Uso de las redes sociales y el ciberespacio como amenaza a la imagen institucional del Ejército Nacional

Alberto Aguilar Gallegos
Erasmo Ordoñez Reyes
Gregory Tapiero Martínez
Julián Rincón Ricaurte

Trabajo de grado para optar al título profesional:
Especialización en Seguridad y Defensa Nacionales

Escuela Superior de Guerra "General Rafael Reyes Prieto"
Bogotá D.C., Colombia

2017

Uso de las redes sociales y el ciberespacio como amenaza a la imagen institucional del Ejército Nacional

Use of social networks and cyberspace as a threat to the institutional image of the National Army

Por: My. Inf. D.E.M. Aguilar Gallegos Alberto.

My. de Cab. D.E.M. Ordoñez Reyes Erasmo.

My. Gregory Tapiero Martínez.

My. Aviación. Julián Rincón Ricaurte.

Estudiantes de la Especialización en Seguridad y Defensa Nacional de la Escuela Superior de Guerra, Bogotá, Col. 2017

RESUMEN

En el principio de los tiempos fue la palabra, después la escritura, más tarde el papel y así sucesivamente se ha llegado a los ordenadores y a su interconexión en el ciberespacio Pero no es hasta la novela "Neuromante" del autor de ciencia ficción William Gibson (1984), donde se cita por primera vez al ciberespacio, al referirse a todos los recursos de información y comunicación disponibles en las redes informáticas, especialmente en Internet. (Reguera Sánchez, 2015)

El ingreso a los medios de información y base de datos, fue el inicio de un nuevo espacio para realizar estrategias, procesos y procedimientos en todos los campos de trabajo y de operación, era un nuevo mundo el que se iniciaba con actividades básicas de automatización y digitalización de procesos, que con el tiempo se fue perfeccionando y fue logrando el desarrollo de no solo un proceso o procedimiento, sino de cubrir miles de ellos a partir de un solo centro de mando.

Estos centros de mando o equipos representan una herramienta facilitadora, pero también una nueva amenaza que puede poner en peligro nuestros sistemas físicos incluyendo nuestros sistemas militares y toda nuestra infraestructura crítica. El incremento del interés por las tecnologías de la información ha llevado a una cada vez mayor implicación de las industrias dedicadas a estas tecnologías en todo tipo de actividades y procesos. (Prieto Oses, 2013)

El ciberespacio es un nuevo dominio de la guerra, prueba de ello es que más de 140 países, entre ellos Colombia, están desarrollando capacidades, herramientas TICS y preparando personal, para combatir posibles amenazas en los sistemas de datos que manejan los sistemas económicos, políticos y de defensa de un Estado, que pueden afectar el funcionamiento de los sistemas de defensa nacional, el sistema bancario y los sistemas de servicios públicos. (Prieto Oses, 2013)

En un futuro será un problema de Estado, que envolverá a las Fuerzas Armadas, los Cuerpos de Seguridad del Estado y a los sectores estratégicos. Es un nuevo problema para la Defensa Nacional, se debe iniciar con el cambio y la creación de herramientas y estrategias que permita obstruir e identificar amenazas potenciales en las redes sociales y el ciberespacio, estas debe ir de acuerdo a la evolución de las nuevas tecnologías.

El presente trabajo a partir de experiencias internacionales y de una investigación de bases de datos a partir de libros, revistas científicas e información, busca recomendar acciones que puede aplicar el Ejército Nacional para contrarrestar posibles acciones amenazantes mediante el empleo de redes sociales y del ciberespacio, las cuales pueden afectar la imagen institucional, la seguridad nacional y hasta el mismo funcionamiento digital de la institución.

PALABRAS CLAVES

Ciberespacio, ciberdefensa, ciberseguridad, redes sociales, internet., netwar.

ABSTRACT.

At the beginning of time was the word, then the writing, later the paper and so on has been reached to computers and their interconnection in cyberspace. But it is not until the novel "Neuromancer" by the author of science fiction William Gibson (1984), where cyberspace is first mentioned, referring to all information and communication resources available on computer networks, especially on the Internet. (Reguera Sánchez, 2015)

Access to the media and database was the beginning of a new space for strategies, processes and procedures in all fields of work and operation, it was a new world that began with basic activities of automation and Digitalization of processes, which over time was perfected and was achieved the development of not only a process or procedure, but to cover thousands of them from a single command center. These control centers or equipment represent a facilitating tool as well as a new threat that can endanger our physical systems including our military systems and, ultimately, all our critical infrastructures. The increasing interest in information technology has led to an ever-increasing involvement of the industries involved in these technologies in all types of activities and processes. (Prieto Oses, 2013)

This in the future may imply a problem of the State, which will involve the Armed Forces, the State Security Corps and the strategic sectors. It is a new problem for the National Defense, it must start with the change and the creation of tools and strategies to

obstruct and identify potential threats in social networks and cyberspace, these should go according to the evolution of new technologies.

The present work, based on international experiences and a database and information research, seeks to recommend actions that can be applied by the National Army to counter potential threatening actions through the use of social networks and cyberspace, which can affect the institutional image, National security and even the digital operation of the institution

KEYWORDS

Cyberspace, cyber-defense, cybersecurity, social networks, internet, netwar.

INTRODUCCIÓN.

Al ser el Ejército Nacional un pilar del Estado colombiano, se ve expuesto a diversas amenazas que buscan dañar la imagen institucional a fin de que pierda la confianza y credibilidad de la sociedad, esto mediante el uso mal intencionado y tergiversado de las redes sociales, por parte de grupos detractores del Estado y de organismos no gubernamentales nacionales e internacionales.

Las redes sociales son un instrumento de difusión masivo en tiempo real, que puede ser utilizado como un sistema de propaganda en contra del Ejército Nacional, buscando su deslegitimación y aprovechando los incidentes ocurridos en cumplimiento de las actividades militares.

Las redes sociales y el ciberespacio serán los medios previstos para las guerras futuras, donde los resultados efectivos de estas serán el sabotaje, el daño de sistemas, la pérdida de credibilidad y el desprestigio de las organizaciones y entes, los cuales buscan

garantizar la seguridad nacional, por esa razón, este trabajo busca recomendar estrategias para responder a la siguiente pregunta ¿cómo minimizar los riesgos de afectación a la imagen institucional por medio de redes sociales?

El Objetivo general del presente trabajo busca realizar un análisis a las posibles amenazas que se pudieran generar con el uso de las redes sociales y el ciberespacio, afectando la imagen institucional y haciendo perder la credibilidad y nivel de confianza de la población civil hacia el Ejército Nacional.

La primera parte del trabajo, hace una descripción sobre antecedentes y ataques mediante el empleo de redes sociales y del ciberespacio a instituciones militares y gubernamentales, los cuales han logrado un impacto negativo sobre la eficiencia y la efectividad de otros Estados, haciéndole perder credibilidad y prestigio ante la sociedad y que puede afectar de manera directa al funcionamiento y existencia de las instituciones.

Asimismo, se realizará un análisis de los riesgos que puedan ser motivo de empleo para el desprestigio de la institución mediante el uso de acciones negativas a partir de las redes sociales y ataques del ciberespacio, los cuales puedan producir sabotajes, perfidia, pérdida de credibilidad y daños irreparables a la imagen institucional.

Finalmente, se adelantara un estudio para recomendar las posibles acciones y herramientas que permitan contrarrestar las acciones negativas y de descrédito desarrolladas mediante el empleo del ciberespacio y las redes sociales y que puedan afectar la imagen institucional y la estructura funcional, manteniendo el prestigio del Ejército Nacional y procurando garantizar el cumplimiento de la misión institucional y el fortaleciendo el apoyo de la población civil.

Para el desarrollo de este trabajo se aplicarán los tipos de investigación descriptiva y cualitativa, iniciando con una consulta de fuentes de información, análisis de documentos de diversos medios de comunicación y organismos especializados de consultoría; posteriormente se realizara un análisis donde se determinara el impacto en la percepción de confianza del Ejército hacia la población civil.

I. ANTECEDENTES DEL DESARROLLO Y ATAQUES MEDIANTE EL EMPLEO DE REDES SOCIALES Y ATAQUES AL CIBERESPACIO.

I.I Estados Unidos y el Desarrollo Cibernético.

Los futuros conflictos entre Estados se desarrollarán en el ciberespacio y con el empleo de los Ejércitos cibernéticos, aunque no son decisivos para la obtención de victorias completas en las guerras, esta dimensión de la guerra si pueden balancear el conflicto hacia un oponente, o en su caso puede dar una ventaja estratégica (disminución de la capacidad militar), la quinta dimensión como es llamada la ciberguerra es un componente de gran importancia y de gran capacidad, que puede dar la ventaja militar y ofrecer una victoria temprana sobre el oponente.

Después del atentado del 11 de septiembre, Estados Unidos implementó y amplió el uso de sistemas de seguridad digitales y tecnologías de la comunicación más sofisticados, los cuales buscaban garantizar la seguridad nacional del territorio y de la población, evitando que se repitieran los hechos ocurridos en Nueva York. También el gobierno norteamericano inicio la campaña de interceptación de redes de comunicación de los grupos islámicos radicales, los cuales posteriormente llevaron a la ubicación de

OSAMA BIN LADEN en Pakistán, lográndose con ello, a su neutralización y la desarticulación del grupo terrorista AL QAEDA.

El fortalecimiento de los sistemas de defensa norteamericanos, se inició a partir de los equipos cibernéticos y el empleo del ciberespacio, se desarrolló un programa de entrenamiento del personal escogido de los cuerpos de seguridad (FBI-CIA en el 2000), la creación de comités con las multinacionales en TICS y bases de datos (Microsoft, Google, entre otros 2002) buscando a futuro, la neutralización de ataques cibernéticos, potencializar la ciberdefensa y la ciberseguridad, mejorar la seguridad de las bases de datos de la infraestructura crítica y de ser utilizada como una herramienta preventiva para posibles ataques terroristas de los países que podían representar una amenaza a Estados Unidos.

Después de haber logrado potencializar los sistemas de ciberdefensa y ciberseguridad, Estados Unidos realizaría el primer ataque hacia un Estado que representaba una amenaza por el desarrollo nuclear y el empleo de este en armas de destrucción masiva; mediante el empleo del MALWARE STUNEXT, Irán, sería el Estado afectado con el uso de este virus, el cual logro sabotear las maquinas centrifugadoras de una planta nuclear y eliminando toda la información que poseía en la automatización de la planta, demostrando con este hecho, la capacidad tecnológica norteamericana sobre los Estados que no se sometieran a los parámetros de control de armas de destrucción masiva y hacia los que puedan representar una amenaza en el vecindario y a nivel mundial. (Castells, 2012)

La carrera armamentista y el desarrollo cibernético en Estados Unidos van de la mano, esta debe garantizar la seguridad del territorio y de su población (Identidad

Nacional Norteamericana), también debe mantenerse como la potencia mundial que administra y dirige los rumbos del mundo, por eso Estados Unidos potencializa el desarrollo de los sistemas de bases de datos y de las TICS, lo que garantizará la soberanía nacional, la protección de la Defensa del territorio, la seguridad económica y financiera de la población, la propia subsistencia del Estado y el dominio de los mercados y de las políticas mundiales. (Owens & Lin, 2009).

I.II ¿QUÉ ES WIKILEAKS?

Es una ONG con sede en Suecia que dispone de una página en Internet que nace en 2006. Su nombre surge como un guiño semántico a Wikipedia (popular enciclopedia digital) y a la publicación de información confidencial denominada "Leak[1]s", ¿Su objetivo? ofrecer un espacio donde cualquiera puede sacar a la luz documentos que contienen evidencias de hechos ilegales. (Altonivel, 2010)

Wikileaks se volvió una página de alto impacto y de gran acceso al público, debido a las informaciones que esta suministraba a la población, donde impactaban de forma negativa a jefes de Estado, Funcionarios Legislativos, grandes industriales, deportistas, actores, cantantes y organismos de seguridad de las Grandes potencias.

En esa página, cualquier particular podía publicar información privilegiada o clasificada que fuese de impacto negativo hacia un Estado o alguno de sus gobernantes, así mismo que demostrara hechos de corrupción, no morales y de violencia por parte de funcionarios estatales, empresas, organismos de seguridad y grupos o comunidades, los cuales se buscan denunciar para que sea visto por la comunidad internacional y que

[1] **Leaks:** filtraciones o fuga

posteriormente fuesen investigados por las autoridades judiciales de acuerdo al delito cometido.

El origen de Wikileaks se inició con base en la página Wikipedia[2], esta facilita que cualquier usuario aporte información para ampliar la red de conocimiento, los usuarios no necesitan tener conocimientos técnicos, simplemente se espera que la información sea real y de primera mano.

El fundador de esta página fue el Australiano Julián Assange, este nunca ha revelado la fuente de la información que recibe. La única condición que impone con su página WikiLeaks es que los documentos sean auténticos. Y hasta la fecha se acumulan 1.2 millones de archivos. (Altonivel, 2010)

Dentro de las condiciones de la información, wikileaks manifestaba el interés en acceder a informaciones de entidades acusadas por violaciones a los Derechos Humanos y actos de corrupción, lo que impulsó a particulares y hackers a ingresar a páginas web y privadas de entidades estatales, medios de comunicación, autoridades y empresas privadas; haciendo que muchos de estas organizaciones se alertaran y posteriormente realizaran denuncias ante las autoridades judiciales.

El sitio comenzó a publicar documentos en 2007. Pero fue hasta abril de 2010 cuando dio la vuelta al mundo, con la publicación de un vídeo en el que se veía cómo dos reporteros de la agencia Reuters fallecían bajo disparos de un helicóptero estadounidense en Irak. En julio de ese año, la organización filtró 77 mil documentos sensibles sobre la guerra de Afganistán y tres meses después, 400 mil informaciones sobre la guerra de Irak. (Altonivel, 2010)

---

[2] **Wikipedia:** Pagina de internet de fácil acceso para búsqueda de información y estadística

A través de miles de documentos, fechados entre 2004 y 2009 y en su mayor parte correspondientes al periodo presidido por George Bush, es posible entender el porqué de las dificultades del Ejército norteamericano, así como seguir el relato de la muerte de civiles. Así las cosas, lo que empezó como un blog de publicación de filtraciones, es hoy uno de los mayores dolores de cabeza que registra la diplomacia de Estados Unidos. (Altonivel, 2010)

Dentro de otros escándalos de wikileaks, se encuentra la filtración de documentos británicos donde se observaba el interés del parlamento en intervenir en las decisiones de los gobiernos de los países adheridos al Reino Unido, entre estos Escocia, lo que impulsó a la población de ese Estado a una serie de manifestaciones violentas y que se iniciara una campaña independiente para la separación del gran Estado británico.

Los países más afectados por los documentos publicados por wikileaks son Estados Unidos, el Reino Unido, Francia, Arabia Saudita, Italia, Rusia, China y España, donde los escándalos de altos diplomáticos hasta funcionarios de gobierno, se han visto involucrados en hechos de corrupción, conflicto de intereses, favores a terceros, violencia intrafamiliar y financiación a grupos terroristas.

WikiLeaks también dio a conocer qué es lo que piensa la administración Obama de la gestión del gobierno de José Luis Rodríguez Zapatero, por ejemplo. También aporta datos sobre las "fiestas salvajes" de Silvio Berlusconi, primer ministro italiano, que suscita "recelos" en Washington; el seguimiento al que se mantiene al ex presidente francés, Nicolás Sarkozy; o, la "sospecha" de que Vladimir Putin es el hombre fuerte en la política de Rusia. Precisamente el gobierno ruso es uno de los más estudiados en los

informes, junto a otros países, como Irán, Pakistán, Afganistán y Turquía. (Hola.com, 2010)

Por todos estos hechos, iniciaron la persecución contra los miembros de Wikileaks, entre ellos el escritor William Assange, países como Reino Unido, Suecia, Noruega y Finlandia han solicitado ordenes de captura junto con Interpol, con el fin de frenar todas las acciones de publicaciones y denuncias que ha hecho esta página en contra de los funcionarios de gobierno.

Wikileaks a través de sus informes, logro poner en jaque a los gobiernos más fuertes del mundo, su director Julián Assange, fue perseguido por el gobierno sueco y el gobierno británico, razón por el cual pidió asilo en Ecuador, logro penetrar a los más fuertes líderes mundiales y demostró que quien domina el Ciberespacio, puede llegar a tener un poder igual de grande como un arma de gran impacto. (Altonivel, 2010)

I.III Los Panamá PAPERS, y su impacto económico

La investigación Panamá Papers fue impulsada por el Consorcio Internacional de Periodistas de Investigación (ICIJ, en inglés) y por el diario alemán Süddeutsche Zeitung. Ésta representa una filtración de más de 11 millones de documentos a los que tuvieron acceso, en un proyecto en el que trabajaron más de 370 periodistas de 100 medios de comunicación de 76 países. (La República, 2016)

Este hecho se dispersó a través de las redes sociales, ocasionando a nivel internacional un imagen negativa sobre el Estado panameño, volcándose hacia al instituciones internacionales de comercio como la OCDE los cuales manifestaban que

Panamá era una economía criminal e ilegal, ocasionando como producto de esto el retiro de inversión extranjera y el declive de la economía.

Con esto se puede demostrar que el empleo del ciberespacio y las redes sociales, pueden ocasionar desprestigio y la pérdida de credibilidad de líderes mundiales, deportistas y personajes públicos, hace ver que los Estados en donde son originarios, administran o trabajan, no tienen las herramientas completas para controlar los recursos y de cobrar los impuestos, mostrándose ineficaces y ante la comunidad internacional como países no viables y de alta corrupción.

El escándalo financiero denominado "Panamá Papers" tendrá efectos inevitables sobre el modelo de la economía panameña, en medio de una pérdida de imagen de país que obliga a proponer un enfoque serio sobre las causas y consecuencias de esa crisis. A esa conclusión llegaron investigadores y representantes de sociedades anónimas consultadas por Bayano digital. (Carrasco, 2016)

I. IV El Ramsomware, último y recién ciberataque que afecto a la seguridad y economía de las grandes potencias.

El año 2017, será recordado entre los organismos de ciberdefensa y ciberseguridad como el más difícil por el ataque de un virus tan poderoso, que arremetió a las grandes potencias europeas y afecto organismos funcionales y de seguridad, entre ellos la sede de Telefónica de Madrid, el sistema de salud británico y el Ministerio de Interior de Rusia, con ello, desprestigiando a las autoridades y los entes de control en el manejo de redes y datos.

El virus se conoció con el nombre de ransomware, éste causa un secuestro exprés de datos y pide un rescate para liberar el sistema. En un tuit, Costin Raiu, el director

global del equipo de investigación y análisis de Kaspersky Lab, empresa de seguridad informática, estimó que se habían registrado en el mundo, más de 45.000 ataques en 74 países. (Tecnologia, el País, 2017)

Este virus no solo afecto a Estados e instituciones, también atacó a computadores personales de miles de personas en Estados Unidos, Europa y Asia, demostrando con ello la gran capacidad de extensión que se hizo viral, al secuestrar cuentas de Microsoft y de cuentas de usuario en redes sociales.

Se podría afirmar que es uno de los peores ataques informáticos presentado en los últimos años, no fue un solo hecho en una organización o en un Estado, este se expandió en más de 74 países, demostrando con ello, la extensión que tiene el ciberespacio y cómo puede afectarse la seguridad nacional y la estabilidad de los Estados, ocasionando un caos real en el mismo devenir de la sociedad.

Ese tipo de virus, que al ser ejecutado en los ordenadores, aparenta ser inofensivo e imita a otras aplicaciones, es el más habitual y representa el 72,75% del malware, de los ataques maliciosos, según los últimos informes de las compañías Kaspersky Lab y PandaLab. (Tecnologia, el País, 2017)

Para organismos internacionales que administran los sistemas de bases de datos y de ciberdefensa y ciberseguridad, este virus fue un aviso para demostrar la vulnerabilidad de las redes de datos y de información que administra muchos países, no basta con tener los mejores programas de seguridad informática y los equipos de alta tecnología, se debe trabajar en actualizar los sistemas de operación y de fortalecer las medidas de seguridad informática que pueda evitar la afectación de la estabilidad del Estado.

La multinacional Microsoft, preocupada por la difusión de este virus, no había dado una respuesta oficial, pero sí contempla que la industria se replantee los criterios y formas en que se actualizan los programas para que la protección frente a vulnerabilidades no dependa tanto de voluntad humana, como de automatismos. (Tecnologia, el País, 2017)

Los ataques son aprovechados por los delincuentes para ingresar a las empresas para acceder a cuentas, información privilegiada y de seguridad nacional, al momento de poseerla, piden el pago de un rescate o para la devolución de las bases de datos que tienen bajo control o dominio; lo que obligó a muchas empresas a solventar grandes cifras de dinero y que las empresas empezaran a realizar mayores inversiones en la seguridad de las bases de datos.

Jakub Kroustek especialista en sistemas manifiesta, que en las redes sociales se habían rastreado hasta 50.000 ataques de WannaCry. También aseguró en el blog de la compañía, Avast, observaron la primera versión de este virus en febrero y que habían encontrado el mensaje de rescate escrito en 28 idiomas. (Tecnologia, el País, 2017)

Este nuevo ataque a las redes de información y bases de datos, demostró que en cualquier momento los Estados y las organizaciones son vulnerables en el ciberespacio, que las futuras guerras (guerras de quinta generación), se efectuarán a partir de acciones de sabotaje y de manipulación de información privilegiada, del daño de sistemas funcionales de equipos de defensa, bancarios, sanitarios, estatales y comerciales; lo que podría ocasionar hasta la pérdida de vidas humanas.

Las guerras del Futuro se efectuarán a partir del ciberespacio, estas no necesitaran de armas y de un enfrentamiento cercano, son acciones donde una sola persona a través de un computador, podrá afectar con mayor impacto un Estado desestabilizando el sistema

económico y financiero, el posible sabotaje de equipos y sistemas militares, la pérdida de comunicación e información y hasta la afectación de la seguridad alimentaria de la población.

II. LOS RIESGOS DEL EMPLEO DE LAS REDES DE DATOS Y EL CIBERESPACIO.

Las redes de datos y el internet son un nuevo espacio de conflicto, esta interacción se desarrolla en un nuevo escenario que se denomina ciberespacio, este involucra todos los equipos y medios que dependan de los sistemas (bancarios, financieros, alimenticos, militares, seguridad), así como los sistemas operativos de las armas.

Los ataques cibernéticos se podrán desarrollar por parte de Estados, de organizaciones y hasta los particulares; es un nuevo conflicto en que no se verá afectada la integridad humana de manera directa, pero los efectos pueden ser nocivos en caso que se ataquen sistemas vitales para la conservación de la vida humana.

El ciberespacio es el nuevo escenario de los conflictos futuros, adicional al escenario terrestre, naval, aéreo y espacial; este escenario brindará garantías a las naciones que desarrollen estrategias de seguridad y defensa para los intereses nacionales y de defensa de los Estados con base en sus sistemas tecnológicos y sus redes de datos. (Rain, Cyberspace Definitions and implications, 2010)

En este nuevo escenario aparecen nueva terminología que se debe tener en cuenta, para entender las herramientas de ataque, las acciones que se pueden cometer y los efectos que se pueden desarrollar para evitarlos.

Las amenazas Informáticas se consideran como las opciones ilimitadas que ejecuta un actor hostil con el fin de adquirir de manera ilegal, información clasificada sobre equipos militares, documentos y procesos, los cuales son ofrecidos a particulares, organizaciones y Estados para venderlos; ganando así una ventaja estratégica y económica sobre el Estado u organización que se haya visto atacado.

Los ataques también pueden ser en contra de la infraestructura crítica de una nación[3], la cual puede repercutir en la desmoralización de la población o sus funcionarios, frente a un eventual ataque militar. (Szentkereszty de Zagón, 2015)

Una acción sobre los sistemas de datos de una represa, de las entidades administradoras de servicios públicos, del sistema de salud o de controles alimenticios, pueden hacer más daño que el mismo empleo de las armas, el riesgo de pérdida de vidas humanas puede ser mayor y los efectos de mayor impacto.

Aparece en el nuevo escenario la palabra Cibernética, que se define como la Ciencia o disciplina que estudia los mecanismos automáticos de comunicación y de control o técnica de funcionamiento de las conexiones de los seres vivos y de las máquinas, hacia estas se pueden presentar los Ataques cibernéticos que son las acciones organizadas y/o premeditadas de una o más personas para causar daño o problemas a un sistema informático a través del ciberespacio. (Reguera Sánchez, 2015)

---

[3] La Infraestructura crítica se define como el conjunto de computadores, sistemas computacionales, redes de telecomunicaciones, datos e información, cuya destrucción o interferencia puede debilitar o impactar en la seguridad de la economía, salud pública, o la combinación de ellas, en una nación. (Comisión de regulación de Comunicaciones, 2009)

La cibernética se convertiría con el pasar de los años, en la base fundamental para el funcionamiento de todo tipo de sistema que ejerce un proceso vital para la existencia de un Estado, desde la misma administración de recursos hasta la identificación de los ciudadanos dentro de un Estado, hoy en día, es imprescindible.

La ciberguerra es un área dentro de las agencias militares de los países que tiene como objetivo encontrar las vulnerabilidades técnicas de los sistemas o redes informáticas del enemigo para penetrarlas y atacarlas, tanto así como para extraer datos e información sensible. En este caso el ciberespacio es el campo de batalla y las armas son programas o aplicaciones informáticas (Sain, 2016)

Las tácticas de combate son la infiltración en redes enemigas, la recopilación de datos, la interferencia de señales inalámbricas, los programas informáticos falsificados y contaminados (a partir de la instalación de "puertas traseras"), ataques a sistemas enemigos a través de virus, gusanos y bombas lógicas, entre otras.

Algunas potencias en materia de ciberguerra[4] son Estados Unidos, China y Rusia, mientras que en un segundo nivel se encuentran Israel y Francia. Otras naciones con capacidad para la guerra cibernética son Taiwán, Irán, Australia, Corea del Sur, India y Paquistán, entre otros. (Sain, 2016)

En este tipo de conflicto el mejor resultado obtenido por algún oponente, no es la pérdida de vidas humanas, es lograr la desarticulación de los sistemas operativos sobre las

[4] La ciberguerra puede ser entendida como una agresión promovida por un Estado y dirigida a dañar gravemente las capacidades de otro para imponerle la aceptación de un objetivo propio o, simplemente, para sustraer información, cortar o destruir sus sistemas de comunicación, alterar sus bases de datos, es decir, lo que habitualmente hemos entendido como guerra, pero con la diferencia de que el medio empleado. (Sánchez Medero, 2012)

armas que funcionan con bases de datos, lograr el sabotaje de las grandes empresas fabricantes de armas y dejar sin comunicación y redes a las fuerzas armadas enemigas, lo que permitirá una posterior acción militar.

El área de guerra cibernética[5] surge a principios de los noventas en el seno de las agencias de seguridad de los Estados Unidos, donde los servicios de inteligencia comienzan a ver la Internet como una potencial herramienta para el espionaje electrónico. (Instituto Español de Estudios Estrátegicos, 2014)

Un nuevo concepto que adquiere significación a partir del desarrollo de este campo es el de infraestructuras críticas de información, también conocidos como sistemas SCADA (acrónimo de supervisión, control y adquisición de datos, en inglés). Son sistemas informáticos que hacen al funcionamiento de los servicios públicos de un país (Sain, 2016)

Las redes de datos y el ciberespacio son los nuevos lugares de conflicto, donde el dominio no se realizará directamente por el empleo de las armas, se efectuará a partir de personas preparadas en el empleo de ordenadores y de sistemas de información, donde no brillará el arma de mayor impacto, se destacarán las mejores acciones en el empleo de los sistemas y de las redes de información.

Todas las bases de datos de talento humano y financieros se emplean a través de bases de datos, por esa razón se debe prever un posible sabotaje por agencias externas o grupos ilegales, todas las bases de datos se emplean a partir de plataformas, de sistemas de datos,

[5] La cibernética cubre todos los equipos y sistemas de información, desde los más básicos hasta los avanzados, estas son las herramientas que mueven todos los sistemas operativos y financieros del Estado

como el caso de bases de datos (plataforma MOCE[6]), plataformas de operaciones, redes de comunicaciones, entre otros, los cuales en caso de verse afectados, pueden ocasionar un daño impactante al funcionamiento de la institución militar.

III. LAS POSIBLES ACCIONES PARA COMBATIR LOS DELITOS EN EL CIBERESPACIO.

El Ciberespacio se puede definir como el ambiente tanto físico como virtual compuesto por computadores, sistemas computacionales, programas computacionales (software), redes de telecomunicaciones, datos e información que es utilizado para la interacción entre usuarios. (Ministerio de Defensa Nacional, 2014)

Es un dominio caracterizado por el uso del espectro electrónico y electromagnético para almacenar, modificar e intercambiar datos a través de sistemas de redes e infraestructuras físicas asociadas (Szentkereszty de Zagón, 2015)

Dentro de los nuevos delitos en el ciberespacio tenemos:

Ciberterrorismo: La convergencia del terrorismo y ciberespacio con el fin de atacar ilegalmente ordenadores, redes e información almacenada en ellos, incluye violencia contra personas o propiedades o, al menos, genera el miedo. ((Ministerio de Defensa Nacional, 2014)

Ciberdelincuencia: Acciones ilícitas que son cometidas mediante la utilización de un bien o servicio informático. (Ministerio de Defensa Nacional, 2014)

Guerra Cibernética: es el conjunto de acciones llevadas por un Estado para penetrar en los ordenadores o en las redes de otro país, con la finalidad de causar prejuicio o alteración (Reguera Sánchez, 2015)

Ciberdelito / Delito Cibernético: Actividad delictiva o abusiva relacionada con los ordenadores y las redes de comunicaciones, bien porque se utilice el ordenador como herramienta del delito, el sistema informático (o sus datos) el objetivo del delito (Ministerio de Defensa Nacional, 2014)

Figura No. 1 Nuevos delitos en el Ciberespacio, Fuente (Ministerio de Defensa Nacional, 2014)

[6] Moce: Modelo por competencias del Ejercito Nacional, plataforma que clasifica al personal militar en habilidades militares, complementarias (educación superior) y bilingüismo.

Para combatir las acciones delictivas dentro del ciberespacio, aparecen los términos ciberseguridad y ciberdefensa, como medios y estrategias de los Estados para evitar que la información y los activos críticos sean atacados a través de las redes de información y del internet y que con estos, se puedan evitar sabotajes, daños estructurales, afectación de los recursos, daños de bases de datos y la perdida de información.

La Capacidad del Estado para prevenir y contrarrestar toda amenaza o incidente de naturaleza cibernética que afecte la soberanía nacional, se denomina Ciberdefensa (Ministerio de Defensa Nacional, 2014)

Las estrategias y herramientas de la ciberdefensa, se adelantan para la protección de la soberanía nacional, con el fin de evitar perdida de información que afecte la seguridad y defensa nacional del estado, en evitar el uso del internet para realizar acciones terroristas, evitar acciones de guerra cibernética y las posibles acciones de espionaje e infiltración.

La capacidad del Estado para minimizar el nivel de riesgo al que están expuestos sus ciudadanos, ante amenazas o incidentes de naturaleza cibernética, se denomina Ciberseguridad (Ministerio de Defensa Nacional, 2014).

Las estrategias y herramientas de la ciberseguridad, se adelantan para proteger las transacciones financieras, la información privada, en la misma protección de los derechos fundamentales (derechos de protección de información, habeas data, a la privacidad, a la protección financiera), los derechos de autor y la propiedad intelectual y todo lo concerniente a las normas administrativas de funcionamiento y operación de las entidades estatales y privadas.

Los ciberataques se consideran como acciones deliberadas para alterar, interrumpir, engañar, degradar o destruir a los sistemas informáticos o redes, o la información y/o

programas residentes o en tránsito por estas redes de sistemas". (Owens & Lin, 2009)

Existen 2 Dos tipos de ciberataques: (Szentkereszty de Zagón, 2015)

1. **Ataques de alta intensidad:** daños de sistemas, equipos, trauma total o perdida de infraestructura, maquinaria.
2. **Ataques de baja intensidad:** sabotaje, recorte en el funcionamiento, alteración de sistemas bancarios y de base de datos

Dentro de los medios para realizar los ataques a las base de datos y a los sistemas digitales se encuentra: (Szentkereszty de Zagón, 2015)

1. **Los Malware:** son software (programas internos y de operación) diseñados para interferir con el funcionamiento de los computadores o para degradar la integridad de las bases de datos.
2. **Ataques DOS (Denial of Service):** consiste en la inundación de una red con información para evitar que los usuarios legítimos tengan acceso a información o servicios. (Bloqueo de acceso)

Los principales actores para realizar los cibertaques a los Estados, empresas, organizaciones, sistemas bancarios y particulares son: (Reguera Sánchez, 2015)

- Atacantes patrocinados por Estados.
- Servicios de Inteligencia y Contrainteligencia.
- Terrorismo, extremismo político e ideológico.
- Hackers

IV. REGULACIÓN DE LA CIBERDEFENSA Y LA CIBERSEGURIDAD

Debido a la acción de trasladar un monumento de los soldados soviéticos fallecidos en la II guerra mundial, en la ciudad de Tallin (Estonia), desde la zona céntrica hacia la periferia, este país de la antigua unión soviética fue blanco de una gran cantidad de ciberataques contra los sistemas de gobierno, financieros y económicos de ese país por parte de Hackers rusos, que no solo afectaron el funcionamiento del país, sino ocasionó un caos en la población que repercutió en manifestaciones en contra del Estado Estonio y el aprovechamiento de Rusia; para convencer a la población en una república federada rusa.

Con esta acción ocurrida en el 2007, a nivel internacional hizo que la OTAN organizara en esa ciudad, el centro de Excelencia para la Ciberdefensa Cooperativa de OTAN (CCDCOE), esta organización con los países miembros de Europa, reunieron esfuerzos para mejorar la capacidad de intercambio, cooperación e información en asuntos referentes a la defensa cibernética y enfocada a la seguridad, ciencia y tecnología.

Debido a la falta de una legislación en el desarrollo de las guerras en el ciberespacio, este centro convoca un grupo de expertos para la seguridad, defensa, ciberseguridad y Derecho Internacional, tomando como ejemplo los convenios realizados en Ginebra (Suiza), el resultado de este fue "el manual de Tallin", dirigido por el profesor Michael Schmitt de la U.S. Naval War College, y que se presentó en Londres el 15 de marzo de 2013. (Reguera, 2015)

La premisa fundamental con la que se empezó a redactar este manual, fue que la guerra no deja de ser tal porque se lleve a cabo en el ciberespacio, es decir, es posible la guerra en el ciberespacio. Aunque a la fecha de hoy no se tengan datos empíricos reales sobre los efectos de las ciberarmas, sólo algunos hechos como los ocurridos en Estonia

(2007) y el uso del Malware Stuxnet contra Irán (2010), se cree que no solo es ciencia ficción y que las posibilidades de efectos nocivos pueden ir más allá de una denegación de servicio. Es necesario poner de relieve que ciertas acciones, como por ejemplo, penetrar ilegalmente en los ordenadores centrales de control de una presa y conseguir descargar el agua, pueden tener el mismo efecto que si se volaran con explosivos las compuertas y el agua pudiera salir de la misma. (Reguera Sánchez, 2015)

En el Derecho Internacional, no hay reglas claras para los Estados en caso de desarrollo o enfrentamientos cibernéticos; por ejemplo Estados Unidos, China y Rusia manejan sus propias normas y legislación para el uso y empleo del Ciberespacio.

Cada una de estas naciones busca de manera individual, el adelanto de las tecnologías para convertirse en potencia mundial y para defender los sistemas informáticos de sus posibles enemigos, también buscan defender las estructuras críticas, la información bancaria, las actividades económicas de la población y de las instituciones, así como la protección de los equipos de seguridad y defensa de los Estados; es una competencia hacia la misma seguridad nacional.

V. LAS REDES SOCIALES COMO ELEMENTOS DECISIVOS DE LA LEGITIMIDAD INSTITUCIONAL.

En Colombia, muchas páginas de las redes sociales Facebook, twitter, instagram entre otras han tratado de afectar al Ejército Nacional empleando imágenes y fuertes declaraciones en contra de las operaciones militares adelantadas por los soldados, o en su caso difamando en acciones que las unidades militares no han desarrollado, estas buscan menoscabar la imagen de la institución frente a la sociedad nacional e internacional.

Figura No. 2 Imagen donde Funcionarios ESMAD al parecer atacan a manifestantes, Fuente ONG Viva País.

La manipulación de las imágenes pueden hacer que no muestren la realidad de las acciones que se presentan en contra de las autoridades y estas se emplean en atacar la acción militar y policial buscando desprestigiar la institución y afectar a los funcionarios para menoscabar la moral y el compromiso misional.

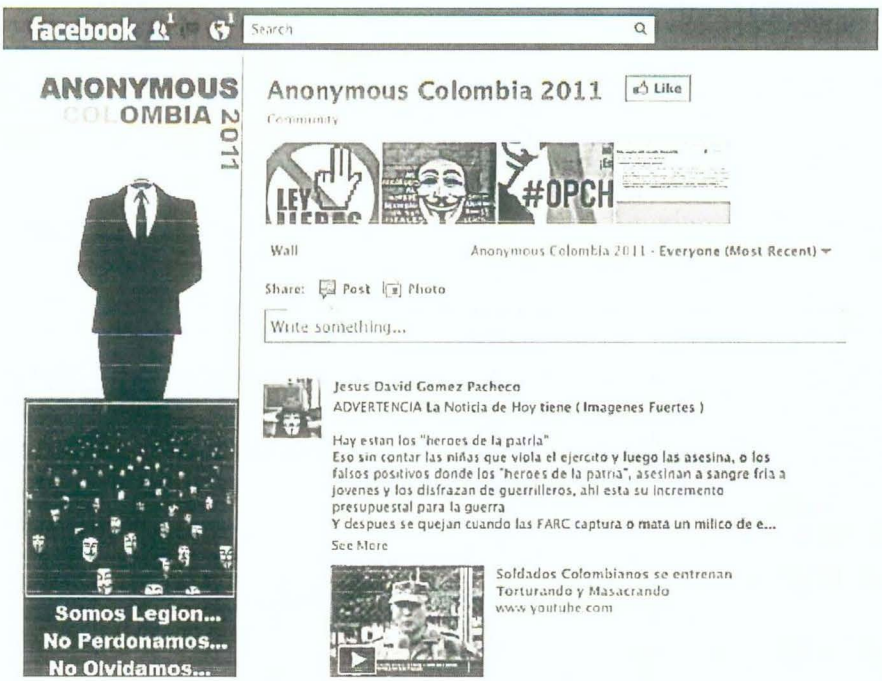

Figura No. 3 Imagen donde denuncian al Ejército mediante el empleo de redes sociales, **Fuente** Policía Nacional 2014

Redes sociales como Facebook tiene grupos y páginas como estas, que a través de mensajes dañinos, tratan de que la sociedad civil observe al Ejército como un enemigo y como delincuentes violadores de los Derechos Humanos, uno de los temas que más se facilitó para manifestar el odio hacia la institución fue el de los mal llamados falsos positivos de Soacha

Figura No. 4 Imagen donde denuncian al Ejército por asesinato de un Indígena, **Fuente** ONG ACNUR 2015

Las redes sociales pueden impactar mucho más de manera negativa en contra de la institución, pueden causar un impacto negativo ante la comunidad internacional, originando sanciones en contra del Estado colombiano, así como la perdida de legitimidad de la institución, que en el futuro puede llevar a investigaciones penales en contra de los integrantes de la fuerza. Uno de los hechos más lamentables fueron las ejecuciones extrajudiciales mal llamados falsos positivos, hecho que afectó la moral del personal militar; muchos oficiales y suboficiales se vieron involucrados en investigaciones y otros fueron a parar en las cárceles.

Muchas de las investigaciones fueron publicadas en miles de redes sociales, páginas web y medios de internet, lo que hizo que se diera a conocer ante la comunidad

internacional una imagen negativa de la institución y la perdida de legitimidad de las Fuerzas Militares, en especial la del Ejército Nacional.

Figura No. 5 Imagen donde denuncian al Estado Colombiano por los Falsos Positivos, **Fuente** ONG ACNUR 2015

La inmediatez de las redes sociales facilita que cualquier ciudadano acceda a la información, los medios de comunicación en su accionar libre y sin principios éticos definidos, se han convertido en una sutil y efectiva arma para atacar la legitimidad del Ejército Nacional; las redes sociales son utilizadas por los enemigos del Estado, para aprovechar la situación coyuntural, poniendo en entre dicho el prestigio logrado por el Ejército Nacional frente a la lucha que lleva en contra de las organizaciones ilegales y grupos guerrilleros por más de 50 años.

Las redes sociales y páginas web, en muchas ocasiones son usadas para atacar a la institución a partir de errores militares o accidentes que se pueden presentar en el desarrollo de operaciones; los medios han modificando la información para desprestigiar la legitimidad institucional; en algunas oportunidades los medios sin esperar los resultados de

una investigación anuncian a través de las redes sociales informes que perjudican el quehacer militar, hasta en algunas ocasiones, se filtran datos e informaciones que pueden perjudicar la cadena de custodia, las evidencias y la judicialización de delincuentes.

La ética del periodismo afirma que las personas que emplean los medios de noticias y redes sociales no pueden alterar los hechos, ni realizar acusaciones directas en contra de los integrantes de las Fuerzas Armadas, sin las respectivas informaciones emitidas por la Fiscalía o de los entes judiciales, pero el afán de protagonismo en algunos medios, así como el interés de grupos que están en contra de las Fuerzas Armadas y hasta los intereses propios de los grupos ilegales, hace que se anuncien o se emitan informaciones equivocadas, haciendo ver de primer impacto en el televidente o el usuario de la red social, un mensaje negativo, de falta de legitimidad y de odio hacia la Institución.

Figura No. 6 Imagen donde acusan al Ejército Nacional por violación al DIH, **Fuente** noticias RCN 2017

Es muy importante que comunicaciones estratégicas y los entes encargados de la ciberdefensa, la ciberseguridad y la acción integral, pueda contrarrestar de alguna forma las informaciones o las acusaciones que se lanzan en contra del Ejército Nacional. Se debe

contrarrestar estas publicaciones para evitar que la institución sea afectada en su prestigio y ante la comunidad nacional e internacional.

VI. Acciones para lograr la Ciberdefensa y la ciberseguridad en Colombia

El Estado colombiano en el 2016, se comprometió a llevar a cabo nuevas acciones para mejorar la seguridad en entornos digitales (...) los ministerios de las TIC, de Defensa y el Departamento de Planeación Nacional presentaron el Documento Conpes 3854, que diseña la Política Nacional de Seguridad Digital hacia la seguridad de las redes de información y las bases de datos. (Peñaredonda, 2016)

El documento es una lista de acciones y políticas que las entidades del Estado estarán obligadas a llevar a cabo en los siguientes cuatro años para mejorar la seguridad en entornos digitales. Este documento reemplaza al Documento Conpes 3701 de 2011, que fijó la política de ciberseguridad hasta 2015 y creó una especie de línea de respuesta frente a las situaciones de riesgo de seguridad informática, la cual estaba a cargo del Ejército y la Policía.

Colombia, se estableció como el primer país latinoamericano en adoptar estrategias y políticas en temas referentes a la ciberseguridad y ciberdefensa, esta iniciativa gubernamental busca proteger a la ciudadanía de los riesgos informáticos, creando tres dependencias: el Grupo de Respuesta a Emergencias Cibernéticas de Colombia (Colcert), el Comando Conjunto Cibernético de las Fuerzas Militares y el Centro Cibernético Policial. (Presidencia de Colombia, 2011)

El Gobierno creó tres dependencias: (Presidencia de Colombia, 2011)

- El Grupo de Respuesta a Emergencias Cibernéticas de Colombia (Colcert), encargado de coordinar a escala nacional los aspectos de ciberseguridad y ciberdefensa.
- El Comando Conjunto Cibernético de las Fuerzas Militares, que tendrá la responsabilidad de salvaguardar los intereses nacionales en el ciberespacio.
- El Centro Cibernético Policial, que estará a cargo de la prevención e investigación y apoyará la judicialización de los delitos informáticos. Para ello, contará con un comando de Atención Inmediata Virtual (CAI Virtual), para recibir las denuncias de los ciudadanos.

Colombia ha evolucionado en los temas referentes a la seguridad y defensa en el ciberespacio, pero no cuenta con el número de personal entrenado suficiente para desempeñarse como soldados especialistas en ciberguerra y como soldados cibernéticos, así mismo no se cuenta con los equipos adecuados para la seguridad de datos y de información sensible, los nuevos retos del Gobierno colombiano deben apuntar en la preparación del personal militar, policial y civil, para contrarrestar ataques cibernéticos y en mejorar los equipos tecnológicos con que cuenta el gobierno, los organismos de control y las FF.MM, con el fin de garantizar la ciberdefensa y la ciberseguridad del Estado.

El ciberterrorismo o terrorismo electrónico es el uso de medios de tecnologías de información, comunicación, informática, electrónica o similar con el propósito de generar terror o miedo generalizado en una población, clase dirigente o gobierno, causando con ello una violencia a la libre voluntad de las personas.

Los fines pueden ser económicos, políticos o religiosos principalmente. (GITS Ciberseguridad, 2012)

Es un nuevo escenario donde no solo participan los Estados, ahora se involucran personas (hackers, crackers), grupos empresariales, industriales, grupos tecnológicos, empresas económicas, bancos y las entidades propias del sector de seguridad y defensa; de ahí la importancia que todo el personal militar esté preparado y pueda tener la capacidad de contrarrestar acciones que puedan afectar la seguridad y defensa nacional y de especializar a personal militar como hackers y de personas idóneas para contrarrestar las acciones de los malware.

A. PROPUESTA ORGANIZACIÓN DE UN COMANDO CIBERNÉTICO CON CAPACIDADES PARA CIBERDEFENSA, CIBERSEGURIDAD Y COMUNICACIONES ESTRATÉGICAS

Aunque en la actualidad existe una dependencia en el comando del Ejército con los temas referentes a la ciberdefensa y ciberseguridad, este no cubre todas las posibles áreas del ciberespacio, donde puede verse afectado la fuerza no solo en la imagen institucional si no en la misma organización, funcionalidad y la seguridad y defensa nacional.

La organización propuesta busca fortalecer las áreas referentes a comunicaciones estratégicas, seguimiento de redes sociales, la atención al usuario y la coordinación con todos los medios de comunicación, para que la información suministrada por la institución, sea verídica y corresponda a los hechos y al marco legal, no alterada y con beneficios a comandantes y terceros, se debe procurar velar por la imagen institucional y no por la imagen de un funcionario.

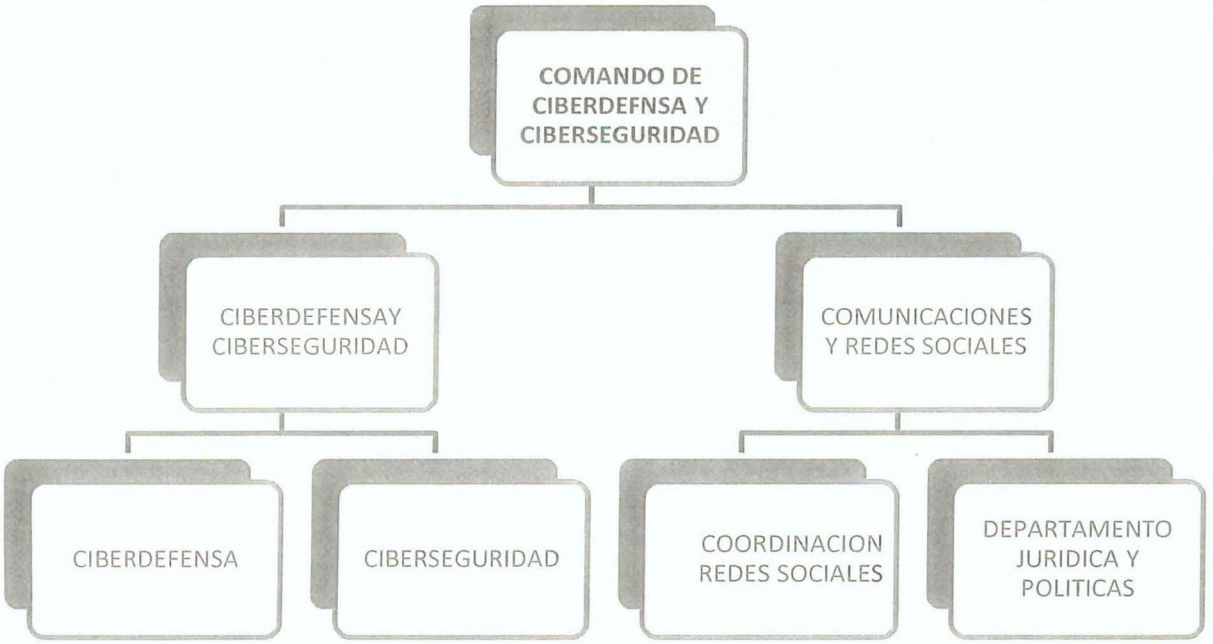

Figura No. 7 Propuesta organización del Comando de Ciberdefensa y Ciberseguridad, **Fuente** Elaboración propia

Esta propuesta de organización, permitirá mejorar las medidas preventivas y de seguridad en el ciberespacio, control en los grupos sociales, emitir políticas para los funcionarios que se encuentren dentro de la institución y para coordinar con las entidades estatales y de información que manipulan o muestran la información del Ejército Nacional.

Esta nueva organización no solo establecerá las políticas sobre los temas referentes a la ciberdefensa y ciberseguridad, todas las políticas referentes a comunicaciones estratégicas en los temas referentes a la seguridad nacional se coordinarán con esta dependencia, así mismo trabaja de manera coordinada con el Comando de acción integral en la emisión de noticias y el empleo de redes sociales

propias con el fin de acrecentar la imagen institucional y la credibilidad ante la sociedad nacional

Se deben buscar las alianzas estratégicas con organizaciones multinacionales (Facebook, Yahoo, Google, Whatsap, Instagram, Microsoft) con el fin de verificar los orígenes de la información difamatoria y perjudicial hacia la legalidad de la institución, con el fin de realizar las respectivas acciones penales y denuncias que puedan llevar cada uno de las personas que suministran ese tipo de información.

B. ARTICULACIÓN DEL COMANDO DE CIBERDEFENSA CON LA COORDINACIÓN DE CONTROL DE REDES SOCIALES Y EL COMANDO DE ACCIÓN INTEGRAL DEL EJÉRCITO

El impacto institucional que se lograría en el momento de articular las tres dependencias en procura de la legitimidad y la imagen institucional es muy positivo, se tendría un gran equipo de seguimiento y verificación en los medios y de las redes sociales, así mismo se podría evitar acciones perjudiciales en contra de la institución a partir del empleo del ciberespacio.

En la actualidad cada dirección o jefatura emite la información que considera necesaria sin que exista una estrategia adecuada de manejo de medios estandarizada, en lo referente a Ciberseguridad, se podría utilizar el ciberespacio realizando mensajes de gran impacto demostrando la legitimidad de la institución, no a partir de resultados operacionales, sino con mensajes de acercamiento hacia la población civil, demostrar los resultados positivos de las jornadas de apoyo, mostrar con imágenes los acompañamientos en proyectos sociales, las obras que se desarrollan donde permite el

desarrollo de regiones, esto demostrará una gran confianza hacia la población obteniéndose hasta las posibles denuncias de acciones ilegales.

Se debe trabajar sobre tres líneas fundamentales

- Impacto: lo que se busca de la población quiera ver
- Aceptación : grado de favorabilidad de la población
- Efecto: resultados después de la campaña

	POBLACIÓN	RED SOCIAL	CIBERESPACIO
IMPACTO	• Empleo de Imágenes favorables de acciones institucionales • Empleo de volantes y propaganda hacia la población en procura del desarrollo social de la región. • Desarrollo de obras con la participación de la población civil • Minimizar afectaciones causadas por informaciones falsas o negativas	• Empleo de redes sociales con iniciativas desarrolladas por el Ejército Nacional • Empleo de las redes sociales para denunciar acciones violatoritas al DIH y los DDHH por parte de grupos Ilegales • Imágenes de gran impacto donde se demuestre la labor del soldado en el cuidado de activos estratégicos, vías de comunicación, en el desarrollo de apoyos humanitarios, desminado entre otros.	• Cero ataques de hackers y crackers al sistema de datos del Ejercito Nacional • Creación de un Ejercito Cibernético • Poseer una barrera contrafuegos en el ciberespacio • Cero sabotajes a sistemas de defensa • Protección de instalaciones militares y de equipos técnicos
ACEPTACIÓN	• Resultados de encuestas favorables hacia la institución • Sonderos en la población civil de la imagen institucional • Evaluación de credibilidad y de legitimidad • Credibilidad de Entes de Control • Certificación por entidades defensoras de DDHH y por parte de Estados.	• Número de veces de la imagen vista • Número de veces de la imagen compartida • Cantidad de personal que le gusta la actividad	• Gran número de personal militar entrenado y capacitado. • Doctrina de ciberdefensa y ciberseguridad ejemplar y de vanguardia • Sobresalientes resultados de aceptación del personal militar por la protección de los datos

	POBLACIÓN	RED SOCIAL	CIBERESPACIO
EFECTO	• Número de denuncias recibidas por la población hacia actos ilegales y grupos ilegales • Apoyo empresa privada y de los entes de control • Apoyo de Estados en elementos de seguridad y defensa • Reducción de acciones sobre tropas y activos estratégicos del Estado.	• Número de veces de la información compartida en redes sociales • Numero de mensajes en señales de agradecimiento o de apoyo a la institución • Número de personas que ingresan a las redes sociales para ver información • Numero de organizaciones que apoya a la institución por las actividades indicadas en redes sociales	• Número de acciones evitadas por hackers y crackers contra los sistemas de datos de seguridad y defensa nacional • Número de personal entrenado y capacitado certificado por entes internacionales • Reconocimientos de otros ejércitos por la calidad operativa de los funcionarios de ciberdefensa y ciberseguridad.

Figura No. 8 Cuadro Análisis Impacto, Aceptación, Efecto, Fuente Elaboración propia

C. FUNCIONES DE LA PROPUESTA DEL COMANDO DE CIBERSEGURIDAD, CIBERDEFENSA Y PROTECCIÓN DE REDES SOCIALES

	DEPENDENCIA	FUNCIONES
1.	**Comando de ciberdefensa y ciberseguridad COCSE**	• Direcciona y controla las políticas y normas de ciberdefensa y ciberseguridad para el Ejército Nacional. • Emite las políticas para el empleo de redes sociales, plataformas, páginas web por parte de las dependencias del ejército, con el fin de evitar ataques cibernéticos, de malware y hackers • Se encarga de coordinar junto con el CEDOC la formación y entrenamiento de personal idóneo en ciberdefensa y ciberseguridad. • Proyecta la creación de un Ejército Cibernético (tomando el ejemplo de China) (GITS Ciberseguridad, 2012), para contrarrestar cualquier tipo de acción en contra de los sistemas y ordenadores • Junto con COMCI, emite las políticas de seguridad informática en el empleo de equipos, ordenadores y redes sociales. • Junto con policía judicial realiza operaciones coordinadas para atacar hackers que afecten la seguridad nacional • Junto con países amigos, organizar plataformas que aseguren la funcionalidad de los equipos de defensa y seguridad nacional.
2.	**Dirección de Ciberdefensa DICID**	• Emite las normas y políticas de seguridad informática y de protección de los equipos, sistemas, armas y operaciones que funcionan a partir de ordenadores y equipos de redes y sistemas que puedan afectar la seguridad nacional y la institución • Realiza control y seguimiento a los ordenadores, sistemas de bases de datos y equipos para evitar que sean atacados por malware, hackers o virus creados por organismos internacionales o Estados que puedan afectar la seguridad nacional. • Coordina con las unidades de inteligencia y contrainteligencia los trabajos de seguridad informáticos y de redes que permita garantizar el funciona miento de la institución y las operaciones militares

3.	**Dirección de Ciberseguridad DICSE**	• Junto con el Ministerio de las TIC, establece los parámetros de los empleos de las redes sociales, con el fin de evitar la afectación de la seguridad y defensa nacional. • Realiza campañas y capacitaciones para la seguridad de los datos y de los ordenadores de los funcionarios de la institución y de las familias del personal militar • Coordina junto con policía judicial y la fiscalía, acciones en contra de hackers, agencias o particulares que atenten contra la seguridad y defensa nacional, los activos estratégicos, servicios públicos o elementos que garanticen la seguridad humana. • Organiza los equipos de ciberseguridad a nivel División para capacitar a la población civil y personal militar.
4.	**Coordinación de control redes sociales COCRE**	• Emite políticas para el personal militar, dependencias y unidades militares para el empleo de redes sociales Facebook, twitter, instagram, entre otras, con el fin de garantizar la imagen institucional. • Realiza el seguimiento a las redes sociales externas para evitar acciones desprestigiantes o maliciosa en contra de la institución. • Recibe quejas y reclamos a través de las redes sociales en acciones donde se puedan vulnerar los Derechos humanos y el DIH • Verifica la instalación de APP y redes sociales, con el fin que cumpla las condiciones de seguridad y garanticen la imagen institucional.
5.	**Coordinación de políticas y Jurídica del ciberespacio COPCI**	• Esta oficina se encargará de poner las quejas ante los entes de control, junto con la Oficina Jurídica del Ejército, en acciones donde se vea vulnerada la imagen institucional o la misión institucional • Verifica el cumplimiento de la normatividad nacional e internacional para el empleo del ciberespacio con el fin de aplicar la normatividad de ciberdefensa y ciberseguridad • Coordina con otros estamento de control y judiciales, el cumplimiento de las normas nacionales para el empleo de las redes de este país

Figura No. 9 **Misiones Funciones de la Propuesta del Nuevo Comando**, Fuente **Elaboración propia**

CONCLUSIONES

Las redes sociales hoy en día son elementos definitivos para el impacto de la institución y para la credibilidad de funcionarios y la Fuerza, con este se puede llegar al corazón y la mente de la población y obtener de esta su apoyo y reconocimiento.

El ciberespacio será el nuevo campo de conflicto, este se encuentra dentro de las guerras de quinta generación y no será definitivo para lograr una victoria sobre un contrincante, peros si decisivo ya que los daños en las ciudades, activos estratégicos, sistemas de armas y el funcionamiento de los organismos del Estado pueden llegar a bloquearse y quedar sin servicio.

El Ejército Nacional debe fortalecer en su organización, dependencias que se encarguen en el seguimiento de las redes sociales y en el ciberespacio, con el fin de evitar el ataque por parte de virus, malware, hackers o particulares que busquen sabotear, minimizar o desprestigiar el Ejército Nacional.

El ciberespacio y las redes sociales han modificado la forma de pensar y actuar de los individuos; es por ello que actualmente tanto las redes sociales como el ciberespacio son objetos de estudio en el ámbito económico político y social lo cual conlleva que la institución profundice en este tipo de análisis logrando una ventaja estratégica para mantener y fortalecer la legitimidad en el pos acuerdo.

Las FF.MM colombianas tiene el reto de formar personal militar especializado en los campos de la ciberdefensa y la ciberseguridad, el país no está libre de ser atacado a partir de las redes de internet y de base de datos, de la afectación de los equipos de sistemas y de manufactura militar a partir de sabotajes y ataques de virus, así como de robo y hurto de bases de datos del personal militar y de la obtención de información reservada que pueda afectar la seguridad y defensa nacional.

Las FF.MM colombianas cuenta con un programa de postgrado en el campo de la ciberseguridad y la ciberdefensa, que prepara a personal militar y civil en el empleo de medidas contra el espionaje y el sabotaje a partir de las tecnologías de la Información y de la internet, pero este no puede quedarse solo inmerso como una actividad académica, las FF.MM debe iniciar la cultura desde las escuelas de formación en el entrenamiento militar para la ciberdefensa y la ciberseguridad, a partir de un currículo que sea el ciberespacio el área de entrenamiento y que las herramientas o medios de trabajo sean las tecnologías de la información y la comunicación.

Recomendaciones

Fortalecer el Comando de Acción Integral a través de funcionarios que manejen las bases de datos y las redes sociales, con el fin de fortalecer la imagen institucional, garantizar la legitimidad del Ejército Nacional y contrarrestar las acciones perjudiciales y negativas de organizaciones y particulares externos a la institución.

Se debe preparar personal militar en el manejo de redes sociales y comunicación estratégica, ciberdefensa y ciberseguridad y en manejo de redes de datos, los cuales con su conocimiento evitarán acciones de sabotaje, ataques de hackers y de grupos ilegales.

Se debe articular la ciberdefensa y la ciberseguridad con las comunicaciones estratégicas, los mejores resultados que garanticen la legitimidad y la protección de la institución se podrán obtener a partir del eficaz y eficiente empleo de las redes de datos, el uso de las redes sociales y del ciberespacio.

En tanto se crea el comando de ciber defensa y ciber seguridad como lo pretende el presente trabajo es pertinente que se elabore un protocolo estandarizado para que los comandos a todo nivel tengan una herramienta adecuada para una posible solución de acciones en contra de la institución

Referencias

Altonivel. (09 de Diciembre de 2010). *La historia detrás de WikiLeaks.* Recuperado el 20 de Junio de 2017, de http://www.altonivel.com.mx/7291-la-historia-detras-de-wikileaks.html

Carrasco, D. (25 de Abril de 2016). *"Panamá Papers" y su impacto sobre la economía.* Recuperado el 20 de Junio de 2017, de http://bayanodigital.com/economia/panama-papers-y-su-impacto-sobre-la-economia/

Castells, M. (2012). *el poder de la era de las redes sociales.* Mexíco: nexos.

Centro de estudios Estrategicos Academia de Guerra de Chile. (09 de Diciembre de 2015). *La Guerra Irrestricta y una nueva definición del concepto "Guerra".* Recuperado el 21 de Mayo de 2017, de http://www.ceeag.cl/index.php/2015/12/09/la-guerra-irrestricta-y-una-nueva-definicion-del-concepto-guerra/

Comisión de regulación de Comunicaciones. (2009). *Resolución CRC 2258* . Bogotá: Comisión de regulación de Comunicaciones.

Fojón, E., & Sanz, Á. (2010). *Ciberseguridad en España: una propuesta para su gestión.* Madrid: Análisis del Real Instituto Elcano, ARI N° 101.

Gits Ciberseguridad. (Marzo de 2016). *Ciberguerra, Ciberespionaje, Ciberterrorismo y Ciberdefensa.* Recuperado el 20 de Junio de 2017, de ¿Estamos preparados? Cibersoldados, Nanotecnología para la guerra, Drones, Derecho Internacional y Legislación.: http://www.gitsinformatica.com/ciberguerra.html

GITS Ciberseguridad. (S.D. de S.D de S.D). *Ciberguerra, Ciberespionaje, Ciberterrorismo y Ciberdefensa.* Recuperado el 22 de Mayo de 2017, de http://www.gitsinformatica.com/ciberguerra.html#echeloncw

Hola.com. (29 de Noviembre de 2010). *La historia de WikiLeaks: filtraciones, documentos secretos y relaciones internacionales.* Recuperado el 20 de Junio de 2017, de http://www.hola.com/actualidad/2010112950140/claves/filtracion/WikiLeaks/

Instituto Español de Estudios Estrátegicos. (14 de Febrero de 2014). *CIBERGUERRA, LOS ESCENARIOS DE CONFRONTACIÓN.* Recuperado el 20 de Junio de 2017, de http://www.ieee.es/Galerias/fichero/docs_opinion/2014/DIEEEO18-2014_Ciberguerra_EscenariosConfrontacion_EguskineLejarza.pdf

La República. (03 de Abril de 2016). *Qué son los Panamá Papers? Conoce los detalles de la mayor filtración de datos de la historia.* Recuperado el 20 de Junio de 2017, de http://larepublica.pe/mundo/757189-que-son-los-panama-papers-conoce-los-detalles-de-la-mayor-filtracion-de-datos-de-la-historia

Ministerio de Defensa Nacional. (2014). *Ciberdefensa y Ciberseguridad.* Bogotá: MINDEFENSA.

Owens, D., & Lin. (2009). *Los Ciberataques y la Guerra cibernetica.* Cambridge: Cambridge University.

Peñaredonda, J. L. (13 de Abril de 2016). *COLOMBIA TIENE UNA NUEVA POLÍTICA NACIONAL DE CIBERSEGURIDAD.* Recuperado el 20 de Junio de 2017, de http://www.enter.co/cultura-digital/colombia-digital/colombia-tiene-una-nueva-politica-nacional-de-ciberseguridad/

Presidencia de Colombia. (14 de Julio de 2011). *Colombia, primer país latinoamericano en adoptar estrategia de ciberseguridad y ciberdefensa.* Recuperado el 20 de Junio de 2017, de http://wsp.presidencia.gov.co/Prensa/2011/Julio/Paginas/20110714_06.aspx

Prieto Oses, R. (S.D. de Abril de 2013). Grupo de Trabajo nº 3 XXXIII CURSO DE DEFENSA NACIONAL. *Guerra Cibernética: Aspectos Organizativos.* Bogotá, Distrito Capital, Colombia: CESEDEN.

Rain, O., & Lorents, P. (2010). *Cyberspace: Definitions and Implications.* Tallin, Estonia: Cooperativa Cyber Defence Centre of Excellence.

Reguera Sánchez, J. (14 de Junio de 2015). *Aspectos legales en el ciberespacio. La ciberguerra y el Derecho Internacional Humanitario.* Recuperado el 20 de Mayo de 2017, de http://www.seguridadinternacional.es/?q=es/content/aspectos-legales-en-el-ciberespacio-la-ciberguerra-y-el-derecho-internacional-humanitario

Reguera, J. (18 de Marzo de 2015). *Aspectos legales en el ciberespacio.* Recuperado el 29 de Mayo de 2017, de http://www.seguridadinternacional.es/?q=es/content/aspectos-legales-en-el-ciberespacio-la-ciberguerra-y-el-derecho-internacional-humanitario

Sain, G. (Febrero de 2016). *¿Que es la ciberguerra?* Recuperado el 29 de Mayo de 2017, de Revista Pensamiento Legal: http://www.pensamientopenal.com.ar/system/files/2016/02/doctrina42952.pdf

Sánchez Alvarez, A. (21 de Marzo de 2016). *Ciberseguridad en China: desafíos del siglo XXI.* Recuperado el 20 de Junio de 2017, de /mo simposio internacional sobre politica China: http://www.politica-china.org/imxd/noticias/doc/1458147464Ana_Sanchez.pdf

Sánchez Medero, G. (2008). Ciberguerra y Ciberterrorismo ¿realidad o ficción? *AMÉRIGO CUERVO-ARGANGO*, 15.

Sánchez Medero, G. (Septiembre - Noviembre de 2012). *La ciberguerra: los casos de Stuxnet y Anonymous*. Recuperado el 29 de Mayo de 2017, de Derecom: https://dialnet.unirioja.es/descarga/articulo/4331298.pdf

Scheinsohn, D. (2011). *Poder y Acción a través de la comunicación estratégica.* Bogotá: Garnica.

Silva, L. (S.D. de Septiembre de 2010). *¿Qué es la guerra irrestricta?* Recuperado el 20 de Mayo de 2017, de Leopoldo Silva Blog: http://leopoldosilva.blogspot.com.co/2010/09/que-es-la-guerra-irrestricta.html

Szentkereszty de Zagón, I. (2015). Ciberespacio y Ciberguerra. *Revista de seguridad y defensa Nacional* (pág. 15). Bogotá: Escuela Superior de Guerra.

Tecnologia, el País. (15 de Mayo de 2017). *El ataque de 'ransomware' se extiende a escala global.* Recuperado el 12 de Junio de 2017, de http://tecnologia.elpais.com/tecnologia/2017/05/12/actualidad/1494586960_025438.html

Tabla de Ilustraciones