociedad red.

Desde una óptica especifica, como la militar, es difícil encontrar autores que teoricen sobre cómo puede influir en la cultura militar, un cambio tan radical como el que estamos viviendo. Pero sí podremos transpolar los conocimientos alcanzados, hacia este particular ambiente.

1.1. La Cibercultura.

Internet, como todos sabemos es una red de computadoras que interactúan e intercambian información. En un principio los sitios web, conocidos como de primera generación o web 1.0, solo proveían información. Es decir los usuarios eran consumidores pasivos de información, la Internet era unidireccional. Posteriormente con la aparición la web 2.0, el usuario se convirtió en el centro de todo. Lee, escribe, edita, deja comentarios, colabora, e invita. Es un entorno colaborativo donde los mismos usuarios generan contenidos de acuerdo a sus gustos e intereses. Constituyéndose una red completamente interactiva y con mayor información[8]. Así surge entre otros sitios de intercambios Facebook, Wikipedia o Youtube.

[8] "Historia de Internet web 1.0, 2.0 y 3.0. Disponible en http://es.scribd.com/doc/19920424/Historia-Del- Internet-Web-10-20-30. Fecha de captura 12/04/12

Actualmente con el avance tecnológico de software, que permite procesar un gran caudal de información, abre el camino hacia la web 3.0. Se pasa del código HTML, basado en la clasificación de contenidos según las palabras y el orden alfabético, a un código que organiza la información atendiendo al significado de las palabras. Esto busca mejorar la organización y acceso de la información. La web 3.0, conocida también como la web semántica, va estructurando una inteligencia artificial colectiva[9]. Donde toda la información cursada es almacenada y usada inteligentemente por los sitios web. De forma tal que permite ofrecer a los usuarios, productos e información de acuerdo a sus gustos personales con el fin de facilitar las actividades diarias.

Este fenómeno, encabezado por las redes sociales suma millones de adeptos, convirtiéndose no solo en una de las principales fuentes dirigidas de entretenimiento e información global, sino dando origen a un nuevo orden cultural, la "Cibercultura"[10].

En éste campo, el pensador Pierre Lévy basa su teoría alrededor del concepto de inteligencia colectiva y el de sociedades basadas en el conocimiento. Él agrupa una serie de fenómenos culturales contemporáneos ligados principalmente, al impacto que han venido ejerciendo las tecnologías digitales de la información y la comunicación sobre aspectos tales como la realidad, el espacio, el tiempo, el hombre y sus relaciones sociales[11].

"En nuestras interacciones con las cosas, desarrollamos competencias. Por medio de nuestra relación con los signos y con la información adquirimos conocimientos. En relación con los otros, mediante iniciación y transmisión hacemos vivir el conocimiento. Competencia, conocimiento y saber, son tres modos complementarios de la transacción cognitiva...". (Inteligencia Colectiva, Pierre Lévy, 2004, p. 18).

En cuanto a la Inteligencia colectiva la interpreta como una forma de inteligencia universalmente distribuida.

[9] "Web 3.0" disponible en http://portal.educ.ar/debates/eid/informatica/publicaciones/que-es-la-web-30-estamos-prepa.php . Fecha 12/04/12.

[10] Cibercultura es la cultura que emerge, o está emergiendo, del uso del computador para la comunicación, el entretenimiento y el mercadeo electrónico. Cultura nacida de la aplicación de las nuevas tecnologías de la información y comunicación como internet. Cultura basada en las ventajas y desventajas de la libertad absoluta, el anonimato, y ciberciudadanos con derechos y obligaciones. http://es.wikipedia.org/wiki/Ciber-cultura. Página en castellano. Fecha de captura 13/08/12.

[11] "Cibercultura, la cultura de la sociedad digita". Pierre Lévy: prólogo de Manuel Medína. - Rubí (Barcelona) : Anthropos Editorial: México: Universidad Autónoma Metropolitana - Iztapalapa, 2007. Disponible en http://www.scribd.com/doc/19977800/Levy-Pierre-Cibercultura. Página en castellano. Fecha de captura 13/08/12.

"¿Qué es la inteligencia colectiva? Es una inteligencia repartida en todas partes, valorizada constantemente, coordinada en tiempo real, que conduce a una movilización efectiva de las competencias. Nadie lo sabe todo, todo el mundo sabe algo, todo el conocimiento está en la humanidad". (Inteligencia Colectiva, Pierre Lévy, 2004, p. 19).

Estos procesos descriptos, que permiten alcanzar el conocimiento, se ven amplificados por las interacciones que se desarrollan bajo las redes sociales apoyadas por las NTIC. Provocando avances culturales y tecnológicos más acelerados.

Según Manuel Castells, el surgimiento de la sociedad red, marca el fin de una era y el comienzo de otra: la Era de la Información[12]. Esta nueva era tiene sus cimientos en hechos históricos y sociales anteriores como el paso de la Oralidad a la Escritura, la aparición de la Imprenta y la Revolución Industrial. Esta revolución tecnológica se caracteriza por su capacidad de penetración en todos los ámbitos de la actividad humana y por el procesamiento del conocimiento, de la información y la comunicación. Algunos de los conceptos que sostiene expresan:

"...la tecnología de redes y la organización en red son sólo medios que reflejan las tendencias inscriptas en la estructura social. El actual proceso de globalización tiene su origen en factores económicos, políticos y culturales... pero... las fuerzas que impulsaron la globalización sólo pudieron desencadenarse porque tenían a su disposición la capacidad de conexión en red global que proporcionan las tecnologías digitales de comunicación y los sistemas de información..." (Comunicación y Poder, Manuel Castells. p. 51).

"Esta forma de comunicación ha surgido con el desarrollo de las llamadas Web 2.0 y Web 3.0, o el grupo de tecnologías, dispositivos y aplicaciones que sustentan la proliferación de espacios sociales en Internet..." (Comunicación y Poder, Manuel Castells. p. 101).

"... su contenido está autogenerado, su emisión auto dirigida y su recepción autoseleccionada por todos aquellos que se comunican" (Comunicación y Poder, Manuel Castells. p. 108).

[12]"El nuevo paradigma tecnológico". Disponible en http://portal.educ.ar/debates/eid/docenteshoy/otras-publicaciones/el-nuevo- paradigma-tecnologico.php. Página en castellano. Fecha de captura 11/04/12.

De los cuales se desprenden las tendencias de los efectos globales dentro de los espacios sociales en internet, donde son los usuarios, a través de sus intereses quienes generan los contenidos. Esta transformación de la comunicación, estructura el conocimiento.

Por otro lado, el pensamiento del crítico y escritor Howard Rheingold, uno de los más influyentes estudiosos de los efectos sociales y culturales de la explosión tecnológica, sostiene que nada nace por generación espontánea. La arqueología de los saberes es una práctica siempre necesaria cuando estudiamos las relaciones entre sociedad, tecnología y comunicación[13].

En la misma línea de pensamiento, el investigador Carlos Scolari, en su libro "Hipermediaciones", aborda el tema sobre el cambio de paradigma comunicacional. Condensa el análisis del nuevo ambiente comunicacional digital en tres partes: El saber comunicacional, El hacer comunicacional y las Hipermediaciones.

"La hipermediación, no es un producto o un medio, son los procesos de intercambio, producción y consumo simbólico que se desarrolla en un medio con una gran cantidad de sujetos, medios y lenguajes, interconectados tecnológicamente de manera reticular entre sí" (Hipermediaciones, Carlos Scolari, p.113-114*).*

De esta manera un modelo clásico de comunicación de los medios masivos (uno a muchos) es desplazado por las nuevas formas reticulares e interactivas de comunicación. Sujetos interconectados tecnológicamente de manera reticular entre sí. Por ello, sostiene que las tecnologías digitales, no sólo transforman el mundo, sino que también inciden poderosamente en la comprensión y percepción que tienen los sujetos de ese mundo[14].

En el último capítulo de su libro "Hipermediaciones" expresa:
"... no son actividades políticamente inertes o neutrales. Todos estos procesos tienen lugar bajo relaciones sociales marcadas por el conflicto y deberían encuadrarse en las confrontaciones hegemónicas que atraviesan la sociedad. Tampoco los discursos teóricos,

[13] http://comunicacionuces.wetpaint.com/page/Biografia+Completa+de+Howard. Página en castellano. Fecha de captura 13/04/12.
[14] Sierra Gutiérrez, Luis Ignacio, Reseña de "Hipermediaciones. Elementos para una Teoría de la Comunicación Digital Interactiva" de Carlos Scolari. REDALYC, Sistema de Informacion científica. http://redalyc.uaemex.mx/src/inicio/ArtPdfRed.jsp?iCve=86011409031. Página en castellano. Fecha de captura 13/04/12.

incluido el de este libro, son neutrales ni gozan de inmunidad de frente a los relatos míticos o a las ideologías". (Hipermediaciones, Carlos Scolari p.173).

Significando el importante papel que juega en las hipermediaciones (procesos de intercambio) la intencionalidad y la subjetividad. Aspecto de relevante importancia para entender los procesos que describiremos en los próximos capítulos.

1.2 Los Nativos Digitales.

El resultado de estos procesos da lugar a la sociedad del siglo XXI. Según Mark Prensky[15], está conformada por los nativos digitales e inmigrantes digitales, dos tipos de sujetos totalmente diferentes, surgidos por la llegada de la tecnología digital. El Nativo digital es aquel que nació cuando ya existía la tecnología digital, es decir aquel que nació después de 1979 y tuvo a su alcance en el hogar, tanto para estudio o para recreación computadoras o celulares. Por el contrario los individuos entre 35 y 55 años que son los inmigrantes digitales. A su vez las distancias entre ambas generaciones son infinitas, y las posibilidades de comunicación y de conducta se vuelven muy difíciles.

El filosofo y escritor Alejandro Gustavo Piscitelli, sostiene, entre otros conceptos, que esta brecha se disminuye con la existencia de mediadores, es decir, intérpretes capaces de poder vivir en estos dos mundos tecnológicos inter-generacionales[16]. También resalta la importancia de entender éste choque de culturas entre los nativos e inmigrantes digitales, que más que una brecha generacional es una brecha cognitiva, una brecha de competencia, de debilidades, de intereses y de motivaciones. Dentro de sus escritos, "Ciberculturas 2.0: en la era de las máquinas inteligentes" y "Nativos digitales. Dieta cognitiva, inteligencia colectiva y arquitecturas de la participación", define las nuevas significaciones de la cultura en red, semántica en red, vida en red, lectura en red, etc. que nos refiere a las implicancias de este nuevo escenario en el ámbito de lo Sociocultural.

La evolución del hombre a través de la interacción intercultural y el desarrollo de lógicas comunicativas y participativas sobre los distintos tópicos que se abordan dentro de la web,

[15] Marc Prensky, consultor y autor estadounidense. Es considerado un líder del pensamiento, conferencista, diseñador internacional de juegos en las áreas de la educación y del aprendizaje, y experto en medios digitales. Acuño el término "nativo digital" en contraposición al "inmigrante digital".

[16] Informe Presentación en feria del Libro 2007. Libro: "Nativos Digitales" Disponible en http://www.educoea.org/portal /La_ Educacion_Digital/laeducacion_141/destacados/Nativos Digitales.pdf. Página en castellano. Fecha de captura 13/04/12.

provocan un crecimiento exponencial del conocimiento. Todos los usuarios pueden ser parte de la información y el conocimiento individual cuenta. La lectura, el aprendizaje, el conocimiento social, la colaboración y las relaciones, están apoyadas en la tecnológica para almacenar más información y hacerla circular más rápidamente y con mayor capacidad de difusión. Éstas dan lugar al concepto conocido como la sociedad red.

Dentro de ella se está adoptando la construcción del conocimiento en base a la "Ética hacker",[17] que consiste en comprender al mundo a través de los sistemas tecnológicos. Cada integrante aporta una parte del conocimiento que posterior mente es integrada e incrementada por un tercero, "n*ingún problema debería resolverse dos veces*"[18]. Significando que toda resolución de un problema debería ser comunicado, para que otros partiendo desde esta base puedan resolver los nuevos problemas, disminuyendo los tiempos de desarrollo.

1.3. Conclusiones Parciales.

- Como hemos visto, con el advenimiento de las redes sociales en internet, favorecidas por los avances tecnológicos digitales, se ha generado un nuevo modo de interrelación entre individuos; donde la anarquía comunicacional, anonimato y masividad de uso, son una constante. Esto ha provocado cambios de gran importancia a nivel social, cultural y del conocimiento, y dan origen a la sociedad red.

- Por otro lado se ve que las redes sociales en internet inciden en la comprensión y percepción que tienen los sujetos del mundo. A su vez, dentro de este escenario no existen actividades políticamente inertes o neutrales, todas están matizadas por intereses, valores e ideologías. Por lo tanto el desarrollo de una conciencia colectiva, puede surgir naturalmente o pude ser inducida.

- A raíz de la evolución de la web, cada vez más aparatos están conectados a ella, celulares, equipos de seguridad, aparatos electrodomésticos, vehículos etc., todos

[17] Def. Ética hacker: Es una nueva ética surgida y aplicada por las comunidades virtuales o cibercomunidades. Se basa en una determinada serie de valores rectores como la libertad de información, la conciencia social, la accesibilidad, la curiosidad, la verdad, la creatividad, la pasión. Su principal mentor es el filósofo finlandés Pekka Himanen.

[18] Disponible en www.elhacker.net. Página en castellano. Fecha de captura 09/08/12.

elementos de uso cotidiano. Hoy, con la incorporación de las NTIC, la web esta cada vez más presente e invisible en nuestra vida cotidiana.

- La era de la Información, la inteligencia colectiva, la sociedad red, las tecnologías digitales, la arqueología de los saberes, los nativos digitales, el procesamiento del conocimiento, de la información y la comunicación son términos propios del ámbito actual, de gran conflictividad ante el cual nos enfrentamos a diario. Su comprensión nos permite ver el potencial peligro que genera en una institución militar si no se toman medidas para afrontarlo, pero también el potencial de oportunidades para cumplir con su misión.

CAPÍTULO II

EL ESCENARIO ACTUAL

Lo expresado en el capitulo anterior, busca describir el efecto que provocan las NTIC como tecnologías disruptivas en el comportamiento social y cultural del hombre. Pero pensar la web como un sistema de redes, solo con el fin de proporcionar servicios o como medio de interrelación entre individuos es caer en un error de concepto. Aquello que percibimos a través de los sentidos y en la seguridad de nuestros domicilios es solo la mitad de la realidad; la otra mitad, la batalla informática, imperceptible al ciudadano común, se desarrolla diariamente y cada vez con más frecuencia, creatividad y eficacia.

Internet desde su concepción ha sido utilizado como una herramienta para fines militares. ARPANET[19] (Red de la Agencia para los Proyectos de Investigación Avanzada de los Estados Unidos), su predecesora, fue concebida durante la guerra fría como una red de informaciones de uso militar[20]. Cuyo fin era permitir el acceso a la información militar desde cualquier punto del país en caso de ataque. Posteriormente, con el transcurrir del tiempo se fue optimizando, se incorporaron universidades y distintas organizaciones gubernamentales, y con la aparición de la PC familiar fue evolucionando hasta convertirse en lo que hoy conocemos como la Word Wide Web (WWW).

La intención del presente capítulo, es exponer los métodos de interacción social utilizados, a través de medios de comunicación digital y redes sociales, mostrando su potencialidad. Detrás de las noticias hay intenciones, que buscan satisfacer necesidades. Por ello no es difícil imaginar la utilización de este medio para obtener información sensible que permita posicionar favorablemente a un actor sobre otro.

Si bien este escenario es poco susceptible de ser comprobado científicamente, intentaremos analizar hechos, a través de noticias y ejemplos históricos, y determinar hacia donde dirigen los esfuerzos los distintos actores.

[19] ARPANET, en ingles Advanced Research Projects Agency Network.
[20] "Historia de Internet" Disponible en http://www.estudiosimbiosis.com.ar/internet, publicado el 14/02/2006. Fecha de captura 12/06/12.

Las noticias que se exponen a continuación, a modo de ejemplo, buscan mostrar una realidad oculta detrás del ciberespacio. La web muestra una pequeña realidad virtual, lo que subyace son las implicancias en lo verdaderamente real. A semejanza del tempano de hielo, lo que se ve es solo una parte pequeña de lo que se esconde.

2.1. La realidad mediática.

El diario Infobae, en la sección tecnología de fecha 03 de Octubre del corriente, publicó la noticia en la cual Wikileaks, el lunes 29 de noviembre de 2010, habría revelado más de 250.000
cables diplomáticos secretos, facilitados a varios medios de prensa europeos. Los mismos habían sido intercambiados entre las embajadas de Estados Unidos de todo el mundo con las oficinas del Departamento de Estado. La divulgación de los contenidos tuvo efecto en cascada con serias implicancias internacionales, de nivel estratégico nacional y operacional.[21]

Wikileaks o wiki-filtraciones en español, es un sitio web que publica información crítica filtrada de corporaciones, gobiernos, organizaciones, instituciones, individuos famosos etc.
A partir de ése momento el blog adquirió reconocimiento internacional siendo visitado por millones de personas. Esta organización no gubernamental, fomenta la contribución de información de terceros garantizando el anonimato de la fuente, mediante la utilización de software de encriptación de datos. Supuestamente, de acuerdo a su sitio oficial no cobra por la información que brinda, solo acepta donaciones que permiten su subsistencia[22]. Hoy su líder Julian Asange, se encuentra en el ojo de la tormenta mediática a raíz de su solicitud de asilo político a la embajada de Ecuador en Londres, debido al pedido de extradición de Suecia para ser juzgado en ese país por delitos comunes.[23]

La noticia refleja el grado de eficiencia de un actor, en este caso una organización no gubernamental, para obtener y difundir una serie de documentación secreta que comprometió internacionalmente a la principal potencia mundial.

[21] Disponible en http://www.infobae.com/notas/666898-WikiLeaks-y-la-libertad-de-expresion-en-internet.html.Fecha de captura 10/09/12.
[22] Sitio oficial wikileak . Disponible en http://wikileaks.org/. Fecha de captura 10/08/12.
[23] "Ecuador concede asilo político a Julia Asange" Disponible en http://www.abc.es/20120816/internacional/abci-assange-ecuador-201208161415.html. Fecah de captura 18/08/12.

El lunes 10 de septiembre del corriente, en el blog español Uniradionoticias.com, publicó la siguiente noticia:

"Talibanes se hacen pasar por mujeres atractivas en Facebook. Los talibanes han utilizado fotos de mujeres atractivas como foto principal en sus perfiles, y han agregado a soldados como amigos en su cuenta. Con esta operación soldados talibanes están consiguiendo datos y recopilando información sobre posibles operaciones militares".[24]

El documento también concientiza a familiares y amigos de los soldados, de lo peligroso que puede ser compartir información en internet que incluya nombres de personas, lugares y actividades realizadas.

Otra noticia en la que se evidencia el uso de las redes sociales como medio para conocer al oponente, es la del máximo líder de la guerrilla colombiana que sigue a través de Twitter al presidente de Colombia, Juan Manuel Santos.

… Lo más curiosos es que entre los escasos 5 usuarios que el máximo jefe guerrillero eligió para seguir figura el del propio presidente de Colombia. Y no sólo llamó la atención la necesidad de "Timochenko" de mantener vigilado al mandatario, sino que fue su primera opción: Santos es el primer usuario que "Timochenko" buscó no bien se registró en Twitter. [25]

La noticia publicada el 27 de Septiembre del 2010, en el Blog de Radio Francia Internacional, muestra como la capacidad e ingenio puede ser aumentada por el potencial que brinda este medio. A través de la infección de un virus informático se logro afectar la central nuclear de Bushehr.

"Una guerra electrónica ha sido lanzada contra Irán. El gobierno iraní denuncia que un ataque informático contra sus infraestructuras industriales infectó 30.000 computadoras.".[26]

El día lunes 2 de abril del corriente, el diario Clarín, muestra gráficamente cual es la situación

[24] "Talibanes en Facebook" Disponible en http://www.uniradionoticias.com/noticias/insolito/articulo143745.html. Fecha de captura 10/09/12.

[25] "El Jefe de las FARC sigue a Santos en Twitter" Disponible en http://america.infobae.com/notas/57807-El-jefe-de-las-FARC-sigue-a-Santos-en-Twitter. Fecha de captura 11/08/12.

[26] Disponible en http://www.espanol.rfi.fr/oriente-medio/20100927-una-guerra-electronica-ha-sido-lanzada-contra-iran. Fecha de captura 13/08/12

del ambiente informático, donde casi la mitad de las computadoras familiares en Argentina, fueron víctimas de ataque informáticos.

"La encuesta realizada por la empresa de seguridad informática Eset, muestra que, el 44,9% de los usuarios hogareños argentinos tuvo una intromisión en su computadora. En un año los ataques de malware (software maligno) a computadoras domésticas crecieron un 17%. Los hackers apuntan al robo de identidad y usan las redes sociales para obtener datos". [27]

Asimismo distintos especialistas en seguridad informática entrevistados por Leo González Pérez, periodista del diario Clarín, en la nota sostienen:

- Jorge Mieres, experto de Kaspersky Lab (empresa proveedora de antivirus). "*En gran medida las maniobras tendientes al robo de información sensible centran sus esfuerzos en los usuarios hogareños debido a que habitualmente ellos desconocen ciertas estrategias empleadas por los atacantes*".

- También Carlos Aramburu, de McAfee (empresa proveedora de antivirus), coincide: "*Los antivirus falsos, los programas de ejecución automática y los troyanos (malware que se presenta como programa aparentemente legítimo e inofensivo) son los modos de ataques que más han crecido en el último trimestre. Y todos estos programas van en la misma dirección: robo de datos e identidad*".

- Cristian Borghello, consultor independiente y director del portal Segu-Info, dice que "*hay dos rubros en los que se nota un incremento particularmente fuerte de ataques. Por un lado, el phishing*[28]*, la obtención de datos confidenciales mediante e-mails, SMS engañosos o sitios falsificados. Y por otro, el robo de identidad, que consiste en usar el nombre de otro para fines varios: desde abrir una cuenta en una red social para difamar hasta hacer compras en su nombre*".

[27] Disponible en http://www.clarin.com/hardware/ano-mitad-PC-sufrieron ataque_0_674932618 .html. Fecha de captura 10/08/12.

[28] Phishing: obtención de datos confidenciales mediante e-mails, SMS engañosos o sitios falsificados para luego robar o Estafar.

2.2. Intervención de las Redes Sociales en los Conflictos Armados.

Durante los conflictos de los últimos veinte años, Kosovo en 1999, Afganistán 2001, Iraq 2003, Estonia 2007, Georgia 2008, Irán 2010, países árabes al norte de África en 2011 y Medio Oriente en general en 2012, las operaciones informáticas tuvieron un papel protagónico y trascendental.

Por ejemplo, durante el conflicto entre Israel y Palestina, la utilización de las redes sociales ha sido una muestra de creatividad e ingenio, cuyo fin es informar y a la vez buscar la aprobación mediática internacional.

Los israelíes, utilizan oficialmente distintos medios informáticos para informar o desinformar sobre sus acciones. Aparte del blog oficial de las Fuerzas Armadas de Israel, cuenta con un canal en YouTube en el que se muestra un parte diario de guerra, con imágenes del combate. A su vez en Twitter contestan preguntas, mostrando la situación actual en la región[29].

Para el caso palestino la cadena mediática Al Jazera creó un blog, denominado "War on Gaza" donde la información es aportada por ciudadanos. Aquí cualquier persona puede enviar información. Otros sitios como Demotix, Gaza Siege y AllVoices, replican los procedimientos buscando informar y desinformar, al igual que los sitios webs rivales.[30]

La información encaminada e interpretada por los diferentes medios de comunicación social, se ha convertido en un factor de vital importancia para erosionar la moral de combate del enemigo, crear un relato que legitime el accionar, e influir en la población para soportar un esfuerzo bélico.

[29]"Conflicto palestino israelí". Disponible en http://www.rosario3.com/tecnologia/noticias.aspx?idNot=43272 Fecha de captura 11/08/12

[30]"War of Gaza". Disponible en http://elpais.com/diario/2010/06/08/opinion/1275948011_850215.html, Fecha de captura 10/08/12

2.3. Argumento práctico.

A modo de ejemplo, el siguiente caso de información obtenida de facebook, busca mostrar el potencial y grado de exposición que generan las redes sociales en internet[31].

El día 09 de agosto del corriente, en Facebook se ingreso en la sección de "personas que quizás conozcas" y se eligió un usuario de la armada de Brasil. Dentro de su cuenta se obtuvo información sobre 145 oficiales de la Marina de Brasil, 15 de la Marina de Chile y 25 de la Marina Argentina. Los atributos explícitos que se pudieron obtener en la mayoría de los casos fueron:

- Nombre y apellido.
- Jerarquía.
- Fecha de ingreso, promoción a la que pertenece.
- Destinos en los que estuvo.
- Estudios realizados.
- Fotos personales y profesionales.
- Vínculos y amistades.
- Gustos y preferencias (equipo de futbol con el que simpatiza, libros, películas, temas de actualidad que sigue etc.).
- Como está constituida su familia, edades y lugar de residencia.

Otro detalle a tener en cuenta, que no se uso, es la herramientas geo-etiquetado, que agrega información geográfica instantánea del lugar donde se encuentra el usuario. Cabe aclarar que para la obtención de los datos mencionados no se ha utilizado ninguna herramienta de intromisión, ni de hackeo.

Dentro del estudio del componente militar, como ya sabemos, la inteligencia busca conocer las personalidades y cultura de los individuos integrantes de otras fuerzas armadas. A ellos se lo conoce como inteligencia biográfica o semblanza de oficiales extranjeros. En otros tiempos obtener ésta información para un servicio de inteligencia hubiera llevado años de

[31] N de Autor: Ésta información es pública, y cualquiera puede verificarla entrando en Facebook. Por razones de claridad y no desviar la atención del objetivo del presente capitulo, no se expondrán los resultados.

investigación, de intervención de oficiales y de archivos. Hoy a través de estas redes sociales se puede obtener un mayor grado de información, sobre el cual elaborar inteligencia.

Como los hechos se comprueban mientras que las opiniones se discuten, con las noticias seleccionadas, sumadas al ejemplo práctico realizado en Facebook, se buscó reflejar el alto grado de vulnerabilidad de los sistemas en general y el de los individuos en particular. A su vez mostrar que las redes sociales son la principal fuente de convergencia de las operaciones mediáticas.

La realidad nos muestra que quienes quedan mejor posicionados ante la opinión pública nacional e internacional, son aquellos que ganan la batalla mediática. Usan a la web como una herramienta donde la creatividad y la aplicación del conocimiento tecnológico acompañan y materializan el logro de objetivos autoimpuestos.

2.4. Conclusiones parciales

- El grado de exposición de los individuos en las redes sociales le permiten saber a un oponente preparado qué consumimos, deseamos, opinamos, leemos, escribimos, votamos, pensamos y con quiénes nos relacionamos.

- Por otro lado los medios de comunicación han dejado de ser percibidos por los actores como el principal acceso a la opinión pública.

- Hoy, a raíz de la incorporación de las NTIC, la web esta cada vez más presente e invisible en nuestra vida cotidiana. La realidad nos muestra que todas las noticias, conflictos entre países, organizaciones etc., se desarrollan en la web y tienen consecuencias en la vida real.

- El papel de las nuevas tecnologías es crucial en el desenvolvimiento de los futuros conflictos armados.

CAPÍTULO III

ANÁLISIS DE LA SITUACIÓN

3.1. Doctrina Militar.

Las operaciones informáticas que se han evidenciado durante los últimos conflictos nacionales e internacionales se pueden agrupar, al igual que en la doctrina militar, en operaciones de seguridad, psicológicas, engaño militar, guerra electrónica, ataque físico y ataque por red informática. [32] Entre ellas podemos mencionar:

- Las acciones de sobreinformación, entendiendo como tal, la saturación de información verídica o falsa con el fin de confundir al oponente.
- La obtención de información, a través de la interceptación de mensajes o acceso a bancos de datos digitales.
- La propagación de virus informáticos buscando afectar la información del oponente.
- Interrumpir, modificar o recortar la información.
- Afectar las estructuras informáticas para la conducción y control de los sistemas.
- La realización de operaciones de velo y engaño, utilizando la web como complemento para la llegada al oponente.
- Infiltración de personal calificado en las redes sociales.
- Denegación dirigida de servicios (DDOS).
- Diseminar propaganda.

Estas operaciones se desarrollan dentro del escenario virtual, se incluyen dentro de la definición de guerra informática, entendiéndola como *"las acciones que se realizan para alterar la información y los sistemas de información del adversario, mientras se protege la información y los sistemas de información propios"*[33]

[32] Junta de Jefes de Estado Mayor, Joint Doctrine for Information Operations , Joint Publication 313, Octubre de 1998, en I-9

[33] Junta de Jefes de Estado Mayor, Department of Defence Dictionary of Military and Associated Terms, Joint Publication 102, abril de 2001, p. 20 3

3.2. Identificación del problema en el teatro de operaciones.

El problema para las FF.AA., no es intrínseco de internet pero sí a través de la web es que se generan los problemas que vamos a identificar. Hoy, el poder de la imagen en tiempo real, contribuye a la legitimación de una operación o credibilidad de una institución. Pero a raíz de la aparición de las NTIC, no resulta sencillo controlar la información que se quiere mostrar. La generación de material audiovisual por parte de cualquier individuo le permite transmitirlo, a través de las redes sociales, a una audiencia ilimitada, sin restricciones, sin costo económico alguno y fundamentalmente on-line. Con las implicancias para el desarrollo de una operación que esto puede significar.

Claramente se aprecia, que el uso que se hace de este medio, es el causante de los problemas. Por ello abordaremos la temática desde dos ópticas distintas, la del individuo y la del elemento técnico que se utiliza para acceder a la web. Su distinción permitirá adoptar, a posteriori, medidas para neutralizarlos y/o explotarlos. Sobre esta base se puede empezar a identificar cuáles son las fuentes de estos problemas.

En el primer grupo, el problema radica, en la fuga de datos derivada de la cesión involuntaria de información por parte del usuario. Generalmente producto de dos factores:

- Por ignorancia o descuido del personal militar en el manejo de la información.
- Por el grado de exposición que tiene el personal militar al usar la web.

El otro aspecto, el tecnológico, facilitado por la interacción del uso de las NTIC, especialmente las redes sociales, que pueden afectar a las instituciones militares en tiempos de paz y guerra en todos los niveles operacionales. (Estratégico, Operacional y Táctico).
Son los siguientes:

- Por la vulnerabilidad de las redes militares específicas.
- Por desconocimiento de las capacidades de los equipo y de las tecnologías usadas para el ingreso a la web e intercambio de información.

Finalmente, podríamos mencionar como otra fuente originadora de problemas en todo tiempo, al plexo normativo vigente (ver Anexo 1), que es escaso y carece de la eficiencia necesaria para resguardar datos; y la eficacia para juzgar a los individuos/organizaciones, que cometan intrusiones en redes informáticas especificas y/o personales.

Con el fin de dar una visión integral de las implicancias en este escenario, y profundizar el tema se procederá a definir cuáles son las fortalezas, debilidades, vulnerabilidades y oportunidades, de las fuerzas militares.

Fortalezas.

- Las FFAA son un sistema organizacional jerárquico, estructurado y subordinado, capaz de detectar y adoptar contramedidas hacia las amenazas.
- Capacidad de accionar simultáneamente tanto defensiva como ofensivamente, bajo una directiva, ya sea dentro o fuera de un teatro.
- Capacidad de planeamiento.
- Dirección y control centralizado y ejecución descentralizada.
- Disciplina en el cumplimiento de la orden. Unidad de dirección.

Oportunidad.

- Velocidad de cambio y adelanto tecnológico.
- Constante evolución del escenario informático.
- La creatividad como campo para el desarrollo de actividades.
- Relación costo beneficio, permite el acceso y su utilización a actores de escasos recursos.

Amenazas.

- Uso de tecnología informática desarrollada por otros países.
- Subestimación de los riesgos potenciales en este ámbito.
- Filtración de información por desconocimiento de los miembros de las FFAA.
- Exposición de las operaciones militares a raíz del uso de tecnología digital.
- Ámbito para el desarrollo de acciones de inteligencia del oponente.

Debilidades

- Dificultad en reconocer el problema.
- Grado de exposición de la información y de los integrantes de las FFAA.

- Dificultad en codificar leyes claras y precisas.
- Imposibilidad en la identificación del enemigo.
- Dificultad en verificar la veracidad de la información.
- Omnipresencia de internet en la vida diaria de los individuos.
- Dependencia informática de los sistemas tecnológicos que usan las fuerzas armadas.
- No existen medidas preventivas que puedan dar una seguridad absoluta, pero síi se puede atenuar.
- Toda información que este en un sistema, puede ser capturada.
- Lentitud en la formulación del diseño que permitan hacer frente a este escenario y al igual que su implementación,

3.3. Análisis de Fortalezas, Oportunidades, Debilidades y Amenazas (FODA).

Usando las fortalezas para tomar ventaja de las oportunidades.

- Desarrollar y ejecutar tareas de desinformación y/o saturación de información.
- Desarrollar cripto-sistemas, con algoritmos propios.

Superando las debilidades tomando ventaja de las oportunidades

- Generar leyes que sancionen el uso de la información privada.
- Utilización de programas de software abiertos.

Usando las fortalezas para evadir las amenazas

- Utilización de procedimientos para rechazar amenazas y desarrollo de doctrina propia.
- Concientizar al personal sobre el nivel de riesgo de la documentación que maneje y adiestrar al mismo a tomar las medidas para evitar riesgos
- Constituir un órgano contralor de seguridad informática de las FFAA.

Minimizar las debilidades y evitar amenazas

- Desarrollo de equipos que permitan interferir sistemas tecnológicos dentro del TO y prever sistemas alternativos de comunicaciones seguras.
- Desarrollo de doctrina a nivel operacional y estratégico.

La interrelación de los factores considerados, en el análisis FODA, nos permite definir un grupo de medidas que permitirán neutralizar las acciones de un posible oponente. Las mismas, se exponen a continuación.

- Adoptar e inculcar una actitud precavida al personal militar, es el mejor punto de partida para mantenerse a salvo de ataques informáticos.
- El personal militar debe concientizar a familiares y amigos, de lo peligroso que puede ser compartir información en internet que incluya nombres de personas, lugares, actividades, etc.
- Desarrollo propio de software basado en lenguajes informáticos abiertos[34].
- Adopción y desarrollo de herramienta de obtención de información, que maximicen el anonimato y el escenario anárquico propio de la Web.
- Creación de un observatorio o red que reúna, comparta y estudie las experiencias de los integrantes de la fuerza.
- Modelar alternativas que nos brinden seguridad y que permitan pasar a la ofensiva.
- Adiestrar e instruir personal capacitado para identificar las acciones informáticas del oponente.
- Determinar estrategias de cooperación inter-fuerzas.
- Confeccionar servicios de seguridad informática propios, seguros y confiables.
- La dependencia tecnológica de los sistemas informáticos es una de las mayores vulnerabilidades, adoptar medidas que permitan conocer todas las tareas en segundo plano que realizan los distintos software.
- Elaboración de sistemas criptográficos con algoritmo de diseño propio.
- Desarrollar y proporcionar y elementos básicos de protección de nuestros medios tecnológicos.
- Utilización de centros de bases de datos seguros.
- Poner el concepto de Ciberguerra dentro de la doctrina conjunta, y a la Ciberdefensa activa, entre nuestras prioridades.

[34] Sistemas abierto, se refiere a los sistemas informáticos configurados para permitir el acceso sin restricciones por parte de personas y de otros sistemas.

3.3. CONCLUSINES PARCIALES.

- Las FFAA son un sistema organizacional jerárquico y estructurado, con capacidad de planeamiento, y que ejerce la dirección centralizada y la ejecución descentralizada. Por ello reúne las condiciones óptimas para incorporar y cumplir medidas tendientes a mitigar o neutralizar amenazas de índole informática.

- La constante evolución del escenario informático, ocasionado por la velocidad del cambio y los adelantos tecnológicos, brindan a este escenario un alto grado de imprevisibilidad.

- Lo único que se sabe con certeza es que las recetas del mundo real para lograr el control, no son aplicables al mundo virtual. Por ello la creatividad, el conocimiento y los recursos son los pilares para hacerle frente.

CONCLUSIÓN FINAL

De las conclusiones parciales arribadas en los capítulos precedentes surgen las siguientes reflexiones:

Como hemos visto, con el advenimiento de las redes sociales en internet, favorecidas por los avances tecnológicos digitales, se ha generado un nuevo modo de interrelación entre individuos, donde la anarquía comunicacional, anonimato y masividad de uso, son una constante dentro de este nuevo paradigma. Esto ha provocado cambios de gran importancia a nivel social, cultural y del conocimiento, dando origen a la sociedad red.

Otro aspecto analizado indica que las redes sociales en internet poseen la capacidad de incidir en la comprensión y percepción que tienen los sujetos del mundo, dando lugar al surgimiento de una conciencia colectiva. Asimismo, su amplio uso a través de las NTIC permite la interacción entre individuos, entre estados y organizaciones de todo tipo. Dado que ellas son herramientas, que poseen un gran potencial para accionar masivamente, se pueden utilizar para orientar o inducir a pensar o actuar de diferentes maneras.

Esto ha roto el monopolio relativo que ejercían los medios de comunicación como fuente de información sobre los conflictos políticos, religiosos, económicos y armados. La manipulación de este escenario, brinda la capacidad de mediatizar los conflictos, formar opinión y en muchos casos, concretar las opiniones en acciones. Un ejemplo de esta capacidad es el desarrollo del conflicto conocido como La Primavera Árabe[35]. A su vez, proporciona a oponentes y a quienes operan desde grupos clandestinos un fácil acceso a la información individual y global.

Dada la tecnología actual, resulta imposible prescindir de la red, es una realidad con la que debemos enfrentarnos a diario. En ella, interactúan miles de millones de personas y pese a los grandes esfuerzos por querer controlarlo, todavía no se ha podido. Muchas potencias mundiales han entendido que solo aquellos que lo aborden seriamente, invirtiendo tiempo y recursos materiales y tecnológicos tendrán una oportunidad en el futuro.

[35] La Primavera Árabe, término utilizado por la prensa internacional para referirse a una serie de alzamientos populares en los países árabes, principalmente del norte de África.

Los militares por manejar información, que puede ser sensible para un estado, son un objetivo muy rentable para aquellos grupos que buscan información y tienen la capacidad de influir. De aquí el planteo que se hiciera con la formulación de la hipótesis.

De lo planteado y analizado, se puede afirmar que las FFAA Argentinas, deben prepararse para hacer frente a las vulnerabilidades que provoca el uso de la tecnología digital. Dentro de ellas las redes sociales serán la fuente de mayor fuga de información.

La investigación fue desarrollada desde una óptica más bien del tipo defensivo, buscando neutralizar al oponente. Sería conveniente para futuras líneas de investigación indagar sobre la adopción de acciones que permitan utilizar ofensivamente la internet. Así mismo otra línea de investigación pasaría por las implicancias para las FFAA de la llegada de los "Nativos Digitales", tema que se toco muy superficialmente, pero que amerita una mayor profundización.

El ciberespacio, cuya columna vertebral es internet, es un escenario con el cual las instituciones militares deben aprender a convivir. Como toda nueva tecnología disruptiva dentro de un escenario, genera nuevas vulnerabilidades y amenazas, pero también puede presentar oportunidades y fortalezas, si se lo entiende y acciona en consecuencia. Como escenario anárquico, aquel que logre un área de control ejerce poder sobre ella, contrario sensu, aquel que no la controle quedara a merced de quien lo haga. Esto obliga a las FFAA a comprender y tomar un rol protagónico dentro de este escenario.

Dentro de su imprevisibilidad, lo único que se sabe con certeza es que las recetas del mundo real para lograr el control, no son aplicables al mundo virtual. Por ello la creatividad, el conocimiento y los recursos son los pilares para hacerle frente.

Como sostiene Manuel Castell, "*el poder reside en el cerebro de los individuos. De acuerdo a lo que pensamos hacemos, siempre favoreciendo nuestros intereses y valores. Por lo tanto quien gana la batalla de las mentes gana la batalla del poder"*.[36]

[36] Presentación del libro "Comunicación y Poder" Manuel Castells. Foro Complutense 17/11/2009.

BIBLIOGRAFÍA

A. LIBROS.

- Castells Manuel, 2009, "Comunicación y Poder". Editorial Alianza.

- Pierre Lévy. 2007. "Cibercultura: informe al consejo de Europa". Anthropos.

- Piscitelli Alejandro Gustavo. 2009. "Nativos digitales. Dieta cognitiva, inteligencia colectiva y arquitecturas de la participación". Buenos Aires: Santillana.

- Rheingold Howard. 2004. "Multitudes inteligentes: la próxima revolución social" Barcelona, Gedisa.

- Scolari, Carlos. 2008. "Hipermediaciones, Elementos para una Teoría de la Comunicación Digital Interactiva". Barcelona, Gedisa.

- Scolari, Carlos. 2005, **"**Hacer Clic: Hacia Una Socio-semiotica de las Interacciones Digitales" Barcelona, Editorial Gedisa, S.A.

B. REVISTAS, BOLETINES, FASCÍCULOS

- Department of Defense Dictionary of Military and Associated Terms, Joint, Publication 102, Abril de 2001, p. 20 3.

- Joint Doctrine for Information Operations, Joint Publication 313.Octubre de 1998, en I-9.

- Military Review, Hispanoamericana septiembre/octubre 2003.

C. DE INTERNET

1. Ardrey, Robert. "La evolución del hombre: la hipótesis del cazador". Disponible en http://en.scientificcommons.org/34184701. Página en castellano. Fecha de captura 09/05/12.

2. Bretau Roger. "El poder de las Redes Sociales", disponible en http://www.suite101.net /content/redes-sociales-y-las-relaciones-a15670. Pagina en castellano, Fecha de captura 27/04/2012.

3. Comunicación y poder, una reseña, por Carlos A. Scolari. Disponible en http://www.scribd.com /doc/59580159/Comunicación-y-Poder-Una-reseña. Pagina en castellano, Fecha de captura: 20/05/2012.

4. Cibercultura. http://es.wikipedia.org/wiki/Ciber-cultura. Página en castellano. Fecha de captura 13/08/12.

5. "Cibercultura, la cultura de la sociedad digita". Pierre Lévy: prólogo de Manuel Medína. - Rubí (Barcelona) : Anthropos Editorial: México: Universidad Autónoma Metropolitana - Iztapalapa, 2007. Disponible en http://www.scribd.com /doc/19977800/Levy-Pierre-Cibercultura. Página en castellano. Fecha de captura 13/08/12.

6. "Conflicto Palestino Israeli". Disponible en http://www.rosario3.com/tecnologia /noticias.aspx?idNot=43272 Fecha de captura 11/08/12

7. Diario Infobae. "Internet es la mayor máquina de espionaje que jamás se haya visto". Disponible en http://www.infobae.com. Fecha de publicación miércoles 16 de marzo del 2011. Pagina en castellano, Fecha de captura: 06/04/2012.

8. "El poder de la Comunicación". Disponible en, http://www.comunicacionclave.mx /CGI-BIN/index.php?option.com_content&view=article&id=9:revolución-jasmin-como-destruir-un-imperio-en-treinta-dias&catid=6:noviembre 10&Itemid=3. Página en castellano. Fecha de captura 13/08/12.

9. "El nuevo paradigma tecnológico". Disponible en http://portal.educ.ar/debates /eid/docenteshoy/otras-publicaciones/el-nuevo-paradigma-tecnologico.php.Página en castellano. Fecha de captura 11/04/12.

10. Ética hacker: Disponible en www.elhacker.net. Página en castellano. Fecha de captura 09/08/12.

11. "Ecuador concede asilo político a Julia Asange" Disponible en http://www.abc.es/ 20120816/ internacional/abci-assange-ecuador-201208161415.html. Fecha de captura 18/08/12.

12. "Guerra electrónica contra IRAN". Disponible en http://www.espanol.rfi.fr/oriente-medio/20100927-una-guerra-electronica-ha-sido-lanzada-contra-iran. Fecha de captura 13/08/12

13. "Historia de Internet" Disponible en http://www.estudiosimbiosis.com.ar/internet, publicado el 14/02/2006. Fecha de captura 12/06/12.

14. "Historia de Internet web 1.0, 2.0 y 3.0". Disponible en http://es.scribd.com/doc /19920424/Historia-Del- Internet-Web-10-20-30. Fecha de captura 12/04/12.

15. Informe Presentación en feria del Libro 2007. Libro: "Nativos Digitales" Disponible en http://www.educoea.org/portal/La_Educacion_Digital/laeducacion_141/destacados /Nativos Digitales.pdf. Página en castellano. Fecha de captura 13/04/12.

16. "Jefe de la FARC sigue a Santos en Twitterr" Disponible en http://america .infobae.com/notas/57807-El-jefe-de-las-FARC-sigue-a-Santos-en-Twitter. Fecha de captura 11/08/12.

17. "La mitad de las PC en Argentina Sufrieron ataques informáticos" Disponible en http://www.clarin.com/hardware/ano-mitad-PC-sufrieron ataque_0_674932618.html. Fecha de captura 10/08/12

18. "La Sociedad de la Información en el Siglo XXI: Un requisito para el desarrollo". Disponible en http://www.slideshare.net/isidreb/sociedad-de-la-informacin-en-el-siglo-xxi-reflexiones-y-conocimiento-compartido. Página en castellano. Fecha de captura 14/08/12.

19. Periodismo ciudadano. "Evolución positiva de la comunicación". Disponible en, http://www.scribd.com/doc/74211965/ Página en castellano. Fecha de captura 12/07/12.

20. Plexo normativo Jurídico Argentino. Disponible en http://infoleg.mecon.gov.ar /infolegInternet/anexos/105000-109999/107145/norma.htm Fecha de captura 10/08/12

21. Plexo normativo Jurídico Argentino. Disponible en http://www.informaticalegal. com.ar/legislación-informática/ Fecha de captura 10/08/12

22. Plexo normativo Jurídico Argentino. Disponible en http://www.ciberderecho.com.ar /legislacion.htm Fecha de captura 10/08/12

23. Sanchez Carlos. "Redes sociales, cohesión social". Disponible en http://www.slideshare.net/carlosl.sanchez/bienestar-redes-sociales-cohesion-social. Artículo publicado en internet en el mes de febrero del 2011. Pagina en castellano, Fecha de captura: 20/06/2012.

24. Scolari Carlos A. **"**¿Cerca de la revolución? Las redes sociales salen a la calle". Disponible en http://hipermediaciones.com/2011/01/30/%C2%BFcerca-de-la-revolucion-las-redes-sociales-salen-a-la-calle. Pagina en castellano. Fecha de captura: 26/06/2012.

25. Sierra Gutiérrez, Luis Ignacio, Reseña de "Hipermediaciones. Elementos para una Teoría de la Comunicación Digital Interactiva" de Carlos Scolari. REDALYC, Sistema de Informacion científica. http://redalyc.uaemex.mx/src/inicio/ArtPdf Red.jsp?iCve=8601 1409031. Página en castellano. Fecha de captura 13/04/12.

26. Sitio oficial Wikileak. Disponible en http://wikileaks.org/. Fecha de captura 10/08/12.

27. Rheingold Howard, "Electric Minds archive now available". Disponible en http://www.rheingold.com. Artículo publicado en internet el 17 de marzo 2008. Pagina en castellano, Fecha de captura: 20/06/2012.

28. Taboada Laura Ríos. "Redes Sociales disponible en http://www.suite101.net /content/redes-sociales-oportunidad-o-amenaza-a15770#ixzz1KE71r76S. Pagina en castellano. Fecha de captura: 16/03/2012.

29. "Talibanes en Facebook" Disponible en http://www.uniradionoticias.com /noticias/insolito/articulo143745.html. Fecha de captura 10/09/12.

30. Tecnología Disruptiva En línea http://definicion.de/disruptivo. Pagina en castellano Fecha de captura el 08/07/2012.

31. Teheran eleva una protesta por el Ciberterrorismo estatal contra Irán. Disponible en http://haddensecurity. wordpress.com/category /ciberguerra-2/. Pagina en castellano. Fecha de captura: 14/04/2012.

32. War of Gaza". Disponible en http://elpais.com/diario/2010/06/08/opinión /1275948 011_850215.html, Fecha de captura 10/08/12

33. "Wikileak la libertad de expresión". Disponible en http://www.infobae.com /notas/666898-WikiLeaks-y-la-libertad-de-expresion-en-internet.html.Fecha de captura 10/09/12.

34. Wolfgang Gerstenecker. Politik-digital. Disponible en http://e-blogs.wikio.es /bios/de/politik-digital ¿Es peligroso Twitter para las Fuerzas Armadas americanas? Artículo publicado en internet en el 28/10/2010. Pagina en castellano. Fecha de captura: 16/03/2012.

Anexo 1

PLEXO NORMATIVO ARGENTINO VIGENTE

COMERCIO ELECTRONICO

- Anteproyecto de Ley Formato Digital de los Actos Jurídicos. Comercio Electrónico (Presentado en el Congreso en el mes de Agosto de 2000).
- RESOLUCION 412/99 del Ministerio de Economía y Obras y Servicios Públicos. Recomendaciones del Grupo de Trabajo sobre Comercio Electrónico y Comercio Exterior.
- LEY 2.244 de la Ciudad Autónoma de Buenos Aires. Prestadores de Servicios a Consumidores y/o Usuarios.
- LEY 2.817 de la Ciudad Autónoma de Buenos Aires. Se fijan Obligaciones de Proveedores de Bienes o Servicios hacia los Consumidores.

CONTRATOS

- LEY 24.240 de Defensa al Consumidor.
- RESOLUCION 33.463/08 de la Superintendencia de Seguros de la Nación.

CORREO ELECTRONICO

- Anteproyecto de Ley de Regulación de las Comunicaciones Comerciales Publicitarias por Correo Electrónico (SPAM).
- Anteproyecto de Ley de Protección Jurídica del Correo Electrónico.

DELITOS

- Anteproyecto de Ley de Delitos Informáticos.
- LEY 863 de la Legislatura de la Ciudad Autónoma de Buenos Aires sobre Protección del Acceso de los Menores a Páginas Web con Contenido Pornográfico.
- Proyecto de Ley del Defensor del Pueblo de la Nación sobre pornografía infantil en Internet.
- LEY 26.388 de Ley de Delitos Informáticos.

NOMBRES DE DOMINIO

- RESOLUCION 2226/2000 del Ministerio de Relaciones Exteriores, Comercio Internacional y Culto relativa a la Registración de Nombres de Dominio en Internet en la República Argentina.
- RESOLUCION 904/2008 del Ministerio de Relaciones Exteriores, Comercio Internacional y Culto. Modifica y Adecua las Reglas para la Registración de Nombres de Dominio de Internet aprobadas por la Resolución 2226/00.
- RESOLUCIÓN 616/2008 del Ministerio de Relaciones Exteriores, Comercio Internacional y Culto. Incorpóranse caracteres multilingües pertenecientes al idioma español y portugués, para la registración de nombres de dominio de Nivel Superior Argentina (.AR).

DOCUMENTO ELECTRONICO

- LEY 24.624, modificatoria de la Ley 11.672, que considera con pleno valor probatorio a la documentación de la Administración Pública Nacional archivada en soportes electrónicos.

FIRMA DIGITAL

- RESOLUCION 45/97 de la Secretaría de la Función Pública sobre firma digital.
- DECRETO 555/97 sobre firma digital.
- RESOLUCION 194/98 de la Secretaría de la Función Pública que aprueba los estándares aplicables a la "Infraestructura de Firma Digital para el Sector Público Nacional".
- DECRETO 427/98 que dispuso promover el uso de la firma digital en toda la Administración Pública Nacional, otorgándole similares efectos que la firma manuscrita para los actos internos de administración.
- LEY 25.506 de Firma Digital.
- Anteproyecto de Decreto Reglamentario de la Ley Nº 25.506 de Firma Digital.
- DECRETO 2.628/02 que reglamenta la Ley Nº 25.506 de Firma Digital.
- DECRETO 283/2003 que autoriza, con carácter transitorio, a la Oficina Nacional de Tecnologías Informáticas a proveer certificados digitales para su utilización en aquellos circuitos de la Administración Pública Nacional que requieran firma digital.

- Decreto 1028/2003 - Disuelve el Ente Administrador de Firma Digital creado por el Decreto Nº 2628/ 2002 y lo reemplaza por la Oficina Nacional de Tecnologías de Información de la Subsecretaría de la Gestión Pública.
- Decreto 724/2006 - Modifícase la reglamentación de la Ley Nº 25.506.
- Decisión Administrativa 6/2007. Establece el marco normativo de firma digital aplicable al otorgamiento y revocación de las licencias a los certificadores que asi lo soliciten.

INTERNET

- LEY 25.690. Establécese que las empresas ISP (Internet Service Provider) tendrán la obligación de ofrecer software de protección que impida al acceso a sitios específicos.
- LEY 26.032. Establece que la búsqueda, recepción y difusión de información e ideas por medio del servicio de Internet se considera comprendida dentro de la garantía constitucional que ampara la libertad de expresión.
- DECRETO 554/97 que declara de interés nacional al acceso a Internet.
- DECRETO 735/97 que crea la Comisión de Conexión con Internet.
- DECRETO 1279/97 que declara comprendida la garantía constitucional de libertad de expresión para Internet.
- RESOLUCION 2132/97 que adopta el procedimiento de Audiencia Pública para la presentación de inquietudes sobre aspectos relacionados con Internet.
- DECRETO 1018/98 que aprobó el programa "argentin@internet todos" destinado a masificar la utilización de equipamiento multimedia y el acceso a Internet.
- RESOLUCION 1235/98 que determina la inscripción que deben incluir las facturas emitidas por los Internet Providers.
- DECRETO 1293/98 que declara de interés nacional al Proyecto Internet 2.
- DECRETO 1335/99 que declara de interés nacional al Proyecto "Una dirección de correo electrónico para cada argentino".

INTIMIDAD - PROTECCION DE DATOS PERSONALES

- LEY 24.766 de confidencialidad sobre información y productos que estén legítimamente bajo control de una persona y se divulgue indebidamente de manera contraria a los usos comerciales honestos.
- Constitución Nacional modificada en 1994. Art. 43.
- LEY 25.326 de Protección de los Datos Personales.

- LEY 26.343. Incorporación del art. 47 a la Ley 25.326 de Protección de los Datos Personales.
- DECRETO 1.558/2001 que reglamenta la Ley de Protección de los Datos Personales.
- DISPOSICION Nº 1/2003. Apruébanse la "Clasificación de Infracciones" y la "Graduación de las Sanciones" a aplicar ante las faltas que se comprueben. .

PROPIEDAD INTELECTUAL

- DECRETO 165/94 de protección al software.
- LEY 24.425 de ratificación de los Acuerdos Trip's.
- LEY 25.036, modificatoria de la Ley 11.723 de propiedad intelectual, que incluye dentro de las obras intelectuales protegidas a los programas de computación.

PROBLEMA DEL AÑO 2000

- RESOLUCION 125/97 de la Secretaría de la Función Pública que crea la Unidad Ejecutora 2000 a fin de controlar el impacto del problema del año 2000 en la administración pública.
- RESOLUCION 173/99 de la Secretaría de Industria que obliga a quienes comercialicen equipos de computación o programas que dependan de una variable temporal que incluya el dato "año" a colocar una identificación sobre el carácter compatible o no con el año 2000.
- RESOLUCION 512/99 de la Comisión Nacional de Telecomunicaciones que intima a los prestadores de servicios de telecomunicaciones y correo postales a presentar informes sobre la actividad del año 2000.
- COMUNICACIONES "A" 2564, 1654, 2693 y 2959 del Banco Central de la República Argentina a las Entidades Financieras tendientes a lograr la adecuación de los sistemas informáticos para su uso a partir del año 2000.
- CIRCULAR 3708 de la Superintendencia de Seguros de la Nación solicitando información a las entidades aseguradoras referida a las acciones tomadas previendo el problema del año 2000 y alertando sobre sus responsabilidades.