Lineamientos doctrinales en Operaciones Militares Cibernéticas

Samira Andrea Ramos Rodríguez

Trabajo de grado para optar al título profesional:

Maestría en Ciberseguridad y Ciberdefensa

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

2018

MINISTERIO DE DEFENSA NACIONAL

COMANDO GENERAL FUERZAS MILITARES

ESCUELA SUPERIOR DE GUERRA

LINEAMIENTOS DOCTRINALES EN OPERACIONES MILITARES CIBERNÉTICAS

ALUMNO: SAMIRA ANDREA RAMOS RODRÍGUEZ

DIRECTOR: STEVE JONES CHALJUB

MAESTRIA EN CIBERSEGURIDAD Y CIBERDEFENSA

TRABAJO DE GRADO PARA OPTAR EL TITULO DE MAGISTER EN CIBERSEGURIDAD Y CIBERDEFENSA

BOGOTA – COLOMBIA

2018

Nota de aceptación:

_____

_____

_____

_____

_____

_____

_____

Firma del presidente del jurado

_____

Firma del jurado

_____

Firma del

Bogotá D.C., Mayo de 2018

Agradecimientos

Primeramente, agradezco al Ministerio de Tecnologías de la Información y Comunicaciones por el apoyo educativo brindado a funcionarios del sector público y de las Fuerzas Militares en particular, impulsando con ello los caminos de formación y de conocimiento en materia de seguridad digital, coadyuvando al fortalecimiento de la ciberseguridad y ciberdefensa del ciberespacio colombiano.

Agradezco también a la Escuela de Guerra de las FF. MM de Colombia, por haber estructurado y llevado a cabo este integral y formador programa de maestría, así como a mi amado Ejército Nacional a través del cual pude aplicar y extraer las mejores experiencias en materia cibernética, a mis superiores y subalternos por su apoyo al permitirme participar infaltablemente al programa en su totalidad.

Finalmente a mi asesor por haberme brindado la oportunidad de recurrir a su guía y conocimiento y a mis familiares por su apoyo moral, el cual me impulso a seguir adelante en mi carrera profesional.

Resumen

Las operaciones cibernéticas militares OCs consisten en el empleo de un conjunto de capacidades en el ciberespacio, utilizadas para la defensa y protección de las redes, sistemas y activos informáticos propios, a fin de garantizar la libertad de acción en la conducción de operaciones militares en el dominio del ciberespacio y la superioridad militar en este. Tal como las operaciones tradicionales (tierra, mar y aire), estas se encuentran enmarcadas en un proceso sistemático: planeamiento, preparación, ejecución y evaluación, se basan en una serie de principios como lo son los de efecto, disimulación, rastreabilidad y adaptabilidad y se dan en los tres niveles del mando: estratégico, operacional y táctico. Las OCs operan en el entorno del ciberespacio, el cual cuenta con unas características intrínsecas de asimetría, así como una rápida y continua evolución por la influencia de las tecnologías de la Información y las Comunicaciones. El entorno operacional de las OCs está compuesto de una serie de capas que van desde el nivel físico al lógico, y en donde en cada una de ellas emergen una serie de amenazas, muchas de las cuales deben ser afrontadas a través de OCs. Para ello las Fuerzas Militares deberán desarrollar tres capacidades en el ciberespacio: defensa, explotación y respuesta. Bajo este marco se deben realizar acciones deliberadas para obtener la superioridad militar en el ciberespacio y negarle esta al adversario, a fin de garantizar la seguridad y defensa de la nación. Los tipos de operaciones cibernéticas a ser empleadas por parte de las FF.MM, deben estar orientadas a desarrollar las tres capacidades en el entorno operacional del dominio del ciberespacio. Las operaciones defensivas, la ciberinteligencia y las operaciones ofensivas (ciberataque), permitirá hacer frente a las nuevas amenazas que atentan contra la infraestructura crítica cibernética nacional, así como contar con personal militar con habilidades en la nueva Fuerza multimisión requerida en el proceso de transformación y los nuevos

escenarios bélicos y de paz que se están viendo materializados en la actualidad.

Palabras clave: Ciberespacio, ciberseguridad, entorno operacional cibernético, Operaciones cibernéticas.

Abstract

The military cyber operations OCs consist of the use of a set of cyberspace capabilities, used for the defense and protection of their own networks, systems and IT assets, in order to guarantee freedom of action in the conduct of military operations in the Mastery of cyberspace and military superiority in this. As traditional operations (land, sea and air), these are framed in a systematic process: planning, preparation, execution and evaluation, are based on a series of principles such as effect, dissimulation, traceability and adaptability, and Are given in the three levels of command: strategic, operational and tactical. The OCs operate in the cyberspace environment, which has intrinsic characteristics of asymmetry, as well as a rapid and continuous evolution by the influence of Information and Communication Technologies. The operational environment of the CBs is composed of a series of layers ranging from the physical to the logical level, and where in each of them a series of threats emerge, many of which must be addressed through CBs. For this, the Military Forces must develop three capacities in cyberspace: defense, exploitation and response. Under this framework deliberate actions must be taken to obtain military superiority in cyberspace and deny this to the adversary, in order to guarantee the security and defense of the nation. The types of cyber operations to be employed by the FFM should be aimed at developing the three capabilities in the operational environment of the cyberspace domain. Defensive operations, cyber intelligence and offensive operations (cyberattack) will enable to face new

threats against the national cybernetic infrastructure, as well as, to have military personnel with skills in the new multi-mission force required in the transformation process and the new war and peace scenes that are being materialized currently.

Keywords. Cyberspace, cybersecurity, cybernetic operating environment, cybernetic operations.

Contenido

Abreviaturas, siglas y acrónimos

BCP	Bussiness continuity plan
CERT	Computer Emergency Response Team
CSC	Conciencia situacional del ciberespacio
EVATAC	Evaluación táctica
EVAOP	Evaluación operacional
EPM	Pulso electromagnético
FIRST	Forum on Incident Response Teams
ICC	Infraestructura crítica cibernética
ME	Medidas de efectividad
MR	Medidas de rendimiento
OC	Operaciones Cibernéticas
OCD	Operaciones cibernéticas de defensa
OCDA	Operaciones cibernéticas de defensa activa
OCAS	Operaciones cibernéticas de Administración de ciberseguridad
OCO	Operaciones cibernéticas ofensiva
OE	Entorno Operacional
PRODOC	Proceso de Operaciones

Glosario

Acciones Preventivas: Tienen como misión principal la prevención de los ataques antes de que ocurran y abarca el despliegue de recursos de manera óptima para mejorar la seguridad de la red y la implementación de planes de mitigación (parches, actualizaciones, etc.,). (Escuela Superior de Guerra, 2015. *Diplomado de Ciberseguridad y Ciberdefensa* [ppt]).

Acciones Reactivas: son las acciones en tiempo real a realizar como respuesta a incidentes de seguridad. Los cursos de acción generados podrán ser de una manera totalmente automática, sin intervención del operador, o de una manera semiautomatizada, donde opciones se presentan para la selección y aprobación del operador. (Escuela Superior de Guerra. 2015. *Diplomado de Ciberseguridad y Ciberdefensa* [ppt]).

Amenaza: La posibilidad de compromiso, pérdida o robo de información clasificada o de servicios y recursos que la soportan. Una amenaza puede ser definida por su origen, motivación o resultado y puede ser deliberada o accidental, violenta o subrepticia, externa o interna. (Revista de la OTAN. 2011. *Nuevas amenazas: el ciberespacio.* Recuperado de https://www.nato.int/docu/review/2011/11-september/Cyber-Threads/ES/index.htm).

Amenaza informática: La aparición de una situación potencial o actual donde un agente tiene la capacidad de generar una agresión cibernética contra la población, el territorio y la organización política del Estado. (Ministerio de Defensa de Colombia. 2016. *Manual de ciberdefensa conjunta para las FF.MM.,* p. 97).

Ataque cibernético: Acción organizada y/o premeditada de una o más personas para causar daño o problemas a un sistema informático a través del ciberespacio. ((Ministerio de Defensa de Colombia. 2016. *Manual de ciberdefensa conjunta para las FF.MM.,* p. 97).

Brecha de seguridad: Una acción u omisión, deliberada o accidental, contraria a la Política de Seguridad de la OTAN o normativas de aplicación de la Política que resulte en un compromiso real o potencial de información clasificada OTAN o los servicios y recursos que la soportan. (Revista de la OTAN. 2011. *Nuevas amenazas: el ciberespacio.* Recuperado de https://www.nato.int).

Botnets: Los botnets (robots de la Red) son redes de ordenadores zombis. Las redes han aumentado de modo exponencial, según informes de la Fundación Shadowserver y se emplean para realizar ataques, envíos masivos de correo basura y espionaje contra empresas. Un botnet se crea infectando ordenadores sin que sus propietarios lo sepan. Cada máquina reclutada por el virus se pone en contacto sigilosamente con el cibercriminal a la espera de sus órdenes. (Instituto Español de Estudios Estratégicos. 2010. *Cuaderno de estrategia 149 Ciberseguridad retos y amenazas a la ciberseguridad nacional en el ciberespacio.* España: Imprenta del Ministerio de Defensa).

CSIRT: (Computer Security Incident Response Team) Equipo de Respuesta a Incidentes de Seguridad cibernética, por su sigla en inglés. Es una capacidad o equipo que ofrece servicios y apoyo a las partes interesadas definidas para la prevención, manejo y respuesta a incidentes de seguridad informática. Así mismo, se hace necesario hacer distinciones entre el "Grupo de

Seguridad", "CSIRT Interno" y "CSIRT Coordinador". (European Union Agency for Network and Information Security ENISA. 2006. *Cómo crear un CSIRT paso a paso.* Recuperado de https://www.enisa.europa.eu/publications/csirt...up.../fullReport).

Ciberespacio: Es 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. (Comando General de las FF.MM. *Directiva Permanente No. 101/CGFM-JEMC-CCOC-29.52.* Bogotá D.C).

Ciberdefensa: Es la capacidad del Estado para prevenir, detectar y neutralizar toda amenaza o acto hostil de naturaleza cibernética que afecte la soberanía nacional, independencia, integridad y orden constitucional. (Comando General de las FF.MM. *Directiva Permanente No. 101/CGFM-JEMC-CCOC-29.52.* Bogotá D.C).

Ciberseguridad: Es el conjunto de herramientas, políticas, conceptos de seguridad, salvaguardas, directrices, métodos de gestión de riesgos, acciones de prevención, investigación y atención del delito, formación, prácticas idóneas, seguros y tecnologías que pueden usarse para proteger los activos informáticos y los usuarios en el ciberespacio. (Comando General de las FF.MM. *Directiva Permanente No. 101/CGFM-JEMC-CCOC-29.52.* Bogotá D.C).

Cibercrimen/Ciberdelincuencia: Conjunto de actividades ilegales asociadas con el uso de las tecnologías de la información y las comunicaciones, como fin o como medio, que atenten contra la integridad, disponibilidad y confidencialidad de la información, los datos y los sistemas

informáticos. (Comando General de las FF.MM. *Directiva Permanente No. 101/CGFM-JEMC-CCOC-29.52.* Bogotá D.C).

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, bien porque sea el sistema informático (o sus datos) el objetivo del delito. (Comando General de las FF.MM. *Directiva Permanente No. 101/CGFM-JEMC-CCOC-29.52.* Bogotá D.C).

Cibernética: 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. (Real Academia de la Lengua Española. Recuperado de http://www.rae.es/search/node/cibernetica).

Cibernético: Adjetivo masculino y femenino para denominar todo cuanto tiene relación con la cibernética: órgano cibernético, proceso cibernético o que está especializado en cibernética, así como también a la persona que se dedica a ella. (Real Academia de la Lengua Española. Recuperado de http://www.rae.es/search/node/cibernetico).

CiberTerrorismo: Un ciberataque para causar la inutilización o interrupción de redes de ordenadores o comunicaciones para generar temor o intimidar a la sociedad con un objetivo ideológico. (Instituto Español de Estudios Estratégicos. 2010. *Cuaderno de estrategia 149 Ciberseguridad retos y amenazas a la ciberseguridad nacional en el ciberespacio.* España: Imprenta del Ministerio de Defensa).

Ciberinteligencia: mediante el uso de medios informáticos, la recopilación de información de los sistemas TIC, de potenciales adversarios u objetivos mediante la consulta de fuentes abiertas, la realización de espionaje con malware tipo APT y la aplicación de técnicas de ingeniería social. (Escuela Superior de Guerra, 2015. *Diplomado de Ciberseguridad y Ciberdefensa* [ppt]).

Ciberguerra: El concepto de ciberguerra es el de guerra llevada al dominio del ciberespacio. (Escuela Superior de Guerra, 2015. *Diplomado de Ciberseguridad y Ciberdefensa* [ppt]).

Ciberataque: Forma de ciberguerra / ciberterrorismo donde combinado con un ataque físico o no se intenta impedir el empleo de los sistemas de información del adversario o el acceso la misma. (Instituto Español de Estudios Estratégicos. 2010. *Cuaderno de estrategia 149 Ciberseguridad retos y amenazas a la ciberseguridad nacional en el ciberespacio.* España: Imprenta del Ministerio de Defensa).

Código Dañino o Malicioso: Software capaz de realizar un proceso no autorizado sobre un sistema con un deliberado propósito de ser perjudicial. (Malware. Recuperado de http://www.alerta-antivirus.es/seguridad/ver_pag.html?tema=S).

Control: Medios para manejar el riesgo; incluyendo políticas, procedimientos, lineamientos, prácticas o estructuras organizacionales, las cuales pueden ser administrativas, técnicas, de gestión o de naturaleza legal. (Comando General de las FF.MM. *Directiva Permanente No. 101/CGFM-JEMC-CCOC-29.52.* Bogotá D.C).

Capacidad. Es el conjunto de factores (Sistema de armas, infraestructura, personal y medios de apoyo logístico) asentados sobre la base de unos principios y procedimientos doctrinales que pretenden conseguir un determinado efecto militar a nivel estratégico, operacional o táctico, para cumplir las misiones asignadas. (Ministerio de Defensa de Colombia. 2016. *Manual de ciberdefensa conjunta para las FF.MM.,* p. 97).

Capacidad de ciberdefensa. Es el conjunto de sistemas, infraestructura personas, medios de apoyo y procedimientos doctrinales, que permiten cumplir con la misión de defender también el ciberespacio. (Ministerio de Defensa de Colombia. 2016. *Manual de ciberdefensa conjunta para las FF.MM.,* p. 97).

Capacidades Respuesta: Medidas y acciones a tomar ante amenazas o para mitigar los efectos de los ataques. (Escuela Superior de Guerra, 2015. *Diplomado de Ciberseguridad y Ciberdefensa* [ppt]).

Defensa Activa: son las acciones tomadas para planear, dirigir, ejecutar y evaluar ciberataques en orden restablecer el control sobre un sistema o neutralizar el origen del ataque. (Ministerio de Defensa de Colombia. 2016. *Manual de ciberdefensa conjunta para las FF.MM.,* p. 74).

Defensa Pasiva: Acciones tendiente a poner defensas, guardas, pero no se toma ninguna acción, confiar en la resistencia para agotar al adversario por agotamiento o disuasión. (Centro superior de

estudios Ministerio de Defensa España. 2012. *Monografía 126 El Ciberespacio nuevo escenario de confrontación*. España: Imprenta del Ministerio de Defensa).

Defensa Reactiva: Son las acciones que se deben ejecutar una vez que se haya producido el ataque del enemigo, diferentes en función de si este ha tenido éxito o no. Serán las acciones encaminadas a la recuperación y aumento de la disponibilidad de los sistemas o averiguar en qué sistemas se ha producido un daño o robo de información, cómo ha sucedido y poner los medios para evitar su repetición. (Centro superior de estudios Ministerio de Defensa España. 2012. *Monografía 126 El Ciberespacio nuevo escenario de confrontación*. España: Imprenta del Ministerio de Defensa).

DDoS: Los ataques DDoS (Distributed Denial of Service) son una forma relativamente sencilla y efectiva de hacer caer a una Web. Las acciones se pueden realizar de forma voluntaria siguiendo las instrucciones dadas para iniciar el ataque a una hora señalada en una convocatoria mediante foros en la Red o utilizando redes de ordenadores previamente infectados por virus (botnet) de forma que los usuarios ni siquiera son conscientes de que participan. Los ataques DDoS no siempre tienen un trasunto ideológico. Cada vez más responden a puras extorsiones. Se están trasladando a Internet los mismos esquemas que empleaba la mafia en el mundo físico. (Instituto Español de Estudios Estratégicos. 2010. *Cuaderno de estrategia 149 Ciberseguridad retos y amenazas a la ciberseguridad nacional en el ciberespacio.* España: Imprenta del Ministerio de Defensa).

Detectar: Cualquier observación de actividades maliciosas o sospechosas y cualquier recopilación de información que proporciona información sobre las amenazas de seguridad actuales o riesgos.

(Centro superior de estudios Ministerio de Defensa España. 2012. *Monografía 126 El Ciberespacio nuevo escenario de confrontación*. España: Imprenta del Ministerio de Defensa.).

Disponibilidad: Sistema tanto hardware como software, se mantienen funcionando eficientemente y es capaz de recuperarse rápidamente en caso de fallo. (Escuela Superior de Guerra, 2015. *Diplomado de Ciberseguridad y Ciberdefensa* [ppt]).

Explotación: es el objetivo es explotar las vulnerabilidades identificadas en el análisis previo para intentar obtener el acceso de nivel de administrador de los sistemas objetivo, o de otro tipo de acceso en cuentas de usuario, para a continuación, lanzar ataques contra otros sistemas de la Red desde el host que se ha visto comprometido. Si es posible, se instala un conjunto de herramientas en los hosts bajo control para acceder a otras máquinas y conocer sus vulnerabilidades. (Centro superior de estudios Ministerio de Defensa España. 2012. *Monografía 126 El Ciberespacio nuevo escenario de confrontación*. España: Imprenta del Ministerio de Defensa).

Exploit: Pieza de software, un fragmento de datos, o una secuencia de comandos con el fin de automatizar el aprovechamiento de un error, fallo o vulnerabilidad, a fin de causar un comportamiento no deseado o imprevisto en los programas informáticos, hardware, o componente electrónico (por lo general computarizado). . (Instituto Español de Estudios Estratégicos. 2010. *Cuaderno de estrategia 149 Ciberseguridad retos y amenazas a la ciberseguridad nacional en el ciberespacio.* España: Imprenta del Ministerio de Defensa).

Evento Informático: Cualquier suceso observable en un sistema de información y comunicaciones. (Revista de la OTAN. 2011. *Nuevas amenazas: el ciberespacio.* Recuperado de https://www.nato.int).

Equipo Rojo: Arte de aplicar un pensamiento estructurado, independiente y crítico, además de sensible a alternativas culturales, desde diferentes perspectivas, para cuestionar los supuestos propios y analizar a fondo los resultados potenciales, con el fin de reducir los riesgos y aumentar las oportunidades. (Centro superior de estudios Ministerio de Defensa España. 2012. *Monografía 126 El Ciberespacio nuevo escenario de confrontación*. España: Imprenta del Ministerio de Defensa).

Eficacia: Capacidad de lograr el efecto que se desea o se espera. (Real Academia de la Lengua Española. Recuperado de http://www.rae.es/search/node/eficacia).

Integridad: la propiedad de salvaguardar la exactitud e integridad de los activos. (Real Academia de la Lengua Española. Recuperado de http://www.rae.es/search/node/integridad).

Función de conducción. Es un grupo de tareas y sistemas (personas, organizaciones, información y procesos) unidos por un propósito común que los comandantes utilizan para llevar a cabo las misiones y cumplir con los objetivos. Las fuerzas utilizan las funciones para generar poder de combate. (Ejército de Colombia, 2013, *Libro estructural CEDEF,* Bogotá D.C).

Gestión del Riesgo: Aproximación sistemática, basada en la valoración de las amenazas y las vulnerabilidades, para la determinación de las contra-medidas necesarias para la protección de la información o los servicios y recursos que la soportan. (Departamento Nacional de Planeación. 2016. *Lineamientos para la administración del riesgo en los procesos del DNP.* Bogotá D.C.)

Gestión de Incidentes: Definimos la gestión de incidentes como un servicio que involucra a todos los procesos o tareas asociadas con el "Manejo" de eventos e incidentes. (SOC-CCOC)

Honeypot: Es un software o a un grupo de ordenadores cuyo objetivo es atraer a potenciales atacantes, simulando ser sistemas vulnerables o débiles a los ataques. Es una herramienta de seguridad informática utilizada para recoger información sobre los atacantes y sus técnicas. (Centro superior de estudios Ministerio de Defensa España. 2012. *Monografía 126 El Ciberespacio nuevo escenario de confrontación*. España: Imprenta del Ministerio de Defensa).

Incidente Informático: Cualquier evento adverso real o sospechado en relación con la seguridad de sistemas de computación o redes de computación. (Carniege Mello University. *CSIRT ask frequently.* Recuperado de http://www.cert.org/csirts/csirt_faq.html CERT/CC).

Infraestructuras críticas: Es 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 CRC. 2009. *Resolución CRC 2258 de 2009.* Recuperado de http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=38498).

Internet de las Cosas: la reunión de personas, procesos, datos y cosas para hacer conexiones en red más relevantes y valiosas que nunca, convirtiendo la información en acciones que crean nuevas capacidades, experiencias más ricas, y oportunidades económicas sin precedentes para las empresas, los individuos y los países. (CISCO. *Internet of Everything.* Recuperado de CISCO http://www.cisco.com/web/ES/campaigns/internet-de-las-cosas/index.html).

Integridad: Capacidad que garantiza que la información no sea modificada, incluyendo su creación y borrado, solo por el personal autorizado, no solo se refiere a modificaciones intencionadas, sino también a cambios accidentales o no intencionados. (Escuela Superior de Guerra, 2015. *Diplomado de Ciberseguridad y Ciberdefensa* [ppt]).

IP (Internet Protocol): Etiqueta numérica que identifica, de manera lógica y jerárquica, a una interfaz (elemento de comunicación/conexión) de un dispositivo (habitualmente una computadora) dentro de una red que utilice el protocolo IP. (International Organization for Standardization, Recuperado de http://www.iso.org).

Malware: Tipo de software que tiene como objetivo infiltrarse o dañar una computadora o sistema de información, sin el consentimiento de su propietario, ejemplo: virus, troyanos, gusanos, rootkits, scareware, spyware, adware, crimeware. (Wikipedia. *Malware.* Recuperado de https://es.wikipedia.org/wiki/Malware).

Ofensiva: Capacidad para conocer al adversario, tomar la iniciativa para atacar y tener posibilidades de contraatacar. En las operaciones ofensivas se encuentra: Ciberespionaje y Ciberataque. (Centro superior de estudios Ministerio de Defensa España. 2012. *Monografía 126 El Ciberespacio nuevo escenario de confrontación*. España: Imprenta del Ministerio de Defensa).

Operaciones Cibernéticas: Acciones tomadas de forma deliberada para obtener la superioridad en la información y denegarle esta al enemigo, combinada con la guerra electrónica, se utiliza para interrumpir, perturbar, inutilizar, degradar o engañar los Sistemas de Mando y Control, anulando su capacidad para tomar decisiones con eficacia y oportunidad, preservando a la vez los Sistemas de Mando y Control propios y amigos. (Centro superior de estudios Ministerio de Defensa España. 2012. *Monografía 126 El Ciberespacio nuevo escenario de confrontación*. España: Imprenta del Ministerio de Defensa).

Ofuscación de la información: proceso de encubrir la información haciéndola más confusa de leer e interpretar. Es distinto de la criptografía, en la cual los mensajes y la información se cifran. (Centro superior de estudios Ministerio de Defensa España. 2012. *Monografía 126 El Ciberespacio nuevo escenario de confrontación*. España: Imprenta del Ministerio de Defensa).

Phishing: Los ataques de «phishing» usan la ingeniería social para adquirir fraudulentamente de los usuarios información personal (principalmente de acceso a servicios financieros). Para alcanzar al mayor número posible de víctimas e incrementar as sus posibilidades de éxito, utilizan el correo basura («spam») para difundirse. Una vez que llega el correo al destinatario, intentan engañar a los usuarios para que faciliten datos de carácter personal, normalmente conduciéndolos a lugares

de Internet falsificados, páginas web, aparentemente oficiales, de bancos y empresas de tarjeta de crédito que terminan de convencer al usuario a que introduzca datos personales de su cuenta bancaria, como su número de cuenta, contraseña, número de seguridad social, etc. (Malware. Recuperado de http://www.alerta-antivirus.es/seguridad/ver_pag.html?tema=S).

Respuesta a Incidentes: las medidas adoptadas para resolver o mitigar un incidente, coordinar y difundir información, e implementar estrategias de seguimiento para evitar que el incidente vuelva a ocurrir. (Ministerio de Defensa de Colombia- SOC Comando Conjunto Cibernético).

Resiliencia: Capacidad de un material, mecanismo o sistema para recuperar su estado inicial cuando ha cesado la perturbación a la que había estado sometido. (Real Academia de la Lengua Española. Recuperado de http://www.rae.es/search/node/resiliencia).

Riesgo Informático: Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. (International Organization for Standardization. *ISO Guía 73:2002.*Recuperado de http://www.iso.org).

Rootkit: Es una herramienta que sirve para ocultar actividades ilegítimas en un sistema. Una vez que ha sido instalado, permite al atacante actuar con el nivel de privilegios del administrador del equipo. Está disponible para una amplia gama de sistemas operativos. (Malware. Recuperado de http://www.alerta-antivirus.es/seguridad/ver_pag.html?tema=S).

Seguridad Lógica: Consiste en la aplicación de barreras que resguarden el acceso a los datos y sólo se permite acceder a ellos a las personas autorizadas. (International Organization for Standarditazion. *Seguridad de la información.* Recuperado de http://www.segu-info.com).

SOC: (Security Operation Center): Encargado de ofrecer servicios para prevenir, gestionar y responder a incidentes de seguridad de la información que se presenten a operadores de la infraestructura crítica (PIC) de empresas públicas y privadas de Colombia. (Comando General de las FF.MM. *Directiva Permanente No. 101/CGFM-JEMC-CCOC-29.52.* Bogotá D.C).

Spam: Correo basura Correo electrónico no deseado que se envía aleatoriamente en procesos por lotes. Es una extremadamente eficiente y barata forma de comercializar cualquier producto. La mayoría de usuarios están expuestos a este correo basura, más del 80% de todos los e-mails son correos basura. No es una amenaza directa, pero la cantidad de e-mails generados y el tiempo que lleva a las empresas y particulares relacionarlo y eliminarlo, representa un elemento molesto para los usuarios de Internet. [*Spam*. Recuperado dehttp://www.alerta-antivirus.es/seguridad/ver_pag.html?tema=S].

Spyware: Código dañino diseñado habitualmente para utilizar la estación del usuario infectado con objetivos comerciales o fraudulentos como puede ser mostrar publicidad o robo de información personal del usuario. (Centro Criptológico Nacional. 20026. *Guía STIC 400:2006*).

Telecomunicaciones: Toda transmisión y recepción de signos, señales, escritos, imágenes y sonidos, datos o información de cualquier naturaleza por hilo, radiofrecuencia, medios ópticos u

otros sistemas electromagnéticos. (Ministerio de Tecnologías de la información y comunicaciones. 2010, *Resolución MinTIC 202 de 2010*).

TIC (Tecnologías de la Información y las Comunicaciones): Conjunto de recursos, herramientas, equipos, programas informáticos aplicaciones, redes y medios; que permiten la compilación, procesamiento, almacenamiento, transmisión de información como voz, datos, texto, video e imágenes. (Ministerio de Tecnologías de la información y comunicaciones. 2009. *Ley 1341/2009 TIC*).

Troyano – Caballo de Troya: Introducción subrepticia en un medio no propicio, con el fin de lograr un determinado objetivo. Diccionario de la Lengua Española. Vigésimo segunda edición. Programa que no se replica ni hace copias de sí mismo. Su apariencia es la de un programa útil o inocente, pero en realidad tiene propósitos dañinos, como permitir intrusiones, borrar datos, etc. (Centro Criptológico Nacional. 20026. *Guía STIC 430:2006*).

Virus: Un virus de computadora o un gusano de computadora es un programa de software malicioso que puede auto replicarse en computadoras o redes computacionales, sin que usted sepa que su equipo se ha infectado. (Kaspersky. *Gusanos informáticos: cómo protegerse.* Recuperado de http://latam.kaspersky.com/co/internet-security-center/threats/viruses-worms).

Violación de Políticas de Seguridad: Cualquier incumplimiento accidental generado por un ente externo o interno de la política predeterminada de seguridad de la información de una entidad. (Ministerio de Defensa de Colombia- SOC Comando Conjunto Cibernético).

Vulnerabilidad: Una debilidad, atributo o falta de control que permitiría o facilitaría la actuación de una amenaza contra información clasificada OTAN o los servicios y recursos que la soportan. (Revista de la OTAN. 2011. *Nuevas amenazas: el ciberespacio.* Recuperado de https://www.nato.int/docu/review/2011/11-september/Cyber-Threads/ES/index.htm).

Zombies: Nombre que se da a los ordenadores que han sido infectados de manera remota por un usuario malicioso con algún tipo de software que, al infiltrarse dentro del propio ordenador manipulado y sin consentimiento del propio usuario, un tercero puede hacer uso del mismo ejecutando actividades ilícitas a través de la Red. (Instituto Nacional de Tecnologías de la Comunicación España - INTECO – CERT).

Introducción

Cada año un porcentaje mayor de los procesos y herramientas en los que se basa el accionar militar tanto en el nivel estratégico, operacional y táctico en Colombia, se apoyan en y ha migrado de medios físicos o análogos a las redes digitales y el internet público. Las bases de datos de inteligencia, los sistemas de armas, transporte, logística y los sistemas de comando y control, son una muestra de la tendencia tecnológica en las Fuerzas Militares de la actualidad. Los sistemas aislados e inaccesibles ahora permiten la movilidad de los usuarios y corren bajo infraestructuras informáticas que mejoran el procesamiento, consulta y presentación de los datos, en el proceso de toma de decisiones y la ejecución operacional en el campo de batalla. Sin embargo; así como los avances de la informática han permitido que los sistemas de defensa y ataque de las Fuerzas Militares se estén tejiendo en sistemas más poderosos a través del ciberespacio, así mismo se hacen más atractivos para los adversarios, ya que les otorga a estos, la posibilidad de inhabilitar dichos sistemas, a través de un ataque con tan solo un clic desde una red de computadoras.

Parte de esta revolución tecnológica ha permitido que en los últimos años haya cambiado notoriamente el ambiente operacional; el carácter del conflicto contemporáneo ha provocado un cambio significativo en el enfoque de la lucha de guerra. Las causas del conflicto han variado, así como la naturaleza de las capacidades adversarias, en donde su accionar puede ir desde ataques físicos hasta ataques mediante armas cibernéticas. Dichos cambios deberán tener implicaciones significativas en la planificación y conducción de las operaciones militares, ya que la guerra es un proceso adaptativo que necesitará ser revisado continuamente, dado la inminente evolución del entorno en el que se ven establecidas las relaciones de los Estados y sus individuos.

A su vez, si bien es cierto se encuentran al interior de las Fuerzas diferentes Unidades y Comandos de Ciberdefensa encargadas de hacerle frente a estas nuevas formas de amenaza, se adolece de doctrina en esta materia. Esto tiene como consecuencia una disminución en el accionar operacional, así como la duplicidad de funciones y baja cultura de ciberseguridad. Es por esta razón que el desafío actual de las Fuerzas Militares consiste en ejercer presencia y mantener seguro el ciberespacio, para garantizar así su libre accionar en el mismo y conseguir la efectividad en toda la gama de dominios y operaciones militares. Para ello se deberán generar los lineamientos para dimensionar su operar en el dominio del ciberespacio, al igual que entrenar al personal en las respectivas tácticas y procedimientos, con el fin de enfrentar estos nuevos retos y coadyuvar con la seguridad económica y social de la nación.

El objetivo del presente documento es, entonces, construir doctrina cibernética. Para ello, se realizó una revisión bibliográfica sobre fundamentos en materia operacional en el ciberespacio utilizados por diferentes Fuerzas Militares a nivel mundial, las buenas prácticas de ciberseguridad y la teoría operacional militar. Por medio del análisis de diversas fuentes, se presenta un escrito enfocado a establecer los tipos de operaciones cibernéticas en y a través del ciberespacio, los métodos y técnicas a emplear para llevar a cabo cada una de ellas, así como un modelo para la conducción de operaciones cibernéticas que sirva como base en la instrucción, entrenamiento y capacitación de las tropa y constituya una herramienta de conducción de la guerra para los comandantes.

1. Formulación del problema

1.1 Planteamiento del problema

En el marco del primer CONPES 3701 de 2011 "Lineamientos de Política para Ciberseguridad y Ciberdefensa", nacen organizaciones en el interior del sector Defensa, encargadas de la protección y defensa de la infraestructura cibernética del país en el ciberespacio; a su vez en cada una de las Fuerzas se constituyen las Unidades Cibernéticas y/o de Ciberdefensa con la misión de proteger y defender sus infraestructuras tecnológicas de las amenazas tanto internas como externas, dotadas con muchas herramientas tecnológicas , pero sin la debida fundamentación teórica de las actividades y funciones que los llevarían a la consecución del fin con que fueron creadas e incluso sin formación y entrenamiento en la misma.

Los conceptos de Ciberdefensa empezaron a ser tratados por las Fuerzas Militares en el año 2011 mediante el CONPES 3701, al ser un término nuevo y desconocido no ha sido difícil generar doctrina al respecto; ya que esta se construye a través del tiempo, fruto de experiencias y la aplicación de mejores prácticas, sin embargo se deben dar los lineamientos operacionales que permitan generar el aprovechamiento de la capacidad, legitimen el actuar de la Fuerza en el ciberespacio y sean el inicio doctrinal que con el tiempo deberá ser enriquecido.

En el proceso de transformación que sufre el Ejército Nacional; a través del CEDEF (Comité Estratégico de Diseño del Ejército del Futuro, 2013) se establece la Ciberdefensa como un área estratégica de capacidad dentro de la función de la guerra del Mando y Control. Dicha capacidad podrá ser estructurada y alcanzar su estado de efectividad mediante la combinación de mínimo cinco componentes: Doctrina, Organización, Material y Equipo, Personal e Infraestructura. En

diferentes Comités de Revisión Estratégica e Innovación (CREi), como el realizado en el año 2015 por las Comunicaciones Militares, se establece la doctrina como una de las iniciativas prioritarias para el desarrollo de la capacidad cibernética. Actualmente, sólo se cuenta con procedimientos y guías elaboradas por el Comando Conjunto Cibernético (CCOC) y una Directiva Ministerial 2014-18 en Políticas de Seguridad de la información, debidamente aprobada, así como socializada; sin embargo, adolece de fundamentos propios de la Ciberdefensa militar.

Aunque en el año 2012 el Ejército Nacional mediante el Comité Estratégico de Transformación e innovación (CETI), a través de la línea estratégica No. 4, referente a la actualización del material doctrinario del Ejército, se elaboraron 11 manuales: Operaciones Especiales, Inteligencia, Fuegos, Apoyo de la Defensa de la Autoridad Civil, Protección, Sostenimiento, Operaciones Defensivas y Ofensivas, Proceso de Operaciones, Mando Tipo Misión, Liderazgo y Derecho Operacional; en ninguno de ellos se contemplan doctrina de operaciones cibernéticas ni el desarrollo de las mismas en el dominio del ciberespacio, así como tampoco se elaboró un compendio doctrinario en Operaciones Cibernéticas.

La ausencia de doctrina de Ciberdefensa ha generado al interior de la Fuerza una falta de conocimiento de la capacidades que la Ciberdefensa puede aportar en el apoyo de las operaciones militares tradicionales, falta de unificación de conceptos, desconocimiento en el accionar de las Unidades Cibernéticas e incluso en la tropa al desconocer los tipos de operaciones cibernéticas que se pudieran desarrollar, una falencia y vacío en la doctrina impartida en las escuelas de formación y entrenamiento; así como una baja cultura en Ciberdefensa en todos los niveles y duplicidad en las funciones realizadas al respecto por las diferentes armas.

Por lo anterior el presente proyecto de investigación responderá a: ¿Cuáles son los lineamientos doctrinales operacionales debe conocer y difundir el Ejército como base teórica, para que pueda desarrollar operaciones cibernéticas tanto defensivas como ofensivas y le permitan operar legítimamente en el ciberespacio?.

1.2 Justificación

Con este proyecto de investigación en Doctrina de Ciberdefensa y Ciberseguridad, se establecerán conceptos, características, propósitos y otros aspectos de cada función, misión y operaciones que se deberán tener en cuenta al momento en la que el poder militar deba planear, conducir y ejecutar operaciones defensivas y ofensivas, entre otras en el ciberespacio tanto en tiempo de ciberconflicto, ciberguerra o de paz; basados estos en los principios y teorías de la guerra y el contexto cibernético. Así mismo, proporcionará las responsabilidades en todo el nivel del mando y la interacción militar con organismos gubernamentales y no gubernamentales, las fuerzas multinacionales, y otros aliados estratégicos.

La fundamentación y organización de las operaciones cibernéticas jugarán un papel importante para el Ejército Nacional en la protección y defensa de su infraestructura crítica cibernética y del país y por ende de la seguridad nacional, ya que es necesario que se establezcan métodos, técnicas y tácticas con la cuales el personal de cuadros puedan operar, sin que haya lugar a diferentes criterios y puedan contar con rutas de acción en la conducción de operaciones en el ciberespacio; así como ayudar en los procesos de formación de los militares en el campo de la ciberdefensa y fortalecimiento del recursos humano de esta capacidad.

Al llevar a cabo un desarrollo doctrinario en el dominio del ciberespacio por parte del Ejército Nacional, este se constituirá como una institución moderna, multimisión al servicio de la nación y responsable de su misión constitucional y a los nuevos retos de los cambios del mundo y las nuevas amenazas y riesgos hoy día transnacionales y digitales; así mismo la fundamentación doctrinal permitirá legitimar el accionar de la Fuerza en el ciberespacio; así como mejorar la efectividad de los cursos de acción tomados en operaciones tradicionales y cibernéticas.

Si bien es cierto en el ámbito operacional se habla de cuatro escenarios para el combate Tierra, Mar, Aire y Espacio, con la evolución de la tecnología, la informática y los medios de comunicación, el mundo habla de un quinto escenario o dominio de la guerra, el cual es el Ciberespacio. Por tal razón las FF.MM. no deben ser inferiores al reto y debe de efectuar un papel sobresaliente a través de la doctrina, en este nuevo dominio de la guerra; ya que hoy en día las amenazas potenciales viajan a través de la red poniendo en riesgo toda la infraestructura critica digital de la nación, la cual están llamadas a proteger.

2. Objetivos

2.1 Objetivo General

Estructurar y definir los lineamientos doctrinales base en la doctrina de Operaciones Cibernéticas para el Ejército Nacional y las FF.MM.

2.2 Objetivos específicos

- Generar doctrina para el planeamiento, conducción y evaluación de operaciones militares en el ciberespacio, como herramienta de conducción de la guerra para los comandantes y personal militar, al mismo tiempo que sirva como base doctrinal en la instrucción, entrenamiento y capacitación de las tropas.
- Regular los conceptos, criterios y procedimientos que, en situaciones de combate en el ciberespacio, deben aplicar las Unidades del Ejército Nacional en el planeamiento, conducción y ejecución de operaciones militares en el ciberespacio.
- Establecer los tipos y propósito de las operaciones cibernéticas militares junto con sus técnicas, tácticas y procedimientos, identificado los niveles de aplicación y responsables.
- Actualizar la doctrina del Ejército en materia de operaciones cibernéticas; de acuerdo a las nuevas necesidades y restos impuestos a la Fuerza.

3. Metodología

Este proyecto es un estudio descriptivo, tipo monografía que tiene como objetivo principal realizar una revisión bibliográfica sobre la ciberseguridad y ciberdefensa en el accionar y misión de las Fuerzas Militares, cuyo fin es el identificar las actividades u acciones que a partir de las Tecnología de la Información y las Comunicaciones; así como de la seguridad digital puedan ser aplicadas en el entorno operacional militar, para garantizar la defensa y seguridad de la soberanía nacional en el entorno del ciberespacio, potenciando unas Fuerzas Militares multimisión y a la vanguardia de los nuevos retos y amenazas. Por lo anterior el tipo de investigación a utilizar es del tipo de investigación cualitativa desarrollada a través del pensamiento analítico, partiendo de la revisión doctrinal de las propias Fuerzas y Ejércitos de otros Estados del mundo y de autores de la comunidad académica y del sector privado, para generar nuevo conocimiento y desarrollo del componente doctrinal para la capacidad de Ciberdefensa, a fin de que pueda ser utilizada como herramienta de instrucción y operacional.

Para el proyecto se realiza una búsqueda sistemática en las principales bases de datos y-o motores de búsqueda y literatura científica, desde el portal ofrecido por la biblioteca virtual de la Escuela de Guerra, a través del cual se puede acceder a las principales bibliotecas universitarias que se encuentran en red. La búsqueda se fundamentó en artículos de revista, monografías y datos obtenidos desde los sitios web oficiales de algunas entidades militares a nivel mundial y otras del ámbito nacional. La búsqueda también se amplió a los motores recurrentes de búsqueda como Mozilla, google y yahoo. En la búsqueda se tuvieron en cuenta las siguientes palabras clave: ciberoperaciones, defensa activa, defensa pasiva, planeamiento de operaciones, procedimiento operacional cibernético, ciberinteligencia, entre otros. De los grandes retos encontrados en la

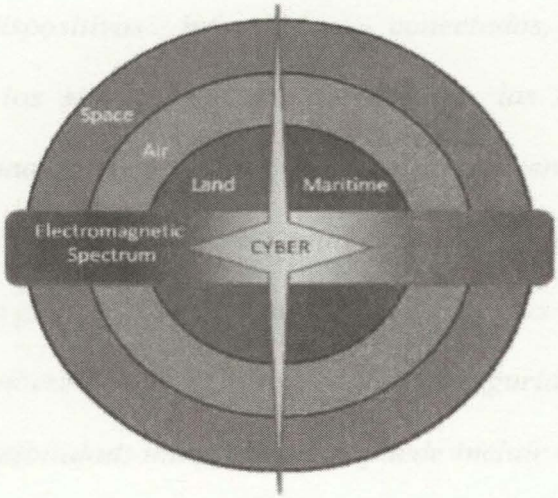
búsqueda para el desarrollo de la monografía, está la primera labor de filtrar la información recolectada y seleccionar los artículos que aporten valor y soporte bibliográfico a la estructuración del documento y, por otro lado, la poca información sobre el tema principal del presente proyecto concerniente a las técnicas y tácticas para el desarrollo de operaciones cibernéticas.

4. Conceptos Fundamentales

4.1 Operaciones cibernéticas (OC)

Las Operaciones Cibernéticas (OC) son las acciones tomadas de forma deliberada para garantizar *la superioridad militar* de la información en y a través del ciberespacio y denegarle ésta al adversario. Es así como las OCs deben ser entendidas en un espectro amplio, como el empleo de capacidades en el ciberespacio cuyo propósito consiste en la defensa y protección de las redes, sistemas y activos informáticos propios, permitiendo de esta manera la libertad de acción en la conducción de operaciones militares en el dominio del ciberespacio o como apoyo a operaciones en otros dominios (tierra, mar, aire, espacio), así como la realización de ataques informáticos con el objetivo de denegar, neutralizar o destruir los sistemas informáticos del oponente y negar la libertad de acción a este.

Figura 1 - Integración Operaciones Cibernéticas



Nota: Tomado de Manual Conjunto Operaciones en el Ciberespacio 3-12 EE.UU.

Lewis, J.A, (2002), define la superioridad militar en y a través del ciberespacio "*como la libertad para llevar a cabo operaciones militares en cualquier momento y lugar, sin interferencias que lo impidan o limiten, geográfica o temporalmente*". Es así como la ventaja operativa en el ciberespacio se basa en la idea de impedir la interferencia o ataque del oponente, de tal manera que la sinergia de las capacidades propias cree los efectos esperados en el campo de combate. Tal como lo explica Lewis, la superioridad no significa la nulidad total de las capacidades implementadas por el adversario, pero ante cualquier intento de interferencia de este, esta debe ser contrarrestada a niveles mínimos de tal manera que tenga poco o ningún efecto en las operaciones.

Las acciones de las OCs deben operar tanto en el ámbito de *la Ciberseguridad* como el de la *Ciberdefensa*. Al respecto de la Ciberseguridad, Feliu (2012) entiende esta como:

> *"El conjunto de herramientas, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de gestión de riesgos, acciones, formación, prácticas idóneas, seguros y tecnologías que pueden utilizarse para proteger los activos de la organización y los usuarios en el ciberentorno. Los activos de la organización y los usuarios son los dispositivos informáticos conectados, los usuarios, los servicios/aplicaciones, los sistemas de comunicaciones, las comunicaciones, y la totalidad de la información transmitida y/o almacenada en el ciberentorno. La ciberseguridad garantiza que se alcancen y mantengan las propiedades de seguridad de los activos de la organización y los usuarios contra los riesgos de seguridad correspondientes en el ciberentorno. Las propiedades de seguridad incluyen una o más de las siguientes: disponibilidad; integridad, que puede incluir la autenticidad y el no repudio; y la confidencialidad".*

De otra parte, la Ciberdefensa de acuerdo a lo enunciado en el CONPES 3854 Política de Seguridad Digital de Colombia (2016), habrá de ser entendida como "*las capacidades militares ante amenazas o actos hostiles de naturaleza cibernética que afecten la sociedad, la soberanía nacional, la independencia, la integridad territorial, el orden constitucional y los intereses nacionales*". A través de esta se deberá defender y preservar la seguridad de los Sistemas de Mando y Control propios y la información que manejan; así como permitir la explotación y respuesta de los sistemas adversarios, para garantizar el libre acceso al ciberespacio de interés militar y permitir el desarrollo eficaz de las operaciones militares y el uso eficiente de los recursos de interés estratégico nacional (Infraestructura crítica cibernética ICC). La Ciberdefensa hace parte y debe garantizar la Ciberseguridad; es decir debe comprender las acciones y medidas necesarias para brindar defensa y protección a la ICC militar y nacional tanto pública como privada.

4.2 Niveles de la guerra en las operaciones cibernéticas

Las operaciones cibernéticas deberán formar parte de la estrategia militar y deberán estar enmarcadas en uno o en todos los niveles de la guerra, ya que una acción de este tipo de operaciones en el nivel táctico u operacional puede tener incidencia en el nivel estratégico. De acuerdo a lo establecido en el Manual de Ciberdefensa Conjunta para las Fuerzas Militares de Colombia 3-38, las operaciones cibernéticas deberán enmarcarse en cada nivel, así:

1) Nivel Estratégico. Las operaciones cibernéticas en este nivel deberán buscar alcanzar los objetivos nacionales establecidos por el Presidente de la Republica, potencializando así, el nivel de acción de las Fuerzas Militares FF.MM e impacto sobre blancos estratégicos de interés

nacional. De tal manera las operaciones estratégicas deberán obedecer a la máxima instancia de planeamiento y conducción implicando la utilización y aprovechamiento de todos los poderes de la nación de forma integrada y coordinada para proteger y asegurar la infraestructura critica cibernética nacional.

2) *Nivel Operacional.* En este nivel se planean, dirigen y conducen de forma secuencial operaciones que contribuyen al logro de los objetivos establecidos por el nivel estratégico. Se emplean todos los recursos militares necesarios para marcar la diferencia en el ciberespacio. Este nivel se halla bajo la dirección y conducción de los comandos de Fuerza o el comando conjunto de operaciones.

3) *Nivel Táctico.* En este nivel se efectúan las operaciones que tienen una influencia directa en el campo de combate, hace referencia a la aplicación directa de las operaciones cibernéticas con el propósito de alcanzar unos objetivos operacionales como garantizar el acceso recurrente a algún activo o servicio informático del adversario. En el nivel táctico las operaciones cibernéticas contribuyen a buscar la superioridad militar; a su vez que pueden contribuir a aumentar el nivel de disuasión del contrincante.

4.3 Principios de las operaciones cibernéticas OC

Las OCs deben seguir imperativos categóricos como reglas fundamentales en la táctica de su accionar, que a saber son: el objetivo, el propósito, la ofensiva, economía de fuerzas, maniobra, unidad de mando, seguridad, sorpresa y sencillez. Los conceptos de dichos principios se

encuentran definidos en el Manual EJC 3-10-1 de Combate Irregular, el Manual EJC 3-225 Misiones Regulares de la Compañía de Infantería y el Manual MFE 3-05 de Operaciones Especiales del Ejército de Colombia.

Sin embargo, para la ejecución de OCs se deben adicionalmente seguir una serie de principios diferenciales que las distinguen de las operaciones convencionales:

1) Principio de efecto. Las OCs deben producir efectos que se traduzcan en ventaja estratégica, operacional o táctica que afecten el mundo real, incluso si estos efectos no se dan el mismo dominio cibernético.

2) Principio de disimulación. Se deben tomarse medidas para mantenerse oculto en el ciberespacio, de tal manera que la trazabilidad de las acciones ofensivas cibernéticas y de explotación tomadas en contra de los sistemas de tecnología de la información y las comunicaciones del oponente no sean detectables. El propósito es enmascarar así la autoría y el punto de origen de estas acciones.

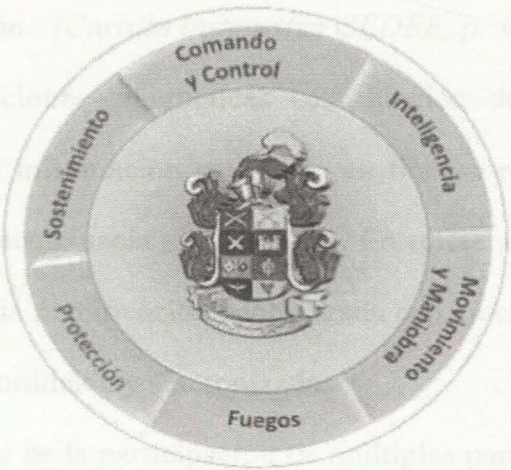
3) Principio de rastreabilidad. Se deben tomar medidas para detectar la acción ofensiva cibernética y exploratoria, en contra de los sistemas de tecnología de la información y las comunicaciones propias. Casi siempre, las acciones llevadas a cabo en el ciberespacio implican movimiento o manipulación de los datos, que pueden estar registradas en los sistemas de TIC propios.

4) Principio de adaptabilidad. Las OCs deben adaptarse a la característica de mutabilidad del ciberespacio, manteniendo la proactividad frente a los cambios repentinos e impredecibles que se producen en el entorno operacional cibernético.

4.4 Las funciones de la guerra en las operaciones cibernéticas

Las Operaciones Cibernéticas se deben integrar a las funciones de conducción de la guerra, a través de los siete sistemas operacionales del campo de batalla. El comandante en el planeamiento debe integrar cada uno de los siguientes sistemas a fin de cumplir la misión efectivamente, a continuación, se analizarán las distintas funciones de la guerra en relación con las operaciones cibernéticas:

Figura 2 - Funciones conducción de la guerra – Ejército



Nota: Tomado cartilla instructivo CEDEF

1) Sistema de Mando y Control. El mando y control abarca las actividades y procedimientos empleados por el comandante para planear, dirigir, coordinar las unidades y equipos asignados en la realización de su misión.

> *"El mando y control se concibe como el ejercicio de la dirección y autoridad de un comandante para dar cumplimiento a la misión, incluye el manejo apropiado de la información, la asesoría del Estado Mayor, la versatilidad en los cursos de acción, el control de la disciplina táctica de la unidades comprometidas por parte de los mandos subalternos y la integración de todos los medios de comunicación e informática para obtener una actualización de la batalla en tiempo real, que permita la toma de decisiones. Para ello se sirve de dos componentes: un Sistema de Comando y Control mediante el cual administra y gestiona información a través de sus componentes (personal, redes, sistemas de información, procesos y procedimientos, instalaciones y equipos); y la Acción Integral que es la encargada de administrar y dar uso adecuado a la información, llevando a cabo operaciones de información" (Cartilla instructivo CEDEF, p. 12).*

En el campo de las operaciones cibernéticas esta función de la guerra corresponde a proporcionan al comandante la información suficiente en tiempo real que le permita tomar y ejecutar decisiones más rápidamente hacia el adversario. En referencia al mando, en las OCs se deberá emplear principalmente la planificación centralizada con ejecución descentralizada de las operaciones, pero de manera coordinada y sincronizada.

Así mismo las OCs requieren de la participación de múltiples partes interesadas y/o aliados y pueden simultáneamente apoyar varias misiones, es así que requerirán de una amplia coordinación, planificación de las tareas y responsabilidades por cada tipo de OC a emplear y de la integración temprana de los requisitos y capacidades. Para ellos los comandantes coordinarán el despliegue y

el empleo de las capacidades de OC para cumplir con la misión asignada, ya que algunas unidades de OC pueden estar geográficamente separadas del teatro de operaciones apoyado. De esta manera se garantizará el ritmo, sincronización y conducción de las OCs.

En razón a que las Ocs crean efectos en el ciberespacio que pueden impactar incluso el espacio físico, requerirán de la coordinación interagencial de los esfuerzos diplomáticos, jurídicos y del gobierno, así como de la integración de las capacidades del ciberespacio con las de tierra, mar y aire. Las actividades, prioridades y restricciones en las Ocs deberán por tanto ser identificadas en coordinación entre las Fuerzas y los organismos del Estados. A su vez en esta fase será necesario evaluar los impactos potenciales para la Fuerza y el País de cualquier curso de acción planeado, postura y cambios en la configuración observados de la actividad adversa.

2) Sistema de Inteligencia.

"Se entiende como el sistema que integra las capacidades de la inteligencia, contrainteligencia (abierta y en cubierta), en los niveles estratégico, operacional y táctico. Este contempla la utilización de medios técnicos y tecnológicos para anticipar, prevenir, contrarrestar, neutralizar y persuadir potenciales amenazas internas y externas." (Cartilla instructivo CEDEF, p. 13).

La inteligencia recogida en el ciberespacio puede provenir desde fuentes del orden nacional u otras y puede ser información de objetivos estratégicos, operativos o tácticos. La comprensión del Entorno Operacional OE es fundamental para esta función de la guerra en el planeamiento de operaciones cibernéticas. Una de las formas de conocer el OE es a través de la ciberinteligencia.

3) Sistema de fuegos.

"Su objetivo es proveer fuego dentro del concepto de operaciones terrestres y sus competencias (maniobras de armas combinadas, seguridad de área extensa y operaciones especiales), permitiendo el uso de los elementos del poder de combate, brindado libertad de acción a las unidades de maniobra y negándosela al enemigo, así como garantizar la seguridad y supervivencia, concentrar los fuegos, brindar respuesta oportuna y garantizar la movilidad". (Cartilla instructivo CEDEF, p. 13).

Dependiendo del objetivo, el fuego en el ciberespacio puede ser ofensivo o defensivo y deberá tenerse en cuenta desde la fase de planificación hasta la de ejecución. A la hora de emplear el fuego en el Ciberespacio, tal como lo afirma el Manual Conjunto de Operaciones del Ciberespacio de los EE.UU 3-12, se deberán considerar aspectos como la *focalización y la coordinación*, la primera consiste en la de selección y priorización de objetivos en el ciberespacio (detener un ataque de DoS, Accesar un Sistema de Comando y Control, entre otros), junto con la búsqueda de una respuesta apropiada para ellos, por medio de los requisitos operacionales y las capacidades cibernéticas, los objetivos se deben basar en lo que el comandante quiere lograr, en lugar de las formas y los medios que tiene para alcanzarlo. En la segunda se deben entender los objetivos, las intenciones, las capacidades y limitaciones de todos los actores involucrados (Unidades Militares, Fuerzas, entidades nacionales y multinacionales), con el fin de conducir asertivamente las Ocs; ya que, si dos entidades/Unidades crean efectos sobre el mismo objetivo en el ciberespacio, sus acciones no coordinadas podrían exponer o interferir con las acciones de uno o ambos.

De otro lado, los apoyos de fuego son más eficaces cuando se integran con diferentes capacidades tanto cibernéticas como no cibernéticas (*integración).* Finalmente, a todo apoyo de

fuegos debe realizarse una *evaluación,* consistente en la medición de la eficiencia y la eficacia de estos, así como su contribución al cumplimiento de la operación.

Aunque la evaluación tradicional de las operaciones militares se ha dado en términos de daños físicos; del lado de las operaciones cibernéticas, se deberá realizar una evaluación de los daños funcionales de los activos y sistemas del adversario, que inicie desde un nivel micro a un objetivo específico hasta nivel macro, evaluando el efecto funcional creado en todo el sistema.

4) Sistema de movimiento y maniobra.

"Comprende las tareas y los sistemas relacionadas con el empleo de las unidades en combinación con fuegos de apoyo, proyección de la fuerza, movilidad y contra movilidad. Los comandantes se valen de este sistema para concentrar los efectos de la potencia de combate en el lugar y momento decisivo." (Cartilla instructivo CEDEF, p. 13).

El movimiento y la maniobra en el dominio de tierra involucra el despliegue de Unidades en un área operativa determinada, moviéndose dentro de esa área para obtener una ventaja operacional en apoyo de objetivos operacionales. Para ellas un componente esencial de la planificación es el concepto de *terreno clave*, el cual es cualquier localidad o zona, cuya captura o retención ofrece una ventaja notable a cualquiera de los combatientes. Podrían incluir las principales líneas de comunicación; puntos clave de acceso para la defensa, puntos de observación y puntos de lanzamiento para el apoyo de fuegos; u oportunidades para crear cuellos de botella. En el Ciberespacio, el terreno clave implica enlaces de red y nodos que son esenciales para tanto para los sistemas de comunicación amigos como del adversario.

Otro componente de maniobra en el ciberespacio es el *movimiento de datos*. En este contexto corresponde al ancho de banda (cableado o inalámbrico), el rendimiento de los datos puede ser físicamente establecido por la infraestructura de comunicaciones implementada, esto puede considerarse análogo a las líneas de comunicación en los dominios físicos. La capacidad de maniobrar el flujo de datos de una línea física a otra, por ejemplo, desde cables terrestres hasta comunicaciones satelitales, es un ejemplo de mantener la libertad de maniobra en el ciberespacio. El movimiento y la maniobra en el ciberespacio pueden ocurrir en las tres capas de este: La capa física, la capa lógica y la capa de ciberusuarios.

5) Sistema de protección.

"Proyecta para enfrentar a un enemigo adaptable y flexible, genera la seguridad de militares y garantizar la seguridad de los activos vitales de la Fuerza, proteger las instalaciones militares y garantizar la seguridad y el apoyo a las unidades de maniobra." (Cartilla instructivo CEDEF, p. 13).

La protección es algo difícil dentro del ciberespacio; ya que los adversarios pueden crear múltiples efectos en cascada que pueden no estar restringidos por la geografía física, civil/militar, y ampliar significativamente el área que requiere protección. En el ciberespacio la protección incluyen no sólo la infraestructura (computadoras, cables, antenas y equipo de conmutación y enrutamiento), sino también el Espectro Electromagnético, los datos y las aplicaciones de las que dependen las operaciones militares. La clave para la protección del ciberespacio es la gestión de buenas prácticas de seguridad de las redes y sistemas propios; y la capacidad de monitorear, detectar y prevenir el tráfico hostil.

La protección del ciberespacio propio y amistoso debe utilizar una combinación de capacidades defensivas u operaciones de seguridad informática. Las actuales tecnologías de seguridad de las redes, la verificación de las configuraciones de red y la gestión de vulnerabilidades pueden ofrecer una buena protección a la infraestructura tecnológica y la información de la Fuerza. Sin embargo, no las protegen de usuarios mal entrenados que no emplean prácticas de seguridad adecuadas. Por lo anterior, es necesario asegurarse de que el personal entienda y sea responsable de la seguridad cibernética.

6) Sistema de sostenimiento

"Provee el apoyo y servicios para garantizar la libertad de acción, extender el alcance operacional y prolongar la resistencia. Incluye tareas relacionadas con mantenimiento, transporte, abastecimiento, servicios de campaña, neutralización de material explosivo, apoyo de recursos humanos, administración de finanzas, apoyo de servicios de salud, apoyo religioso e ingeniería militar." Cartilla instructivo CEDEF, p. 13).

El sostenimiento es la provisión de servicios logísticos y de personal necesarios para mantener y prolongar las operaciones hasta el logro exitoso de la misión. Es así que las Unidades cibernéticas deben identificar las capacidades requeridas, los activos críticos del ciberespacio, evaluar el riesgo, asegurar la redundancia (incluidas las alternativas no ciberespaciales) y ejercer activamente los planes de continuidad operacionales, para responder a cortes o acciones adversarias que degradan o comprometan el acceso o confiabilidad del ciberespacio.

Debido a los avances en TI que se desarrollan rápidamente, los comandos cibernéticos tienen la necesidad de incorporar rápidamente nuevas capacidades del ciberespacio en su arsenal.

Adicionalmente, puede necesitar la capacidad de actualizar rápidamente sus propias redes para aprovechar nuevas tecnologías. Es así como muchos sistemas críticos con el tiempo pueden requerir componentes, software o actualizaciones de firmware, que de no actualizarse generen riesgos de seguridad. Sin embargo, con el despliegue de nuevas tecnologías se deberán evaluar los requisitos y riesgos incrementados e ir en concordancia con las políticas de seguridad informática establecidos por la Fuerza.

Por último, un componente clave para un efectivo sostenimiento es una Fuerza bien entrenada, este entrenamiento debe estar orientada tanto al personal quien desarrolla directamente operaciones cibernéticas como los usuarios finales y deben estar orientadas en todo el espectro de las capacidades de ciberdefensa.

4.5 Riesgos de las operaciones cibernéticas

El proceso de toma de decisiones permite identificar, gestionar y controlar los riesgos, lo cual es requerido e indispensable también para el desarrollo de operaciones. Los riesgos relacionados con las operaciones cibernéticas se agrupan en cuatro categorías:

Riesgos operacionales. Se refieren a las consecuencias que las amenazas del ciberespacio representan para la eficacia de la misión. Dichas consecuencias pueden representar lesiones o muerte de personal, daño o pérdida de equipo o propiedad, degradación de capacidades, la degradación de la misión o incluso el fracaso de la misión, por causa de ciberataques, entre otras.

Riesgos técnicos. Corresponden a vulnerabilidades explotables en las propias infraestructuras tecnológicas, de comunicaciones y control. Estas vulnerabilidades afectan directamente la capacidad del Ejército para proyectar el poder militar y apoyar la misión.

Riesgos jurídicos. Los comandantes y tomadores de decisiones deben evaluar y considerar posibles efectos en cascada y colaterales debido a la acción operacional cibernética en contra posición a las normativas, leyes y derechos civiles en el ciberespacio.

Riesgos de seguridad operacional. Son los riesgos derivados del compromiso que tiene el recurso humano para usar de manera segura los activos de información y esta. Por lo anterior deberán estar sensibilizados y se deberán tomar acciones para protegerlos.

4.6 El campo de batalla cibernético

El Entorno Operacional EO es el conjunto de las condiciones, circunstancias e influencias que afectan el empleo de capacidades y decisiones del comandante. El Entorno Operacional de las Ocs debe ser entendido como Entorno Operacional de la Información, el cual se compone de las Infraestructuras de Tecnología (TI) y datos de residentes, Internet, las redes de telecomunicaciones, sistemas informáticos y diferentes sistemas de controladores. Comprender plenamente el ciberespacio y su relación con los dominios físicos (tierra, mar, aire y espacio) es el primer paso en la *planificación de operaciones ciberespacio* y el entendimiento del entorno operacional actual.

Entorno operacional cibernético= El ciberespacio

El Ciberespacio para las FF.MM de Colombia, se define como:

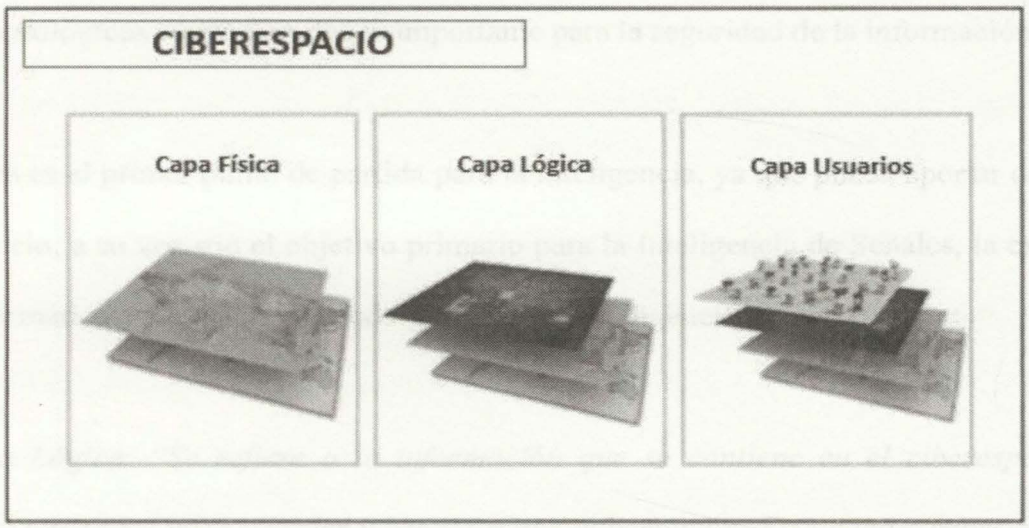
> *"El ambiente, tanto físico como virtual, compuesto por sistemas computacionales, programas y aplicaciones (software), redes de telecomunicaciones incluido el internet, datos e información y la infraestructura física asociada que es utilizada para la interacción entre usuarios, entre máquinas y entre máquinas y usuarios"* (Manual de Ciberdefensa Conjunta para las FF.MM, 2016).

De lo anterior se puede concluir que el Ciberespacio se caracteriza por su naturaleza artificial, al ser creado por el hombre y se ha hecho crítico para las operaciones militares. En la actualidad se ha convertido en un nuevo escenario estratégico, en un nuevo campo de batalla o en una extensión de este, ya que a través de este se producen comportamientos o fenómenos de confrontación, bajo el empleo de técnicas informáticas nuevas. Así mismo para la sociedad en general es ahora un conducto primario para sus transacciones, ejemplos como los controles de fabricación, la distribución de servicios públicos, la banca, las comunicaciones y la distribución de información digital la han emergido en una sociedad cada día más interconectada. Si bien esta evolución ha beneficiado significativamente a la sociedad, también ha creado serias vulnerabilidades, el aumento de la dependencia a internet ha expuesto a las infraestructuras críticas, la salud pública y el bienestar económico de los países; ya que los adversarios a través del ciberespacio pueden intentar negar, degradar, manipular, interrumpir o destruirlas, afectando así el desarrollo económico y social de una nación.

Continuando con el ciberespacio, de acuerdo a lo detallado por Libicki, (2006), este se puede describir en términos de tres capas, cada una con diferentes vulnerabilidades y objeto de un tipo concreto de ataques.

Ciberespacio = Capa física + Capa Lógica + Capa de los Ciberusuarios.

Figura 3 - Capas del Ciberespacio



Nota: Tomado de Monografía 126 El Ciberespacio nuevo escenario de confrontación.

1) Capa física. "Es aquello que podemos ver y tocar en el ciberespacio, Es el medio en el que viajan, se procesan o almacenan los datos, se compone del hardware, software de sistemas e infraestructuras (cableadas, inalámbricas, enlaces cableados, enlaces Electromagnéticos, satélites u ópticos) de las redes y los conectores físicos (cables, cables, radiofrecuencia, routers, conmutadores, servidores y computadoras)".

Para un Ejército esta capa está compuesta de los sistemas de comando y control (C2), torres de microondas, computadoras, laptops, teléfonos inteligentes, computadoras, tablet, o cualquier otro dispositivo de hardware e infraestructura de apoyo que permiten al personal de cuadros y unidades militares realizar operaciones.

La principal vulnerabilidad que encontramos en esta capa tiene que ver con la fabricación de dichos elementos, la alteración en la fabricación de componentes por terceros países, es una técnica potencial en la manipulación de sistemas informáticos. La dependencia en la adquisición de elementos tecnológicos supone un riesgo importante para la seguridad de la información que estos contienen.

Esta capa es el primer punto de partida para la inteligencia, ya que puede aportar datos útiles del ciberespacio; a su vez son el objetivo primario para la Inteligencia de Señales, la explotación de redes informáticas, inteligencia de código abierto e inteligencia humana.

2) Capa Lógica. "Se refiere a la información que se contiene en el ciberespacio y las herramientas utilizadas para acceder y procesar esa información. Esta capa comprende el nivel semántico que proporciona las aplicaciones, programas y desarrollos de software para que los usuarios puedan gestionar y compartir información y la capa sintáctica que corresponde a las instrucciones (protocolos, sistemas operativos, lenguajes de programación) que los diseñadores de software y usuarios introducen en el sistema y son básicos para que los sistemas se comuniquen entre ellos".

En esta capa es donde se ejerce el C2 de las Fuerzas Militares y donde residen la intención del comandante. Las acciones en esta dimensión afectan el contenido y el flujo de la información. Los ataques más conocidos en esta capa son el ciberespionaje a los datos clasificados, a la propiedad

intelectual y la intrusión dada por la imperfección en la programación y puertas traseras que son utilizadas para controlar ilegítimamente los sistemas.

3) La capa de los ciberusuarios. "Los ciberusuarios representa el nivel más alto de abstracción de la capa lógica en el ciberespacio. El ciberusuario es la gente real en la red, estos pueden relacionarse directamente con una persona o entidad real, incorporando algunos datos biográficos, direcciones de correo electrónico e IP, páginas Web, números de teléfono, etc". Sin embargo, un individuo en el ciberespacio puede tener múltiples identidades virtuales. Una solo ciberpersona puede tener múltiples usuarios. En consecuencia, la atribución de la responsabilidad y la focalización en el ciberespacio se hace más compleja.

La capa humana en el ciberespacio es la más vulnerable de todas, debido a la deficiencia en la formación de usuarios o el exceso de confianza. El sabotaje o el robo suele requerir la participación física de algún usuario autorizado. La concienciación de los usuarios a todo nivel es la base de la seguridad en esta capa.

Como hemos visto el ciberespacio es un conjunto de capas o planos; sin embargo, en el nivel operacional el ciberespacio presenta las mismas variables que un campo de batalla tridimensional, concepto como los de velocidad, sorpresa, conquista de la posición, avance resultan aplicables, las Fuerzas Militares deberán de ser capaces de operar en todos los dominios (tierra, mar y aire) para conseguir en un dominio integral. Como se mencionó el Ciberespacio es otro campo de batalla semejante al terreno en las operaciones de tierra, en donde por ejemplo un punto clave para el caso de operaciones terrestres puede ser una colina, un puente sobre un río y en el caso cibernético podrían ser un canal de comunicaciones dedicado para el C2, una cuenta de usuario desde el cual se lanzará el cibereataque.

Es así que al analizar el Ciberespacio como el terreno operacional podemos hacer una analogía con el terreno físico, por ejemplo, las listas de control de acceso, un cortafuegos se pueden considerar obstáculos ya que estos pueden limitar la libertad de movimientos en una red. Los obstáculos en el ciberespacio pueden ser naturales o artificiales como el caso del enmascaramiento de IPs. Del mismo modo los puntos clave están relacionados con sistemas, dispositivos, protocolos, datos, cuentas de usuario; los cuales en caso de ser controlados representan una marcada ventaja para el atacante. Las rutas de aproximación del Ciberespacio pueden ser considerados como los canales inalámbricos o de fibra óptica que conectan enrutadores y diferentes dispositivos activos en la red; así mismo una vía de acceso en una red puede ser una conexión HTTP a un servidor web.

En la tabla se relacionan diferentes puntos claves (objetivos) en el terreno operacional cibernético en los diferentes niveles de la guerra.

Tabla 1 - Objetivos en el Ciberespacio según los niveles de la guerra.

CAPAS	PTOS CLAVE	TÁCTICO	OPERACIONAL	ESTRATÉGICO
Física	Hardware, direcciones físicas	USB, tel móvil, router, servidor	Cables de comunicación regional, sistemas de defensa antiaérea, sistemas de C2	Centros de datos de una Fuerza, entidad gubernamental o infraestructura crítica.
Lógica	Software, protocolos,	Sistema operativo de Pc de una red local	Servidores web, DNS, sistemas de información operacional o de inteligencia	Software y protocolos que gestionan una infraestructura crítica.
Ciberusuarios	Cuentas de usuario, certificados	Cuenta de administración local	Credenciales de los administradores de sistemas	Cuentas y contraseñas de figuras políticas, o de manejo a nivel gubernamental y del sector privado económico.

Nota: Elaboración propia a partir de Martín (2016).

4.6.1 Características del Ciberespacio

Variedad de autores han identificado diferentes características de este nuevo dominio de la guerra e instrumento de poder militar, dentro de los cuales se encuentra López de Turiso, J. (2012), que en resumen establecen los siguientes rasgos distintivos del ciberespacio.

1) A través de la capa física el ciberespacio se integra con el resto de dominios, estableciendo con ello su ubicuidad, lo que posibilita una fácil infiltración y anonimato por parte del adversario y una difícil rastreabilidad del mismo.

2) El ciberespacio evoluciona de una manera acelerada ya que sigue la evolución tecnológica de las TIC, permitiendo por el intermedio de estas requerir muy poco equipamiento para generar efectos considerables, ya que la zona de combate puede extenderse hacia cada una de las casas de los ciudadanos y cortarle los suministros básicos que este necesita para su supervivencia. De tal manera se podría conseguir a través de este un conflicto asimétrico.

3) El elemento humano en el ciberespacio exige un área de competencia y experiencia profesional diferenciada al resto de los dominios y requiere una formación específica. Así como de una estrecha coordinación entre todos los organismos estatales y privados para su defensa.

4) El número de amenazas aumenta diariamente, por lo tanto, el adversario solo necesitará encontrar una vulnerabilidad en los activos tecnológicos, mientras que la defensa requerirá asegurarlas todas.

5) En el Ciberespacio el principal medio no son las armas sino la información que en la defensiva se ha de proteger y en la ofensiva se ha de negar, alterar o sustraer al enemigo. Las armas defensivas para el ciberespacio están compuestas por tecnologías de análisis y control de tráfico de res, hardware y software de seguridad y las armas ofensivas serán el resultado de I+D+i. De tal manera estos medios no solo están al alcance de los Estados sino de toda la población que disponga de un acceso a la red.

6) Las operaciones en el Ciberespacio se rigen por los principios de la guerra. Disponen de un objetivo único, operacional y táctico; precisa de la acción ofensiva súbita que le proporcione la iniciativa, demanda concentración de Fuerzas con una distribución de recursos eficientes, tanto en ofensiva como en defensiva, se maniobra con seguridad, mediante acciones de ciberespionaje, para obtener una posición ventajosa sobre el adversario y todo ello bajo un mando único al más alto nivel.

Con base en lo anterior, se considera al Ciberespacio como un nuevo escenario, desde el cual se puede influir sobre el exterior del mismo, y que además requiere de defensa y protección. El Ciberespacio debe ser tenido en cuenta tanto desde el punto de vista civil como del militar, ya que se ha hecho tan crítico como la tierra, el mar, el aire y el espacio. Si no se controla adecuadamente, se puede ver amenazada la nación en su Seguridad Nacional.

4.6.2 Amenazas en el ciberespacio

El dominio del ciberespacio es ahora un conducto primario para transacciones vitales para cada faceta de la vida moderna que, si bien han permitido la evolución de la sociedad, también ha creado serias vulnerabilidades y amenazas. Las amenazas enemigas siempre han existido en tiempos de guerra o conflicto, pero con la incursión de escenarios informáticas en las actividades de las FF.MM se ha generado el aumento de un nuevo tipo de amenazas cibernéticas; formando parte de las nuevas amenazas que el actuar militar deberá enfrentar en el ámbito de las comunicaciones y transmisión de su información. Pero el daño en el ciberespacio no se ha limitado únicamente al factor ofensivo, la utilización del Ciberespacio para captar, financiar y entrenar terroristas, ha generado otra forma de amenaza para la seguridad de los Estados.

Una Amenaza cibernética puede ser definida como una "*potencial violación de las propiedades de la información en lo que respecta a su confidencialidad, integridad y disponibilidad*". (Manual de Ciberdefensa Conjunta para las Fuerzas Militares de Colombia 3-38).

Las amenazas pueden ser clasificadas de acuerdo a sus características, impacto, origen y actores en accidentales o intencionales. *Las amenazas accidentales* son las que ocurren sin una intención premeditada y *las amenazas intencionales* son las que resultan de actos deliberados en contra de la seguridad de un activo. Las amenazas también pueden ser activas o pasivas, *activas* cuando dan como resultado el cambio en la operación de un sistema, ya sea por la modificación de datos y la destrucción de equipos físicos; en tanto que, *la amenaza pasiva* no involucra cambios en los sistemas y cuyo propósito es obtener información de los sistemas sin afectar los recursos. (Guía de Estrategia de Ciberseguridad de la ITU).

Pueden ser también *físicas* al operar en la capa física del Ciberespacio, dentro de esta categoría se incluye tanto la destrucción real (robo) de los elementos de hardware, como también su inutilización física, mediante, por ejemplo, pulsos electromagnéticos, la forma de afrontarlos es con medidas de protección física o perimetral de las instalaciones donde se encuentran los elementos susceptibles de ser saboteados y finalmente las *amenazas lógicas* que operan en el nivel semántico, sintáctico y la capa de usuarios y consiste en la manipulación de los sistemas cibernéticos, bien sea insertando o activando software con un propósito malicioso, o perturbando las capacidades del sistema comprometido. (Sebastian, M., 2011).

Los cuatro tipos principales de amenazas cibernéticas según Flynn, Cristin & Nicholas, J. P. (2013) son: el cibercrimen, el espionaje militar y político, el espionaje económico y el ciberconflicto.

1) Cibercrimen. Son los actos en los que las TICs son utilizadas para propósitos criminales o usadas como herramientas para cometer acciones ofensivas como, fraude, robo de propiedad intelectual, abuso o daño de sistemas tecnológicos y daños a la infraestructura crítica cibernética.

2) Espionaje militar y político. Esta amenaza incluye casos en que las Naciones-Estado, intentan o logran obtener información sensible militar, de agencias gubernamentales o información industrial.

3) Espionaje Económico. Esta categoría se aplica a los gobiernos (o terceros que actúan en su nombre) robando la propiedad intelectual creada en otras naciones, o empresas que roban información de sus competidores.

4) Ciberconflicto o ciberguerra. Es un tipo de guerra asimétrica tiene implicaciones significativas debido a los ataques cibernéticos. El Internet hace posible que las personas u organizaciones con pocos recursos, anónimos y difíciles de rastrear involucren a un Estado-Nación en conflicto cibernético o ciberguerra.

Existen algunos factores condicionantes que han permitido la potencialización de las anteriores amenazas en el Ciberespacio:

1) El manejo de múltiples identidades de los ciberusuarios así como la adopción de técnicas de enmascaramiento han permitido la ubicuidad del internet, facilitando la infiltración, la explotación y el sabotaje.

2) Los ataques en el ciberespacio pueden requerir muy poco equipamiento y esfuerzo, proporcionando una ventaja a adversarios con muy pocos recursos.

3) El origen de los ciberataques puede ser muy difícil de trazar y rastrear, debido a la característica de ubicuidad que presenta el internet y la ubicación transnacional de las redes.

4) Una sola vulnerabilidad en la red puede impactar negativamente en el ciberespacio, mientras que del lado de la defensa en necesario cerrar la totalidad de las vulnerabilidades para reducir el impacto.

5. Proceso para el desarrollo de operaciones militares cibernéticas

Las operaciones del ciberespacio pueden llevarse a cabo en una variedad de contextos y circunstancias, la decisión de utilizar las capacidades del ciberespacio se debe basar no sólo en los objetivos generales de la operación sino también en los riesgos de posibles respuestas adversas y otros efectos potenciales sobre la operación. Como cualquier tipo de operación, estas deberán obedecer a un proceso sistemático. El propuesto, está basado en el Proceso de Operaciones PRODOP, con el cual se busca el cumplimiento de los objetivos planificados, con el empleo de los medios y recursos de manera efectiva.

El proceso de operaciones cibernéticas se debe componer de las siguientes fases: Planeamiento, preparación, ejecución y evaluación.

5.1 Fase de Planeamiento

De acuerdo a lo establecido en el Manual MFE 5-0 Proceso de Operaciones del Ejército de Colombia, el planeamiento es "*el arte y la ciencia de entender la situación, imaginar un estado final deseado y trazar formas efectivas para conseguirlo*".

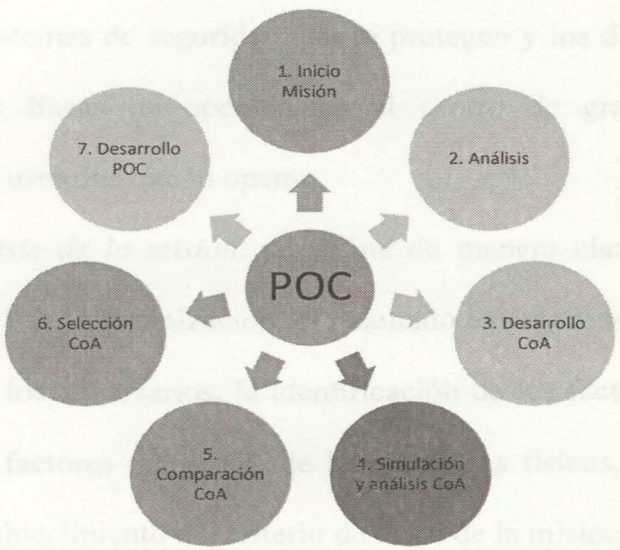
En las OCs en la fase del planeamiento se establece la forma general en la que se planifican, prepararán, ejecutarán y evaluarán los resultados tanto a nivel estratégico como operacional de las actividades de protección y defensa del ciberespacio. Los efectos directos de todas las acciones en el Ciberespacio deberán ser determinadas de antemano a través de esta fase, a su vez esta fase se apoya en el conocimiento que surge de las operaciones en el contexto situacional definido

(ciberinteligencia); así como de la adquisición de información de organizaciones gubernamentales, no gubernamentales y naciones aliadas.

Las operaciones del ciberespacio siempre deben ser planificadas como parte de operaciones y campañas tradicionales, operaciones de respuesta a crisis y operaciones de contingencia y ante atención de desastres.

La planificación debe surgir de un proceso analítico que aporta los detalles sobre los recursos, las funciones y la sincronización entre las diferentes capacidades necesarios para cumplir con los objetivos de la misión, al final la planificación permitirá la transformación de objetivos estratégicos en actividades que se manifiestan en términos de cursos de acción CoA, sustentados en las capacidades operacionales establecidas anteriormente. En la planificación se deberán realizar un conjunto de acciones las cuales se establecen en la siguiente figura, el proceso de planificación propuesto es el Proceso Militar para la Toma de Decisiones PMTD: Fase inicial, análisis de la misión, desarrollo de CoA, simulación y análisis de CoAs, comparación de CoA, selección de CoA y Desarrollo del POC.

Figura 4 - Proceso para la Toma de Decisiones



Nota: Elaboración propia basada en Manual MFE 5-0 Proceso de Operaciones del Ejército de Colombia

En la fase *inicial* del proceso se revisan los documentos estratégicos, se diseñan los objetivos de la misión, se identifican y analizan los blancos de ataque o puntos clave derivados del proceso de gestión de riesgos y se determina el alcance inicial de la operación, entre otras. Lo fundamental en esta fase de la OCs es integrar las capacidades tecnológicas con la organización responsable directa o indirectamente de la operación.

Teniendo en cuenta los siguientes conceptos en donde los *objetivos operacionales* son aquéllos que se han de conseguir mediante una operación para alcanzar la situación final deseada, el *centro de gravedad* es aquella característica o capacidad que proporciona libertad de acción, potencia física, por la cual su eliminación o pérdida conducirá a la derrota de un adversario, los *puntos decisivos s*on aquellos desde donde se puede alcanzar los centros de gravedad propios o del enemigo y que las *líneas de operaciones* unen los puntos decisivos a través del tiempo y el espacio en el camino hacia el centro de gravedad, podemos a manera de ejemplo considerar que en una OC el objetivo podría ser ganar y mantener el control del sistema C2 del adversario, cuyo centro de gravedad será el propio C2 que le garantiza el mando y control sobre las tropas , los puntos de decisivos serán los sistemas de seguridad que lo protegen y los dispositivos de red y servidores que lo integran, las líneas de operaciones al centro de gravedad serán los enlaces de comunicaciones y los usuarios que lo operan.

La fase de *análisis de la misión,* se define de manera clara la misión y se evalúan los requerimientos a nivel de la organización, el resultado en esta fase puede ser la identificación de las Fuerzas aliadas y los adversarios, la identificación de los factores críticos para la misión, la identificación de los factores relevantes de los dominios físicos, de información y lógicos del Ciberespacio y el establecimiento del criterio de éxito de la misión, entre otros.

En La fase *del desarrollo de los Cursos de Acción CoA,* se explotan los productos de la fase de análisis, entre las funciones para esta fase se tienen: la identificación de los efectos deseados definidos por la misión en el nivel operacional y estratégico, los efectos indeseados que pudieran impactar en los objetivos planteados y el análisis y la identificación de los riesgos, entre otros.

Una vez definidos los CoA estos deben ser simulados y contrastados con los CoA del adversario obtenidos por fuentes de ciberinteligencia. En la fase de *simulación y análisis de CoA,* las acciones corresponderán adicionalmente a la redefinición y ajustes a los CoA y la evaluación del riesgo correspondiente.

La fase de *comparación de CoAs,* requiere del análisis y la evaluación de los diferentes CoA por parte de todo el personal involucrado. Se determinarán y evaluarán las fortalezas y debilidades de cada CoA desde las diferentes perspectivas presentes. Las acciones más significativas en esta fase son el análisis y comparación de cada CoA contra la misión y las tareas, y su priorización.

En la fase de *selección de CoAs* el personal a cargo de la misión, debe plantear una recomendación al mando, y relacionar la manera en la que el CoA seleccionado contribuye al logro de la misión. Es fundamental que la recomendación sea realizada de manera clara y precisa para que pueda ser comprendida por todos los involucrados en la toma de decisiones.

En la fase final correspondiente al *desarrollo del plan,* una vez seleccionado y aprobado el CoA, el personal de cuadros llevará a cabo el plan, para ello se deberán considerar todos los aspectos para lograr interiorizarlo en la organización de los diferentes niveles del mando y garantizar la efectividad del mismo. Con el desarrollo del plan se podrán identificar las deficiencias en las capacidades cibernéticas involucradas y las recomendaciones para solucionarlas.

El planeamiento en las operaciones cibernéticas nos permitirá obtener el *Concepto Operacional Cibernético*. Este se constituirá en un elemento de expresión de la decisión del Comandante, en materia operacional para la misión. En él se describe completa y ordenadamente lo que se pretende realizar para conseguir los objetivos operacionales, el propósito para la conducción de las operaciones, el método y la situación final deseada.

Una vez seleccionado y aprobado el CoA se elaborará el Concepto operacional Cibernético, el cual deberá contener como mínimo los siguientes elementos:

1) Situación: Descripción de las circunstancias que han requerido el desarrollo de una operación en y a través del ciberespacio.

2) Misión: Definición clara y concisa del propósito y tipos de capacidades a usarse en el ciberespacio, el Comandante responsable de realizarla, y el tiempo probable para su ejecución.

3) Ejecución: Descripción de la forma en la que el Comandante entiende que la operación debe ser ejecutada., basado en el análisis situacional, relación de los puntos decisivos y los centros de gravedad propios y del adversario.

4) Apoyo logístico: Descripción de los apoyos requeridos para el eficaz cumplimiento del CoA y de la misión.

De manera general en el nivel operacional cibernético se deberán realizar dos tipos de planes: *Planeamiento preventivo y el planeamiento de ejecución o respuesta de crisis.* El plan preventivo

es un planeamiento a mediano o largo plazo, que normalmente se deberá realiza en tiempos de paz, aunque también puede llevarse a cabo ante la inminencia de una crisis para prever una serie opciones que puedan dar solución a las posibles contingencias que pudieran presentarse, dentro de este tipo de planes se encuentra El resultado final de este tipo de plan es el *Plan de contingencia o continuidad BCP,* este plan deber ser un compendio de un plan de recuperación de desastres de naturaleza típicamente tecnológica DRP que responda a una interrupción de los servicios tecnológicos para restablecer las funciones críticas de la institución y de la generación de resiliencia en los activos tecnológicos base en el cumplimiento de la misión.

Lo primero que se debe realizar en un BCP es un análisis del impacto al negocio (BIA), éste es básicamente un informe que muestra el coste ocasionado por la interrupción de los procesos críticos de la organización, para con esto clasificar los procesos en función de su criticidad y establecer la prioridad de recuperación, para finalizar con una estrategia de recuperación fundamentada en unas medidas preventivas, de detección y correctivas que eliminen la amenaza completamente, minimice la probabilidad de que ocurra o minimice su efecto.

Otro de los planes preventivos es el un *plan de defensa cibernética permanente,* de otro lado los *planes de manejo de crisis* se inician por lo general ante una situación de crisis sobrevenida prevista o bien para resolver una amenaza operativa de ejecución inminente, en algunos casos requerirá de la aplicación de un BCP ya existente y de los planes de defensa. Lo importante es tener en cuenta que los lineamientos establecidos en estos planes deben ser tenidos en cuenta en la fase de planeamiento del PRODOP.

5.2 Fase de preparación de Operaciones Cibernéticas

"*La preparación consiste en aquellas actividades realizadas para mejorar la capacidad ejecutar una operación. La preparación crea condiciones que mejoran las oportunidades en aras del éxito de las Fuerzas amigas. Requiere acciones de todas las personas en diferentes niveles del mando, para asegurar que la Fuerza está entrenada, equipada y lista para ejecutar operaciones. La preparación ayuda a entender mejor la situación y los roles dentro de la operación*" (Manual MFE 5-0 Proceso de Operaciones" del Ejército Nacional).

En el Ciberespacio las actividades que conforman la fase de preparación serían:

1) *Efectuar coordinaciones y ejecutar enlaces.*

2) *Iniciar la recolección de información.*

3) *Iniciar las operaciones de defensa de las infraestructuras.*

4) *Iniciar los preparativos de las redes y los sistemas.*

5) *Iniciar los preparativos de sostenimiento, continuidad y resiliencia.*

6) *Conducir ensayos de los cursos de acción.*

7) Revisar y ajustar el POC.

8) Completar la organización en las especialidades requeridas.

9) Entrenar.

Es preciso entender que para llevar a cabo operaciones militares en el ciberespacio, es necesario realizar coordinaciones con entidades y compañías públicas, privadas y mixtas, como los Operadores de Infraestructuras Críticas, Proveedores de Servicio a Internet, Empresas de Telecomunicaciones, entre otros, con el fin de garantizar que los medios y recursos estén a disposición total en el empleo militar en dicho entorno operacional. A su vez se debe contar con el personal con los perfiles requeridos para cada tipo de operación, y este personal debe revisar el plan y probarlo a través de plataformas de simulación y/o en entornos controlados, que emulen las estructuras tecnológicas a neutralizar del adversario. Deben también en esta etapa probarse los Planes de Continuidad o Contingencia, lo cual permita la recuperación de la Fuerza en los tiempos máximos permitidos y hacer reajustes a dichos planes, según se requieran; así mismo, realizar la preparación en la configuración de las herramientas de hardware y software para ejecutar la operación.

5.3 Fase de ejecución de Operaciones Cibernéticas

Es poner el plan en acción mediante la aplicación de capacidades en el ciberespacio, en base al planeamiento establecido. En este contexto toda acción llevada en el ciberespacio deberá estar

sometida a la autoridad relevante de, quien dirigirá las tareas garantizando la sinergia entre los participantes. Así el proceso resultante para la ejecución de Ocs puede ser pensado como una cadena de eventos centrado en una postura ofensiva, analogía que será de especial valor al momento de desarrollar estrategias de ciberseguridad (Mosso, J. 2000).

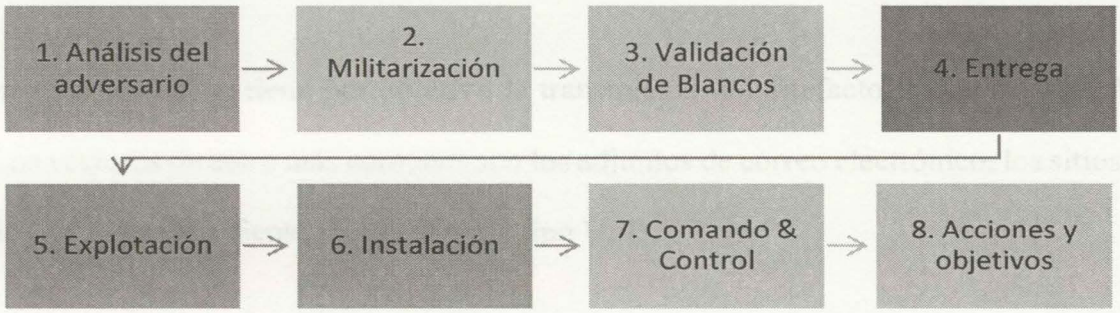
Navajas, R. (2006), decía al respecto de la ejecución de operaciones militares, que el comandante debe considerar cuatro aspectos operacionales claves, que no deben ser vistos de manera independiente:

> *"**CONFORMAR** un ambiente operacional. Para afectar la voluntad y resolución de los tomadores de decisión político-estratégicos adversarios, en combinación con otras actividades estratégicas, con el propósito de generar una percepción de derrota en la mente del enemigo. Simultáneamente, generar el apoyo necesario para las acciones de la fuerza.*
>
> ***ATACAR** la voluntad y cohesión del enemigo. Hacer que sus fortalezas sean irrelevantes. Atacar medios críticos mediante el apoyo de fuegos y maniobra para atacar su voluntad y continuar con el combate.*
>
> ***PROTEGER** el Centro de Gravedad de la fuerza. Es particularmente importante cuando se emplean fuerzas conjuntas y multinacionales.*
>
> ***EXPLOTAR** la situación por todos los medios disponibles (directos o indirectos). La habilidad de la explotación exitosa, descansa en un análisis y administración de riesgos y*

vulnerabilidades que permita identificar y generar oportunidades adelantadas, la agilidad de observar lo inesperado y hacer permanente los aspectos temporales ya alcanzados".

Con base en lo anterior, para esta fase se propone la aplicación de la adaptación de un proceso utilizado por las FF. AA de los EE.UU, el cual relaciona ocho pasos:

Figura 5 - Proceso de Ejecución de Ocs



Nota: Elaboración propia basado en el proceso de las FF.AA de EE.UU

1) Análisis del adversario. En este paso se determina la manera en la que opera el adversario en el largo plazo, permitiendo obtener información sobre los patrones ofensivos del adversario, es decir sobre sus TTP, herramientas, blancos y formas de proceder para lograr sus objetivos estratégicos. Aquí se deben identificar los factores comunes y producir la inteligencia necesaria para seleccionar de CoA defensivos adecuados.

2) Militarización. En este paso se deben desarrollar las capacidades cibernéticas generadas por la dinámica del Ciberespacio, apuntando a completar las capacidades en base al entorno operacional de la operación.

3) Validación de blancos. En base a los blancos seleccionados en las fases de planificación, este eslabón del proceso consiste en la generación de la inteligencia necesaria para su validación o para la modificación de la lista. Además, se prevé el desarrollo de la inteligencia necesaria a fin de lograr el efecto deseado sobre estos.

4) Entrega. Este paso tiene por objetivo la transmisión del artefacto malicioso al ambiente objetivo. Los vectores de entre más comunes son los adjuntos de correo electrónico, los sitios Web, y los medios de almacenamiento removibles de tipo USB.

5) Explotación. Una vez transmitido y entregado el artefacto, en la fase de explotación se dispara o inicia el código malicioso. La explotación requiere de vulnerabilidades a nivel de sistema operativo o aplicaciones, de características o funcionalidades asociados a las TIC, o de la utilización de la ingeniería social.

6) Instalación. En este paso se obtiene el acceso y/o entrada a los sistemas u objetivos adversarios, con el fin de garantizar persistencia en el ambiente objetivo, para ello se vale de tácticas como troyanos o puertas traseras.

7) Comando y Control. Una vez instalado y garantizado la persistencia, se establece una cadena de comunicación entre el objetivo y una entidad que lo controla C2, de esta manera se puede ejecutar el plan previsto.

8) Acciones y objetivos. Luego de haber cumplido con éxito las primeras siete fases, el adversario se está en la capacidad de desarrollar el plan ofensivo y lograr sus objetivos, ya que se encuentra con el acceso y control del blanco adversario. Las acciones pueden estar dirigidos a la obtención de resultados cibernéticos directos o indirectos sobre componentes de infraestructura crítica.

5.4 Fase de evaluación de las Operaciones Cibernéticas

La evaluación es la medición del progreso en el cumplimiento de una tarea, de la creación de un efecto o del logro de un objetivo, (Manual MEF 5-0 del Ejército de Colombia). Al respecto el manual establece que debe ser una actividad continua durante todas las fases del proceso de operaciones, durante el planeamiento, esta se debe centrar en el entendimiento de las condiciones actuales de un ambiente operacional. Durante la preparación, la evaluación se debe centrar en determinar el grado de alistamiento de las propias tropas para ejecutar la operación y en la verificación de los supuestos sobre los que se basa el plan. Durante la ejecución, la evaluación se centra en valorar el progreso de la operación. Con base en la evaluación, se dirigen los ajustes a la orden, asegurándose de que la operación se mantenga enfocada en el cumplimiento de la misión.

La evaluación de las OCs debe estar pensada en un enfoque en tres capas, compuesto de una evaluación física de daños, una evaluación de los daños funcionales y una evaluación de los efectos indirectos con respecto a los resultados funcionales creados en el sistema objetivo.

El proceso de evaluación debe estar encaminado a: 1) Evaluar los efectos de las operaciones cibernéticas desarrolladas, 2) Determinar del grado de avance sobre los objetivos, 3) Mejorar el desarrollo de futuras acciones, 4) Producir la realimentación necesaria para la toma de decisiones, y 5) Aportar datos para la determinación del retorno de la inversión.

En el Ejército de Colombia *las apreciaciones dinámicas, las revistas después de la acción (RDA) y el plan de evaluación,* se constituyen en instrumentos utilizados para la evaluación. *El plan de evaluación debe incluir la medición de la efectividad, el desempeño e indicadores que ayuden al comandante y el Estado Mayor a evaluar el progreso hacia el cumplimiento de las tareas y la consecución de objetivos*, (Manual de proceso de operaciones del Ejército de Colombia).

Las operaciones cibernéticas deben ser evaluadas tanto a nivel táctico, como operacional y estratégico.

1) Evaluación operaciones cibernéticas a nivel táctico. Consiste en la determinación de la efectividad de las operaciones tácticas en base a la recolección y el análisis de un conjunto de indicadores tácticos objetivos, de tipo cualitativo y cuantitativo, previamente definidos en las fases de planificación. El resultado de este tipo de evaluación indica a los mandos medios y altos de mando la necesidad o no de desarrollar más acciones.

Esta evaluación es una medida de efectividad en términos de los efectos directos producto de las tareas tácticas desarrolladas contra las tareas tácticas asignadas. Para realizar esta evaluación

se debe valer de análisis cualitativos o cuantitativos respondiendo a preguntas tales como ¿Se realizó la acción prevista?, ¿Se creó el efecto directo previsto?, ¿Ha cambiado el estado del objetivo?

2) Evaluación operaciones cibernéticas a nivel operacional y estratégico. Este tipo de evaluación es destinada a soportar el juicio analítico de la estrategia implementada, es decir de los fines, las formas y los medios empleados para el logro de los objetivos. Permite determinar el progreso en el esfuerzo para lograr los objetivos operacionales y estratégicos planteados, y en base a este se genera información de realimentación destinada a ajustar la estrategia y los CoA futuros.

Este tipo de evaluación es donde se evalúan los efectos indirectos, se mide el progreso hacia los objetivos operacionales y estratégicos y se formulan recomendaciones para los ajustes de la estrategia y la acción futura como el contraataque. La evaluación operacional y estratégica es una medida de *eficacia* en relación a que ayudan a medir el progreso hacia el estado final y de *rendimiento* porque mide los métodos utilizados y los medios de la estrategia.

6. Clasificación, Métodos y técnicas de las operaciones cibernéticas

Dentro de la doctrina anglosajona, en el Plan de Capacidades 2016-2028, El Ejército de los Estados Unidos; así como la de países como España, Brasil y otros países que integran la OTAN, establece para las Operaciones militares en el Ciberespacio, el desarrollo de las siguientes capacidades:

1) Defensa del ciberespacio. Para ello se propone adoptar medidas a través del ciberespacio para proteger, analizar, detectar, y responder a la actividad no autorizada en los sistemas de información y comunicaciones o de control automatizado. Las acciones de defensa cibernética no sólo buscan proteger los sistemas de un adversario externo, sino también de su explotación desde dentro de la propia organización.

2) Explotación en el ciberespacio. Las capacidades en explotación consisten en la recolección de inteligencia, llevadas a cabo o través del ciberespacio para recopilar datos de los sistemas de información y comunicaciones del adversario.

3) Respuesta en el ciberespacio. La respuesta se debe componer de las medidas adoptadas a través del ciberespacio para interrumpir, negar, degradar o destruir la información manejada por los sistemas de información y comunicaciones del posible adversario o los propios sistemas de información y comunicaciones.

De acuerdo a las anteriores capacidades planteadas por diferentes ejércitos del mundo, se

propone desarrollar los siguientes tipos de operaciones militares en y a través del Ciberespacio, cuyos métodos y tácticas se fundamentan en diferentes teorías y procedimientos desarrollados en Ciberseguridad, emanados de diferentes organismos como ENISA, CCN, ANSI, y la ITU, entre otros.

La siguiente tabla presenta los tipos de operaciones a desarrollar en las FF.MM de Colombia, encaminadas a desplegar las capacidades requeridas para la defensa y protección; así como la consecución de la superioridad militar y la libertad del accionar militar en el Ciberespacio.

Tabla 2 - Clasificación y tipos de Operaciones Cibernéticas

CAPACIDAD	TIPO OC
DEFENSA	**OCD.** Operaciones Cibernéticas de Defensa **OCDA.** Operaciones Cibernéticas de Defensa Activa. **OCAC.** Operaciones cibernéticas de Administración de la Ciberseguridad.
EXPLOTACIÒN	**OCI**. Operaciones de Ciberinteligencia
RESPUESTA	**OCO.** Operaciones Cibernéticas Ofensivas

Capacidad Defensiva

La defensa en las Operaciones Cibernéticas tiene como objetivo proteger y asegurar el ciberespacio de las amenazas cibernéticas. Dichas actividades deben estar enmarcadas en el ámbito de la gestión de la ciberseguridad, del monitoreo, detección y análisis de actividad no autorizada, así como fortalecer la capacidad de resiliencia del componente cibernético propio.

Las operaciones defensivas deben ser acciones destinadas a:

- Repeler, resistir, rechazar o destruir un ataque y contraataque del enemigo.
- Crear condiciones favorables para la acción ofensiva.
- Economizar fuerzas para ser empleadas en una acción más decisiva

- Destruir o reducir la capacidad enemiga para la acción ofensiva o negar la entrada del enemigo.

Para el desarrollo de la capacidad defensiva cibernética, se pueden desarrollar las siguientes operaciones cibernéticas:

6.1 Operaciones Cibernéticas de Defensa OCD

El objetivo de las OCD es defender y proteger los sistemas cibernéticos propios y amigos en el ciberespacio. Son acciones consistentes en preservar las capacidades militares en el ciberespacio; a través de la protección de los datos, redes, sistemas de información y comunicaciones. Las OCD responden a la actividad no autorizada o alertas de amenazas contra la infraestructura cibernética militar, aprovechando la Ciberinteligencia u otras capacidades militares según sea necesario.

Las OCD responden a las amenazas tanto internas como externas del ciberespacio que impactan los sistemas cibernéticos defendidos. Las medidas defensivas internas incluyen acciones de aseguramiento de la misión para restablecer dinámicamente, re-asegurar, redireccionar, reconstituir o aislar las redes locales degradadas o comprometidas, garantizando de esta manera un acceso seguro de la Fuerza al Ciberespacio.

Las OCD pueden llevarse a cabo en respuesta a un ataque, explotación, intrusión. La misión de las OCD se lleva a cabo usando capas adaptables profundidad, con elementos de apoyo mutuo de la protección digital y física. Es decir, las OCD se fundamentan en el empleo de *Defensa en Profundidad.*

La Defensa en profundidad se define en la guía CCN-STIC-400 como "*Estrategia de protección consistente en introducir, múltiples capas de seguridad que permitan reducir la probabilidad de compromiso en caso de cada una de las capas falle y en el peor de los casos minimizar el impacto*".

Esta estrategia propone un enfoque defensivo que implanta protecciones o mecanismos de seguridad en todos los niveles de modelo OSI (Open System Interconection), Las medidas de seguridad a implementar en cada capa podrán variar en función del entorno de la operación del sistema; sin embargo, el principio base o general permanece inalterable, pudiendo ser de acuerdo a la siguiente tabla.

Tabla 3 - Herramientas de defensa en profundidad

CAPA DE DEFENSA	ESTRATEGIA DEFENSA EN PROFUNDIDAD
APLICACIÓN	Cortafuegos de aplicación, proxy reverso, sistemas de prevención de intrusos, encriptación, control de acceso autenticación.
TRANSPORTE	Mecanismos de cifrado como Socket Secure Layer SSL o Transport Secure Layer TLS
RED	Cortafuegos, sistemas de protección de intrusiones de red y correlación de eventos
FÍSICA	Plataformas de sandboxes, arquitecturas de alta disponibilidad y sistemas de recuperación, mantenimiento de los equipos, sistemas de extinción automática de incendios, sensores de humo, sistemas de control de acceso.

Así el principio fundamental detrás de este concepto es el de dificultar las acciones del atacante, a través de las diferentes medidas de seguridad, aplicadas a cada una de las capas, de tal forma que cada sensor del sistema detecte las actividades maliciosas. Cuando una capa se ve comprometida, las medidas de detección, reacción y recuperación, permiten reaccionar, disminuyen la probabilidad que otras capas se vean comprometidas.

Las OCD se sub clasifican a su vez en: Preactivas, proactivas y reactivas.

*1) **Operaciones cibernéticas de defensa preactivas**.* Son las que se ejecutan antes de que se produzca el ataque del enemigo. Entre ellas están la concienciación y formación de usuarios y técnicos, y la definición de normas y procedimientos que permitan la instalación y configuración correcta de hardware, software y las acciones de disuasión.

a. Métodos de las operaciones de defensa preactiva – Gestión de la ciberseguridad. Es aquel que permite el establecimiento, y mejora de la ciberseguridad en los sistemas cibernéticos de la Fuerza; a través de la definición de normas o políticas, instrucciones técnicas, procedimientos, guías, planes que garanticen la integridad, disponibilidad y confidencialidad de las infraestructuras cibernéticas internas o propias.

Dentro de las técnicas para este tipo de operaciones encontramos:

- *Técnica de diseño de Políticas, normas, guías y procedimientos*. Como lo establece la Guía CCN-STIC-400, definir una política es definir un marco general administrar los riesgos asociados al procesamiento de información y de la seguridad digital de la infraestructura tecnológica y de comunicaciones, por medio del cual se orientarán todas las acciones a seguir por parte de todos los funcionarios y usuarios de los sistemas cibernéticos de la Fuerza. En este caso se deberán adicionalmente diseñar y aplicar procedimientos y guías para la administración segura de los activos en el ciberespacio, tales como: Procedimientos de gestión de usuarios y contraseñas, Procedimiento de control de cambios, Procedimientos de Backups y recuperación, Procedimientos para el desarrollo seguro de software, Procedimiento de clasificación de la información, entre otros.

- *Técnica de gestión de activos y clasificación de la información.* Se debe lograr y mantener una protección adecuada de los activos organizacionales, efectuando una identificación clara de los activos de la institución, estableciendo responsables sobre los mismos y clasificándolos de acuerdo a su impacto en el cumplimiento misional de la Fuerza. Así mismo deberá clasificarse toda la información física y digital y deben establecerse los procedimientos para su correcto tratamiento.

- *Técnica de gestión de riesgos de seguridad.* El análisis de riesgos es la técnica a través de la cual se puede obtener una visión clara y priorizada de los riesgos a los que se enfrenta una Organización, tiene como propósito identificar los principales riesgos a los que una entidad está expuesta, ya sean desastres naturales, fallos en infraestructura o riesgos introducidos por el propio personal. En este sentido deben identificar los riesgos de seguridad más significativos que pueden afectar a la operativa de la institución y priorizar medidas a implantar para minimizar la probabilidad de materialización de dichos riesgos o el impacto en caso de materializarse.

- *Técnica de planificación de continuidad de la operación.* A través de esta técnica se deben diseñar los protocolos de alertas, responsabilidades y comunicación, las medidas de control y planes de restablecimiento de servicios. Adicionalmente se deben hacer los ensayos al plan.

- *Técnica de planificación de la recuperación ante desastres.* Esta técnica permite establecer las estrategias de recuperación de servicios, los procedimientos para ello, una vez notificado el tiempo de contingencia.

- *Técnica de vigilancia tecnológica.* A través de esta técnica se busca captar información del exterior y de la propia organización sobre ciencia y tecnología, seleccionarla, analizarla, difundirla y comunicarla, para convertirla en conocimiento para tomar decisiones con menor riesgo y poder anticiparse a los cambios.

- *Técnica de sensibilización.* A través de esta técnica se deben diseñar y desarrollar programas de sensibilización de los funcionarios a todo nivel, que permitan mejorar las habilidades de los usuarios, administradores de seguridad y de TICs, en el manejo seguro de las plataformas cibernéticas y de la información.

- *Técnica de inspecciones de ciberseguridad.* Las inspecciones de seguridad constituyen el medio que permite valorar el estado de la información manejada por los sistemas contra la pérdida de confidencialidad, integridad o disponibilidad, ya sea accidental o intencionada, así como la protección de la integridad y disponibilidad de los propios sistemas que sustentan dicha información. La evaluación exhaustiva de la eficacia de las medidas de seguridad de un sistema cibernético a través de técnicas y procedimientos de verificación constituye una actividad crítica llevada a cabo por la propia Organización y busca garantizar que se han adoptado las contramedidas y salvaguardas adecuadas para la protección de los sistemas.

Siguiendo los pasos propuestos en la Norma de Seguridad de las TIC del Centro Criptológico Nacional CCN-STIC-400, las inspecciones de seguridad deben seguir como mínimo los siguientes pasos:

El primero se refiere al *análisis, el cual consiste* en la supervisión de la gestión de riesgos y la aplicación de los requisitos de seguridad a la misión de la institución y esté acorde con los objetivos estratégicos de esta. Estas actividades son llevadas a cabo a través de revisión de la documentación, visitas in situ y entrevistas con los usuarios y responsable.

El segundo paso propuesto en la norma es la *verificación*, la cual consiste en la comprobación de la implementación de controles de seguridad y en el análisis de vulnerabilidades sobre los procesos de la organización, en esta se contemplan actividades como: Análisis del flujo de información en el Sistema (análisis de tráfico), grado de cumplimiento de la lista de comprobación aprobada para el Sistema, empleo de herramientas de seguridad (verificación automática) para determinar el estado de seguridad del Sistema ante vulnerabilidades conocidas, análisis manual del sistema operativo y aplicaciones en busca de agujeros de seguridad (verificación manual), gestión del software del Sistema, y evaluación TEMPEST (Transient Electro Magnetic Pulse Emanation Standard) del Sistema.

Como último paso propuesto se tiene el *test de intrusión,* el cual consiste en un ataque activo a los sistemas basado en pruebas de intrusión con el fin de medir el nivel de acceso al sistema, para el desarrollo de esta fase se requiere el desarrollo de las siguientes actividades: Ataque, conocido por los responsables de la institución, intentando penetrar en el sistema a pesar de las defensas implementadas, ataque, sin conocimiento por parte de los responsables de la institución, intentando penetrar en las defensas del sistema.

- *Técnica de evaluar la eficacia de los controles de seguridad.* A través de esta técnica se incluyen todas las acciones encaminadas a medir la eficacia (aspectos técnicos y procedimentales)

real de las medidas y/o controles de seguridad implementados en los sistemas cibernéticos de la institución. Estas actividades deben hacerse a petición del jefe de ciberseguridad.

*2) **Operaciones cibernéticas de defensa proactiva**.* Son las que se ejecutan en el momento en el que se detecta el posible ataque del enemigo. Estarán basadas principalmente en normas y procedimientos (análisis de eventos, determinación de atribuciones, desconexión de sistemas, lanzamiento de contraataques). Dentro de estas se pueden distinguir dos tipos de reacciones defensivas:

Reacción Pasiva. Es en la que tan solo se ponen defensas, protecciones guardas, pero no se toma ninguna acción.

Reacción semiactiva. En las que las defensas establecidas toman pequeñas acciones no agresivas, como cortar las comunicaciones o bloquear direcciones IP.

Los métodos y técnicas a emplear en este tipo de operaciones son:

a. Método de detección de actividad maliciosa. Consiste en la recopilación de una amplia gama de sensores, base para el análisis que separe los flujos de tráfico entre entidades maliciosos, que permita la evaluación de la situación. Se compone a su vez de las siguientes técnicas:

- *Técnica de recopilación de datos de sensores.* Esta técnica consiste en recoger en un repositorio global, los datos de las actividades en curso; a través de la utilización de sensores y la

alineación de la sintaxis de los datos. Los sensores incluyen los sensores de detección de intrusos, escáneres de vulnerabilidad, informes de registro de eventos de dispositivos como cortafuegos, servidores y proxys entre otros. Además de la recolección de datos, estos tienen que ser pre procesados para unificar la sintaxis y los puntos de referencia

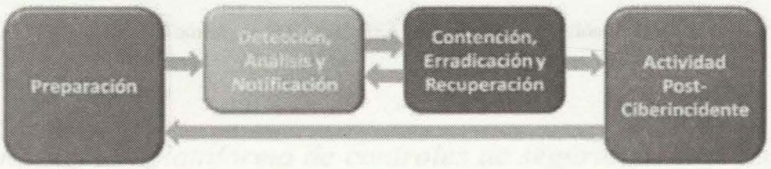
- *Técnica de evaluación de entidades.* Consiste en la fusión de las observaciones de los sensores en entidades asociadas, con entidades comunes, clasificando estas según sean dañinas o no. En el ciberespacio una entidad es cualquier conjunto de datos relacionados de alguna manera, por ejemplo, los datos asociados a una página web, una llamada de voz sobre protocolo IP o un ataque de denegación de servicio distribuido. A su vez se compone de: *Normalización de los datos de sensores, Correlación de datos de sensores, Asignación de atributos de las entidades, Caracterización de entidades.*

- *Técnica de evaluación de la situación.* Este método consiste en reconocer actividades, entidades como relaciones entre entidades, sus actores, así como su significado y contexto. Se compone de las siguientes técnicas: *Técnica de correlación de entidades, técnica de localización técnica de la fuente de ataque, técnica de Interpretación de la actividad y el contexto.*

- *Técnica de Gestión de incidentes de seguridad.* La gestión de ciberincidentes es un proceso cuyo objetivo es recuperar el nivel habitual de funcionamiento del servicio y minimizar en todo lo posible el impacto negativo en la organización de forma que la calidad del servicio y la disponibilidad se mantengan.

De acuerdo a la guía CCN-STIC- 403 Gestión de Incidentes de la seguridad del Centro Criptológico de España y la Guía para la Administración de Incidentes de ENISA, el proceso de gestión de incidentes se divide en tres fases: *DETECCIÒN, TRIAGE o ANÁLISIS y RESPUESTA DEL INCIDENTE.* Dichas fases pueden ser vistas dentro del ciclo de vida del ciberincidente como lo muestra la figura.

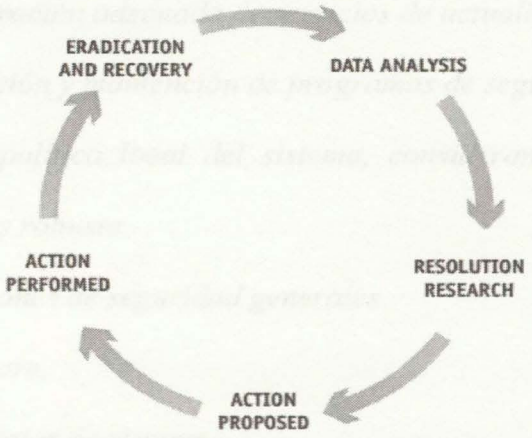
Figura 6 - Ciclo de vida de un ciberincidente



Nota: Tomado de la Guía CCN-STIC-403

Los ciberincidentes pueden detectarse usando distintas herramientas, con diferentes niveles de detalle y fidelidad: sistemas automatizados de detección (incluyendo la utilización de IDS/IPS de red o de servidor, software antivirus y analizadores de logs, entre otros) o medios manuales (como la notificación de problemas por parte de los propios usuarios), en la etapa del triage se determina la prioridad de las acciones con base en la severidad del ciberincidente, a su vez se subdivide en tres fases: Verificación, clasificación inicial y asignación. En la fase de respuesta se iniciará la resolución del ciberincidente, Esta es la fase más larga en la cual se deberá liderar la mitigación del mismo, dicha respuesta está basada en un ciclo: *Análisis de datos, investigación de la resolución, acciones propuestas, acciones realizadas y erradicación/recuperación.*

Figura 7 -Ciclo de respuesta a ciberincidentes



Nota: Tomado de la Guía ENISA para la administración de Incidentes

b. Método de instalación plataforma de controles de seguridad. Este método corresponde a la implementación y configuración en modo activo de protecciones en múltiples capas de seguridad que permitan reducir la probabilidad de compromiso en caso de cada una de las capas falle y en el peor de los casos minimizar el impacto, dicha técnica corresponde al tema tratado en apartes anteriores como Defensa en profundidad.

c. Método de aseguramiento de infraestructura de TI. El endurecimiento (hardening) es el proceso de asegurar un sistema mediante la reducción de vulnerabilidades en el mismo, esto se logra eliminando software, servicios, usuarios; innecesarios en el sistema; así como cerrando puertos que tampoco estén en uso. Esta técnica debe ser aplicada siempre que se lleve a producción un servicio en las redes propias. Dentro de las técnicas de endurecimiento encontramos:

- *Configuraciones necesarias para protegerse de posibles ataques fisicos o de hardware de la máquina.*

- *Instalación segura del sistema operativo.*
- *Activación y/o configuración adecuada de servicios de actualizaciones automáticas.*
- *Instalación, configuración y mantención de programas de seguridad.*
- *Configuración de la política local del sistema, considerando varios puntos relevantes: Política de contraseñas robusta.*
- *Configuración de opciones de seguridad generales*
- *Restricciones de software.*
- *Configuración de servicios de sistema*
- *Configuración de los protocolos de Red.*
- *Configuración adecuada de permisos de seguridad en archivos y carpetas del sistema.*
- *Configuración de opciones de seguridad de los distintos programas.*
- *Configuración de acceso remoto.*
- *Configuración adecuada de cuentas de usuario.*
- *Cifrado de archivos o unidades según las necesidades del sistema.*
- *Realizar y programar un sistema de respaldos frecuente a los archivos y al estado de sistema. En*
- *Activación de auditorías de sistema.*
- *Sistema de respaldos frecuente a los archivos y al estado de sistema.*

d. Método análisis dinámico de riesgos, ataques y daños. El análisis dinámico de riesgos es un método por el cual se evalúa el riesgo de manera continua y automática para poder proyectar la situación actual en el futuro y poder predecir el impacto. Este análisis de riesgos se diferencia del

tradicional, ya que es automático y continuo. Hace uso de varios métodos de cálculo que toma varias variables de diferentes técnicas, como:

- *Técnica de valoración de activos.*
- *Técnica de evaluación de la amenaza.*
- *Técnica de gestión de vulnerabilidades.* Esta técnica consiste en la identificación, evaluación y corrección de vulnerabilidades (huecos de seguridad cibernética) en los sistemas de información, telecomunicaciones y aplicaciones. Esta técnica debe ir más allá de la evaluación de las vulnerabilidades, ya que categoriza los activos y clasifica las vulnerabilidades según el riesgo; así como establece los cursos de acción y jerarquización de las tareas de remediación.

La gestión de vulnerabilidades debe incluir las siguientes acciones:

- Obtención de un inventario y nivel de categorización por criticidad, de los activos de TI de una empresa, lo que incluye servidores, infraestructura de redes, estaciones de trabajo, impresoras y aplicaciones.
- Detección de las vulnerabilidades existentes mediante escáneres de red, escáneres de vulnerabilidades y software de pruebas de penetración automáticas y determinación de los niveles de riesgo.

- Remediación de sistemas y activos vulnerables y presentación de informes sobre las medidas adoptadas.

- *Técnica de hacking ético.* Esta técnica es posterior a la Gestión de Vulnerabilidades, o parte de las base y de la información de aquellas vulnerabilidades que pudieran ser explotables, ya que consiste en la realización de ataques a los activos cibernéticos, con el fin de evaluar el estado real de seguridad. El resultado final indica los puntos débiles y que pasos se deben realizar para eliminar dichas debilidades o mitigarlas caso de no ser posible su eliminación. Existen tres modalidades de test de hacking ético: *El test de caja negra* parte sin tener información relevante de la organización como direccionamiento IP, se parte desde cero, por lo general se realiza para intrusión de infraestructura y de aplicaciones, *el test de caja blanca* recopila con anticipación toda la información posible para evaluar la seguridad, incluyendo código fuente de aplicaciones, archivos de configuración, planos de red, entre otros; Las pruebas que se pueden realizar con esta técnica son las siguientes: Revisión de código fuente y auditorías de red, por último el *test de caja gris* Combina test de caja negra y caja blanca, hace pruebas con métodos similares a los de caja negra, simulando ataques reales. Sin embargo, en el test de caja gris se dispone de información técnica del sistema y se le permite pedir información adicional.

3) ***Operaciones cibernéticas de defensa reactiva.*** Son las que se deberán ejecutar una vez que se haya producido el ataque del enemigo, indiferente si esta ha tenido o no éxito. Serán las acciones encaminadas a la recuperación y aumento de la disponibilidad de los sistemas o averiguar en qué

sistemas se ha producido un daño o como ha sucedido un robo de información; así como la puesta de los medios para evitar su repetición.

Los métodos y las técnicas a emplear en estas operaciones son las siguientes:

a. *Método de recuperación ante ciberataques*. Corresponde a las actividades realizadas para recuperarse de un ataque mediante la restauración del sistema y la información a su estado original y propiedades de seguridad. Se compone de las siguientes técnicas:

- *Restauración de la integridad del sistema.*
- *Restauración de integridad de la información.*
- *Restauración de la disponibilidad del servicio.*
- *Registro de la información comprometida.*

b. *Método de análisis forense digital*. Como lo refiere López, M. (2007), el análisis forense digital es conjunto de principios y técnicas que comprende el proceso de adquisición, conservación, documentación, análisis y presentación de evidencias digitales y que llegado el caso puedan ser aceptadas legalmente en un proceso judicial. Por evidencia digital se entiende al conjunto de datos en formato binario, esto es, comprende los ficheros, su contenido o referencias a éstos (metadatos) que se encuentren en los soportes físicos o lógicos del sistema atacado.

Una vez identificado el ciberincidente, se deben seguir una serie de fases en la AFD: *Recopilación de evidencia, Preservación de la evidencia, Análisis de la evidencia, Documentación y presentación de resultados.*

Recopilación de evidencia. En esta fase se obtienen copias de la información que se sospecha que puede estar vinculada con algún incidente. De este modo, hay que evitar modificar cualquier tipo de dato utilizando siempre copias bite a bite con las herramientas y dispositivos adecuados. Cabe aclarar este tipo de copia es imprescindible, debido a que nos dejara recuperar archivos borrados o particiones ocultas, arrojando como resultado una imagen de igual tamaño al disco estudiado. Rotulando con fecha y hora acompañado del uso horario, las muestras deberán ser aisladas en recipientes que no permitan el deterioro ni el contacto con el medio. En muchos casos, esta etapa es complementada con el uso de fotografías con el objetivo de plasmar el estado de los equipos y sus componentes electrónicos. Se recomienda la utilización de guantes, bolsas antiestáticas y jaulas de Faraday para depositar dispositivos que puedan interaccionar con ondas electromagnéticas como son los celulares. En esta fase de deben realizar mínimo las siguientes tareas y para mayor información refiérase a la RFC 3227:

- Interpretar comandos en modo consola (cmd, bash).
- Enumerar puertos TCP y UDP abiertos y sus aplicaciones asociadas (fport, lsoft).
- Listar usuarios conectados local y remotamente al sistema
- Obtener fecha y hora del sistema (date, time).
- Enumerar procesos activos, recursos que utilizan, usuarios o aplicaciones que los lanzaron (ps, pslist).

- Enumerar las direcciones IP del sistema y mapear la asignación de direcciones físicas MAC con dichas IP (ipconfig, arp, netstat, net).
- Buscar ficheros ocultos o borrados (hfind, unrm, lazarus).
- Visualizar registros y logs del sistema (reg, dumpel).
- Visualizar la configuración de seguridad del sistema (auditpol).
- Generar funciones hash de ficheros (sah1sum, md5sum).
- Leer, copiar y escribir a través de la red (netcat, crypcat).
- Realizar copias bit-a-bit de discos duros y particiones (dd, safeback).
- Analizar el tráfico de red (tcpdump, windump).

Preservación de la evidencia. En esta etapa se debe garantizar la información recopilada con el fin de que no se destruya o sea transformada. Es decir que nunca debe realizarse un análisis sobre la muestra incautada, sino que deberá ser copiada y sobre la copia se deberá realizar la pericia. De este modo, aparece el concepto de cadena de custodia, la cual es un acta en donde se registra el lugar, fecha, analista y demás actores que manipularon la muestra. En muchos casos deberemos utilizar las técnicas de Hashes para identificar de forma unívoca determinados archivos que podrían ser de gran utilidad para la investigación.

Análisis de la evidencia. Cuyo objetivo es reconstruir con todos los datos disponibles la línea temporal del ataque o timeline, determinando la cadena de acontecimientos que tuvieron lugar desde el instante inmediatamente anterior al inicio del ataque, hasta el momento de su descubrimiento. Para ello se debe llegar a los siguientes objetivos: *reconstrucción de la secuencia*

temporal del ciberataque, determinación de cómo se realizó el ciberataque, identificación de autor(es) del ciberataque y evaluación del impacto causado al sistema.

Documentación del ciberincidente. Si bien esta es una etapa final, se debe ir documentando todas las acciones, en lo posible, a medida que vayan ocurriendo. Aquí ya se debe tener claro qué fue lo sucedido, e intentar poner énfasis en cuestiones críticas y relevantes a la causa. Se deben citar y adjuntar toda la información obtenida, estableciendo una relación lógica entre las pruebas obtenidas y las tareas realizadas, asegurando la repetibilidad de la investigación.

6.2 Operaciones Cibernéticas de Defensa Activa OCDA

Este tipo de operaciones utiliza técnicas de ataque con el único propósito de parar o mitigar un ataque en curso. Pueden tener como objetivo retomar el control sobre los recursos propios o sofocar ataques neutralizando la fuente de los mismos.

Las OCDA son aquellas acciones defensivas deliberadas, autorizadas que se toman fuera de las redes y sistemas cibernéticos propios para derrotar un ataque en curso y de esta manera defender las capacidades del ciberespacio. Las OCDA deben ser autorizadas de acuerdo con las reglas permanentes de participación y cualquier regla complementaria aplicable de compromiso y que puede elevarse al nivel de uso de la Fuerza. En general este tipo de operaciones obedecerán a *contramedidas* que solo degradará, y no derrotarán o contratacarán, las actividades de un adversario.

Contramedidas en el ciberespacio. Son esa forma de ciencia militar que por el empleo de dispositivos y/o técnicas, tiene como objetivo el deterioro de la efectividad operativa de la actividad enemiga. En el ciberespacio, las contramedidas identifican la fuente de una amenaza en los sistemas cibernéticas propias y amigos y utilizan técnicas no intrusivas para detener o mitigar la actividad ofensiva en el ciberespacio., por ejemplo, con el empleo de IPS en modo activo. Las contramedidas no son de naturaleza destructiva, normalmente sólo afectan la actividad maliciosa, pero no a los sistemas fuente de amenazas, y finalizan cuando la amenaza se detiene. Las contramedidas en el ciberespacio no deberían obstaculizar significativamente las operaciones o la funcionalidad de la red en la que se están empleando, ni deben causar intencionalmente lesiones o la pérdida de vidas.

Los métodos y técnicas cibernéticas que se pueden emplear en este tipo de operaciones pueden ser:

a. Método de reconfiguración de la topología de los sistemas. Este método consiste en la modificación de la estructura de los sistemas de información y comunicaciones, incluyendo sus servicios, software, hardware, su interconexión, así como la configuración de cualquiera de sus módulos o componentes, se compone de las siguientes técnicas:

- *Reubicación de los servicios de información.*
- *Compartimentación de sistemas.*
- *Cierre de componentes y servicios.*
- *Revocación de credenciales.*

- *Actualización de hardware, software y su configuración.*
- *Control del flujo de tráfico de red.*

b. Método de decepción. Con esta táctica se crean de forma estática y dinámica áreas del sistema TIC en las que el atacante pueda desarrollarse sin impacto, lejos de la operativa normal del sistema. Dentro de las tácticas tenemos: sandboxing, honey net, protección de DNS autoritativos, DMZ de seguridad.

6.3 Operaciones Cibernéticas de Administración de Ciberseguridad OCAC

Estas operaciones corresponden a las acciones tomadas para diseñar, construir, configurar, asegurar, operar, mantener y sostener los sistemas y redes de comunicaciones propias y amigas, de tal manera que se garantice la disponibilidad de datos, integridad, confidencialidad, así como la autenticación de usuario / entidad y el no repudio.

Estas incluyen acciones que abarcan toda la infraestructura cibernética, incluyendo el control de configuración y parches, formación de usuarios, seguridad física y diseño de arquitectura segura, operación de sistemas de seguridad basados en host y firewalls, y cifrado de datos. A pesar de que muchas actividades de operaciones de OCAC son actividades regulares en el funcionamiento de la ciberseguridad, estas no deben ser consideradas rutinarias o sin importancia, ya que su efecto agregado establece el marco de seguridad del que dependerán en última instancia, todas las misiones de la Fuerza.

Dentro de los métodos planteados para este tipo de operaciones se tienen:

- Gestión de activos.

- Seguridad física y del entorno.
- Mantenimiento y operación de las plataformas de ciberseguridad
- Protección contra código malicioso.
- Gestión de seguridad de las redes de datos.
- Gestión de medios removibles.
- Control de acceso a usuarios.
- Control de acceso a las redes.
- Control de acceso a las aplicaciones y la información.
- Criptografía.
- Actualizaciones de firmware y software.

Capacidad de explotación

La explotación por su parte, incluye el empleo de capacidades de recolección de información de inteligencia, llevadas a cabo a través del uso de redes de computadoras y demás capas del ciberespacio, para recopilar datos de los sistemas de información y comunicaciones del posible adversario y de las propias.

Las acciones encaminadas a las operaciones de explotación componen el conocimiento inmediato tanto del adversario como del propio y los aliados, así como de toda la información pertinente sobre las actividades en el ciberespacio. La explotación se obtiene de una combinación de actividades de inteligencia y operativas tanto en el ciberespacio, como en el resto de dominios, llevadas a cabo tanto de manera unilateral como a través de la colaboración con aliados estratégicos del sector público y privado. Los productos de explotación deben comprender:

- La comprensión del adversario y el aliado; así como de otras actividades relevantes del ciberespacio.
- La evaluación de las capacidades cibernéticas amigas.
- La evaluación de las capacidades cibernéticas e intenciones del adversario.
- El análisis de las vulnerabilidades cibernéticas del adversario y del aliado.
- La comprensión de la información que fluye a través de las redes para deducir su propósito y criticidad.
- La comprensión de los efectos y el impacto en la misión, resultante de las degradaciones en el ciberespacio amigo y también adversario.

6.4 Operaciones de Ciberinteligencia

Este tipo de operaciones las constituyen las acciones de inteligencia llevadas en y a través del ciberespacio para obtener información que pueda ser necesaria para apoyar operaciones cibernéticas futuras o en curso, dichas actividades deben sincronizarse e integrarse en las etapas de planificación y ejecución de las operaciones en el Ciberespacio. Las actividades se centran en la ciberinteligencia táctica y operacional; así como en el entendimiento del ciberespacio propio o del adversario para apoyar la planeación militar y la toma de decisiones. En la etapa de ejecución se emplean acciones relacionadas con la información para influenciar, interrumpir, corromper o usurpar la *toma de decisiones del adversario* en el ciberespacio; así como neutralizar sus sistemas de inteligencia, mientras que se salvaguardan las propias, para ello se valen de técnicas como el engaño o de los dominios físicos para cumplir su misión.

La inteligencia recolectada en el ciberespacio puede provenir de los sistemas propios y de diversas fuentes tanto nacionales como externas y pueden servir a requisitos estratégicos, operativos o tácticos y se basan fundamentalmente en la *conciencia situacional*.

La conciencia situacional de acuerdo a la afirmación de Endsley, M.R (2000) es *"Una representación mental y comprensión de los objetos, eventos, gente, estados de los sistemas, interacciones, condiciones ambientales y cualquier otro tipo de factores de una situación específica que puedan afectar al desarrollo de las tareas humanas, bien sean complejas o dinámicas"*.

De tal manera realizando una comparativa podemos decir que la ***conciencia situacional del Ciberespacio (CSC)***, corresponde al conocimiento del Ciberespacio amistoso y adversario; así como de información pertinente y relativa al ciberespacio y el Espectro Electromagnético (ESM), aplicando un análisis y juicio a dicha información, para determinar las relaciones entre las variables operacionales y de misión. Una CSC completa y precisa es crítica, para la toma rápida de decisiones en un Entorno Operacional EO cambiante; ya que este es un compendio de condiciones, circunstancias e influencias que afectan el empleo de las capacidades y las decisiones del comandante. El comandante debe evaluar continuamente el EO; a través de una combinación de elementos como: Informes, observación personal y automática e inteligencia de diversas actividades que se producen en el Ciberespacio.

Una conciencia o entendimiento situacional del ciberespacio, debe analizar este desde diferentes perspectivas; para ello se deben usar las variables operativas en combinación de las variables de misión. Se debe, por lo tanto, describir el entorno operacional en términos de ocho variables operativas PEMSITIM: Política, Económica, Militar, Social, Información, Tiempo, Infraestructura, y Medio ambiente y las variables de Misión METT-TC: Misión, Enemigo,

Terreno, Tropa, Tiempo y Consideraciones civiles. A continuación, se establecen algunos ejemplos en respuesta cibernéticas para las variables:

Variables Operacionales

- ***Política.*** ¿Qué infraestructura tecnológica, de comunicaciones y control requieren más esfuerzo en seguridad y defensa, para garantizar la disponibilidad y funcionamiento confiable e íntegro del Gobierno?.
- ***Económica.*** Qué infraestructura tecnológica, de comunicaciones y control requieren más esfuerzo en seguridad y defensa, para garantizar la disponibilidad y funcionamiento confiable del Sector Financiero y económico?.
- ***Militar.*** ¿Qué infraestructura tecnológica, de comunicaciones y control es utilizada por el enemigo y/o adversario para habilitar sus actividades?.
- ***Social.*** ¿Qué nodos de redes permiten la comunicación con las infraestructuras críticas y de la población para protegerlos de posibles efectos negativos de las operaciones cibernéticas?
- ***Información.*** ¿Cuál es la naturaleza de los datos que influye en las operaciones cibernéticas?.
- ***Infraestructura.*** ¿Qué redes y nodos hacen parte de la infraestructura crítica cibernética?
- ***Medio Ambiente.*** ¿Cómo se afectan las infraestructura tecnológica, de comunicaciones y control, con las radiaciones electromagnéticas, las inundaciones y terremotos?
- ***Tiempo.*** ¿Qué tiempo es el óptimo para crear efectos que soporten la misión?

Variables Misionales

- ***Misión.*** ¿Qué elementos de las operaciones cibernéticas podemos emplear para garantizar la unidad de la misión?, ¿Qué tareas esenciales deberán ser direccionadas para producir efectos?
- ***Enemigo.*** ¿Cómo podemos aprovechar la información sobre las capacidades e intención de la amenaza?, ¿Qué vulnerabilidades del adversario pueden ser explotadas?
- ***Terreno.*** ¿Cuáles son las oportunidades y riesgos de las operaciones del ciberespacio, cuando las condiciones meteorológicas pueden causar impacto en las TICs?.
- ***Tropa.*** ¿Qué recurso humano internos y externos están habilitados para integrar, sincronizar y ejecutar operaciones cibernéticas?
- ***Tiempo.*** ¿Cómo podemos realizar efectos decisivos en la maniobra, con el tiempo establecido?
- ***Consideraciones civiles.*** ¿Cómo podemos emplear operaciones cibernéticas sin causar efectos en los no combatientes?

Así mismo, la conciencia situacional o entendimiento del Ciberespacio debe realizarse a través de tres niveles: *Nivel de percepción, nivel de concepción y nivel de proyección.* En cada uno de los cuales se deberá obtener la correspondiente información, tal como lo muestra la tabla, en cada nivel se obtiene información del ciberespacio propio y del adversario.

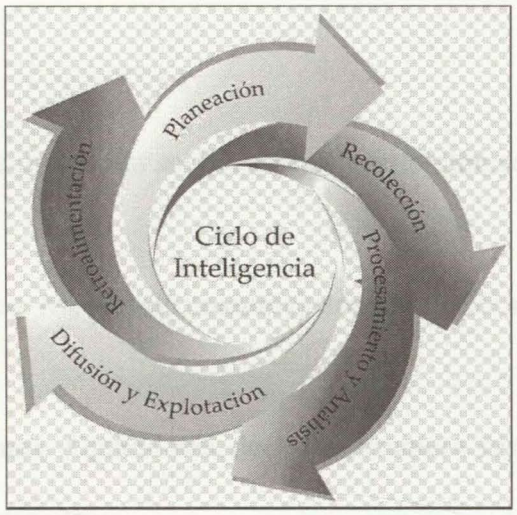
Tabla 4 - Acciones en los niveles de la conciencia situacional del Ciberespacio

NIVEL	EO AMISTOSO	EO ADVERSARIO
PERCEPCIÒN	Mantener actualizada la información de las redes amistosas.	Buscar y recopilar información sobre las tecnologías de seguridad y defensa utilizadas por el adversario.
	Recopilar información que se obtenga de los diferentes incidentes que se presenten.	Recopilar información que se obtenga de los diferentes incidentes que se presenten.
	Monitorización constante de redes	Monitorización constante sobre las actividades que adelantan los adversarios relacionadas con el ciberespacio.
COMPRENSIÓN	Analizar el estado de las redes.	Identificar vulnerabilidades inherentes a las tecnologías utilizadas por el adversario.
	Analizar la información obtenida de los diferentes incidentes informáticos.	Identificar las vulnerabilidades que fueron explotadas dentro de las redes del adversario
	Análisis de riesgos dentro de las redes amistosas.	Análisis de línea de acción que esté desarrollando el adversario.
PROYECCIÒN	Catalogar los riesgos según su probabilidad y nivel de impacto.	Identificar medios y métodos de explotación de las vulnerabilidades identificadas.
	Identificar las líneas de acción que permitan mitigar y/o controlar vulnerabilidades.	Planear acciones que impidan al adversario afectar la seguridad de las redes amistosas.
	Planear accione permanentes frente a las situaciones de las redes amistosas.	

Nota: Tomando de Diapositivas de la clase de Concepto Operacional Maestría Ciberseguridad y Ciberdefensa ESDEGUE

Las Operaciones de ciberinteligencia se desarrollan utilizando el ciclo de inteligencia: planeación, recolección, procesamiento, análisis, difusión y empleo. El ciclo de inteligencia es entendido como la secuencia mediante la cual se obtiene información, se transforma en inteligencia y se pone a disposición del mando, consta de cinco fases, así:

Figura 8 - Ciclo de Ciberinteligencia



Nota: Centro de Investigación y Seguridad de México CISEN. México. Recuperado de http://www.cisen.gob.mx/intCicloInt.html.

1) *Planeación.* Durante esta fase del ciclo se determinan las necesidades de inteligencia, se prepara un plan para su obtención, se organizan los medios y se efectúa el mando, coordinación y control de todos ello, los cuales se mantienen durante todo el ciclo.

2) Recolección. Consiste en la obtención de la información requerida y precisada para producir la inteligencia necesaria, la cual es recolectada a través de una variedad de métodos, se explotan sistemáticamente, las fuentes de información. Para la producción de ciberinteligencia se pueden emplear las siguientes formas:

Fuentes Técnicas. Para las operaciones de ciberinteligencia serán la interceptación de sistemas de Telecomunicaciones, observación satelital, sensores de correlación, Redes Honey pot,

analizadores de tráfico de red, sistemas de desencripción, correlacionadores de eventos, escáner de vulnerabilidades, entre otros.

Fuentes Humanas. A través de ingeniería social, avatar, infiltración en redes sociales.

Fuentes de información pública. Medios de comunicación convencional e internet.

Fuentes entidades y organismos. Operadores de infraestructura crítica, CERTs, Agencias civiles nacionales y extranjeras, entre otros.

3) *Procesamiento.* Durante esta fase del ciclo de Ciberinteligencia, se debe realizar la recepción, registro, organización, clasificación y valoración de la información recolectada, acorde con los objetivos identificados.

4) *Análisis.* Durante esta fase, se logra la transformación de los datos recolectados en Inteligencia, a través de procesos analíticos que permitan, de una manera lógica y ordenada, decantar e interpretar la información recopilada y procesada a fin de poder establecer los posibles cursos de acción enemigos, tanto actuales como potenciales o la evolución de las posibles ciberamenazas.

5) *Difusión y empleo.* La difusión es la fase final del ciclo de Ciberinteligencia. Básicamente, contempla la entrega, oportuna, clara, precisa y lógica, de la información de Inteligencia. La difusión debe estar enmarcada por la compartimentación, seguridad, y vigencia de la información

con el fin de garantizar su integridad y disponibilidad para el desarrollo de operaciones de Ciberdefensa.

6.5 Operaciones de Contraciberinteligencia

La contraciberinteligencia en el ciberespacio son todas aquellas actividades relacionadas con la identificación de la ciberamenaza, de tal manera que se evite que el adversario obtenga la información secreta. Las operaciones de contraciberinteligencia estarán encaminadas a supervisar el comportamiento del personal interno legalmente autorizado por la institución para el manejo de información y los sistemas. La contraciberinteligencia debe ser proactiva y preventiva en su enfoque a través de actividades como la creación de desinformación, enmascaramiento de la información; así como el descifrado de la información del adversario. La contrainteligencia es una función de inteligencia que proporcionará a los mandos de todos los niveles, un detallado conocimiento de las amenazas, vulnerabilidades y riesgos *internos* a los que la información se ve expuesta por el propio personal de la Fuerza. Estas operaciones a su vez negarán al adversario la oportunidad de llevar a cabo el ciberterrorismo, ciberespionaje y cibersabotaje, a las redes contra las fuerzas propias. Para conseguirlo es necesario identificar las vulnerabilidades de las fuerzas propias a las operaciones de obtención de inteligencia de un adversario.

Dentro de los métodos planteados para este tipo de operaciones, se establecen los siguientes:

a. *Método obtención de información de fuentes abiertas.* Este método se realiza en la fase de recolección a través de distintas fuentes como las mencionadas anteriormente.

b. Conciencia situacional. Este método fue descrito anteriormente y es requerido en la etapa de planeación de las Operaciones Cibernéticas.

c. Sistemas de engaño cibernético. Este método consiste en implantar señuelos (honey net) a donde los ataques del adversario son redirigidos, El servicio cibernético de engaño debe ser lo más auténtico posible, y debe enviar las mismas respuestas de la red que un servicio real. Si la emulación es incompleta, los atacantes podrán detectar el engaño y podrán eludir el elemento de engaño. El resultado final de esta estrategia es una red de engaño eficaz, lista para atrapar a los atacantes y distribuir datos de ataque para que las herramientas de ciberseguridad hagan su trabajo.

Capacidad de Respuesta.

La respuesta en las operaciones cibernéticas está orientada a la aplicación de la fuerza en ya través del ciberespacio; ya que incluye las medidas y acciones a tomar frente a amenazas y ataques de naturaleza cibernética. Los propósitos de la respuesta comprenden:

- Acceder tanto por medios directos como a distancia, a redes, sistemas o nodos objetivos, con el fin de garantizar el acceso que requieren las acciones de respuesta contra los objetivos identificados.

- Permitir el acceso recurrente tanto por medios directos como a distancia, a redes, sistemas o nodos objetivos, para garantizar el acceso requerido por las acciones de respuesta.

- Acceder, recopilar y explotar la información del adversario marcada como objetivo, por medios directos o a distancia, con el fin de detectar, disuadir, denegar y derrotar a las acciones y libertad de acción del adversario.

- Habilitar la capacidad de agregar, administrar, descifrar, traducir, analizar e informar sobre todos los datos recogidos en los sistemas de gestión del conocimiento, con el fin de apoyar las OCs.

- Proporcionar capacidades ofensivas tanto a distancia como de forma expedicionaria, con el fin de detectar, disuadir denegar y derrotar las acciones y libertad de acción del adversario en el Ciberespacio.

- Atacar (negar, degradar, engañar, interrumpir o destruir) las redes del adversario y su infraestructura crítica, con el fin de detectar, disuadir, denegar o derrotar las acciones y libertad de acción del adversario, integrando la defensa en profundidad y garantizando la libertad de acción propia y del adversario, en el momento y lugar de nuestra elección. Así como mapear y entender al adversario y otras estructuras específicas del ciberespacio, a fin de garantizar todos los aspectos de las OCs.

- Rastrear, localizar y predecir las actividades del adversario en el ciberespacio, a fin de garantizar la respuesta y del conocimiento de la situación.

- Atacar la información del adversario con el fin de disuadir, socavar, o engañar a los adversarios, con el fin de apoyar la efectividad de las acciones en el Ciberespacio; así como los objetivos de la misión.

- Mitigar o evitar las medidas de defensa del adversario con el fin de poder ejecutar las capacidades ofensivas propias.

6.6 Operaciones Cibernéticas Ofensivas OCO

Las operaciones ofensivas son aquellas acciones cibernéticas cuya ejecución crean efectos tanto directos como indirectos en el ciberespacio adversario (campo de batalla); a través de técnicas que permiten interrumpir, alterar, degradar, engañar y/o destruir sistemas de cómputo, información, redes, programas entre otros, con el propósito de impactar el normal funcionamiento y desarrollo de las operaciones del enemigo y permitir la libertad de acción propia y aliada.

El efecto directo de las OCOs es la afectación de la disponibilidad, integridad y disponibilidad de los sistemas (redes, aplicaciones, infraestructura de C2, etc) objetivo que han sido atacados. Los efectos indirectos corresponden al nivel de afectación como resultado de la fuerza aplicada y que recae en otros sistemas de mayor relevancia operacional. Los efectos indirectos no son fácilmente reversibles toda vez que pueden implicar la reconstrucción de infraestructura, la modificación de sistemas o la pérdida irrecuperable de activos. Las OCOs operan bajo las siguientes acciones:

1) Negar. Para degradar, interrumpir o destruir el acceso, operación o disponibilidad de un objetivo

en un nivel especificado durante un tiempo especificado. La negación evita que el adversario use sus recursos y capacidades.

2) *Degradar.* Se refiere a disminuir la capacidad de operacional del objetivo.

3) *Interrumpir.* Consisten en negar completamente, pero temporalmente el acceso u operación de un objetivo. La interrupción puede considerarse un caso especial de degradación cuando el nivel de degradación seleccionado es del 100 por ciento.

4) Destruir. Negar permanentemente, completamente e irremediablemente el acceso a una operación de un objetivo, por parte del adversario.

5) Manipular. Controlar o cambiar la información del adversario, sistemas de información y/o redes de manera que apoye los objetivos del comandante y la misión.

Las operaciones ofensivas pueden ser combinadas con otras capacidades como el ataque electrónico o el físico para negar o manipular la información y la infraestructura del adversario. A su vez deben combinar medios políticos, de inteligencia y tecnológicos para detectar y analizar actividad maliciosa, al tiempo que se ejecutan acciones de respuesta, con autorización previa, para eliminar ataques hostiles antes de que puedan causar algún impacto.

Tal como lo relaciona el Manual de Ciberdefensa Conjunta de las FF.MM de Colombia 3.38, para el desarrollo de operaciones cibernéticas ofensivas se deben tener presente ciertas consideraciones como:

1) En razón a que en la mayoría de operaciones el sistema central se ve afectado por sistemas informáticos subyacentes a este, como por ejemplo una base de datos, entonces los efectos indirectos cobran una mayor relevancia sobre los efectos directos de la operación.

2) Los efectos directos, causados por una operación ofensiva, pueden normalmente ser reversibles en poco tiempo; por lo tanto, es indispensable la rapidez y coordinación de las demás operaciones a fin de lograr el impacto deseado.

3) El grado de incertidumbre en el desarrollo de las operaciones ofensivas es demasiado alto, por las diversas variables de configuración que pueden existir en un sistema de datos y sus implicaciones; en consecuencia, se debe identificar la necesidad militar y establecer una ponderación entre la ventaja militar y el daño colateral o los efectos indirectos.

4) El tiempo de planeamiento es mucho más extenso que el tiempo de ejecución en el ciberespacio. Si bien el planeamiento puede abarcar meses o incluso años, la ejecución puede llevarse a cabo en milésimas de segundo.

5) A diferencia de las operaciones militares conocidas, aéreas, terrestres o navales, las operaciones en el ciberespacio pueden ser mucho menos costosas que las citadas, toda vez que

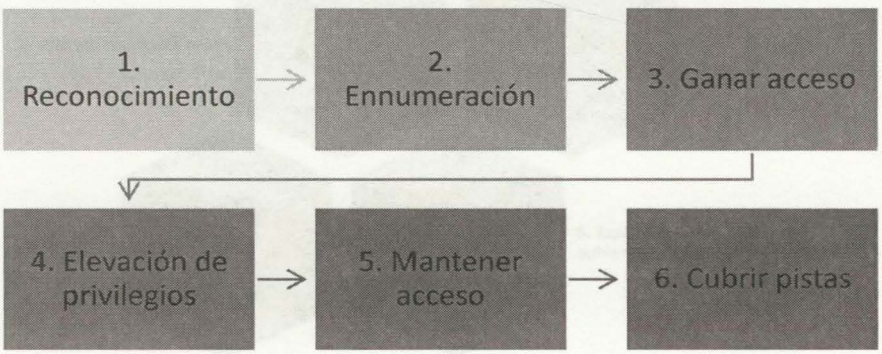
puede ser generadas por un solo atacante, con recursos y medios tecnológicos económicos y de fácil obtención.

6) La identidad u origen de los atacantes puede ocultarse con gran facilidad.

El método para desarrollar operaciones cibernéticas ofensivas es *el Ciberataque*, Este método consiste en una maniobra ofensiva para atacar a sistemas de información como lo son infraestructuras, redes computacionales, bases de datos que están albergadas en servidores remotos, por medio de actos maliciosos usualmente originados desde diferentes que también sustraen, alteran o destruyen un blanco específico mediante el ataque de un sistema vulnerable.

Basado en la metodología empleada por Ec-Council para ejecutar un ciberataque, se deberán llevar a cabo las siguientes fases:

Figura 9 - Fases de un ciberataque



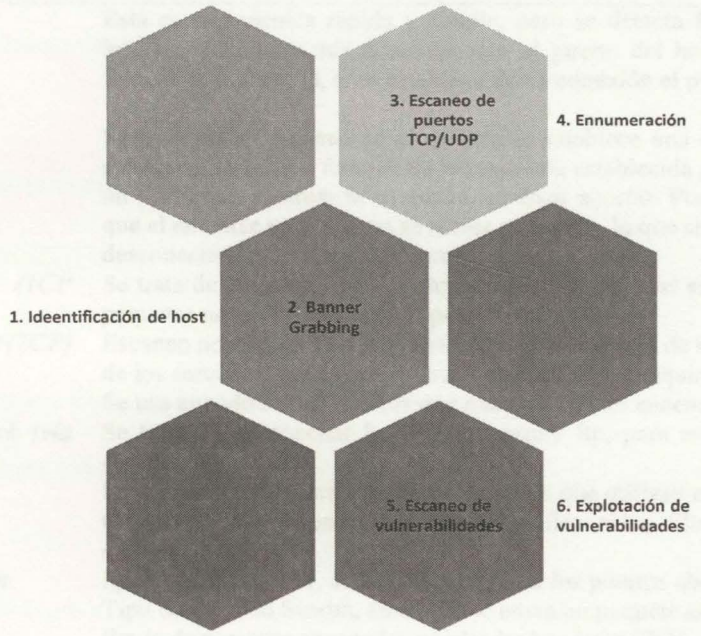
Nota: Hacking ético. Recuperado de https://www.owasp.org/images/5/51/Hacking_Etico_Cacer%C3%ADa_de_Vulnerabilidades.pdf

1) Reconocimiento. Se deberá realizar un footprinting de la Unidad, aplicación u activo cibernético, este footprintig consiste en recopilar toda la información (red, sistema, organización,

empleados) necesaria sobre el objetivo. Dentro del reconocimiento se debe realizar una lista de información de un sistema concerniente a sus servicios y/o puertos abiertos.

2) Enumeración y explotación de vulnerabilidades. En este paso se deben usar herramientas manuales y automáticas de escaneo de vulnerabilidades para descubrirlas, usando recursos como bases de datos de vulnerabilidades de aplicaciones, exploits que permitan su identificación. De acuerdo a las vulnerabilidades detectadas se generan los exploits para aprovechar dichas vulnerabilidades. Esta fase consiste en una serie de pasos que a saber son:

Figura 10 - Pasos fase 3 de un hacking ético



Nota: Hacking ético. Recuperado de www.owasp.org

Identificación de host vivos. La meta de esta prueba es obtener repuestas las cuales demuestren que una dirección IP efectivamente se encuentra activa.

Banner Grabbing. Es una técnica para identificar el sistema operativo en un objeto remoto o aplicaciones detrás de servicios activos.

Escaneo de puertos TCP (Transport Control Protocol)/ (User Datagram protocol) UDP. A través de esta técnica se identifican que puertos se encuentran abiertos o habilitados en un tipo de servicio, así como chequear la existencia de un firewall y el funcionamiento de estos. Algunos tipos de escaneo de puertos son:

Tabla 5 - Tipos de escaneo

Tipos de escaneo de puertos	Descripción
TCP Conect.	Esta es una técnica rápida y simple, pero se detecta fácilmente. Se basa en intentar establecer una conexión con el puerto del host remoto mediante la llamada a connect (), si se establece dicha conexión el puerto estará abierto.
TCP SYN	Se trata de un escaneo en el que no se establece una conexión completa, se establece SYN y en función de la respuesta establecida por el host, se contesta un RST, para rastrear la conexión, es decir abortar. Puede darse el caso en el que al enviarse un SYN, no se reciba respuesta, lo que significa que el host está desconectado o se filtra la conexión a ese puerto.
Stealth Scan (TCP Fin).	Se trata de enviar FIN y esperar la respuesta del host escaneado, si ignora los paquetes enviados entonces el puerto está abierto.
Reverse Ident (TCP)	Escaneo normal de TCP al puerto 113, con el objeto de saber quién es el dueño de los servicios que corren en otros puertos de la máquina.
Ping scan	Se usa cuando se desea saber que máquinas están encendidas.
Bounce Attack (vía ftp).	Se trata de aprovechar la conexión proxy ftp, para escanear a través de un servidor ftp.
UDP scan	Este escaneo mostrará los puertos abiertos que utilizan el protocolo UDP.
ACK scan.	Con esta técnica de escaneo podemos verificar si hay filtrado de paquetes detrás de un firewall.
Windows scan	Igual que el anterior, adicionalmente lista los puertos abiertos.
Null scan	Tipo de escaneo Stealth, en el que se envía un paquete sin banderas levantadas.
Xmas scan.	Envío de paquetes anormales y todas las banderas SYN, ACK, PSH, RST, URG y FIN
Idel scan.	Utiliza host zombies
RCP scan.	Se envía el comando NULL a los puertos TCP o UDP que están abiertos y ver si son puertos RCP, para saber que programa y su versión está corriendo.

Nota: Hacking ético. Recuperado de www.owasp.org

Enumeración. La enumeración consistente en listar de un sistema información dependiendo del servicio o puertos abiertos:

- Enumeración de usuarios (SMTP)
- Enumeración de servicios y puertos (SNMP)
- Enumeración de cuentas de usuarios y dispositivos
- Enumeración de usuarios de red (LDAP)
- Enumeración de hots, direcciones IP, system names, OS (NTP).
- Enumeración de recursos de red.

Escaneo de vulnerabilidades. Se deben usar herramientas manuales y automáticas de escaneo de vulnerabilidades para descubrirlas, usando recursos como bases de datos de vulnerabilidades de aplicaciones, exploits que permitan su identificación.

Explotación de vulnerabilidades. De acuerdo a las vulnerabilidades detectadas se generan los exploits para aprovechar dichas vulnerabilidades.

3) Ganar acceso. Los accesos pueden ser locales o remotos, se trata de conseguir entrar en los sistemas del adversario para inocular la carga dañina.

4) Elevar privilegios. A través de esta fase se tratará de llegar lo más adentro de la infraestructura que pueda, vulnerando otros ordenadores internos, creando puertas traseras para posteriores accesos, entre otros. Las técnicas utilizadas pueden ser: Cracking de contraseñas y escalamiento de privilegios.

5) Inoculación de la carga dañina. La carga define lo que se puede hacer una vez que la vulnerabilidad ha sido explotada: ocultarse, reproducirse, retransmitir dato, destruir o alterar ficheros, bloquear un sistema, entre otros.

6) Mantener acceso. Es la etapa durante la cual el atacante asegura y mantiene el control sobre el objetivo, negándole al adversario su posesión y control.

7) Cubrir pistas. Durante todo el desarrollo del ciberataque se deben manejar técnicas forenses para no dejar rastro.

Dentro de las técnicas del ciberataque podemos emplear las siguientes:

a. Cambios en las direcciones de dominio DNS.
b. Intrusiones no autorizadas.
c. Denegación de servicios DDoS.
d. Saturación de correo.
e. Interferencia electrónica de comunicaciones.
f. BlindRadars (Bloquear tráfico aéreo).
g. Ataque por robo de información.
h. Ataque por anulación de equipos.
j. Ataque por pulso electromagnético.

Dentro de las tácticas de un ciberataque se cuenta con las siguientes:

1. Virus informáticos.

2. Envío masivo de correo no deseado SPAM.

3. La suplantación de remitentes mediante Spoofing. Esta táctica simula la identidad de otra máquina de la red para conseguir acceso a recursos de un tercer sistema.

4. El envío o instalación de archivos espía o keyloggers.

5. El uso de troyanos para control remoto de sistemas o la sustracción de información.

6. El uso de archivos BOT del IRC (Internet Relay Chat). Es un programa que permite que el sistema sea controlado remotamente sin el conocimiento ni consentimiento del dueño.

7. Los Rootkits. Esta táctica utiliza un conjunto de herramientas que consiguen ocultar un acceso ilícito a un sistema informático. Estas herramientas sirven para esconder los procesos y archivos que permiten al intruso mantener el acceso al sistema.

7. Conclusiones

El carácter del conflicto contemporáneo ha provocado un cambio significativo en el enfoque de la lucha de guerra a nivel mundial. El C3IR (comando, control, computación, inteligencia y reconocimiento), requiere de una nueva estrategia, en la cual se adicione el desarrollo de capacidades en el ciberespacio (C4IR), para la ejecución de operaciones cibernéticas, con el fin de garantizar la protección y defensa de las instituciones del Estado, la población, la industria y por ende redunde en el desarrollo económico y social de un país. Pero ello dependerá del uso libre del conjunto de dominios: tierra, mar, aire, espacio y del ciberespacio, con este último se podrá proporcionará influencia y control en el resto.

El apalancamiento de unas nuevas capacidades en el ámbito de la ciberdefensa, aumentará el acceso, velocidad, alcance y precisión de las Fuerzas Militares. El control del ciberespacio en una determinada misión debe ser un requisito previo y fundamental para el desarrollo operacional militar en toda la gama y dominios de las operaciones militares. Por lo anterior es necesario desarrollar doctrina en esta materia; así como mantener formar, entrenar y equipar al personal de cuadros, para que se cree y se generen competencias en el dominio del ciberespacio, por parte de las Fuerzas Militares. A su vez, es importante que el personal militar comprenda las operaciones del ciberespacio en términos de las capacidades defensivas y ofensivas.

Los militares deben defender las infraestructuras establecidas en el ciberespacio frente a las amenazas que se ciernen en ellas, a fin de proteger la información de misión crítica y las capacidades de las Fuerzas Militares.

La creciente dependencia de las FF.MM. en el ciberespacio requiere de personal profesional bien formado y capacitado compuesto por operadores y líderes del ciberespacio que estén

dispuestos a proporcionar las capacidades necesarias para el logro de la misión. Los cibersoldados con conocimientos técnicos y tácticos deben ser personas esenciales para la misión y deben por lo tanto poseer altos niveles de competencia técnica, sólidas habilidades analíticas y una comprensión crítica de la aplicación de la guerra cibernética, que solo será obtenida bajo criterios doctrinales claros.

Los avances tecnológicos han proporcionado al entorno militar los medios para generar efectos decisivos y amplificados en todos los dominios, que tradicionalmente solo eran del dominio cinético, así mismo debido a su acelerada y continua evolución, han generado nuevas fuentes de amenaza, las cuales las FF.MM deben afrontar. Si bien es cierto este documento conforma la base de lineamientos doctrinales en materia de las tipologías y ejecución de operaciones cibernéticas OCs en y a través del ciberespacio, con la formulación de ideas y mejores prácticas, como fundamento doctrinal de este tipo de operaciones, se requiere sin embargo adaptar continuamente los conceptos operativos cibernéticos para aprovechar las capacidades emergentes del ciberespacio y asegurar que las Fuerzas mantengan la ventaja decisiva sobre el adversario, le permitan mantener la superioridad y la ventaja militar. Así como asumir el compromiso de incrementar los conocimientos, habilidades, capacidades individuales y colectivas del talento humano en materia de ciberseguridad y ciberdefensa, para la cual, conceptos como los desarrollados en el presente estudio, deberán ser interiorizados en las Fuerzas.

Bibliografía

Air Force United States. (2010). Doctrine document 3-12: Cyberspace Operations. Recuperado de: www.e-publishing.af.mil.

Centro Criptológico de España CCN. (2013). CCN-STIC-400 Normas de seguridad de las TIC. España: Ministerio de la presidencia.

Centro de Doctrina del Ejército de Colombia. (2016). Manual MFE 3-05 operaciones especiales. Colombia: Imprenta Ejército.

Centro de Doctrina del Ejército de Colombia. (2016). Manual MFE 5-0 proceso de operaciones. Colombia: Imprenta Ejército.

Centro superior de estudios Ministerio de Defensa España. (2012). Monografía 126 El Ciberespacio nuevo escenario de confrontación. España: Imprenta del Ministerio de Defensa.

Cr Niño, J. (2016). Manual de ciberdefensa conjunta para las Fuerzas Militares 3-38. Colombia: Imprenta Fuerzas Militares de Colombia.

Ejército de Colombia. (2010). Reglamento EJC 3-10-1 operaciones de combate irregular: Imprenta Ejército.

Ejército de Colombia. (2010). Manual EJC 3-225 de misiones regulares de la compañía de infantería: Imprenta Ejército.

Endsley, M.R. (2000). Theoretical situation awareness: A critical review. In M.R. Endsley & D.J.Garland (Eds.), Situation Awareness Analysis AD Measurement. Mahwah, NJ.

Estado mayor de la defensa de España. (2009). PDC01 Doctrina para la acción conjunta de las Fuerzas Armadas. España: Ministerio de la Defensa.

European Network and Information Security Agency ENISA. Guide for incident management. Recuperado de: https://www.enisa.europa.eu/.

ICONTEC. (2006). Norma técnica NTC/ISO IEC Colombiana 27001. Colombia: ICONTEC.

Instituto Español de Estudios Estratégicos. (2010). Cuaderno de estrategia 149 Ciberseguridad retos y amenazas a la ciberseguridad nacional en el ciberespacio. España: Imprenta del Ministerio de Defensa.

Joint Commander United States (2013). Joint Publication 3-12 Cyberspace Operations.

Libicki, M. (2007). Conquest in cuyberspace. United States: Cambridge University.

López, M. (2007). Análisis forense digital. Recuperado de: http: // www.codemaster.es.

Galán, C. & Mañas, J. (2016). CCN-STIC-817 Gestión de ciberincidentes. España: Ministerio de la presidencia.

Martín, E. (2016). Los retos de la ciberinteligencia. Recuperado de: http://www.ieee.es/Galerias/fichero/OtrasPublicaciones/Nacional/2016/GC_Cuadernos_Num.53-2016.pdf#page=53

Ministerio de Defensa de Brasil. (2014). MD31-M-07 Doctrina militar de defensa cibernética. Brasil: Ministerio de Defensa.

Mosso, J. (2015). Ciberseguridad Inteligente. Recuperado de: https://arxiv.org/abs/1506.03830.

National Institute of Standards and Technology NIST. (2017). Framework for Improving Critical Infrastructure Cybersecurity. Recuperado de: https://www.nist.gov/cyberframework.

Navajas, R. (2006). El arte operacional y la estrategia conjunta. Recuperado de: http://revistamarina.cl/revistas/2006/3/navajas.pdf

OWASP Hacking ético: Cacería de vulnerabilidades (2015). Recuperado de https://www.owasp.org/images/5/51/Hacking_Etico_Cacer%C3%ADa_de_Vulnerabilidades.pdf.

Unión Internacional de Telecomunicaciones ITU. (2007). Guía de ciberseguridad para los países en desarrollo. Recuperado de: http://www.itu.int.

Ureña, F. (2015). Ciberataques, la mayor amenaza actual. Recuperado de: http://www.ieee.es.

Lista de figuras

Lista de tablas