Escuela Superior de Guerra "General Rafael Reyes Prieto"
Maestría en Ciberseguridad y Ciberdefensa

Lineamientos estratégicos para la defensa de la infraestructura critica en el Comando de Apoyo Operacional de Comunicaciones y Ciberdefensa del Ejército Nacional de Colombia.

MY. EDWIN ORLANDO LEYTON GARZÓN

Director de trabajo de grado
CR. (EC) JOSÉ LUIS BARRERA JURADO

Bogotá, Colombia; 03 de septiembre del 2021.

Dedicatoria

Dedico este trabajo a mi bella familia, quienes han estado todo el tiempo acompañándome y dándome su apoyo, son ellos quienes verdaderamente entienden el sacrificio como militar para alcanzar metas y sueños, a mi hermosa madre quien desde este año me acompaña y guía desde el cielo y finalmente a mi institución que me ha permitido crecer profesionalmente en el quinto dominio de la guerra.

AGRADECIMIENTOS

Mi agradecimiento a mi tutor sr. Cr. Barrera, quien con su experiencia orientó este trabajo para que en un futuro pueda servir como referencia a las Comunicaciones Militares del Ejército Nacional desde el ámbito de la Ciberdefensa y a los docentes de la maestría de Ciberseguridad y Ciberdefensa de la Escuela Superior de Guerra que con su conocimiento me guiaron en la ruta del aprendizaje.

Tabla de contenido

Resumen

En la actualidad existe una constante importancia por la defensa de infraestructuras que tienen un nivel debido a su rol estratégico para el desarrollo social y económico de un Estado, estás consolidan una red que permite ejecutar actividades esenciales y la afectación a las mismas puede generar un impacto desproporcionado en la estabilidad de un país como la infraestructura critica compuesta por la redes como 1) la agricultura y alimentación, 2) servicio de salud, 3) sistema de aguas, 4) salud Pública, 5) servicios de emergencia, 6) sistema de gobierno, 7) industrial de Defensa, 8) información y telecomunicaciones, 9) sistema energético, 10) redes de transporte, 11)sistema financiero, y 12) industria química. (Dark Reading, 2016)

La importancia de esta infraestructura radica en que, a raíz de la tecnificación y digitalización de los procesos administrativos, industriales y operacionales, mucha de la infraestructura estratégica de un Estado ha tenido que implementar nuevos sistemas de la información y comunicación. Sin embargo, el continuo crecimiento de estas redes ha generado una dependencia y también una alta vulnerabilidad frente amenazas provenientes del ciberespacio.

El presente documento tiene el objetivo de establecer los lineamientos estratégicos que debe seguir el Comando de Apoyo Operacional de Comunicaciones y Ciberdefensa del Ejército Nacional con el fin de apoyar la defensa de la infraestructura crítica del Estado colombiano. Lo anterior, teniendo en cuenta la importancia de establecer una estrategia defensiva frente a las nuevas amenazas que provienen del ciberespacio, un escenario digital que en la actualidad evidencia un continuo crecimiento de sus redes, lo cual ha causado que todos los sistemas críticos dependen del uso de nuevas tecnologías de la información para mejorar sus procesos, sin embargo, esta dependencia también los vuelve vulnerables a recibir ataques informáticos de actores ilegales nacionales e internacionales.

Palabras clave: Estado, Infraestructura, cibernética, crimen, violencia, Teoría de la información.

*Palabras claves confirmadas en los tesauros UNESCO.

Abstrac

At present there is a constant importance for the defense of infrastructures that have a level due to their strategic role for the social and economic development of a State, they are consolidating a network that allows executing essential activities and the impact on them can generate an impact disproportionate in the stability of a country such as critical infrastructure composed of networks such as 1) agriculture and food, 2) health service, 3) water system, 4) Public health, 5) emergency services, 6) health system. government, 7) defense industry, 8) information and telecommunications, 9) energy system, 10) transportation networks, 11) financial system, and 12) chemical industry. (Dark Reading, 2016)

The importance of this infrastructure lies in the fact that, as a result of the modernization and digitization of administrative, industrial and operational processes, much of the strategic infrastructure of a State has had to implement new information and communication systems. However, the continuous growth of these networks has generated dependency and also a high vulnerability to threats from cyberspace.

The objective of this document is to establish the strategic guidelines to be followed by the Operational Communications and Cyber Defense Command of the National Army in order to support the defense of the critical infrastructure of the Colombian State. The foregoing, taking into account the importance of establishing a defensive strategy against new threats that come from cyberspace, a digital scenario that currently shows a continuous growth of its networks, which has caused that all critical systems depend on the use of new information

technologies to improve their processes, however, this dependence also makes them vulnerable to receiving computer attacks from national and international illegal actors.

Key Words: State, infrastructure, cybernetics, crime, violence, Information theory.

Introducción

Existe cada vez más organizaciones en el uso de nuevas tecnologías, esto en razón a la implementación de nuevos sistemas de información en el desarrollo de actividades industriales, empresariales y de mercado, lo cual representa un riesgo a la seguridad debido a la vulnerabilidad de esos sistemas y de los datos hacia ciberataques de Estados o de amenazas asimétricas. A esta constante evolución se suman nuevas amenazas a la seguridad digital que pueden afectar el desarrollo de las actividades esenciales para el Estado, de hecho, en los últimos diez años los sistemas digitales son cada vez más atacados por hackers y ciberdelincuentes.

La infraestructura crítica es definida como aquellos sistemas empleados por los gobiernos en donde se materializan los activos nacionales esenciales para el funcionamiento de una sociedad y su economía. Estos bienes son esenciales debido al desarrollo social que se desprenden de estos, cualquier problema a la infraestructura puede generar un impacto crítico en el bienestar del ciudadano, de su entorno y su seguridad (White, 2014).

No obstante, se cuenta con infraestructuras más importantes que otras como, la infraestructura crítica, esta entendida como aquella infraestructura necesaria para el desarrollo de las actividades de un Estado, en el país se tiene identificado trece sectores según la Política Nacional de Protección y Defensa para la Infraestructura Critica Cibernética de Colombia (PNPICCN V 1.0, 2017, p. 22), todos fundamentales para alcanzar los intereses nacionales; con el fin de enfrentar posibles amenazas de enfoque cibernético y mediante el CONPES 3701 se crea el Comité Intersectorial de Ciberseguridad, con el objetivo de prepararse para la defensa de los intereses en este nuevo escenario.

La Unión Europea ha establecido directivas en función de la protección hacia la infraestructura crítica materializadas en el Plan de Seguridad del Operador. Por otra parte,

España, Alemania, Reino Unido y Estados Unidos, tienen sus propios protocolos en favor de la seguridad de su infraestructura crítica centrada en la seguridad informática, de comunicaciones y electrónica. Para estos países existe una prioridad en la protección de la infraestructura crítica debido a los servicios humanitarios, desarrollo y supervivencia que se desprenden de cada uno de los sectores (Kahan, 2015).

Pero, ¿por qué es importante la defensa de infraestructura crítica en los Estados? Para el caso de Colombia, existen muchos peligros y amenazas que pueden afectar la infraestructura crítica nacional y la seguridad del Estado. Durante más de 50 años de conflicto armado en Colombia, se han generado nuevas dinámicas criminales y armadas que ya no se manifiestan de manera física mediante el uso de las armas, así como fuentes de financiación basadas en economías ilícitas que provienen del ciberespacio, mediante el empleo de modalidades delictivas y la ciberdelincuencia. Pero más allá de las implicaciones de las herramientas tecnológicas que pueden ser utilizadas por los criminales y organizaciones armadas, existe infraestructura que depende de los sistemas de información y tecnologías de información y comunicaciones para su funcionamiento, esto nos vuelve blancos de posibles ataques estratégicos para las amenazas de orden interno y también de las que provienen del exterior.

Ahora bien, ¿Cuáles son las amenazas, riesgos y peligros que pueden afectar la infraestructura crítica de Colombia? Principalmente son actores irregulares los que pueden hacer uso de acciones delincuenciales de alto impacto que pueden generar entorpecimiento, daño parcial o permanente en la infraestructura crítica nacional. Para ello se han dispuesto de planes como el Plan Nacional de Protección y Defensa para la Infraestructura Critica, el cual establece una relación del sector industrial, financiero, energético y medio ambiente.

La presente investigación, consiste en reforzar dichos planes de protección para convertirlos en una prioridad del Estado y no solo una responsabilidad de los sectores y darle un enfoque como actualmente lo están manejando los países desarrollados, quienes consideran

que la infraestructura crítica es un interés nacional (González y Santoyo, 2012). Si bien Colombia sigue avanzando en favor de proteger la infraestructura, es necesario también establecer lineamientos estratégicos para la defensa de los sectores, un asunto que es de suma importancia para el Comando de Apoyo de Comunicaciones del Ejército Nacional de Colombia.

Por lo anterior es importante también considerar ¿Qué lineamientos estratégicos debe considerar el Comando de Apoyo Operacional de Comunicaciones del Ejército Nacional de Colombia para la protección de la infraestructura crítica del país?, entre las principales funciones que tiene el Ejército Nacional en Defensa de la infraestructura crítica se encuentra la capacidad de respuesta y recuperación ante las amenazas cibernéticas, desarrollar competencias de seguridad digital y ciberdefensa, así como generar normatividad de manera sinérgica entre los diferentes sectores y agencias a nivel nacional, entre otras líneas estratégicas y de acción.

Teniendo en cuenta que el sistema de defensa cibernética se encuentra en pleno desarrollo y modernización, es importante prepararse a futuro ante posibles amenazas que pueden derivarse de los entornos complejos provenientes del desarrollo de nuevas tecnologías y de comunicación.

CAPÍTULO I Planteamiento de la Investigación

Teniendo en cuenta la importancia de buscar fuentes de información relacionadas con la temática a investigar, resulta importante establecer los principales documentos que abordan la categoría de análisis tales como ciberdefensa y ciberseguridad. Por lo tanto, a continuación, se plasma el Estado del Arte o Estado de la Cuestión, información que permitió la formulación del planteamiento del problema de investigación.

Estado del Arte

En la revisión bibliográfica referente a la infraestructura crítica ligada a la ciberseguridad y la ciberdefensa desde el sector defensa, se encuentran lineamientos de política estatales y estudios académicos que analizan este tema relevante no solo para Colombia, sino para el escenario internacional en general. No se documenta gran cantidad de bibliografía referente al Comando de Apoyo Operacional de Comunicaciones y Ciberdefensa del Ejército Nacional, lo que significa que el estudio que se desarrolla aporta a un vacío de conocimiento existente en esta área, siendo relevante para profundizar en la línea de investigación *Seguridad digital* de la Escuela Superior de Guerra.

Para la consecución de este objetivo, se plantea un punto sobre el cual se centró la revisión consolidada en el estado del arte, teniendo presentes los avances que se han logrado en la normativa del Estado colombiano y el análisis académico. De este modo, se enfoca en los lineamientos generales de la protección de la infraestructura crítica y, en la labor específica del sector defensa y de las capacidades de las Fuerzas Militares en la protección de estos activos estratégicos, desde dos perspectivas: uno de los lineamientos estatales y la otra, de la academia.

- ***Lineamientos estratégicos de la ciberseguridad y ciberdefensa de la infraestructura crítica en Colombia.***

  A. Estado

Se profundiza este propósito desde los lineamientos del Estado, con la expedición del CONPES 3670/2010 *"Lineamientos de Política para la continuidad de programas de acceso y servicio universal a las Tecnologías de la Información y las comunicaciones",* propuesto con el objetivo de definir los lineamientos de política para contribuir a continuar con las iniciativas ligadas al acceso, uso y aprovechamiento de las nuevas tecnologías. Por consiguiente, da responsabilidades para la financiación de este proyecto, así como buscar la sostenibilidad en la participación (Departamento Nacional de Planeación, 2010). Aunque no se refiere directamente a la ciberdefensa y ciberseguridad, es un antecedente de base para el desarrollo de las TIC en Colombia.

Por ello, se retoma el CONPES 3701/2011 *"Lineamientos de política para ciberseguridad y ciberdefensa",* un documento dado desde el Departamento Nacional de Planeación (2011), orientando acciones para el desarrollo de una estrategia nacional para contrarrestar las amenazas informáticas, estableciendo una serie de responsabilidades principalmente al Centro Cibernético Policial (CCP), el Comando Conjunto Cibernético (CCOCI) y el Grupo de Respuesta a Emergencias Cibernéticas de Colombia (ColCERT). En específico, por medio de este documento se identifican unas debilidades: (Para la época) no se contaba con una estrategia de ciberdefensa y ciberseguridad; no se contaba con organismos específicos de respuesta frente a incidentes cibernéticos. Frente a esto, se presenta el objetivo principal de fortalecer la capacidad estatal para enfrentar las amenazas a la seguridad y la defensa en el ámbito cibernético, teniendo en cuenta las capacidades y conocimientos adquiridos para la proyección de sus intereses en el tema.

En efecto, con el CONPES 3854/2016 se establece la *"Política Nacional de Seguridad Digital"* en este elemento se propone un enfoque en la gestión del riesgo en el entorno digital, tomando en consideración dos puntos básicos como lo son: la defensa del país y la lucha contra el cibercrimen. Con el objetivo de identificar, gestionar, tratar y mitigar la materialización de

riesgos digitales, establecen cinco aspectos que contribuyen a este fin: un marco institucional para la coordinación intersectorial; generar condiciones para que las partes interesadas implementen parámetros de gestión del riesgo; mecanismos de participación; fortalecimiento de la defensa y seguridad nacional; enfoque en la cooperación estratégica (Departamento Nacional de Planeación, 2016).

Un punto importante son las definiciones propuestas relacionadas constituyéndose como conceptos oficiales en el Estado. Tres de las más importantes que aportan al desarrollo del presente estudio son:

- Seguridad digital como una situación de normalidad en el ciberespacio que se deriva de la realización de los fines del Estado haciendo uso efectivo de las capacidades de ciberdefensa, implementación de medidas de ciberseguridad y la gestión del riesgo.
- Riesgo de seguridad digital, conceptualizado como una categoría en relación con el desarrollo de actividades en el entorno digital, pudiendo ser una combinación de amenazas y vulnerabilidades que pueden afectar los intereses nacionales hasta el miso orden constitucional.
- Infraestructura crítica cibernética nacional, soportada por las TIC en donde su funcionamiento es indispensable para la prestación de servicios al Estado y a la sociedad en general; de llegar a afectarse o destruirse tiene efectos negativos en el bienestar económico y en el funcionamiento eficaz institucional (Departamento Nacional de Planeación, 2016).

Otro elemento de valor es la complementariedad que se propone entre “seguridad y defensa con la gobernanza, la educación, la regulación, la cooperación internacional, la investigación, el desarrollo y la innovación” (pp. 9-10), como una sinergia orientada al compromiso común de construir un ecosistema digital. Ligado a lo mencionado, amplia el espectro de las partes interesadas abarcando al Estado, pero involucrando a los ciudadanos,

sectores de la economía y organizaciones, estableciendo responsabilidades como actores participantes del ciberespacio.

De manera reciente, por medio del Departamento Nacional de Planeación (2020) se expidió el CONPES 3995 *"Política Nacional de Confianza y Seguridad Digital",* en el cual se resalta la participación creciente de la sociedad colombiana en el entorno cibernético, un ámbito en donde se vienen desarrollando riesgos complejos a la seguridad; se reconoce la gravedad de los ciberdelitos, ataques e incidentes cibernéticos. En este documento se plantea como objetivo general: una política nacional para dar medidas que amplíen la confianza y mejoren la seguridad digital para posicionar y proyectar a Colombia. Es importante ya que, por medio de este, el Estado genera unos lineamientos de inclusión y participación para la ciudadanía, a quien involucra como parte de lo cibernético, no solamente desde los derechos al acceso sino también los deberes y la responsabilidad que tienen para construir una seguridad digital común.

Actualmente, el gobierno de Iván Duque Márquez dio lineamientos de política en el sector defensa para avanzar en temas del escenario digital por medio de la "*Política de Defensa y Seguridad para la legalidad, el emprendimiento y la Equidad 2018-2022"* en la cual la innovación, ciencia y tecnología se consideran como ejes de transformación estratégica. Se identifican desafíos que pueden presentarse por el carácter transnacional del escenario digital al ser global; contando con que este se considera como un dominio junto al terrestre, naval, aéreo y espacial y para ello, se proyecta el desarrollo de un marco jurídico y fomento de la cooperación (Ministerio de Defensa Nacional, 2019).

Ligado a esto, se estableció desde el Ministerio de Tecnologías de la Información y las Comunicaciones (2018) el "*Plan TIC 2018-2022 El Futuro Digital es de Todos"* señalando iniciativas para la transformación y la seguridad digital estatal: la protección y defensa de la infraestructura crítica; la transformación digital; la innovación y la competitividad; la

prevención y reacción ante ataques ciber frente a vulnerabilidades que afecten la privacidad y, por ende, la ciberseguridad. No hace referencia explícita a la ciberdefensa, pero menciona la relevancia de su labor junto con el *"Plan Nacional de Protección y Defensa para la Infraestructura Crítica Cibernética de Colombia" (PNPICCN)* dado desde el CCOCI del Ministerio de Defensa Nacional (2017).

En el PNPICCN se proponen elementos para la operación coordinada, sistemática y eficiente de la infraestructura crítica cibernética en el país, relacionando también un modelo de alertas en términos de impacto, escala y alcance de las amenazas que se presentan como mecanismo esencial de protección. Concretamente, define un plan estratégico a mediano y largo plazo para fortalecer el ecosistema de salvaguardia de la infraestructura crítica siendo caracterizada como un activo nacional. Se menciona la existencia del Sistema Nacional de protección y defensa de infraestructuras críticas, conformado por la sinergia público-privada y social para el funcionamiento de los servicios de la nación; de igual modo, se establecen unas instancias relacionadas para el cumplimiento y garantía de la protección de la infraestructura.

Este documento es importante porque delimita los sectores críticos de la infraestructura en el Estado colombiano, en relación con la alimentación y la agricultura; el agua; el comercio, la industria y el turismo; la seguridad y la defensa; la electricidad; la educación; el sistema financiero; el aparato institucional; los recursos naturales y el medio ambiente; los recursos minero-energéticos; la salud y la protección social; las tecnologías de la información y las comunicaciones y el transporte (Ministerio de defensa Nacional, 2017, p. 22). Así mismo, se promueve la metodología de gestión del riesgo para la prevención por medio de cinco (5) niveles de alerta que permiten evaluar el impacto y las medidas o actividades que se deben realizar para su contención; los niveles identificados en el PNPICCN son:

- *Normalidad:* se pueden llegar a presentar alertas o vulnerabilidades, pero no se constituye como un riesgo significativo para el aparato nacional. Se realizan acciones

de tipo preventivo como el monitoreo, reporte, verificación, mantenimiento e información del Estado de la infraestructura crítica.

- *Bajo:* se identifican incidentes cibernéticos o amenazas independientes entre sí que afectan el 20% de las entidades o servicios, pero no impacta directamente a la población; son acciones que se pueden controlar y mitigar. Se implementan medidas de monitoreo y protección a la infraestructura por parte de la sinergia de partes interesadas y se reporta un seguimiento continuo.
- *Medio:* se presentan incidentes cibernéticos relacionados en varias de las entidades existiendo una posible falta de disponibilidad de los servicios básicos, con un impacto en la población, en la economía, en el medio ambiente y en la seguridad y defensa nacional. Se refuerzan medidas de protección, se implementan planes de contingencia, se ejerce vigilancia y el rol del Ministerio de defensa en la protección y garantía de la ciberseguridad y ciberdefensa se fortalece.
- *Alto*: los incidentes cibernéticos y las amenazas son potenciales, comprometen y pueden afectar activos cibernéticos estratégicos para el Estado, perjudicando a la población, al sistema económico, al medio ambiente y a la seguridad y la defensa de manera significativa; esto no solamente afecta al Estado sino también se emite una alerta a nivel regional y mundial. El monitoreo y la vigilancia son permanentes, los organismos de seguridad del Estado están en constante alerta y se trata de reducir a lo más mínimo el impacto que pueda llegar a tener sobre la infraestructura.
- *Emergencia cibernética:* los incidentes y las amenazas comprometen y afectan activos cibernéticos produciendo una afectación del más del 50% y tiene un impacto crítico en la población, en la economía colombiana, en el medio ambiente y sobre todo en la seguridad y la defensa. Se declara una alerta mundial y regional sobre la emergencia. Las Fuerzas Militares disponen de los medios necesarios para la protección y defensa

de la infraestructura crítica junto con el planeamiento continuo, la ejecución operacional de acciones para restablecer la soberanía y recuperar la estabilidad del Estado.

Con lo anterior, en el documento se puede evidenciar que la afectación sobre el escenario cibernético, en específico, sobre la infraestructura crítica no solamente tiene consecuencias en este dominio, sino que puede llegar a impactar el marítimo, el terrestre y el aéreo; lo cual puede representar una vulnerabilidad significativa para el Estado. Es evidente el rol de las Fuerzas Militares para la protección de esta infraestructura crítica ya que en los niveles de alerta siempre está presente, para desarrollar acciones que promuevan la defensa y la seguridad de la nación. Lo mencionado en este Plan, es fundamental para el estudio porque establece los lineamientos de la política de seguridad digital en Colombia, así como se indican las medidas, los órganos y las posibles afectaciones sobre la infraestructura crítica, siendo un producto de valor agregado para la investigación en este tema.

Así mismo, como se evidencia en los niveles de más alto impacto puede tener una repercusión a nivel regional y global; esto se relaciona con el último "*Global Risk Report*" del Foro Económico Mundial (2021) en donde se identifica que los ataques cibernéticos, las armas de destrucción masiva y el cambio climático se presentan como las principales amenazas de la próxima década, sin embargo, sus efectos pueden evidenciarse en la actualidad. Se presenta la masificación de la información, el fraude y el robo de información y datos personales como aspectos ligados a la posible vulneración de la ciberseguridad y con ello, se evidencia la importancia de la ciberdefensa. En cuanto a la infraestructura crítica se menciona que la afectación que puede llegar a ser por deterioro, afectación o destrucción crítica, puede perjudicar el desarrollo funcional de los sistemas utilizados para el sector público, la administración de armas nucleares, los satélites, entre otros elementos de impacto. Un elemento que se puntualiza es que un sistema de ciberdefensa obsoleto puede representar "el incremento

del cibercrimen con resultados en la disrupción de la economía, la pérdida financiera, tensiones geopolíticas y una inestabilidad social" (Foro Económico Mundial, 2021, p. 89).

La versión del PNPICCN para el año 2018 se enfocó en el sector ambiental determinando los riesgos que existen a nivel cibernético, sobre la posibilidad de que una amenaza se materialice sobre alguna vulnerabilidad generando afectaciones de consideración en servicios de información meteorológica o hidrometeorología. Siendo situaciones que provocan el robo de datos y acciones que afectan en tres aspectos: primero, la tecnología de información (servidores meteorológicos e infraestructura drp); segundo, comunicaciones (lan, red gprs, internet); y, tecnología de operación (bases de datos, sistema operativo, seguridad perimetral, seguridad de la información, coordinador drp) (IDEAM, 2018, p. 27).

De los lineamientos del sector defensa, desde el 2014 el CCOCI ha orientado su misión a proteger este tipo de activos estratégicos como lo es la infraestructura crítica cibernética desde un proceso metodológico que incluye su priorización junto con planes estratégicos. En relación, el CCOCI (2015) creó la *"Guía para la identificación de la infraestructura crítica en Colombia"* definiendo trece sectores esenciales (alimentario, agua, comercio, seguridad y defensa, educación, electricidad, financiero, gobierno, medioambiente, energético, salud, TIC´S, transporte) en donde se establece a la Seguridad y la Defensa. Se encontró un documento producido por CN. José Hernández Murillo (2016) – Jefe de Estado Mayor del CCOC (ahora conocido como CCOCI) sobre la "*Infraestructura crítica cibernética"* en donde se identifican las principales fuentes que desarrollan acciones que perjudican la ciberseguridad cómo lo son los grupos de crimen organizado trasnacional, *hackers*, los servicios de inteligencia extranjeros, entre otros. De igual manera, se presenta a modo de ejemplo casos específicos: Canadá, Australia y España, su estructura y medidas de protección de la infraestructura para evidenciar las similitudes y diferencias en la identificación de infraestructura crítica cibernética.

En relación con la Doctrina conjunta de las Fuerzas Militares colombianas, por medio del MFC 1.0, establecen una definición del dominio del ciberespacio, como global en el ambiente de la información en redes interdependientes de la infraestructura de las tecnologías de información, así como datos de la red, telecomunicaciones, controladores, entre otros (COGFM, 2018).

B. Academia

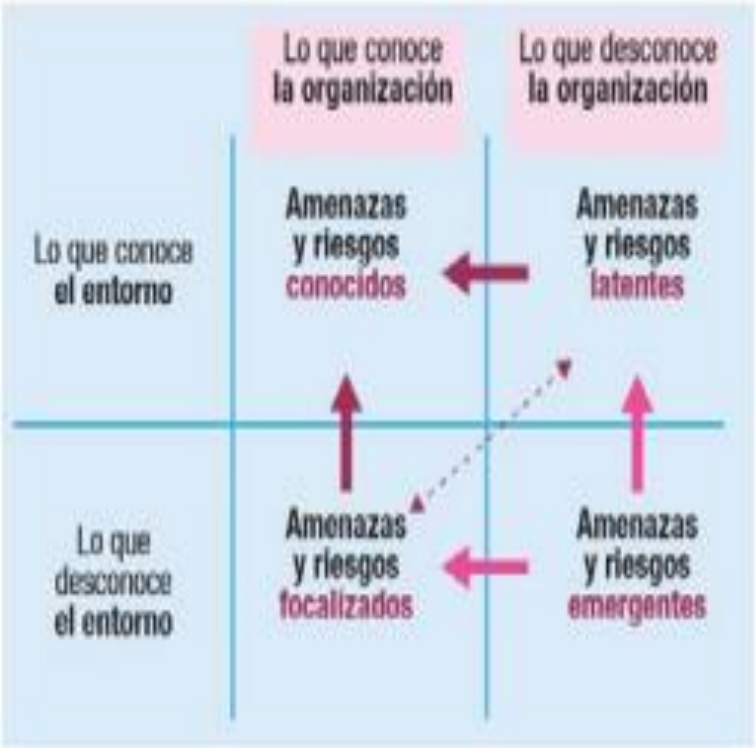
Un elemento específico-relacionado con el tema es explorado por Gaitán (2012): la ciberguerra, aspecto que profundiza desde unas generaciones relacionadas que plantea: *el control psicológico*, con la masificación de información que influye en los razonamientos siendo muchas veces parte de operaciones psicológicas. *El control de la infraestructura crítica del Estado,* un aspecto importante para el estudio, en donde el autor documenta que se dio una transformación por la globalización en donde varias capacidades fueron interconectadas en red como los sistemas financieros, la banca, las empresas, los sistemas de control de tránsito, sistemas de energía, acueductos, redes de comunicación, entre otros, siendo elementos vulnerables en el marco de una interconectividad compleja.

Por lo tanto, la sra. Teniente Coronel Milena Realpe Díaz y el Dr. Jeimy Cano Martínez (s.f.) desarrollan un *paper* sobre las amenazas cibernéticas reconociendo que son múltiples y pueden mutar rápidamente, un elemento que los adversarios utilizan haciendo uso de estas nuevas tecnologías y creando un escenario complejo y dinámico que debe ser protegido por las Fuerzas Militares y de Policía. Aquí es donde las Fuerzas Militares abordan el ciberespacio como un ámbito estratégico, operativo y táctico con el fin de establecer las medidas para la disuasión, contención y protección por medio del fortalecimiento de capacidades militares. La metodología implementada por los autores es diferente a la encontrada en los demás estudios, en razón a que utilizan el instrumento “ventana de AREM” desde cuatro variables en relación

con los riesgos: conocidos, focalizados, latentes y emergentes que pueden llegar a presentar las tecnologías disruptivas para Colombia.

Figura 1.

Ventana AREM



Fuente: Realpe y Cano (s.f., p. 109)

Teniendo en cuenta esto, determinan a la ciberguerra, las ramas letales autónomas, los sistemas autónomos, la guerra autónoma, las ciberarmas de destrucción masiva como principales amenazas. De igual modo, planteando una propuesta para el desarrollo de capacidades cibernéticas en las Fuerzas Militares fundamentado en el modelo de planeamiento DOMPILEM (doctrina, organización, material, personal, infraestructura, liderazgo, entrenamiento y mantenimiento); con ello se delimita en prospectiva la proyección de las Fuerzas Militares en operaciones cibernéticas (Realpe y Cano, s.f.).

En ese sentido, el artículo realizado por Cortés Borrero (2015) constituye un elemento importante en este aspecto, desde un método analítico-descriptivo reflexiona respecto a la

política pública en ciberseguridad y ciberdefensa en el Estado colombiano. Menciona que con el desarrollo de la tecnología han surgido problemas para la seguridad nacional a tal punto que representan una amenaza a nivel global (en específico Estado, sector privado y sociedad). Esto por medio de ataques que pueden llegar a vulnerar la infraestructura crítica del sector económico-financiero, por ejemplo. En Colombia, para contrarrestar estas vulnerabilidades, se han generado políticas públicas enfocadas en el entorno digital; un aporte fundamental es que detalla la principal normatividad nacional e internacional en torno al tema (retomando lo mencionado en el CONPES 3701/2011):

Cuadro 1.

Principal normatividad internacional y nacional en ciberseguridad y ciberdefensa.

Ámbito	**Tipo**	**Especificidad**
Internacional	Convenio sobre la ciberdelincuencia (2004).	Instrumento vinculante junto con el protocolo para criminalizar actos racistas y xenófobo.
	Resolución AG/RES 2004 – Asamblea general OEA	Estrategia integral para crear una red hemisférica, identificar y aplicar normas técnicas, adoptar mecanismos jurídicos para la protección en el escenario ciber.
Nacional	Constitución Política 1991	-Artículos 2, 15, 20, 75, 78.
	Leyes	-Ley 527/1999: Comercio electrónico -Ley 599/2000: Código penal -Ley 603/2000: Control de legalidad de *software*. -Ley 1266/2008: *Habeas Data* -Ley 1273/2009: Delitos informáticos -Ley 1341/2009: Sociedad de la información y las TIC -Ley 1581/2012: Protección de datos personales.
	Decreto	-Decreto reglamentario 1377/2013: Protección de datos personales.
	Especializada	-CONPES 3701/2011 -Norma técnica NTC-ISO/IEC Colombiana 27001

Fuente: Elaborado con datos de Cortés Borrero (2015, pp. 9-10) y CONPES 3701 (2011)

Junto con ello, el autor documenta que se establecen unos organismos del Estado que tienen la función de actuar para la ciberseguridad y la ciberdefensa: la presidencia de la República, el Ministerio de Defensa Nacional, el Ministerio de Tecnologías de la información y de las Comunicaciones, el CCOCI, el CCP y el colCERT, entre otros. En relación, concluye que evidencia un avance, pero insiste en que debe existir una iniciativa común de los sectores público-privado-sociedad para el desarrollo/aplicación de lineamientos en el escenario cibernético (reconocido actualmente como el quinto dominio de la guerra) como una responsabilidad conjunta.

Prieto (2017) desde el Ministerio de Defensa Nacional y colCERT, plantea unos parámetros de gestión y respuesta a los incidentes que se puedan generar sobre la infraestructura crítica y otros aspectos, como ciberespionaje, interrupción de servicios IT, filtración de datos, control sobre sistemas de infraestructura crítica, ciberdelitos, manipulación de información, errores y fallos, *malware*.

Figura 2.

Gestión y Respuesta a Incidentes.

Proactivos	Reactivos	Gestión
Reducir los riesgos de seguridad y su impacto, evitar incidentes cibernéticos	Responder a una amenaza o incidente que pudo haber sufrido una infraestructura o un sistema de información	Mediante los cuales se pretende mejorar todos los conceptos de Ciberseguridad en los ámbitos de formación y sensibilización
• Informes sobre vulnerabilidades presentes en una infraestructura o sistema de información • Gestión de Incidentes • Auditorias y evaluaciones de seguridad • Apoyo en inteligencia cibernética • Apoyo técnico para la mitigación y resolución del incidente • Trabajo colaborativo con los operadores de internet y administradores de dominio	• Gestión de Incidentes • Alertas sobre nuevas vulnerabilidades • Análisis de código malicioso (muestras de malware) • Envió y recepción de información sobre ataques con los homólogos internacionales	• Sensibilizar a entidades tanto públicas como privadas en temas de ciberseguridad • Coordinación de acciones para la identificación, priorización y catalogación de Infraestructuras Críticas. • Talleres de gestión de Incidentes • Eventos de Ciberseguridad

Fuente: Ministerio de Defensa Nacional y colCERT (2017)

Se encuentra un trabajo de grado de Camacho y Amaya (s.f.) quienes realizan descriptivamente una revisión puntual de los lineamientos existentes en relación con la defensa y la seguridad en el ciberespacio, focalizándose en el sector eléctrico en Colombia; encontrando que, si bien es un documento que describe lo existente en específico, no profundiza al respecto, encontrando así una posibilidad de que el estudio que se realiza aporte al desarrollo y análisis del objeto. Así mismo, Fula Perilla (s.f.) por medio de su trabajo de grado retomó los lineamientos del CONPES 3701, aunque el autor no especifica la metodología implementada se evidencia que es un estudio de tipo descriptivo que refuerza la tesis de que se requieren nuevas perspectivas de análisis en relación con el objeto de estudio. Por su parte, Cubillos Ramos (s.f.), plantea y describe los lineamientos del Estado relacionados con la gestión del riesgo en el ciberespacio, reflexionando sobre lo dado desde el Estado, mencionando que la política de seguridad digital está centrada en el sector defensa, por lo cual, debe coordinarse con las demás partes interesadas, contar con personal capacitado; resaltando la importancia en el ámbito militar que tiene el tema, al ser un asunto de seguridad nacional.

Por medio del trabajo de grado del Mayor Verdugo Sierra (2016) titulado *"la importancia de definir la infraestructura crítica en Colombia",* de manera concreta y descriptiva, resalta la importancia de tener un marco legal definido para infraestructura crítica, teniendo presentes los mecanismos que permitan un control centralizado y las responsabilidades de seguridad, mantenimiento y conservación. Resalta el rol de las Fuerzas Militares en la misión de la defensa en este escenario, enfatizando en la priorización que debe existir en cuanto los medios que se requieren para el cumplimiento de este objetivo. En general, el autor expone argumentos conceptuales sobre el tema, pero no es evidente la metodología utilizada, ni un análisis respecto a los términos que se mencionan.

También, Benjamín Montoya Gaitán (2016) plantea en su trabajo de grado, el objetivo de mirar cómo se puede minimizar el riesgo de afectación en caso de un ataque cibernético a

uno de los activos estratégicos de la nación. En su momento, el autor resaltaba la importancia de establecer una estrategia nacional de ciberseguridad y ciberdefensa, constituyéndose como un instrumento a largo plazo, orientado a la protección de los intereses nacionales y también a la construcción de una cultura en seguridad digital como elemento indispensable para construir una visión integral del tema, relacionando la cooperación como un elemento clave.

Jairo Cáceres García (2017) reflexiona en *"Colombia, estrategia nacional de ciberseguridad y ciberdefensa"* sobre lo significativo que fue la consolidación del CONPES 3701 en donde se establece la política de ciberseguridad y ciberdefensa, lo cual posiciona a Colombia como el primer país de América Latina en adoptar un elemento estratégico para la prevención y el enfrentamiento de delitos, junto con la minimización del nivel de riesgo ante amenazas o incidentes cibernéticos (p. 85). El documento presenta una visión multilateral sobre la temática, agregando a la ciberinteligencia como parte integral de la estrategia del Estado para contrarrestar los desafíos que se presenten en el entorno nacional, regional y global.

Jairo Becerra e Ivonne León (2019) concuerdan con lo mencionado por Gaitán Rodríguez (2012) con relación a que las nuevas tecnologías de comunicación y de información dieron la posibilidad de que, en el escenario internacional, la guerra se pudiera virtualizar. Los autores hacen referencia a la cuarta revolución tecnológica con la cual se amplió el espectro de las amenazas que pueden incidir y que requieren la respuesta oportuna del Estado para impedir que los efectos sean devastadores o catastróficos. De este modo, los procesos de producción automatizados y los sistemas de inteligencia artificial, entre otros, generan mayor independencia y pueden llegar a afectar ejes esenciales del Estado como la seguridad y defensa. Uno de los aspectos relevantes del texto es que se retoma la gobernanza digital, que involucra elementos como el Gobierno electrónico, la participación por medio de redes de información, la transparencia política y otros.

Otro de los resultados del estudio realizado por Becerra y León (2019) es el análisis que se hace sobre la figura del Estado, que, por la dinámica de la globalización, se ve inmerso en un proceso en donde debe reconfigurarse y adaptarse a esta nueva realidad, un escenario sin fronteras definidas. Por otro lado, resaltan la gestión del riesgo como el modelo necesario para categorizar el nivel de las amenazas y vulnerabilidades que se presentan para desestabilización del país, identificando la afectación de la infraestructura crítica como una de ellas. En este sentido, como se expuso en el CONPES, el Estado colombiano ya ha adoptado esta metodología para el escenario ciber y el desarrollo de medidas en relación.

Alejandro Bohórquez-Keeney (2019) amplia el desarrollo en la temática desde "*El impacto de la academia en la ciberseguridad",* profundizando en la reflexión sobre la educación, retomando al CCOCI, que la considera como un "servicio esencial para el mantenimiento de las funciones sociales básicas del Estado, y por ello hace parte de la infraestructura informática crítica de Colombia" (pp. 113-114). Esto permite ir más allá de la visión tradicional ligada a la economía, la energía, entre otro tipo de infraestructura ampliamente conocida, y darle paso a un ámbito social que también es parte de esa salvaguardia estatal. El autor plantea también la labor de capacitación que fomenta este sector, siendo expresada la recomendación de que sea mayormente incluida en el desarrollo de política pública en la materia; aunando en la necesidad de un centro de innovación en seguridad digital, en donde la academia sea un articulador con el Estado, el sector privado y la sociedad en general. Uno de los aspectos diferenciadores de este trabajo es la metodología, ya que involucra mesas de trabajo participativas de servidores públicos, miembros de la empresa privada, expertos e investigadores académicos para el análisis de los factores que fueron especificados.

En esta misma línea, Marco Sánchez Acevedo (2019) plantea a la investigación como un elemento esencial dentro de la política de seguridad digital en Colombia, como la base para la generación de estrategias relacionadas. El autor define la ciberdefensa como el conjunto de

acciones, operaciones activas o pasivas[1] y otras medidas desarrolladas en el ámbito de internet, redes y recursos informáticos y de comunicaciones para asegurar el cumplimiento de los servicios para los que fueron desarrollados, impidiendo que actores lo utilicen para desestabilizar. En relación, reafirma lo planteado en el CONPES para la creación de un tanque de pensamiento sobre la gestión de riesgos de seguridad digital en donde la investigación, el desarrollo y la innovación sean los pilares; es aquí donde la academia debe estar vinculada con la investigación para establecer una sinergia entre las partes interesadas, construyendo un ecosistema de seguridad digital y aportando soluciones a las problemáticas para la defensa de los intereses del Estado.

De este modo, en la academia militar se presenta la Estrategia de seguridad digital la cual los Generales Fabricio Cabrera y Helder Bonilla (2020) desde la Escuela Superior de Guerra "General Rafael Reyes Prieto" editan la publicación "*Estrategia Nacional de Ciberseguridad y Ciberdefensa 2020-2030"* por medio de la cual mencionan que se dan "los lineamientos para desarrollar capacidades ofensivas, defensivas, disuasivas y de inteligencia para la protección del Estado […] como una firma de gestionar y mitigar el riesgo […] para responder, recuperar y restaurar las áreas afectadas" (p. 6). Se establece el objetivo de proteger el uso seguro del ciberespacio por los ciudadanos y la Nación; además, se retoma la cooperación entre lo público y lo privado como factor clave para diseñar una arquitectura trasversal en el ciberespacio, orientada desde cinco factores: correspondencia, sinergia, proyección, eficiencia y legalidad-legitimidad. Lo anterior, para proteger los centros de poder estatal: político, económico, social y militar.

[1] Este concepto en específico, el autor lo relaciona con las definiciones dadas por las Fuerzas Militares (2015), así: "la defensa activa es una estrategia determinada en adquirir una capacidad de defensa del ciberespacio, combinando la protección interior de los sistemas, la vigilancia permanente de redes sensibles y la respuesta rápida en caso de ataque, contrarrestando las amenazas ciberespaciales y garantizando acceso al ciberespacio; (y la defensa pasiva es) la estrategia para la protección de los activos relacionados con los sistemas de información a través de controles detectivos, correctivos, disuasivos que contrarresten las posibles amenazas" (Sánchez Acevedo, 2019, p. 39)

En relación con el Global Cybersecurity Index del año 2018, los autores mencionan que se presenta a Colombia con un nivel de compromiso medio, como "países que han desarrollado acuerdos complejos y participan en programas e iniciativas de ciberseguridad" (Cabrera y Bonilla, 2020, p. 18). Se identifica a la región latinoamericana en general con este nivel de compromiso frente a un escenario que describen puede llegar a ser de catástrofe por el ciberterrorismo, el ciberdelito, el ciberespionaje y el *hacktivismo*, elementos dados, por ejemplo, desde la coalición de aviones, emisión de sustancias tóxicas de plantas químicas o ataques a la infraestructura crítica ligado a redes eléctricas y otros aspectos como lo relacionado con la vulneración y robo de datos personales. Este documento aporta un avance en el conocimiento relacionado con la construcción de medidas cibernéticas para la protección del Estado; profundiza en la protección de los activos estratégicos nacionales en los cuales se encuentran las infraestructuras críticas como: redes, servicios, instalación, *software*, información que de ser destruido o alterado generaría un impedimento en el funcionamiento institucional estatal (Cabrera y Bonilla, 2020).

Ximena Cujabante Villamil *et al* (2020) exponen que la visión tradicional en donde la seguridad y defensa estaba focalizada en las Fuerzas Militares, ahora debe constituirse en torno a la necesidad de una política de ciberdefensa y ciberseguridad del Estado. Para ese propósito, existe "la necesidad de integrar una multiplicidad de actores para hacer frente a las ciberamenazas existente" (p. 373). Los autores señalan la situación de conflicto armado para el caso colombiano, en donde ha existido un interés nacional en relación con la protección de la infraestructura crítica física y ahora virtual.

De acuerdo con lo mencionado en la revisión, el impacto del daño es analizado por Milton Ospina Díaz y Pedro Sanabria Rangel (2020) mediante el artículo *"Desafíos nacionales frente a la ciberseguridad en el escenario global: un análisis para Colombia"*, quienes interpretan y analizan sobre la capacidad que tiene un riesgo, ya no es necesario que se

perjudique físicamente alguna infraestructura, sino que virtualmente puede causar daño significativo o por medio de la difusión de información con fines delictivos. Específicamente,

> Los gobiernos y los organismos de seguridad reconocen que en la actualidad existe más riesgo de vulneración a la seguridad, incluyendo los delitos informáticos, ciberterrorismo y las diversas amenazas cibernéticas […] que han causado daños a la sociedad y pérdidas económicas (p. 201).

Finalmente, el estado del arte permite evidenciar la relevancia que tiene el estudio planteado en razón a que profundiza en el análisis sobre la ciberdefensa y su relación con la protección de la infraestructura crítica en Colombia. La mayoría de los lineamientos dados del Estado giran en torno a la ciberseguridad y a la gestión del riesgo relacionada; la academia también hace una reflexión general sobre el tema, pero no se encuentra un documento en donde se especifique la labor y el rol del Comando de Apoyo Operacional de Comunicaciones y Ciberdefensa del Ejército Nacional de Colombia, dejando un espacio que, por medio de la presente investigación, se quiere abordar.

Formulación del problema

Teniendo en cuenta el panorama anterior, se puede establecer como problema principal la vulneración de los sistemas de información como ataques informativos, secuestro de información, sabotaje, entre otros, todos provenientes del ciberespacio (Dark Reading, 2016), una problemática que afecta los sistemas de información y la infraestructura critica del país, entendida como aquellos bienes esenciales necesarios para el funcionamiento de la sociedad, gobierno y Estado.

Dicho la anterior se plantea la siguiente pregunta de investigación ¿Qué lineamientos estratégicos debe considerar el Comando de Apoyo Operacional de Comunicaciones y Ciberdefensa del Ejército Nacional de Colombia para la protección de la infraestructura crítica

del país? Esta pregunta pretende ser contestada por el desarrollo de una serie de objetivos (general y especifico) que se plantean a continuación.

Para los fines de este trabajo se usará un método analítico crítico, que permitirá descomponer y reconocer los elementos principales del problema a tratar -pensado como un todo-. Por medio de esto, se logrará llegar a un fin determinado que tendrá en el proceso un análisis de los elementos puntuales del problema, que, gracias al método elegido y sus usos, se puede aplicar en caminos abstractos (Lopera et al, 2010) como lo es el tema de infraestructura crítica y los lineamientos estratégicos para su defensa. Por lo anterior, la metodología es de carácter cualitativo, debido que comprende un enfoque interpretativo.

De esta forma se analizarán fuentes primarias y segundarias, documentos institucionales, informes, capítulos de libro y artículos científicos, asimismo, se contrastará la información obtenida con la finalidad de validar argumentos de forma objetiva.

Finalmente, se expondrá un documento descriptivo que evidenciará los resultados de un ejercicio critico constructivo que establezca los lineamientos estratégicos para la defensa de la infraestructura critica a considerar por el Comando de Apoyo Operacional de Comunicaciones y Ciberdefensa del Ejercito Nacional de Colombia.

Objetivos de la investigación

Objetivo general

Establecer los lineamientos estratégicos que debe seguir el Comando de Apoyo Operacional de Comunicaciones y Ciberdefensa del Ejercito Nacional para apoyar la defensa de la infraestructura critica del país.

Objetivos específicos

1) Realizar una aproximación teórica y conceptual sobre la importancia de la defensa de infraestructura critica en los Estados.

2) Identificar las amenazas, riesgos y peligros que pueden afectar la infraestructura critica de Colombia.
3) Proponer los lineamientos estratégicos en el Comando de Apoyo Operacional de Comunicaciones del Ejercito Nacional de Colombia para la protección de la infraestructura critica.

Justificación

La presente investigación aborda la importancia de establecer lineamientos para la protección de infraestructura crítica, teniendo en cuenta que la ciberseguridad y ciberdefensa adquirieron relevancia a partir del año 2011. Por tanto, es importante dentro de la doctrina militar desarrollar cultura estratégica enfocada a la protección del ciberespacio como principal elemento a contemplar en los nuevos lineamientos estratégicos de la política de seguridad y defensa nacionales.

Adicionalmente, se pretende despertar el interés por la protección de bienes estratégicos del estado en un contexto de evolución constante de las tecnologías de la información y comunicación. Se trata de profundizar aspectos conceptuales y teóricos que hagan referencia a la importancia de que el estado articule acciones para la protección de bienes importantes para el desarrollo económico y social, debido a que estos hacen parte de los intereses nacionales.

CAPÍTULO II Aproximación teórica y conceptual sobre la importancia de la defensa de infraestructura critica en los Estados.

Aproximación teórica a la Teoría General de Sistemas

Existen diferentes teorías relacionadas a los sistemas de información y comunicación, desde diferentes perspectivas se pueden comprender los múltiples enfoques para la comprensión de un problema social de orden organizacional o de interrelación social. En la actualidad, se evidencia una interacción cada vez mayor referente al desarrollo del nivel tecnológico que se articula con lo económico, social y político (Ministerio de Tecnologías de la Información y las Comunicaciones, 2018). De alguna u otra medida, la forma en que un sistema interactúa con las organizaciones y a la vez comportamientos de las personas, depende de los intereses sociales. En esta medida las organizaciones deben velar por la preservación y la defensa de los derechos y deberes, sin importar el entorno social en que se generen las nuevas amenazas.

Por tanto, es deber señalar la importancia de comprender la interacción social desde el enfoque de sistemas, debido a que el desarrollo tecnológico articulado con otras organizaciones se convierte cada vez en una necesidad por la dependencia, es decir, que existe cada vez una subordinación entre instituciones, tecnologías y desarrollo social.

Lo anterior, es debido a que la sociedad no se puede comprender únicamente desde el aspecto tecnológico o económico, se trata más bien de tener una mirada sistémica integral a todo lo que conforma el Estado y, a su vez, entender que una amenaza genera un impacto sistémico e integral, justamente como sucede desde el enfoque con la seguridad multidimensional.

Dicho lo anterior, el sistema entendido como un conjunto de organizaciones y sectores que integrados los convierte en engranajes sinérgicos que permiten el desarrollo y el bienestar

social, existe un engranaje cada vez más relevante que ha adquirido más importancia y se encuentra relacionado con el desarrollo tecnológico y el manejo de la información, a tal punto de que se ha convertido en un quinto escenario de operaciones militares, económicas e incluso culturales (Maldonado, 2017). En este sentido, ese escenario del uso de las nuevas tecnologías y la información que se convierten en herramientas para la gestión de diferentes sectores que, para este caso puntual, se encuentra relacionado con la infraestructura, un importante componente que está siendo amenazado desde el ciberespacio y, desde el enfoque, permite establecer que el impacto o daño de un sector puede afectar al sistema en su conjunto de manera física-material.

Pero antes de iniciar, se debe realizar una aproximación teórica al concepto de sistemas. En este sentido, la Teoría General de Sistemas desarrollada por Von Bertalanffy, establece la importancia que tienen las diferentes organizaciones para darle forma al organismo, y sustenta que todos se encuentran debidamente conectados y en su defensa la respuesta suele ser conjunta (Arnold y Osorio, 1998).

Para efectos de la presente investigación se tendrá en cuenta la Teoría de Sistemas desde la era de la información, una teoría desarrollada a mediados del siglo XX y que establece la importancia de la mente humana para el desarrollo de la ciencia, los complejos sistémicos de la información y en general todo lo relacionado con la tecnología y cibernética (López, 1998).

Desde esta perspectiva se puede evidenciar que todos los sistemas funcionan integralmente, pero aún más importante, es señalar que la afectación en una institución u organismo puede generar un impacto desproporcionado al sistema en su conjunto. Es por ello, que dichos autores mencionan que los sistemas se están reconfigurando continuamente, es decir, se construyen de acuerdo a las condiciones para mantener su supervivencia. Esta actualidad de las restauraciones o reconfiguración sistémica (cuando existe una crisis) se llama

autopoiesis, y se trata de una cualidad que reproduce y mantiene su supervivencia (Maturana, 1997).

Teniendo en cuenta la importancia de los sistemas, es importante relacionar dicha teoría con el ciber espacio, debido a que también tiene características que lo convierten en un sistema ¿Pero por qué es importante hablar de sistemas en el ciberespacio? Según estos autores mencionan que la existencia de un sistema se acondiciona a las realidades de otros, es decir, un individuo no puede sobrevivir en un entorno en donde no existan otros individuos, animales o plantas. Es decir, en el ciber espacio convergen diferentes actores, capacidades e intereses que le dan forma al entorno. Por tanto, es necesario aproximarse al análisis sistémico para comprender el ciberespacio.

Dicho lo anterior, existen sectores que son importantes para la supervivencia social y, por ello, la seguridad multidimensional defiende que existen amenazas que pueden dañar el desarrollo social en su conjunto. Es por ello, que se plantean diferentes dimensiones que tienen que ver con la seguridad y, estos a su vez, son los que componen un gran sistema que interactúan entre sí. El problema de fondo radica en la existencia de amenazas que están afectando desde el ciberespacio todo el sistema en su conjunto mediante ciberataques a infraestructura crítica, entendida como aquellos sectores esenciales que permiten que funcione la sociedad como la seguridad, el sector alimentario, el sector sanitario, la convivencia, entre otros. Desde esta posición de sistemas, se puede justificar la necesidad de que el sector defensa adecue sus capacidades para la defensa integral de los otros sectores.

Marcelo y Osorio (1998), la sociedad moderna está integrada por un conjunto de elementos que tienen estrechas relaciones y un contacto directo o indirecto. En la era de la tecnología, los sistemas son importantes debido a que permiten la interacción entre un sector y otro, pero que también transforman el entorno y el ambiente donde esto se encuentra. En este

sentido, se puede afirmar la existencia de ciertas dinámicas entre las organizaciones, el entorno y los intereses.

Para Echeverri (2016), es importante considerar conceptos como la ciberguerra, esta noción se ha definido de distintas maneras, probablemente más veces que la guerra. Por ejemplo, la guerra cibernética es un fenómeno de la sociedad que depende de los avances tecnológicos y la penetración que pueden tener en el ciberespacio (red), y la proyección del ciberespacio como futuro escenario de enfrentamientos.

Es así, que el ciberespacio debe ser entendido como un sistema principal, que abarca subsistemas (otras redes de información), debido a que articula a otros sectores. Adicionalmente, desde dicha perspectiva, si bien existen otras organizaciones que afectan el funcionamiento del sistema, especialmente las organizaciones criminales que están haciendo uso de los medios tecnológicos para afectar principalmente el sector financiero o económico, adicionalmente existen otras que afectan los sistemas de seguridad de los Estados desde el ciberespacio, por tanto, la ciberdefensa se convierte en un pilar importante en la defensa de los intereses nacionales. Como se puede ver, desde la teoría de sistemas se puede justificar la importancia de contemplar protocolos de seguridad para la defensa de los sectores que actualmente están haciendo afectados mediante el uso de tecnologías desde el ciberespacio.

Importancia de la aproximación teórica

Es importante considerar que, a raíz de las ciberamenazas, la inteligencia y la contrainteligencia militar enfrentan grandes desafíos en función a salvaguardar los intereses de las instituciones que se desempeñan en función a la seguridad (Mendoza, 2020). Para ello es importante tener en cuenta que existen amenazas o riesgos en donde se determinan la toma de decisiones, es decir, a partir de las vulneraciones y oportunidades que se generan en un determinado escenario sin tomar decisiones técnicas en función a un análisis predeterminado

con un enfoque prospectivo. Lo anterior se traduce en que la inteligencia se considera un método para el procesamiento de la información que tiene como objetivo reducir la incertidumbre en el momento de establecer o definir la toma de decisiones. Este proceso es permanente y debe ser sistemático toda vez que los escenarios cambian y las amenazas cambian.

Si bien es cierto, las tecnologías han impulsado el desarrollo de capacidades del Estado para mejorar las técnicas y metodologías para la detección de peligros o riesgos y contrarrestar las amenazas, el estilismo desarrollo tecnológico también es aprovechado por los actores ilegales, debido a que el acceso a las tecnologías es amplio y no discriminatorio. En este orden de ideas, tiene como primicia de que el acceso a las tecnologías no puede ser limitado, pero puede ser condicionado, es decir, establecer protocolos de prevención y atención cuando se genere un acto ilegal en el desarrollo de las actividades en el ciberespacio, los cuales deben acondicionarse a los marcos regulatorios nacionales e internacionales, debido a que existen actores que operan ilegalmente en la llamada *deep web*.

Por tal sentido, la inteligencia se convierte en una herramienta importante para contemplar los futuros escenarios de riesgos y amenazas, más aún en un quinto escenario o dominio de la guerra donde los estados se encuentran limitados dada las condiciones regulatorias y tecnológicas que tienden a limitar las operaciones militares en un escenario digital, de hecho no se tiene con precisión definida las líneas de acción que debe salvaguardar el Estado ante amenazas de carácter simétrico (entre Estados) y asimétrico (irregularidad).

> La contrainteligencia se refiere a los esfuerzos realizados para proteger las operaciones de inteligencia propias contra penetraciones y disrupciones provenientes de naciones hostiles o sus servicios de inteligencia. Puede ser analítica y operativa. Es ante todo una actividad defensiva, que considera al menos tres actividades. La primera es la recolección: obtener información sobre

> las capacidades de recolección de inteligencia del oponente, que pueden estar dirigidas hacia el servicio propio. La segunda es la defensiva: frustrar los esfuerzos de los servicios de inteligencia hostiles para penetrar el servicio propio. La tercera es la ofensiva: identificar los esfuerzos de una oponente en contra del sistema propio, tratar de manipular dichos ataques ya sea transformando a los agentes del oponente en dobles agentes o alimentándolos de información falsa que reportarán a su central (Lowenthal 2010, 205). (Mendoza, 2020, p.8).

Como consecuencia, la ciberdefensa debe integrar a la inteligencia y contrainteligencia, pues es un escenario volátil incierto que amerita emplear todas las capacidades y recursos que tiene el Estado para analizar el contexto y establecer las estrategias en función a los intereses nacionales.

Aprovechando este escenario de coyuntura, las fuerzas militares también tienen que tomar un rol importante hacia el futuro. Es así qué se debe diseñar un modelo de transformación estratégico, operacional y táctico, que involucre el direccionamiento de la defensa hacia escenarios como el ciberespacio (Ciro y Correa, 2014). Adicionalmente, desistir una transformación de la cultura estratégica debido a que este escenario es transversal a todos los dominios (terrestre, marítimo, aéreo y espacial).

En este sentido, la transformación sistémica en función a contemplar el desarrollo de nuevos roles y operaciones en el ciberespacio, no solo consiste en la adquisición de capacidades y el uso acertado de las mismas, se trata de crear una arquitectura lo suficientemente eficiente para afrontar las nuevas amenazas y en función al plan estratégico de transformación que replantea los futuros escenarios para las fuerzas militares colombianas.

Lo anterior parte de un fundamento constitucional que involucra la importancia de la defensa del interés nacional en cualquier escenario incluyendo el quinto dominio

(ciberespacio). Por tanto, la ciberseguridad y ciberdefensa son competencia también de las fuerzas de seguridad, pues las dinámicas que van en contra de desafiar la autoridad del estado y su monopolio legítimo de la fuerza también se están manifestando en lo digital.

> [...] se habla de la garantía de los derechos individuales y colectivos de las personas, los grupos y las comunidades; es decir, la vida, la honra y los bienes de las personas, sus libertades públicas fundamentales, sus prestaciones y servicios públicos y también de asistencia social reconocida; la igualdad, la no discriminación y también el trato diferencial que resulte justificado; los derechos y bienes colectivos relacionados con el medio ambiente y los recursos y riquezas naturales; la garantía de su propiedad pública o de su aprovechamiento sostenible; la protección del patrimonio público, pero también de las riquezas culturales y los derechos específicos reconocidos a las comunidades etnoculturalmente diversas. La contribución del Ejército a tales fines esenciales generales debe operar como manifestación de la finalidad primordial de defensa que justifica su existencia concreta (Ciro y Correa, 2014, p.32).

Uno de los aportes teóricos que se puede derivar desde la teoría de sistemas, es que existen diferentes características que se deben tener en cuenta: 1) el ambiente, relacionado con el entorno al interior del sistema; 2) el atributo, relacionada con las cualidades estructurales o funcionales del sistema; 3) la cibernética, relacionado con el acopio interdisciplinario de los diferentes procesos que permiten la retroalimentación; y 4) la complejidad, referida a la combinación entre la cibernética, el contexto y la identidad que se genera en el ambiente.

Con estos componentes presentados desde la teoría podemos afirmar las siguientes cuestiones:

Primero, un sistema depende de cómo se configure su entorno, en este sentido desde la ciberdefensa y la ciberseguridad, resulta comprender la importancia de los actores y las amenazas que pueden dañar el funcionamiento de todo un conglomerado de organizaciones que, en este caso, es el Estado y el bienestar general.

Segundo, el relacionado con las cualidades de cómo se encuentra configurado ese sistema y también cuáles son las funciones que desarrolla cada organización. Este aspecto resulta importante, debido a que el sistema normativo y social aún no se ha acoplado al entorno cambiante del ciberespacio, debido a que aún existen muchos interrogantes referentes al uso de las nuevas tecnologías y la información que no se contemplan en el ordenamiento jurídico. Ejemplo de ello, es que se reconoce la importancia de establecer protocolos de ciberdefensa pero aún no se tiene en cuenta con claridad las amenazas y la categorización de las mismas que pueden afectar a las instituciones en su funcionamiento (Osorio, 2007). En el caso de Colombia solo fue hasta el año 2011, que se consideró la importancia de plantear departamentos o unidades militares en la defensa nacional de amenazas que provengan del ciberespacio

Tercero, otro aspecto importante y que también se relaciona con la globalización y la revolución tecnológica es la cibernética, este concepto es empleado para comprender la interconexión de las diferentes disciplinas y pensamientos en un entorno digital. Precisamente una de las características del ciberespacio es la no existencia de barreras de espacio y de tiempo para que las personas puedan interactuar en ese entorno digital

Y, por último, otro aspecto es la complejidad misma del sistema. Si bien es cierto que aún no se tiene con precisión protocolos normativos referente a limitar amenazas en el ciberespacio, es necesario también comprender que la dinámica social y el comportamiento de los individuos se pueden ver afectados en un entorno digital que no es regulado por el Estado, esto es uno de los principales riesgos que se desprenden del ciberespacio y que pueden afectar el mundo físico o lo material.

Razón por la cual este concepto es analizado bajo la evolución de los computadores, la Internet y la dimensión ciberespacial por parte de un Estado (mediante sus fuerzas de defensa y seguridad) con el objetivo de causar daños suntuarios sobre otro (Estado), mediante el desarrollo de ataques cibernéticos que van dirigidos hacia su infraestructura crítica (Gaitán, 2013).

¿Pero por qué es importante la teoría de sistemas? Interpretar el problema al ciberespacio desde esta teoría, permite afirmar la idea de la necesidad de crear lineamientos jurídicos y protocolos de seguridad desde el Ejército Nacional de Colombia para darse a las circunstancias del entorno y prevenir la afectación de las operaciones del Estado en su conjunto por parte de la criminalidad y/o grupos armados organizados. Pero desde la ciberdefensa, es importante también comprender la existencia de un sistema internacional donde los Estados se encuentran permanentemente en disputa y este entorno complejo puede afectar los intereses de un estado en las diferentes esferas y mediante el ciberespacio.

Dicho lo anterior Prieto (2013) afirma que la ciberguerra es "El uso de capacidades basadas en la red de un Estado, para interrumpir, denegar, degradar, manipular o destruir información residente en ordenadores y redes de ordenadores, o los propios ordenadores y las redes de otro Estado" (p.4.)

Es así que, si combinamos la teoría y las definiciones conceptuales, podemos determinar de que no se puede ver la seguridad y la defensa únicamente es del plano físico sino también desde un plano digital que no es material, pero que puede tener un pacto físico mediante la manipulación y el sabotaje de sistemas esenciales para el Estado.

Marco conceptual

La teoría de los sistemas y el concepto de seguridad multidimensional: una perspectiva sistémica

Se tiene que abordar la importancia de la seguridad en la era de la información, toda vez que se debe identificar y categorizar las nuevas amenazas provenientes de un escenario digital y no físico. Es vital proteger sectores estratégicos nacionales en razón al nivel de impacto que pueden generar sobre las finanzas del Estado y sobre la propiedad pública un daño parcial o importante de bienes estratégicos.

Lo anterior, es debido a que los ciberataques provenientes desde otros Estados han aumentado sistemáticamente en los últimos 20 años. Por ejemplo, uno de los Estados de mayor afectación es Estados Unidos debido a que se evidencia un creciente interés de los actores irregulares para desestabilizar las finanzas de ese Estado y también afectar el sistema político al interior del país mediante el empleo de ciberataques o también el uso del ciberespacio como las redes sociales (Benavides-Astudillo, Fuertes-Díaz y Sánchez-Gordon, 2020). Al respecto de lo anterior, se menciona:

> Los ciberataques son actos criminales ejecutados a través de un ordenador u otra tecnología informática con el fin de causar algún daño o extorsión tanto físico (cuando se ataca a personas o propiedades) como tecnológico (cuando se ataca a otros equipos y sistemas informáticos). Cuando dichos ataques se llevan a cabo para tratar de lograr un fin religioso, ideológico o político se trata entonces de una manifestación. Miguel Ángel Poveda Criado y Begoña Torrente Barredo 512 Opción, Año 32, No. Especial 8 (2016): 509 - 518 ciberterrorismo. Existen dos tipos de ciberataques que pueden ser ejecutados por terroristas: ataques a infraestructuras informáticas y ataques a infraestructuras físicas. [...] Los terroristas pueden llevar a cabo estos ataques a través de internet u otro recurso informático para distorsionar o causar algún daño en las infraestructuras de las

> Tecnologías de Información y Comunicación (TIC). Se trata entonces de ataques a datos y sistemas informáticos que no pretenden causar ningún perjuicio físico en personas o propiedades, aunque al final ese daño casi siempre se produce por la conexión entre la tecnología y la realidad [...] (Poveda y Torrente, 2016, p. 512-513).

Para Kevin Coleman (2008), citado por Echeverri (2016), "un conflicto que utiliza transacciones hostiles o ataques a ordenadores y redes en un esfuerzo por interrumpir las comunicaciones y otras piezas de la infraestructura, como un mecanismo para infligir daño económico o alterar y atacar las defensas" (p.9).

Sobre la Ciberguerra

En consecuencia, esta teoría emplea lo que ha sido el desarrollo de la inteligencia artificial en los diferentes sistemas informáticos y como estos se articulan a un modelo de organización algorítmica que en el mundo moderno está definiendo el desarrollo de las operaciones y relaciones entre los seres humanos.

Para efectos de la presente investigación se tendrá en cuenta la Teoría de la Información, una teoría desarrollada a mediados del siglo 20 y que establece la importancia de la mente humana para el desarrollo de la ciencia, los complejos sistémicos de la información y en general todo lo relacionado con la tecnología y cibernética (López, 1998).

Pero un aspecto más preocupante es el relacionado con la seguridad nacional, está entendida como la afectación de los intereses importantes para todo el Estado. En el caso particular del hemisferio americano, desde el año 2003 la Organización de Estados Americanos -OEA- establece una serie de amenazas emergentes que no solo se pueden enfrentar de manera militar, debido a que, a raíz del crecimiento de los grupos criminales y organizados, se

identificó un deterioro en el bienestar e igualdad social (Zavaleta, 2015). Así mismo, se evidencia que muchas de las amenazas ya emplean el uso de nuevas tecnologías.

Lo importante del enfoque de la seguridad multidimensional, radica en que el Estado tiene que ampliar la categoría de las nuevas amenazas y no solo enfrentarlas de manera física o material, sino también emplear estrategias de orden estructural tales como la adecuación de la infraestructura del Estado para evitar los riesgos y peligros. Por ejemplo, el sector alimentario, el sanitario y el medioambiental (Kerber, 2004), son otras dimensiones que deben contemplarse para la defensa de sus intereses. Dicho lo anterior, se propone que el Estado garantice el funcionamiento de sectores esenciales para el desarrollo humano y, por tanto, garantice la protección de la estructura teniendo en cuenta el nuevo entorno social qué están haciendo a raíz de las nuevas amenazas que provienen de la internet (Rodríguez, 2016).

Así las cosas, es importante contemplar el sector del ciberespacio, esto debido a que muchas de las transacciones de todos los sectores convergen en este espacio digital y también aumenta el número de probabilidades de que se presente una vulneración.

Es así que se amplía la gama de escenarios en donde el Estado debe articular esfuerzos y establecer lineamientos estratégicos para la protección de sectores vitales para la sociedad (Rodríguez, 2016). Este tipo de sectores tienen infraestructura o activos estratégicos que permiten garantizar el bienestar general de un Estado, a estos se les llama *infraestructura crítica*.

Infraestructura Crítica

Actualmente el sistema internacional enfrenta una nueva reconfiguración del poder, un proceso para el restablecimiento de un nuevo orden mundial donde los aspectos económicos, militares, políticos y sociales siguen representando factores importantes para alcanzar predominio a nivel internacional.

Desde la Teoría Realista de las Relaciones Internacionales, se asume al sistema internacional como anárquico, es decir un sistema relacional complejo y sin ley, donde los principales actores son los Estados. Dichos actores se desenvuelven en el sistema según su naturaleza, la cual está encaminada en principio a salvaguardar su supervivencia mediante el incremento sistemático de su poder. El poder entendido como la capacidad económica, militar y política de un Estado para influenciar, persuadir u obligar a otros actores actuar según sus intereses.

Desde la perspectiva Raymond Aron entiende al Estado como el principal sujeto de la Relaciones Internacionales (En adelante: RR. II), por lo cual su accionar se considera racional en tanto este va encaminado a la búsqueda de un equilibrio de poder (Aron, 1895). Por ende, al ser el principal actor y teniendo en cuenta su naturaleza, no existe autoridad superior al Estado. En síntesis, los Estados permanecen en constante lucha y su accionar está guiado por sus intereses.

En resumen, la teoría realista presenta la siguiente diferenciación de dos dimensiones del poder; El poder tangible comprendido por el componente geográfico, los recursos naturales y las personas. El poder intangible comprende la situación estratégica, la habilidad técnica, estabilidad económica y política. Según Hans Morgenthau, el poder no solo se basa en lo militar, sino que existe una dimensión política igual de importante en las RR. II; la política exterior y la diplomacia son los medios que el Estado emplea para conseguir la consecución de sus intereses por vía no armada y no violenta (Morgenthau & Thompson, 1986).

Los Estados han ido fortaleciendo la defensa de su Infraestructura Critica (IC) e Infraestructura Critica Cibernética (ICC), por tal el Estado Colombiano y con base al artículo 217 de Constitución Política Colombiana, ha realizado esfuerzos en pro de llegar a mantener una defensa constante de amenazas nacionales e internacionales de su infraestructura critica; 1) alimentación y agricultura, 2) agua, 3) comercio, industria y turismo, 4) seguridad y defensa,

5) educación, 6) electricidad, 7) financiero, 8) gobierno, 9) recursos naturales y medio ambiente, 10) recursos minero energéticos, 11) salud y protección social, 12) tecnologías de información y comunicaciones y 13) transporte (PNPICCN, 2017); sin embargo, los acercamientos y la cooperación con entidades de carácter público y privado aún está dando sus primeros pasos, al respecto se cita que "Los países con experiencia en la protección de infraestructuras críticas han definido sus sectores estratégicos previamente. En este sentido, Colombia ha iniciado un camino que permitirá garantizar la prestación de servicios esenciales a la sociedad" (González, 2019, párrafo 1); de esta manera realizar una aproximación sobre la importancia de la defensa de la infraestructura critica.

> [...] los nuevos delitos y sus penas, podemos decir que las leyes deben estar atentas a los cambios constantes de las amenazas, porque de no hacerlo los delincuentes sacarían un gran partido de ello. Así la UE y sus miembros, siguen la línea de estandarizar todo lo posible los delitos y sus legislaciones propias antiterroristas, para en consecuencia poder combatir de forma compacta y unida este germen llamado ciberterrorismo. De forma seguida, al análisis legislativo y hablando ya de las directrices defensivas, tras nuestro análisis, intuimos que para el éxito en la lucha contra el ciberterrorismo, no sirve un sistema de defensa nacional simple y convencional, además de la tecnología más moderna, se necesita un conjunto de sistemas de defensa que a su vez se unen a otros, creciendo según aumentamos fronteras, esto nos hace concluir que la ciberdefensa es un gran entramado mundial de sistemas defensivos. [...] (Pons, 2017, p.17).

La infraestructura crítica es un concepto que se implementó por el Programa Europeo para la Protección de Infraestructuras Críticas en el año 2006, el cual contemplo la definición de una serie de sectores importantes como: el energético, alimentario, el suministro de agua, el

de la salud pública, los sistemas de transporte, los servicios de seguridad, el sector de telecomunicaciones y el sistema económico-financiero (Unión Europea, 2007).

El problema puntual radica en que estos sectores son vulnerables y muchos de estos hacen el empleo de sistemas de información para el desarrollo de sus operaciones, un aspecto que, desde el escenario del ciberespacio, puede ser un punto de vulnerabilidad en la estrategia de defensa y seguridad, en razón que el sabotaje o el daño a uno de estos sistemas puede causar un mal mayor (Lozano y Páez, 2015).

Dicho lo anterior, se puede establecer la importancia de comprender el ciberespacio como un entorno sistémico y que integra muchos sectores y también articularlo a la importancia de la seguridad multidimensional, especialmente el relacionado con la *ciberseguridad* y *ciberdefensa* (Pons, 2017), debido a que la dependencia cada vez mayor en las llamadas sociedades de la información, son motivo de consideración por parte de las Fuerzas Militares.

Partiendo de la importante posición geográfica y estratégica del país en el continente; así como su fuerte alianza y lazos comerciales, militares y tecnológicos con las principales potencias globales; hay que hacer claridad que el país no cuenta con una Estrategia de Seguridad Nacional definida, por esta razón es dispendioso realizar un acercamiento a las amenazas y riesgos que pueden afectar la infraestructura crítica, así como realizar una exposición de las posibles situaciones que a la fecha no han permitido que se desarrolle esta estrategia (Ministerio de Defensa Nacional, 2017).

> El crimen informático ha llegado a niveles organizacionales, de hecho Fernández (2013) destaca la importancia que reviste la complicidad interna, por intermedio del personal que labora en la misma, quienes sin importar los valores de respeto y lealtad, perjudican la vulnerabilidad de la información de la organización, volviéndose inclusive en algunos casos, en algo codiciado que, además, es muy bien remunerada por los delincuentes cibernéticos, que buscan

> el desprestigio o robo de información confidencial, con la intención de chantajear o liquidar las empresas. (Acosta, Benavides & García, 2020, p. 2-3).

Finalmente, se puede mencionar que el Ejército Nacional a través del Comando de Apoyo Operacional de Comunicaciones y Ciberdefensa, viene adelantando su participación en la reunión del comité de infraestructura critica el cual es orientado por el Comando Conjunto Cibernético del Comando General de las Fuerzas Militares; sin embargo, es necesario dar un enfoque en el cual se observe con mayor claridad su posición frente a la capacidad de brindar seguridad y defensa ante la protección de infraestructura crítica y por tal motivo indicar los lineamientos estratégicos que debe tener esta unidad al momento de participar en la reunión que orienta el CCOCI como integrante del comité intersectorial de ciberseguridad (Comando Conjunto Cibernético, 2016).

CAPÍTULO III Identificar las amenazas, riesgos y peligros que pueden afectar la infraestructura critica de Colombia

La infraestructura crítica depende del desarrollo e implementación de las nuevas tecnologías, debido a que el desarrollo de un mundo digitalizado genera la dependencia de las instituciones y sectores por la red. En esta medida, los sectores importantes para el desarrollo social y político de los Estados serán vulnerables a las amenazas multisectoriales.

A continuación, se identifican una serie de amenazas, riesgos y peligros a los que se ve expuesta la infraestructura crítica en el escenario contemporáneo, pues la adquisición de nuevas capacidades de las amenazas que emplean el dominio del ciberespacio, tiende a potencializar el margen de daño en razón al empleo de los nuevos medios (medios digitales) y los modos en que se emplean (ilegalidad, irregularidad).

La infraestructura crítica hace parte de todo el sistema de gobierno en los Estados modernos, y por su misma importancia estratégica para el desarrollo los estados también son altamente vulnerables a riesgos y amenazas fruto de las nuevas amenazas de carácter simétrico y asimétrico.

Uno de los ejemplos que recientemente ha sido objeto de análisis de los diferentes sistemas de riesgos en materia de seguridad informática, fueron los ataques generados después del 11 de septiembre en los Estados Unidos (Korstanje, 2010) y los que fueron identificados por el servicio inteligencia norteamericano, en estos se evidencian los múltiples ataques a los que fueron sometidos centrales nucleares no solo en Estados Unidos sino también en Irán. Esto indica que independientemente del contexto social y el conflicto a nivel internacional entre los diferentes Estados (Rakkah, 2005), existe una fuerte tendencia para buscar el daño y sabotaje de infraestructuras estratégicas, entre las cuales principalmente se encuentra la infraestructura energética (energía) y vial (carreteras) que hace parte de la infraestructura crítica.

Según el instituto LISA, un instituto especializado en la formación en inteligencia, ciberseguridad y defensa, hace mención la existencia de vulneraciones a la seguridad de los sistemas energéticos a nivel mundial, puntualizando en los sistemas que se encuentran relacionados una producción de energía nuclear.

Por otra parte, y siguiendo la línea del instituto LISA, menciona también la importancia de los sistemas esenciales relacionados con funciones vitales como la salud, integridad física, el bienestar social y el factor económico, cualquier vulneración de la infraestructura en los diferentes campos de acción puede generar una grave afectación al desarrollo de las funciones de un gobierno. En este sentido el Centro de Protección de la Estructura y Ciberseguridad (CNPIC), menciona la existencia de diferentes factores de riesgo y de amenaza que pueden interrumpir el funcionamiento de los sistemas esenciales para la supervivencia no solo del Estado, sino de las personas, para ello es importante categorizar la importancia de los diferentes tipos de infraestructura, para ello se define:

Infraestructura crítica, es entendida como aquella infraestructura estratégica que proporciona servicios esenciales y cuyo funcionamiento indispensable permite la prestación de los servicios para la supervivencia del Estado. En su defecto, cualquier riesgo inminente de amenaza puede generar una grave perturbación o destrucción de gran impacto sobre los servicios esenciales.

Infraestructura estratégica, es entendida como aquellas instalaciones, redes, sistemas, equipos físicos y de alta tecnología en donde descansa el funcionamiento de los servicios esenciales. Bajo estas perspectivas se puede afirmar que toda infraestructura crítica resulta siendo un activo estratégico para la prestación de servicios esenciales, y por lo tanto, los daños pueden ser físicos o virtuales y, bajo está lógica, se evidencia una alta alteración de estos sistemas ante ataques terroristas o ataques que provengan del ciberespacio, sin importar el

origen del riesgo de la amenaza se pueden generar grandes consecuencias al funcionamiento esencial de los servicios.

El CNPIC, fue constituido en el año 2007, el Ministerio del Interior de España aprobó la creación de un centro de protección teniendo en cuenta la necesidad de proteger las infraestructuras nacionales. Para ello se estableció un plan de seguridad de infraestructura crítica y también se catalogó a nivel nacional todas esas infraestructuras críticas, estableciendo como resultado la existencia de más de 3.500 infraestructuras importantes para la nación, al respecto se reconoció como objetivo del centro:

> [...] establecer las estrategias y las estructuras adecuadas que permitan dirigir y coordinar las actuaciones de los distintos órganos de las Administraciones Públicas en materia de protección de infraestructuras críticas, previa identificación y designación de las mismas, para mejorar la prevención, preparación y respuesta de nuestro Estado frente a atentados terroristas u otras amenazas que afecten a infraestructuras críticas. (Ministerio del Interior de España, 2011, Articulo 1).

Desde esta lógica, son muchos los factores de riesgo y fuentes de amenaza que pueden alterar la estabilidad de cualquier estado, y bajo esta perspectiva, la caída de la infraestructura crítica supondría la paralización de los servicios en los diferentes campos de acción del estado, esto incluye los sistemas de seguridad y defensa, al respecto se cita “las infraestructuras críticas son todos aquellos sistemas físicos o virtuales que facilitan funciones y servicios esenciales para apoyar a los sistemas más básicos a nivel social, económicos, medioambiental y político” (Instituto LISA, 2009, párrafo 11).

Por lo anterior, es importante también comprender la dinámica evolutiva de la amenaza, esto teniendo en cuenta que las diferentes fuentes de peligros y riesgos dependerán del reconocimiento del contexto social, las capacidades tecnológicas de ambos bandos y, el marco jurídico existente para comprender los cambios sociales en materia tecnológica y enmarcada en la globalización.

Amenazas a la infraestructura crítica

En el contexto contemporáneo son múltiples las amenazas que pueden ser factor de desestabilización en el funcionamiento de la infraestructura, entre estos se encuentran dos categorías importantes a establecer: las *amenazas de carácter simétrico* relacionadas con la acción inteligente de Estados antagonistas para desestabilizar o impactar los sistemas estratégicos de un estado mediante acciones relacionadas con el empleo de la fuerza o el empleo del poder de manera inteligente, bien sea por el espionaje o el sabotaje; 2) las *amenazas de carácter asimétrico*, estás relacionadas con grupos irregulares que emplean métodos y estrategias poco comunes para sostener utilidades en diferentes escenarios. En esta categoría hay múltiples factores de riesgos que se pueden desprender del ciberespacio y en los cuales no solamente están relacionados los grupos terroristas sino también las organizaciones criminales armadas que hacen uso de los medios tecnológicos para el sostenimiento de campañas de desestabilización a los Estados.

Colombia debe construir una Ley de ciberdefensa y ciberseguridad para garantizar la integridad nacional en el quinto dominio, defender la soberanía nacional y salvaguardar los intereses del Estado ante los futuros escenarios hostiles del sistema internacional. La estrategia debe enfocarse en el fortalecimiento del sistema institucional, el poder civil y la planeación de la seguridad y defensa nacional.

Se debe precisar que el tipo de estrategia que debe contemplar la disuasión y contención como principales estrategias. La contención en el ámbito nacional, debido a que la Fuerza Pública con el acompañamiento de las demás instituciones deben contrarrestar el creciente de la delincuencia organizada y de grupos armados en la actual coyuntura nacional. ¿Por qué la contención? En respuesta, la contención establece como principal objetivo "[…]evitar que un oponente en busca de expansión territorial actúe para lograr sus pretensiones… Es la estrategia de mantener al adversario sobre la "raya" (Matallana, s.f, p.1). En este sentido, el fin último de dicha estrategia consiste en disminuir las expectativas del oponente, hasta que el mismo se canse y abandone sus pretensiones y/o intereses.

Como segundo elemento de la ley, se debe emplear una estrategia de disuasión en el ámbito internacional. ¿Por qué la disuasión? La estrategia de disuasión se considera como estrategia de defensa. Esta es empleada siempre y cuando el poder sea creíble, por lo tanto, Colombia debe fortalecer sus capacidades militares con la adquisición de material bélico para la defensa debido a que el fin último de esta estrategia es evitar una acción del enemigo (Matallana, s.f).

La estrategia aquí empleada pretende frenar el crecimiento de las amenazas nacionales, debido a que la contención como estrategia pretende en fin último evitar el fortalecimiento de los enemigos para que alcances sus objetivos criminales.

Actualmente no se puede emprender una estrategia de ataque directo debido a las implicaciones internacionales por emplear las Fuerzas Militares para resolver problemas de orden interno. En cambio, si se emplea una estrategia que limite el crecimiento de los grupos armados ilegales y las nuevas amenazas se limitaría el margen de maniobrabilidad del criminal, claramente con la abierta posibilidad de hacer uso de la fuerza en casos excepcionales.

Si se tiene en cuenta que son múltiples las problemáticas sociales asociadas a las secuelas producidas por el conflicto armado interno colombiano y que repercuten por ejemplo

sobre el pueblo ecuatoriano como problemas relacionados con el narcotráfico, la extorsión, el tráfico de armas y el contrabando. No obstante, en los últimos 10 años se presenta un fenómeno migratorio ilegal desde Ecuador que evidencia una lógica de proliferación de las dinámicas ilegales, pues la frontera se presenta como un punto de convergencia entre las múltiples redes criminales entre las cuales se encuentra la red de tráfico de personas. En este sentido las fronteras suelen ser abiertas y dinámicas, imposibles de controlar (Mancuso, 2017). Para el mismo autor, muchas de las dinámicas son planeadas y ejecutadas desde el ciberespacio, esto representa una clara vulneración a la ciberdefensa de un Estado, pues las nuevas organizaciones criminales hacen uso de los medios digitales para impulsar su margen criminal. Desde Esta perspectiva, el ciberespacio adquiere importancia y, con ello, establecer las capacidades, medios y métodos para la defensa de los intereses nacionales desde el estado.

Desde la proliferación de los nuevos delitos informáticos y ataques propios de amenazas externas hacia el Estado, se puede establecer una relación de impacto negativo a las que se puede ver expuesta la infraestructura critica, debido a que las amenazas, vistas como la fuente del riesgo y peligro, pueden impactar la infraestructura critica generando un daño material o, en su defecto, impidiendo el funcionamiento.

Sin importar el origen de las amenazas, se puede establecer dos categorías fuente que hacen uso del empleo del ciberespacio para imponer su voluntad. Es por ello, que el nivel de riesgo es alto en razón a que uno de los aspectos que favorecen el accionar criminal es el anonimato de las acciones realizadas desde los medios digitales.

> […] La modernización ha traído consigo, que el manejo de la información, se realice mediante procesadores informáticos, que permiten almacenar una cantidad considerable de información y, que, al mismo tiempo, se pueda acceder de manera rápida y efectiva a esos datos. La información puede ser de cualquier tipo (personal, empresarial, financiera-bancaria, societaria), siendo esta

> apetecida por los llamados delincuentes informáticos con la intención de sacar provechos de tipo oneroso, por intermedios del chantaje, desprestigio y hasta secuestro de la información sustraída. (Acosta, Benavides & García, 2020, p. 5).

Es importante destacar que las infraestructuras críticas son muy similares en diferentes países, lo que varía es el grado de complejidad y uso de las nuevas tecnologías debido a la gran diferencia en el manejo de los recursos estratégicos del Estado por medio de ese tipo de infraestructura. Resulta diferente hablar de la red energética de los Estados Unidos en comparación con la red de países poco desarrollados como Colombia, el nivel de vulnerabilidad en estos escenarios dependerá también del empleo y uso de los sistemas de información y de seguridad, pues los protocolos suelen variar de acuerdo a normativas y legislaciones nacionales.

Adicionalmente también es importante destacar que existen diferentes fuentes de amenazas y riesgos propios de cada estado, mientras que Estados Unidos tiene un factor de riesgo más alto al recibir ciberataques a su infraestructura crítica tanto de naturaleza simétrica da la rivalidad con otros Estados, Colombia está más expuesta a recibir ataques de un origen o naturaleza asimétrica, dadas las condiciones de conflicto armado interno y la multiplicidad de actores criminales trasnacionales que emplean métodos irregulares o insurgentes. Cómo se ha mencionado, en ambos casos es importante reconocer el desarrollo tecnológico y las capacidades con que cuenta el sistema de seguridad del Estado, pero al mismo tiempo también comprender los intereses y capacidades de los actores ilegales.

Importancia de la evolución de la amenaza para determinar el riesgo

Para Hurtado (2014), el mundo globalizado tiende a evidenciar errores estructurales (organización y comprensión de los problemas sociales en función al bienestar social e

intereses del Estado) que dificulta la gestión administrativa de la seguridad por parte del Estado frente a contemplar la situación externa de la dinámica evolutiva de las amenazas y para ello es importante contemplar la defensa como un medio fundamental en el desarrollo de políticas públicas. Por lo tanto, este problema evidencia brechas importantes conocidas como riesgos, en el marco del planeamiento estratégico. Este concepto se entiende como la posibilidad de que exista una situación de anormalidad que impacte no solo en la seguridad del Estado, sino que impida la garantía de los intereses nacionales.

Con respecto a lo anterior, resulta importante señalar que la infraestructura por el nivel de importancia estratégico y su nivel de esencialidad para el funcionamiento del Estado, debe representar una prioridad para la protección de los intereses nacionales. Como consecuencia, se debe considerar que el nivel de riesgo varía en función de la ubicación de la infraestructura, el sector, y finalmente, el número de las amenazas.

En el caso colombiano, evidentemente las amenazas al ser de carácter asimétrico, el mayor factor de riesgo, proviene de las organizaciones armadas ilegales, donde el ataque a la infraestructura crítica ha provenido de atentados terroristas. Por ejemplo, los ataques a oleoductos petroleros, debido a que son el principal objetivo para generar un impacto negativo a la seguridad nacional.

Ahora bien, a raíz de la implementación de las nuevas tecnologías teniendo en cuenta a Sánchez Hurtado (2014), y la necesidad de proteger aspectos estructurales indispensables para el Estado, es necesario implementar una serie de protocolos para la protección de las amenazas en Colombia, y contemplar los diferentes factores de riesgos especialmente el relacionado con el ciberespacio, que como ya se mencionó, es un nuevo dominio de la guerra que ha traspasado las fronteras.

Para ello, y teniendo en cuenta los avances en materia de ciberseguridad y ciberdefensa por parte de los países europeos, puntualmente tomando el caso de España, se estableció una

serie de Marcos estructurales que dieron forma al CNPIC, estos referidos a cada uno de los sectores de la industria como: El financiero, la administración de gobierno, el sistema de agua potable, alimentación, energía, ciberespacio, nuclear, químico, investigación, salud, TIC y transporte.

Para el caso colombiano, los sectores de mayor riesgo son el de transportes, el financiero y el energético, tres sectores que a lo largo de los años han sido objeto de atentados físicos por parte de las estructuras armadas ilegales. Pero, ahora bien, cabe preguntarse ¿Por qué es importante considerar el factor ciberespacio en la estrategia nacional de defensa y seguridad? Cómo se ha mencionado, la dinámica las amenazas tiende evolucionar frente al contexto social y a contemplar otras capacidades para la conducción de sus hostilidades, es por ello que, pese a que las amenazas tradicionales no han empleado el ciberespacio como un medio para atentar contra los intereses del Estado, no se puede negar la probabilidad de que este medio sea un modo para el desarrollo de las operaciones, especialmente para el planeamiento de las estrategias subversivas. En consecuencia, el estado debe estar preparado para la contención de los riesgos y sus amenazas, en tanto que uno los sectores de mayor vulneración es el financiero y el de TIC.

Para Poveda Criado y Torrente Barredo (2016), los temas relacionados con la ciberdefensa no son solo los considerados como ataques terroristas, sino también debe contemplar la planeación estratégica como una herramienta terrorista. En este sentido es de señalar qué las redes sociales y el ciberterrorismo hacen parte de un fenómeno social con una alta probabilidad de generar riesgos debido a aspectos como; el bajo costo, premeditación, selectividad, anonimato, acciones que no requieren la presencialidad.

Desde esta lógica, y según indica la tendencia evolutiva de la amenaza, se puede inferir que desde el ciberespacio se comienza a catalizar la probabilidad de riesgo y peligro, pues el nivel de daño puede ser igual o mayor que el de un ataque físico a la infraestructura. Es una

medida en que cada vez más la infraestructura crítica depende de los sistemas tecnológicos para funcionar, es por ello que, de acuerdo al Instituto LISA, las tecnologías de la información y comunicación de un Estado hacen parte de esa infraestructura crítica.

Dicho lo anterior, se propone tener cuatro principales responsables para la protección de la infraestructura, estos son: los gobiernos, organizaciones competentes (en este caso los diferentes ministerios), los operadores críticos (relacionados con los cooperadores de cada una de la infraestructura) y las cuartas partes (otros actores que no necesariamente son públicos, sino que también pueden pertenecer al sector privado).

Cómo se evidencia en lo anterior, no solo los actores armados ilegales son los que convergen en el ciberespacio, también existen actores no gubernamentales qué son necesarios tenerlos en cuenta para la protección de la infraestructura crítica. En resumen, el factor de riesgo suele multiplicarse conforme al involucramiento de los distintos actores en el sistema de seguridad para la protección de la infraestructura crítica, pues la desconfianza y el desconocimiento en el manejo de la información y cumplimiento de los diferentes protocolos, también son factores de riesgo.

Factores de riesgo y amenazas

Cada vez que se profundiza en temas de Seguridad y Defensa a nivel internacional, se evidencia un reiterado cambio de perspectiva frente al enemigo, un ciclo que parece ser evolutivo y se condiciona en función de las dinámicas coyunturales que proporciona el escenario y la lucha de los sujetos-actores en los diferentes Campos de Acción (económico, político, social y militar). No obstante, cada vez que se identifica un llamado “enemigo”, el sistema pareciese transformarse bajo un discurso. Esto evidencia no solo la importancia del poder de facto o coercitivo del empleo y uso de la Fuerza, sino a factores inmateriales como la

gestión de la información y del conocimiento haciendo recordar la frase de Winston Churchill la cual reza “La historia la escriben los vencedores” (Churchill, 1945).

Así las cosas, el fenómeno de la globalización, además de dinamizar las prácticas económicas y comerciales, transformó formas de relación social que son guiadas por actores preponderantes internacionales que influencian por diferentes medios (mercado, diplomacia, política, etc) transforman las realidades sociales. Esto ha generado que nuevas amenazas emerjan del escenario digital y, sobre todo, vulneren la estabilidad de la seguridad y defensa desde el escenario ciberespacial.

Cuando se refiere a factor, entendido como la variable que puede descomponer o influenciar en la estabilidad, orden y seguridad, se pueden identificar múltiples amenazas que tienen un nivel de peligrosidad. En el marco de la ciberdefensa, es importante identificar los factores (amenazas que generan riesgos y peligros) en los diferentes campos de acción del Estado; económico, social, cultural, político. Según Ardila (2018), los factores de amenazas pueden registrarse desde diferentes dimensiones, pero lo más importante, es contener el nivel e impacto sobre el ecosistema de seguridad. Es así que un factor no solo condensa a la misma amenaza, sino también sus efectos, de allí es importante la inteligencia para comprender el nivel de riesgo y peligro.

Lo anterior, hace creer que a pesar de vivir en un mundo cada vez más globalizado y democrático, los Estados siguen enmarcados en el paradigma realista estructuralista del poder, lo cual implica que el Estado sigue manteniendo un papel importante en el sistema internacional e influencia de esta manera a los demás actores del sistema bajo sus intereses. No obstante, otros actores institucionales y asimétricos amenazan cada vez más su autoridad. Por ejemplo, las prácticas criminales como el narcotráfico y su cadena evolutiva que inicia desde el cultivo de coca hasta el tráfico y microtráfico son prácticas cada vez más socialmente aceptadas. Asimismo, se suma el hecho de la importancia de los medios de comunicación en

un escenario de dominio (ciberespacio) difícil de regular que, a manos de actores del crimen organizado y terroristas, resulta un medio desestabilización (Ardilla, 2018).

Son múltiples los factores de riesgos que pueden dañar o impactar sobre los intereses vitales y estratégicos del Estado, y con ello existe también fuentes de peligro que se pueden desprender de las amenazas. Es decir, por cada fuente de amenaza existe una probabilidad (riesgo) de que pueda ocurrir una contingencia. Tomando como referente el Plan Nacional de Protección de las Infraestructuras Críticas de España se pueden determinar diferentes fuentes de amenaza, estas son:

1. El terrorismo, una de las dimensiones más amplias provenientes de las amenazas de carácter asimétrico, donde convergen una intención política y unas capacidades armadas. Para el caso colombiano, este factor es una de las principales fuentes de amenaza y también presenta un alto nivel de riesgo para la infraestructura crítica, debido a que los actores armados emplean diferentes medios para desestabilizar la seguridad y el orden del Estado, por ello, la mejor forma de hacerlo es impactando contra industrias vitales y esenciales para el Estado como el energético, el de seguridad (sistema de defensa y seguridad) y el financiero. Al respecto se cita_

> [...] el ciberatacante se siente seguro, ya que no se expone físicamente a su víctima ni mucho menos a la posible intervención de las fuerzas de seguridad, dado que su acción delictiva se realiza a distancia; sensación de cómoda impunidad, al saber que hay lagunas legislativas a nivel internacional, por lo que muchos de los delitos cometidos no se castigan. Además, el delincuente aprovecha el anonimato de sus ciberacciones al ser complicado identificar al atacante; cualquier usuario que tenga un equipo informático y conexión a internet, con unos conocimientos técnicos que están al alcance de cualquiera y con una inversión económica no elevada, puede ejecutar un ciberataque;

> cualquier ciberataque conlleva un efecto de vulnerabilidad y falta de protección individual; y por último estos ataques sacuden la opinión pública y tiene gran difusión en los medios digitales de todo el mundo. (Pons, 2017, p.4).

Teniendo en cuenta la importancia de la dimensión sistémica, es importante contemplar que existe un paralelismo entre lo legal y lo ilegal, es por ello que el uso de las nuevas tecnologías no es exclusivo de la legalidad y, en consecuencia, los criminales y actores ilegales pueden hacer uso de las nuevas tecnologías para impulsar su accionar criminal. Si bien esta capacidad puede ser adquirida por cualquier ciudadano, es importante destacar la importancia de crear un marco regulatorio para acondicionar los comportamientos desviados que tienden a afectar los intereses individuales e integrales de los individuos como una organización, que a largo plazo también repercuten en el interés nacional (Acosta, Chacón & Jiménez, 2020).

De acuerdo con Acosta, Chacón & Jiménez (2020), los estados deben trabajar en función a salvaguardar los intereses nacionales y comprender mejor el entorno que los rodea, pues en el planeamiento estratégico los riesgos a que la estrategia puedan fallar son una condicionante para la eficiencia y eficacia de las políticas públicas. En este orden de ideas la principal amenaza que enfrenta Colombia y que puede aumentar su accionar criminal en función a la implementación de las nuevas tecnologías son los Grupos Armados Organizados y los Grupos Delincuenciales Organizados, estatus amenazas emergentes cada vez hacen uso de las nuevas tecnologías de la comunicación y la información debido a que la complejidad de los mercados y la oferta y demanda de servicios ilegales han crecido desde los escenarios grises caracterizados por la baja regulación (Porras, Molina, Ardila y Acosta, 2020).

Colombia se enfrenta a grandes desafíos económicos y sociales en el ámbito nacional e internacional debido a la Firma del Acuerdo Final de Paz entre el Gobierno Nacional y las Fuerzas Revolucionarias de Colombia el 24 de noviembre del año 2016. Producto del nuevo escenario de transición, también llamado escenario de pos-acuerdo, la Fuerza Pública se

convierte en la principal herramienta del Estado para ejercer y mantener el orden social a lo largo del territorio nacional. En este sentido el próximo Gobierno Nacional debe dar prioridad a la estabilización del orden público con el fin de evitar la proliferación y fortalecimiento de nuevas estructuras armadas que actualmente disputan el control territorial, bien es el caso de Los Pelusos, El Clan del Golfo, las disidencias de las Farc, ELN, etc. Por lo tanto, las fronteras terrestres se convierten en puntos estratégicos de interés nacional para el establecimiento de una agenda nacional que posibilite el control territorial periférico. Situación que convierte en vulnerable la infraestructura critica producto de posibles atentados contra la infraestructura estratégica.

Según Giral-Ramírez, Celedón-Flórez, Galvis-Restrepo y Zona-Ortiz (2017), existe una alta inversión del sector público y privado en investigación y desarrollo de proyectos energéticos en Colombia, siendo el sector eléctrico uno los propiciadores del desarrollo de la equidad social y la mitigación del impacto ambiental, de hecho es uno de los sectores con nuevos retos y necesidades que demanda un sistema integral de atención materializándose en la necesidad de fortalecer el esquema normativo y el regulatorio. De igual manera los autores resaltan la importancia de la cadena de conversión eléctrica en Colombia, pues resulta importante contemplar las tecnologías de la información y la comunicación para fortalecer el mercado energético.

Según Juan Sánchez (2012), la dinámica de la amenaza es un proceso integrado y sistemático que inicia con la categorización de la amenaza (obstáculo, antagonismo, presión y presión dominante).

Para el caso del terrorismo, no se evidencia un modelo estándar que permita identificar y categorizar a la amenaza en un nivel claro, pues el terrorismo son todas aquellas acciones realizadas por un actor asimétrico bien sea guerrilla, grupos fundamentalistas religiosos o agrupaciones armadas para sembrar el terror. Según Tania Rodríguez (2012), define al

terrorismo como “El uso del miedo como factor desestabilizador en las sociedades y su materialización [...]” (p.73). La autora clasifica el terrorismo en dos niveles; el regional-local y el global-internacional, siendo este último asociado a agrupaciones provenientes del Medio Oriente, particularmente las agrupaciones religiosos y fundamentalistas como el Estado Islámico y Al Qaeda, grupos considerados en ese nivel por Estados Unidos y la Unión Europea.

Con respecto, al nivel de amenaza, señalado por Sánchez (2012), el terrorismo a nivel mundial se caracteriza por llegar a ejercer una “presión” referenciada por cumplir con las características de interferencia, capacidad y voluntad, llegando en algunos casos a evolucionar en una “presión dominante” por cumplir con las anteriores características sumando el efecto “desestabilizador”. A lo anterior, Javier Jiménez (2015), sostiene que el terrorismo en Medio Oriente se caracteriza por mantener una capacidad desestabilizadora debido a que “[..] la violencia provoca reacciones irracionales que llevan a romper la estabilidad emocional de sociedades, gobiernos y Estados” (párrafo 30).

Por lo anteriormente planteado, en la dinámica evolutiva de la amenaza, el terrorismo internacional llega al nivel de hipótesis de conflicto y, en algunos casos, alcanza la hipótesis de guerra. Ejemplo de ello, es el caso de los atentados del 11 de septiembre, donde EE. UU declaró “la Guerra contra el Terrorismo” empleando la fuerza en Afganistán en una coalición internacional iniciada en la Organización del Tratado Atlántico Norte -OTAN-.

Por otra parte, retomando el apartado anterior frente a las dinámicas de la globalización, sostiene Jiménez (2015), que uno de los medios implementados por el terrorismo es la propaganda. En este último caso, siguiendo a Oscar Palma, se categoriza como terrorismo comercial debido a que existe una probabilidad de convergencia entre empresas criminales, actividades criminales, entidades terroristas y actividades terroristas.

Ahora bien, ¿Cómo contrarrestar el terrorismo internacional en el ciberespacio? Según Oscar Palma, no existe una normatividad internacional que establezca una política clara para

frente al terrorismo, pues las instancias jurídicas resultan débil frente a dicha problemática, por eso el único activo estratégico es el manejo de la información, especialmente en cuanto a identificar la amenaza se refiere.

Hasta la fecha, se han implementado diferentes estrategias para combatir el terrorismo por parte de los Estado que van desde la conformación y alianzas estatales e interinstitucionales, hasta las acciones militares. En el caso de las Organización de las Naciones Unidas, se conformó la Oficina de Lucha Contra el Terrorismo, la cual tiene dos pilares de acción: evitar la propagación del terrorismo y combatirlo. En este sentido se estableció un "Plan de Acción" basadas en protocolos internacionales y resoluciones aprobadas por el Consejo de Seguridad de la ONU. Estas medidas comprenden: la condena sistemática de las acciones, prevenir y combatir acciones y establecer una cooperación internacional, todas estas relacionadas y articuladas (Oficina de Lucha Contra el Terrorismo, 2006).

Lo anterior, no solo evidencia la importancia de la dependencia del sistema industrial por la demanda de la energía, sino que este sector también se ha convertido en un puente de desarrollo social y económico para el país, por lo tanto, la necesidad de la protección desde el sector de la ciberseguridad y ciberdefensa se constituye también en un factor para la reducción de riesgos y peligros.

De acuerdo con el Departamento Nacional de Planeación (2016), mediante el Conpes 3854-Política Nacional de Seguridad Digital, la seguridad digital se ha convertido también en un Pilar para la seguridad y defensa nacional, debido a que busca no solo la creación de un sistema de vigilancia y protección, sino que también comparte dos aspectos fundamentales; la defensa del país y la lucha contra el cibercrimen, al respecto se cita:

> [...] las condiciones para que las múltiples partes interesadas gestionen el riesgo de seguridad digital en sus actividades socioeconómicas y se genere confianza en el uso del entorno digital, mediante mecanismos de participación activa y

> permanente, la adecuación del marco legal y regulatorio de la materia y la capacitación para comportamientos responsables en el entorno digital. (Departamento Nacional de Planeación, 2016, p.3).

Es importante también mencionar que dicha estrategia establecida en la Política Nacional de Seguridad Digital en Colombia, busca una visión basada en la gestión de riesgos, que, de acuerdo con los diferentes ministerios, busca duplicar los esfuerzos y fortalecer la eficiencia para la contención de amenazas. Para ello, el Grupo de Respuesta a Emergencias Cibernéticas de Colombia -colCERT- (2021), es un organismo que busca coordinar a nivel nacional los aspectos de la ciberseguridad y ciberdefensa direccionadas a la protección de la infraestructura crítica frente a emergencias que atenten contra la seguridad y la defensa nacional. El fin último de este grupo consiste en fortalecer la capacidad de respuesta a incidentes.

Ahora bien, teniendo en cuenta los diferentes sectores de la industria y la presencia de Grupos Armados Organizados (GAO), son las principales fuentes de amenaza debido a que aumenta sustancialmente el nivel de probabilidad de riesgo relacionado con el empleo del terrorismo para desestabilizar. Se debe señalar que la fuente (amenaza) puede generar probabilidad de riesgos (incidentes), sin embargo, esto depende también de las condiciones de seguridad para su contención (a menor condición de seguridad, va hacer el mayor el riesgo de ocurrencia de una contingencia).

2. el crimen organizado, es una amenaza de carácter transnacional que se caracteriza por ser flexible y de difícil rastreo, es una de las principales fuentes de amenaza con gran capacidad de desestabilización en vista de que su principal objetivo es el sistema financiero, un sector que determina en gran parte la buena gobernanza del Estado. Según el Instituto LISA (2009), se tiende a silenciar cada vez más medios violentos para la estabilización, es decir, cada vez las estrategias no están relacionadas con la lucha frontal sino con una estrategia no violenta

(armada) relacionada más con la manipulación (poder inteligente-no uso de fuerza sino de otros medios). Esta categoría se caracteriza porque estos factores están relacionados con el crimen y tienden a establecer al ciberespacio como un escenario de intercambio de demanda y oferta, que posteriormente, puede verse materializado con el uso de la fuerza mediante homicidios, expresiones de violencia y delincuencia.

> [...] pueden usar las herramientas informáticas como objeto de ocasionar daños, lanzando ataques de cualquier tipo contra equipos informáticos, redes o información recogida en ellos. También, pueden ejecutar atentados a través del empleo de cualquier acción de las contempladas anteriormente contra los sistemas individuales y de redes, causando daños físicos, y por último, pueden servirse de internet para su propaganda, incitación, amenazas, hacer proselitismo, financiar sus ataques y reclutar a nuevos simpatizante (Pons, 2017, p.8).

Para Pons Gamón (2017), los ciberdelincuentes avanzan rápidamente en la aplicación de técnicas y métodos para la violación de sistemas de seguridad, de hecho, las autoridades avanzan más lentamente en la medida en que no han adoptado marcos jurídicos y normativos para la contención de un problema moderno. A esto también se le suma la falta de cuerpos de seguridad especializados para la contención de amenazas delictivas en el ciberespacio, en gran parte eso está marcado por el desconocimiento y la falta de regulación de comportamientos ilegales en ese escenario. De igual manera, para el autor es importante reconocer que la evolución del cibercrimen, las ciberamenazas y la ciberdelincuencia, hacen parte de una difícil contención de su accionar, debido a que el ciberespacio es un gran escenario de zonas grises. A lo anterior, se resalta:

> En el ámbito ciber, las respuestas por parte de autoridades nacionales e internacionales han sido dispares, teniendo especial protagonismo las políticas antiterroristas –infiltración y monitorización, por parte de los servicios de inteligencia, de actividades y comunicaciones con objeto de prevenir acciones terroristas y recabar pruebas que puedan ser empleadas judicialmente– y contraterroristas, mediante la creación de mandos especializados [...] (Poveda y Torrente, 2016, p. 517).

En esta medida se reconoce que uno de los factores de mayor riesgo sigue siendo el sector financiero, consecuentemente seguido del sector relacionado con las TIC, debido a que existe un alto índice de amenazas en materia de ecuación de la información en zonas de alto nivel de producción financiera. Según la Agencia Europea para la Seguridad de las Redes de la Información (ENISA), las amenazas provenientes del ciberespacio se materializan en malware, spam, robos, fraudes, fuga de información y ciberespionaje, entre otros. Por ejemplo, un alto nivel de peligro es la negación de servicio también conocido (DDos), el cual consiste en contener a los usuarios acceder a recursos y servicios de una organización con el fin de solicitar un rescate.

3. Espionaje, es una las prácticas empleadas por actores simétricos o empresas extranjeras que viola la ciberdefensa de un Estado. Esta práctica suele ser común en empresas que emplean la inteligencia como una práctica competitiva. Esta práctica es empleada para afectar los intereses geopolíticos entre Estados y también representa una de los cíberriesgos y ciberamenazas que pueden prevenirse con el fortalecimiento de protocolos de seguridad de la información. En este caso, los sectores más afectados son el sistema de telecomunicaciones e información y también el sistema de defensa nacional. Así mismo, esta práctica tiende a desestabilizar no solo el sistema de infraestructura crítica, sino también generar un impacto en las operaciones gubernamentales.

Finalmente, *causas naturales*, estas son las fuentes de amenaza que tienden a ser imprevisibles, esto comprende considerar también a las fuentes de riesgo y peligros relacionadas con el contexto físico natural (medio ambiente-desastres naturales). Sí bien no hace parte propiamente de un problema de seguridad y defensa, un daño a gran escala (incidente ambiental-desastre) puede impedir el funcionamiento de los sistemas vitales para el Estado y con ello es importante considerar este factor de amenaza dentro de la política de seguridad y defensa, según lo plantea el Instituto LISA. Por ello, cualquier impacto material provocado por el hombre o la naturaleza debe ser objeto de la comprensión de las políticas públicas.

Amenazas a la infraestructura crítica económica

Teniendo en cuenta lo anteriormente mencionado, se pueden identificar tres factores fuentes de amenaza a la infraestructura crítica que pueden provenir del ciberespacio y que pueden afectar los intereses nacionales en Colombia. 1) el terrorismo, esté relacionado por grupos de presión dominantes como los grupos armados organizados existentes en Colombia y que pueden hacer uso del ciberespacio para preparar y atentar contra la infraestructura del Estado colombiano; 2) el crimen organizado, está relacionado con los grupos de delito común que pueden ser orquestados y financiados por sectores para la desestabilización selectiva de la infraestructura crítica. En este caso, es importante señalar que es una de las fuentes de amenaza más comunes que puede variar el nivel de riesgo y peligrosidad, todavía es que depende de los actores que se encuentran detrás de las acciones; y finalmente 3) el relacionado con los ataques de amenazas externas provenientes de otros Estados rivales, aunque es una de las fuentes poco comunes, estas pueden generar un mayor impacto y por tanto representar un nivel alto de riesgo debido a que los estados tienden a tener todas las capacidades de inteligencia y recurrir a recursos tecnológicos para generar ataques más contundentes hacia la infraestructura. Se debe señalar que los peligros no solo pueden prevenir de procesos provocados por el hombre, sino

que existen variables que pueden catalizar el impacto de la amenaza como el entorno social y ambiental. Ejemplo de lo anterior, se menciona

> En el ámbito de la lucha contra el terrorismo, establece diferentes líneas de acción: actuar contra el terrorismo desde su origen (prevención); disminuir nuestras vulnerabilidades (protección); hacer frente a la actividad terrorista (persecución); y preparar la respuesta para restablecer la normalidad (resiliencia). Por otra parte, en el ámbito de la ciberseguridad, marca seis líneas de acción, que van desde el incremento de la capacidad de prevención, detección, investigación y respuesta ante las ciberamenazas, hasta la intensificación de la colaboración internacional. (Pons, 2017, p.3).

En esta medida, y teniendo en cuenta el nivel de riesgo de peligro y las fuentes de amenaza, se pueden determinar cuatro sectores importantes a tener en cuenta para el establecimiento de marcos normativos y protocolos de seguridad de la información en el ciberespacio. Lo anterior, teniendo como ejemplo los marcos y experiencias internacionales, por lo tanto, se evidencia que estos son los más atacados desde el ciberespacio; 1 *el sector energético*, debido a que proporciona la mayor parte del funcionamiento de los demás sectores, es decir, el factor energético transversal actual infraestructura crítica mencionada en el primer capítulo; 2 *el sector de la seguridad*, al igual que la anterior este resulta también transversal en materia de protección puedes concentra dos ejes estratégicos la defensa nacional y la seguridad nacional. Adicionalmente es importante considerar este sector como uno de los pilares a fortalecer en las políticas de ciberseguridad y ciberdefensa, pues la mayor parte de la lucha y contención de las amenazas consiste en el fortalecimiento de este sector. 3. *Las telecomunicaciones y los sistemas de información*, es también considerado uno de los pilares

para el desarrollo tecnológico y el manejo de la seguridad de la información, debido a que la mayor parte de la digitalización de los procesos industriales y administrativos de un estado descansa en estos ministerios. 4) *sistemas de transporte*, en el caso colombiano este también ha sido uno de los más vulnerables debido a que mayor parte de la infraestructura industrial se ve representado en el mantenimiento de la cadena logística, y con ello, es importante no sólo acondicionar el sistema de carreteras y redes de transporte terrestres sino también las marítimas, esto implica la actualización de las capacidades tecnológicas y digitales y también se ve representado en un mayor riesgo para que se vean materializados los peligros.

> [...] las autoridades mundiales encargadas de defender y aplicar leyes enciendan motores, para evitar y perseguir este tipo de delitos. Analizando los alcances e implicaciones de los medios informáticos en acciones delictivas, podemos hacer un recorrido por la definición de ciberterrorismo, partiendo que "delito informático o ciberdelincuencia, es toda aquella acción ilegal que se da por las vías informáticas o que tiene como objetivo destruir y dañar ordenadores, medios electrónicos y redes de internet" (Urueña Centeno 2015, 2). Muchos de esos delitos, aún no están tipificados como tales en la ley y se definen actualmente como abusos informáticos. La forma más destructiva de ciberdelincuencia es el ciberterrorismo donde convergen el ciberespacio y el terrorismo, por lo que esta forma de acción utiliza las tecnologías de la información para conseguir sus fines, intimidando, atemorizando y causando daño a sus víctimas. Actualmente, para la preparación y ejecución de casi la totalidad de acciones terroristas están apoyadas cibernéticamente o utilizan en algún momento medios cibernéticos en su realización bien para comunicación o acción. [...] (Pons, 2017, p.7).

En consecuencia, todos los sectores de la infraestructura crítica tienen un nivel de riesgos y peligros que amerita ser contemplados a la luz de las necesidades y capacidades con que cuentan estos, para ello es importante considerar una evaluación de las capacidades tecnológicas que tiene el estado y los diferentes ministerios para la contención de las ciberamenazas. Es así que teniendo en cuenta el ejemplo del caso de España, es importante también considerar la generación de protocolos transversales direccionados a la contención de las amenazas e identificación de las diferentes fuentes, un aspecto que es necesario y amerita ser evaluados en las diferentes políticas sectoriales que emplea el país, pues hace falta reconocer la red de infraestructura crítica identificar los factores y riesgos de inestabilidad para la adquisición de capacidades tecnológicas.

Son dos aspectos que se deben solucionar en la frontera; la ocupación del territorio y la estabilización del orden público. Por lo tanto, Colombia debe establecer una estrategia de contención del crimen organizado producto de la migración ilegal sobre el territorio nacional. La estrategia debe establecer una ley de seguridad y defensa nacionales, acuerdos de corporación entre las Fuerzas de Seguridad bilaterales en materia de ciberdefensa. Reconociendo el escenario estratégico derivado del Acuerdo Final de paz, Colombia debe establecer una ley de seguridad y defensa nacionales para evitar la proliferación de actores armados y establecer un control normativo para el ciberespacio, debido a que se contempla como un escenario alto de riesgo y peligro.

Dicha normativa de ciberdefensa debe estar respaldada por acuerdos de cooperación bilateral, en tanto que el problema del ciberespacio es una responsabilidad de Estados. Por lo tanto, un acuerdo de cooperación operacional y de intercambio de información (inteligencia) representaría una herramienta efectiva para la lucha contra estructuras criminales y, de esta manera, evitar la convergencia entre actores ilegales.

Para finalizar, Colombia se enfrenta a un escenario estratégico debido a que las decisiones políticas que se tomen por el próximo gobierno nacional sin importar la posición en contra o a favor de los acuerdos de paz, debe estar articulada al mantenimiento y consolidación del orden público mediante el empleo de las Fuerzas Militares, quienes deben seguir apoyando a la Policía Nacional en materia de orden público desde el ciberespacio, pues la debilidad del Estado sigue siendo la falta del ejercicio de un poder de facto sobre sus dominios, especialmente el quinto dominio.

CAPÍTULO IV Lineamientos estratégicos en el Comando de Apoyo Operacional de Comunicaciones del Ejercito Nacional de Colombia para la protección de la infraestructura critica

Teniendo en cuenta la infraestructura crítica y las amenazas que esta enfrenta a nuevas amenazas provenientes del ciberespacio, identificadas en el capítulo anterior, se propondrán cuatro lineamientos estratégicos que pueden guiar al Comando de Apoyo Operacional de Comunicaciones y Ciberdefensa del Ejército Nacional de Colombia (CAOCC) en la ejecución de sus funciones. Lo anterior, con base en las capacidades que están contenidas en la TOE del CAOCC, así como en la directiva permanente No. 000201 del 2017 Lineamientos de Ciberseguridad y Ciberdefensa para el Ejército Nacional y a su vez con lineamientos estratégicos propuestos en otros países latinoamericanos, ajustándose así a los recursos locales y a su vez a las necesidades en la región. Especialmente en el camino esbozado por Chiza e Izureta (2020), relacionado a la prevención, detección, protección y recuperación.

El primer lineamiento estratégico se construye sobre el pilar de la prevención, y sobre las capacidades del CAOCC referentes a la realización de un esfuerzo operacional que permitan la visualización, entendimiento, descripción, conocimiento y conciencia de las situaciones que amenacen o sean potenciales amenazas. Se propone entonces la cooperación entre dependencias homólogas de las Fuerzas Militares colombianas, en materia de educación y enseñanza sobre ciberseguridad y ciberdefensa, las amenazas identificadas y los roles que cada una de las instituciones podría cumplir. Esto, con el fin de consolidar unas bases comunes y un lenguaje que permita prevenir las amenazas a la infraestructura crítica. Las políticas de prevención dan la posibilidad de dar un camino de acción que permita disminuir ataques a la infraestructura crítica ya mencionada. Esto no sólo sería positivo en materia de recursos, sino también en el fortalecimiento de la ciberseguridad, encabezada por la Policía Nacional, y la ciberdefensa, encabezada por las Fuerzas Militares de Colombia. Las políticas de prevención

relacionadas a otros aspectos de la seguridad han sido altamente importantes para combatir la criminalidad (Quintero Cordero, 2020). En el caso del CAOCC, sus capacidades y experiencia en materia operacional y comunicacional, posibilitan que sea parte de la construcción de dichas políticas, con el aporte de información relevante. Así, este primer lineamiento apunta a la consolidación de un rol estratégico activo, que le permita al CAOCC ser parte de la creación de políticas preventivas relativas a la ciberseguridad y la ciberdefensa, en pro de la protección de infraestructura crítica. Los aportes del CAOCC podrían ser en materia de experiencias adquiridas, capacidades actuales y necesarias a futuro, y posibilidad de trabajo conjunto entre FF.MM.

El segundo lineamiento estratégico orientado a la detección y la capacidad del CAOCC relacionada con el uso de tecnologías modernas y el desarrollo tecnológico. En este sentido, se recomienda fijar una mirada estratégica en dos sentidos. El primer, en cuanto al desarrollo de tecnología local, la cual se convierte en una ventaja para los países (Espitia, Agudelo & Buitrago, 2020), esto podría dar paso a la consolidación de tecnología militar colombiana que permita realizar detecciones tempranas sobre riesgos y amenazas que estén afectado a la infraestructura crítica del país. Esto no sólo representaría una acción positiva a nivel interno, ya que se desarrollaría a partir de las capacidades y necesidades propias, sino que también posicionaría al país como desarrollador de tecnología de esta índole. Segundo, la detección de ataques o amenazas, desde el uso de la tecnología tanto disponible como propia, significaría la identificación temprana de este tipo de afectaciones, lo cual traería consecuencias positivas en materia de garantías de seguridad. En cabeza del CCOCI se viene consolidando estrategias que reúnen a las dependencias homólogas de las FF.MM y a otros actores como el sector privado, con el fin de la consolidación de la propuesta de desarrollo tecnológico propio. Este eje de detección, se presenta como una oportunidad importante, ya que una de las necesidades principales que supone el ciberespacio es la necesidad de constantes monitoreos (Candau,

2019). Esto, también permitiría al CAOCC lograr alcanzar su misión de apoyar activamente, al Ejército Nacional de Colombia, en operaciones de Comando, Control, Comunicaciones, Computación y Ciberdefensa.

El tercer lineamiento estratégico se encuentra sobre la línea de la protección, el cual también se relaciona con la capacidad del CAOCC de proveer información y desarrollo tecnológico para operaciones. Esto incluye desde la protección de datos hasta la protección de la navegación en el ciberespacio, lo cual permitiría consolidar planes estratégicos que disminuyan las posibilidades de vulneración (Páez, 2020). En el tema específico de la infraestructura crítica, Morán (2019) explica que la protección desde el ámbito de la ciberseguridad y ciberdefensa se deben dar desde una consolidación de herramientas, leyes, políticas y conceptos relativos a la seguridad y la amenazas, lo cual permitirá consolidar estrategias que afronten las posibles vulneraciones. En ese sentido, el CAOCC se identifica como un espacio ideal para la concepción de operaciones desde la mirada de la protección, ya que las capacidades de esta unidad se enfocan en garantizar el máximo apoyo operacional en materia de cibernética.

Figura 3

Operaciones cibernéticas

Fuente: Elaboración propia con referencia a partir del Manual FF.MM. 3-38

De hecho, uno de los roles estratégicos que se identifica para el CAOCC se relaciona a la propuesta de Páez (2020), la cual se centra en entender que "la protección de las infraestructuras críticas pretende la ejecución de una evaluación de riesgos cuyo objetivo final sea restablecer acciones a realizar o que componentes y medidas deben ser adoptadas para minorar el riesgo que ha de afrontarse" (p. 27). Sobre lo anterior, el CAOCC posee la ventaja de haber realizado un trabajo continuo sobre la identificación de infraestructura crítica y amenazas, fortalecido también en el mismo trabajo. En ese sentido, dicha identificación da luces sobre qué se debe proteger y cuáles son los grados de prioridad.

El cuarto lineamiento estratégico se basa en la recuperación y es probablemente uno de los más importantes, este se relaciona con la capacidad del CAOCC relativa a la integración de

capacidades que permitan ejercer de forma eficaz los elementos y funciones de conducción de la guerra. Según Aguirre (2017) la recuperación en materia de ciberseguridad significa:

> Desarrollar e implementar apropiadas actividades para mantener los planes de resiliencia y restaurar las capacidades o servicios que se vieron afectados debido a un evento de ciberseguridad. La categoría recuperar soporta la recuperación oportuna a las operaciones normales para reducir el impacto de un evento de ciberseguridad (p. 63).

Para Vargas, Recalde y Reyes (2017), la ciberdefensa se ha convertido en una prioridad en las agencias gubernamentales debido a la proliferación de ataques terroristas en Francia, esto generó una creciente militarización del territorio y, consecuentemente, contener de manera coordinada los atentados mediante la distribución de la propaganda. Es importante considerar la responsabilidad que tiene el Estado para salvaguardar la seguridad y defensa desde diferentes escenarios, puntualizando que uno de los escenarios importantes empleado por los actores terroristas en donde se genera mayor probabilidad de riesgo, peligro y daño, es el ciberespacio.

La cultura estratégica juega un rol importante en el diseño de la estrategia a nivel general y operativo, hecho por el cual es importante resaltar la importancia de la eficiencia de la administración pública y el diseño de políticas que sean contundentes a resolver un problema socialmente relevante para la seguridad y defensa nacional. En este sentido, el componente humano juega un papel importante para la construcción de políticas públicas en el sector defensa, reconociendo también importancia de que este mismo pueda fortalecer la comprensión de los nuevos escenarios relacionados con las amenazas emergentes del quinto dominio (Ardila, Jiménez & Acosta, 2018).

Es así que el *factor humano* representa un catalizador para potencializar la eficiencia la gestión administrativa de la defensa, especialmente es relevante señalar la importancia de que el personal que compone el análisis prospectivo de los escenarios futuros en la era digital este

capacitado en función al desarrollo e implementación de nuevas tecnologías. La ciberdefensa debe ser un pilar fundamental en la planeación estratégica, pues como se ha señalado anteriormente resulta transversal a las diferentes áreas del conocimiento y también de los dominios del Estado.

Con lo que se busca es aportar no solo la adquisición de capacidades, la implementación y uso de estas nuevas tecnologías de la comunicación e información, se trata de ampliar el panorama de análisis y comprensión sobre el contexto social que enfrenta hoy por hoy los Estados, y que hasta la fecha ningún Estado ha logrado consolidar un dominio permanente, eficiente y contundente contra las amenazas.

Abordando desde el caso colombiano, el estado enfrenta grandes retos en materia de desarrollo tecnológico y fortalecimiento de las capacidades existentes, necesidades que deben ser entendidas de manera sistémica pues las tecnologías y la información son parte fundamental de todas las armas y todas las fuerzas que componen el Estado (Ardila, Jiménez & Acosta, 2018). Desde un enfoque multidimensional, el poder nacional también radica en la importancia de comprender de manera integral las herramientas con que cuenta el Estado y cómo se han aplicado futuro, además de que estás no deben ser comprendidas desde un escenario de confrontación abierta entre Estados, sino en función a las nuevas amenazas que suelen sugerir son irregulares.

En este orden de ideas se resalta la interdependencia entre la estructura del estado y la seguridad nacional en el ciberespacio, es por ello que la agenda en función a la ciberdefensa direccionada a contemplar aspectos importantes como los intereses geopolíticos, la geoestrategia y, sobre todo, el desarrollo de tecnologías de la información y comunicación. Por lo tanto, el ciberespacio se convierte en un quinto dominio multidimensional que impacta en las relaciones del ser humano.

Uno de los aspectos importantes para consolidar la ciberdefensa en la agenda de seguridad nacional es que en el año 2020 cerca del 60% de la población tiene acceso a internet, esto representa un crecimiento de la economía mundial cerca del 10% del Producto Interno Bruto a nivel mundial, de acuerdo a Klimburg (2012, citado por Vargas, Recalde y Reyes (2017). Esto quiere decir que el crecimiento del uso de nuevas tecnologías ha generado una dependencia de la humanidad por el empleo pelo digital en todos los campos de acción del ser humano, al mismo tiempo ha generado una alta vulnerabilidad de ataques que pueden afectar el interés de un individuo o una organización. Al respecto se cita:

> [...] los Estados, organizaciones regionales y órganos de seguridad y defensa, han empezado a realizar un cambio en su estrategia con el fin de lograr enfrentar las amenazas en el ciberespacio o al menos disminuir su impacto. Los ejemplos de acciones en cada país son innumerables, entre los que podemos citar: (1) Alemania, con el lanzamiento de su Estrategia de Seguridad Cibernética, la creación de su Centro Nacional de Ciberdefensa y la publicación de su Plan Nacional para la protección de Infraestructuras de información (NPIIP) en el 2011 (Acosta 2009); (2) España, que ha creado un Centro y un Plan Nacional de Protección de las Infraestructuras Críticas en el 2011 y también un Mando Conjunto de Ciberdefensa en el 2013 (Acosta 2009); y (3) Francia, que ha creado una Agencia de Seguridad para las Redes e Información (ANSSI) y una Estrategia de Defensa y Seguridad de los Sistemas de información en el 2011 (Acosta 2009). Algunos países en Latinoamérica no han sido la excepción, pues han realizado esfuerzos para aportar a su estrategia en ciberdefensa y ciberseguridad. (Vargas, Recalde y Reyes, 2017, p.7).

Esto implica la necesidad de una estrategia de reacción que permita enfrentar de manera efectiva y eficaz cualquier vulneración hacia la estructura crítica. En materia de ciberseguridad

y ciberdefensa el ambiente es altamente inestable y la tecnología avanza en grandes proporciones y en tiempos cortos. Es por esto que los ataques, a pesar de preparación preexistente, pueden suceder. Sin embargo, el eje de la recuperación da la posibilidad de ampliar el panorama sobre las necesidades y capacidades que debe tener el CAOCC y que puede aportar en materia de operaciones de recuperación de infraestructura crítica cibernética.

Figura 4

Lineamientos estratégicos

Fuente: Elaboración propia.

¿Por qué lineamientos estratégicos sobre los pilares de prevención, detección, protección y recuperación?

Teniendo en cuenta la misión específica del CAOCC, su rol dentro del organigrama del Ejército Nacional de Colombia y sus capacidades, se identificó la necesidad de concebir

recomendaciones direccionadas a lineamientos estratégicos desde cuatro niveles. Esto, principalmente, por dos razones: en primer lugar, estos pilares permitirán consolidar una planeación organizada, que permita asignar roles claros para combatir las amenazas que enfrenta la infraestructura crítica en el país; en segundo lugar, estos pilares aportan flexibilidad a la construcción de estrategias, ya que el CAOCC puede, con el paso del tiempo tener nuevas capacidades, lo cual permitiría tener unas bases dinámicas que se adapten tanto a transformaciones dentro del CAOCC, como al contexto que es altamente cambiante.

En este sentido, la propuesta de lineamientos estratégicos sobre los cuatro pilares mencionados se evidencia también en la revisión de literatura sobre políticas de ciberseguridad y ciberdefensa.

Para Rodríguez (2016), la ciberdefensa se ha consolidado en el ámbito de las relaciones internacionales y el derecho internacional con una contundente controversia, esta última relacionada con la falta de capacidad del Estado para contrarrestar las amenazas provenientes del ciberespacio. Para ello este autor indaga sobre la importancia de contemplar los medios y métodos no particulares que deben ser empleados en ciberoperaciones, estos deben estar acondicionados a las capacidades propias que tienen las fuerzas de seguridad y también en función a las amenazas. Por lo tanto, sin plantear las estrategias y, sobre todo, contemplar la transformación de Marcos regulatorios a nivel internacional y nacional referente al acceso y uso de las nuevas tecnologías, pues actualmente muchas de las personas son vulnerables con el simple hecho de la emplear teléfonos móviles, computadoras en cualquier otro dispositivo digital que les permita acceder a la red. Como resulta hiriente los expertos hablan de la importancia de la permanente actualización de las capacidades en ciberdefensa.

Adicionalmente, se debe contemplar que además de la vulnerabilidad de los sistemas informáticos y también el obstáculo en función a la adquisición de capacidades (no todos los estados tienen el mismo presupuesto para actualizar y adquirir capacidades tecnológicas

avanzadas), resulta también importante considerar las nuevas amenazas provenientes del ciberespacio, particularmente los relacionados con el ciberterrorismo que amenaza la seguridad interna de un estado da la manipulación hostil que se da mediante la comunicación en las diferentes redes sociales y, por otra parte, el empleo del ciberespacio por actores ilegales para el desarrollo de hostilidades en el marco de la ciberguerra. En ambos casos no se tiene claridad frente a la identificación y fuente de la amenaza, toda vez de que no sólo los actores irregulares hacen el empleo de sus dispositivos digitales, sino también los Estados que emplean a terceros para el desarrollo de operaciones que atenten contra los intereses nacionales de un Estado, es decir, la amenaza desde el ciberespacio resulta compleja en identificar, contener, contrarrestar o judicializar.

Dicho lo anterior es importante considerar la confluencia de marcos normativos en la comunidad internacional para proteger a las personas frente al mal uso de las nuevas tecnologías. En esta corriente se hace precisión de la importancia del acceso a infraestructuras críticas, debido a que estas pueden ser vulnerables a las amenazas y causar un alto daño e impacto sobre la seguridad a nivel multidimensional. Por lo tanto, el principal responsable de la seguridad y defensa de las amenazas provenientes del ciberespacio es el Estado y, con ellos, es importante brindar responsabilidades al sector privado.

> [...] la seguridad en estos términos implicaría que valorar aspectos como la seguridad en las comunicaciones no está directamente vinculada con un acto de guerra. Para la postura que entiende que Internet se constituye en una amenaza cierta y muy relevante a la seguridad internacional no se puede minusvalorar la seguridad en las comunicaciones. De hecho, otro de los aspectos centrales de la seguridad puede denominarse como cívico-política. La seguridad de las comunicaciones de individuos y estados está más en entredicho que nunca antes. [...] (Rodríguez, 2017, p.7)

Joyanes (2017) explica que esta mirada es una oportunidad para la cooperación entre el sector privado y el público, lo cual en el caso colombiano resulta pertinente ya que existe una estrecha relación entre el sector público y privado de las tecnologías de defensa. En ese sentido, si se consolidan estrategias de prevención, detección, protección y recuperación, se pueden construir lenguajes comunes entre los dos sectores mencionados, y así fortalecer los recursos tanto materiales como humanos para afrontar las amenazas a la infraestructura crítica colombiana. Este proceso incluiría la participación del CAOCC como una unidad articuladora de las estrategias. Dentro de esta propuesta, también se reconocen los avances que el sector privado ha realizado en el ámbito de la ciberseguridad, debido al uso sofisticado de tecnologías y, a su vez, de consolidación de fines claros al proceder en su accionar. Joyanes (2017) habla sobre el denominado Decálogo de Ciberseguridad, el cual tiene diez pilares:

1. Analizar los riesgos. 2. Los responsables de seguridad. 3. Seguridad en el proyecto de trabajo. 4. La protección de la información. 5. Movilidad con seguridad. 6. Protección antimalware. 7. Actualización y parcheo. 8. La seguridad de la red. 9. Monitorización. 10. Seguridad gestionada (p. 36).

Estos pilares permiten evidenciar que existe una preocupación desde los cuatro ámbitos que sirven como guía para los lineamientos estratégicos del presente trabajo, sin embargo, es importante agregarle un pilar más que amerita ser tenido en cuenta a la propuesta que adelanta Joyanes enfocado al factor humano, el cual se catalogaría como el undécimo, teniendo en cuenta el papel que juega la capacitación de los hombres que aplicaría la propuesta de la matriz. A lo largo de los diez ítems se pueden ver la prevención, la detección, la protección y la recuperación como constantes. Dicho esto, se fortalece la necesidad de crear una mirada hacia los avances realizados en otros sectores en referencia a la ciberseguridad y ciberdefensa. Esto también ha traído consigo no solamente la creación de lineamientos generales, sino también de

manuales específicos que traen procedimientos para alguna de las etapas, por ejemplo, Ayala (2016) consolidó el paso a paso para la recuperación de infraestructura que ha sido atacada. Al tener este tipo de guías, se hace evidente la importancia de crear lineamientos estratégicos que van de la mano con procesos similares en otros países y sectores, ya que la ciberseguridad es un ámbito que requiere cooperación y que tiene un componente altamente transnacional.

Tabla 2.

Matriz evaluativa

No.	Pilar	MATRIZ EVALUATIVA IDENTIFICACIÓN ICCN			
		PREVENCIÓN	DETECCIÓN	PROTECCIÓN	RECUPERACIÓN
		(0-5)	(0-5)	(0-5)	(0-5)
1	Análisis de riesgos				
2	Responsable de seguridad				
3	Seguridad Proyecto				
4	Protección de la información				
5	Movilidad con seguridad				
6	Protección antimalware				
7	Actualización y parcheo				
8	Seguridad de la red				
9	Monitorización				
10	Seguridad gestionada				
11	Factor humano				
TOTAL					

Fuente: Elaboración propia.

Teniendo en cuenta lo anterior, Sánchez (2018) realiza una revisión de las capacidades y políticas del Ministerio del Interior de España para la protección de infraestructura crítica en relación a ataques cibernéticos. Dentro de este análisis, el autor trae a colación la existencia de herramientas sobre los cuatro pilares que adopta la propuesta direccionada al CAOCC, y así mismo, explica la necesidad de "potenciar los instrumentos que tiene el Estado con el fin de mejorar la prevención, detección, reacción, análisis, recuperación, respuesta, investigación y coordinación ante este tipo de incidentes, configurados como una parte de la amenaza asimétrica que debemos contrarrestar" (Sánchez, 2018, p. 83). Esta mirada presenta otro ejemplo del uso de las categorías propuestas para la construcción de los lineamientos estratégicos para el CAOCC en el Ejército Nacional. Este análisis en particular esboza un

elemento que resulta importante para el contexto colombiano, ya que menciona que las capacidades se deben fortalecer a partir de instrumentos estatales, los cuales pueden consolidarse a través de dependencias que tengan definidos lineamientos estratégicos concisos y que respondan a la misma lógica de la cadena de prevención, detección, protección y recuperación. Lo cual, si es adoptado por el CAOCC, podría representar una ventaja significativa para la ocupación de un rol de liderazgo al momento de enfrentar amenazas cibernéticas a la infraestructura crítica de Colombia.

Finalmente, Sánchez (2018) también explica que este modelo de prevención, detección protección, y recuperación, no sólo ayuda a la consolidación de políticas y cuerpos normativos que ayuden a la ciberseguridad de un país, sino también a la creación y fortalecimiento de capacidades de dependencias específicas que ya estén a cargo de temas relacionados con ciberseguridad e infraestructuras críticas. Esto, resulta pertinente para los fines de este trabajo, teniendo en cuenta que los lineamientos estratégicos del CAOCC que se proponen acá, buscan aportar desde las capacidades que están contempladas en las capacidades de esta dependencia. Lo cual apunta no a crear nuevas capacidades, sino a robustecer las ya existentes. Esto significa que, este modelo de los cuatro pilares aporta de manera específica al CAOCC en sus funciones referentes a la gestión de la ciberseguridad y ciberdefensa en el ejercicio de sus capacidades en cuanto a los ataques cibernéticos, ampliando la visión de la protección hacia los caminos de la prevención, detección y recuperación también. Representando así la posibilidad de un desarrollo mayor de las capacidades del CAOCC, en relación tanto a la tecnología como a los recursos humanos.

Conclusiones

La revisión teórica y conceptual desde la perspectiva de la teoría general de sistemas permitió crear una mirada particular en la importancia de la ciberseguridad enfocada en la infraestructura crítica de los países. Esta mirada aporta al entendimiento de concebir a la infraestructura crítica como un sistema integral y no desde la división de ámbitos como el económico y/o social, esto permite dar un primer paso hacia la construcción de acciones relativas a la ciberseguridad que entiendan la complejidad de los sistemas que conforman las infraestructuras críticas en Colombia. Esta complejidad se ve altamente influenciada por las nuevas tecnologías, que, si bien representan enormes ventajas en el manejo y funcionamiento de dicha infraestructura, también crean vulnerabilidades en el ciberespacio, que pueden conllevar a afectaciones mayores en los sistemas. En ese sentido, identificar la importancia de hablar desde los sistemas en el ciberespacio, da la oportunidad de ampliar la mirada de la gestión de ciberataques, y considerar la importancia de la creación de estrategias de ciberseguridad que contemplen los sistemas en su totalidad y no parcialmente. Especialmente, en el mundo actual donde los sistemas de infraestructura crítica, que son altamente vulnerables a ciberataques, sostienen necesidades básicas que, de ser afectadas, pueden influir en la seguridad alimentaria, sanitaria, y nacional, lo cual puede concebirse desde la llamada seguridad multidimensional. Dicho esto, esta primera aproximación teórica permitió identificar cuatro características -el ambiente, el atributo, la cibernética, y la complejidad- que fueron útiles al momento de identificar la infraestructura crítica del país y las amenazas que enfrenta.

La identificación de la infraestructura crítica del país y las amenazas que esta enfrenta, se observa que a partir de lo esbozado en el marco conceptual y teórico. Esto permitió que, la infraestructura en mención, se expusiera desde la mirada de los sistemas y la complejidad del mundo ciber en el que está inmersa. En este caso se explicó que la infraestructura crítica es

aquella que es estratégica y que aporta los servicios básicos, por lo cual cualquier afectación no solamente atenta contra la población beneficiada, sino también al Estado mismo y sus funciones; mientras que la Infraestructura Critica Cibernética Nacional es aquella que además de prestar los servicios básicos para la supervivencia del Estado, es la que concentra el uso de los medios digitales, informáticos y de comunicación que son necesarios para el desarrollo de actividades propias de la modernidad y la globalización. Esta última es inherente a las dinámicas productivas del ser humano, pues cada vez las actividades son más dependientes a los procesos digitales y tecnológicos, de allí su importancia estratégica.

En ese sentido, las principales amenazas que se encuentran son de carácter simétrico y asimétrico, las primeras tienden a ser como actores principales Estados enemigos y las segundas, grupos al margen de la ley. Lo cual explica que las acciones que, desde la ciberseguridad, pueden ser materia de amenazas, responden tanto a espionaje y sabotaje, como a otras estrategias menos comunes. Esto explica entonces cómo es necesario que se tome en cuenta el escenario dinámico de la evolución de las amenazas para así poder entender los riesgos que enfrentan las infraestructuras críticas en el país. Se concluyó que, en Colombia, las amenazas son principalmente asimétricas, ya que es altamente probable que provengan de grupos al margen de la ley que pueden ser de carácter interno como particulares o ya como colectivos al servicio de grupos armados organizados (GAO) y/o grupos delincuenciales organizado (GDO), así mismo se debe considerar grupos o gobiernos del exterior que busquen la desestabilización del orden interno, por lo cual, los factores de riesgo son complejos por los métodos utilizados por estas organizaciones criminales. Sobre esto, se expuso que en Colombia la infraestructura crítica más vulnerable es la relativa a los transportes, el financiero y el energético.

Lo anterior, permitió que, a través tanto de la mirada teórica y conceptual, como de la contextualización de la infraestructura crítica y sus amenazas en Colombia, se realizara una propuesta de lineamientos estratégicos enfocada en una de las principales unidades junto con el CCOCI que tienen a su cargo la ciberdefensa del país: el Comando de Apoyo Operacional de Comunicaciones del Ejército Nacional de Colombia. Esto se realizó con base en las capacidades mismas de esta unidad, y sobre la propuesta de crear lineamientos estratégicos que correspondieran a cuatro pilares: prevención, detección, protección y recuperación. Los cuales fueron identificados a través de políticas y estrategias de otros Estados, como España y Argentina. En ese sentido, la concepción de lineamientos a través de los cuatro pilares le permitirá al CAOCC una flexibilidad y amplitud mayor en sus capacidades, al igual que un lenguaje común para la cooperación dentro y fuera del país, ya sea tanto con el sector público como con el privado. Lo cual va de la mano, con los esbozado por la teoría de los sistemas y la particularidad de las amenazas del caso colombiano. También, le dará la posibilidad al CAOCC y al Ejército Nacional de Colombia, de crear una posición de liderazgo para la consolidación de la ciberdefensa y ciberseguridad en el país, teniendo en cuenta los avances ya realizados por dicha dependencia, pero a su vez, las posibilidades de adaptación al contexto cibernético que es altamente dinámico, y que podrán ser dadas gracias a los cuatro pilares propuestos a lo largo de este trabajo.

Finalmente, se puede concluir que la ciberseguridad y ciberdefensa en Colombia debe ser concebida desde una mirada integral, que logre responder tanto a las necesidades como las capacidades del país, no sólo en materia tecnológica, sino también de recursos humanos y entrenamiento. En ese sentido, la perspectiva desde la teoría de sistemas y su relación con el contexto colombiano, permitieron entonces aterrizar la mirada específicamente al CAOCC. Lo cual evidencia las ventajas de realizar dicho ejercicio en otro tipo de dependencias de la misma

índole en Colombia, para así afrontar las amenazas que el espacio cibernético trae consigo. En consecuencia, el presente análisis provee, en tres partes, categorías que pueden servir para la creación de un lenguaje común al momento de construir lineamientos estratégicos para afrontar las amenazas de la infraestructura crítica: en un primer momento, la concepción de la infraestructura crítica desde la teoría general de sistemas; en un segundo momento, el análisis del contexto colombiano para la identificación tanto de infraestructura crítica como de riesgos, teniendo en cuenta sus cambios en el tiempo; y, en un tercer momento, la utilización de la mirada de prevención, detección, protección y recuperación, como un esquema funcional para las dependencias a las que les atañe las responsabilidades de la ciberseguridad y ciberdefensa. Esto, buscar convertirse en una propuesta integral que permita crear unas bases, a partir de la experiencia del CAOCC, pero que a su vez respondan a las capacidades y recursos propios de cada una de los actores estatales y privados que puedan aportar en cualquiera de las etapas relativas a la prevención, detección, protección y recuperación de las amenazas a la infraestructura crítica de Colombia.

Referencias

Acosta, H., Chacón, N., & Jiménez, J. (2020). Lineamientos estratégicos para combatir los Grupos Armados Organizados en el escenario de pos-acuerdo. (En proceso de Publicación). En: Payá, C., y González, M. *La Gestión del Riesgo. La Inseguridad Jurídica y las Amenazas a la Seguridad*. (pp. 103-124). Thomson Reuters. ISBN: 978-84-1345-678-2

Acosta, Maria G., Benavides, Merck M., & García, N. (2020). Delitos informáticos: Impunidad organizacional y su complejidad en el mundo de los negocios. *Revista Venezolana de Gerencia*, 25(89),351-368. [fecha de Consulta 2 de Agosto de 2021]. ISSN: 1315-9984. https://www.redalyc.org/articulo.oa?id=29062641023

Ardila, C., Jiménez, J., & Acosta, H. (2018). Una aproximación a la Política de Seguridad y Defensa desde la cultura de seguridad y defensa nacionales (pp. 134-149). En: *Políticas Públicas y Gestión Pública en Colombia: Estudios de Caso*. Centro de Investigaciones y Altos Estudios Legislativos - CAEL. Secretaría General del Senado de La República de Colombia. ISBN Digital: 978-958-59641-8-1

Ardilla, C. (2018). *La estrategia de ciberdefensa en Colombia: una política pública en constante construcción*. Bogotá

Arnold M., y Osorio, F. (1998). Introducción a los Conceptos Básicos de la Teoría General de Sistemas. *Cinta de Moebio,* (3). https://www.redalyc.org/articulo.oa?id=10100306

Aron, R. (1895). *Paz y Guerra entre las naciones*. Madrid, España: Alianza.

Becerra, J. y León, I. (2019). *La Seguridad digital en el entorno de la Fuerza Pública, diagnósticos y amenazas desde la gestión del riesgo.* En Medina, G. La seguridad en el ciberespacio. Un desafío para Colombia. https://doi.org/10.25062/9789585216549.03

Benavides-Astudillo, E., Fuertes-Díaz, W., Y Sánchez-Gordon, S. (2020). Un experimento para crear conciencia en las personas acerca de los ataques de Ingeniería Social. *Revista Ciencia Unemi*, 13(32), PP. 27-40.

Bermúdez, E y Martínez, G. (2001). Los estudios culturales en la era del ciberespacio. Convergencia. *Revista de Ciencias Sociales*, 8(26). https://www.redalyc.org/articulo.oa?id=10502601

Bernal, C. (2016). *Metodología de la investigación*. Cuarta Edición.

Bohórquez-Keeney, A. (2019). *El impacto de la academia en la ciberseguridad.* En Medina, G. La seguridad en el ciberespacio. Un desafío para Colombia. https://doi.org/10.25062/9789585216549.03

Cabrera, F. y Bonilla, H. (Ed). (2021). *Estrategia Nacional de Ciberseguridad y Ciberdefensa -ECDCS- 2020-2030.* Ministerio de Defensa Nacional. https://doi.org/10.25062/9789585254558

Cáceres García, J. (2017) Colombia, estrategia nacional em ciberseguridad y ciberdefensa. *Airuniversity Vol. 29*(1). https://www.airuniversity.af.edu/Portals/10/ASPJ_Spanish/Journals/Volume-29_Issue-1/2017_1_09_caceres_s.pdf

Camacho, R. y Amaya, A. (S.f.). Ciberseguridad y ciberdefensa en Colombia [Trabajo de grado]. *Universidad Piloto de Colombia.* http://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/2984/Trabajo%20de%20grado.pdf?sequence=1

CCOCI. (2017). *Plan Nacional de Protección y Defensa para la Infraestructura Crítica Cibernética de Colombia.* https://bit.ly/2Q2RUuB

Ciro Gómez, A., y Correa Henao, M. (2014). Transformación estructural del Ejército colombiano. Construcción de escenarios futuros. *Revista Científica General José*

María Córdova, 12(13),19-88. ISSN: 1900-6586. https://www.redalyc.org/articulo.oa?id=476247221002

Clarke, R. & Knake, R. (2010) *Cyber War: The Next Threat to National Security and What to Do About It*. New York, Estados Unidos: Harper-Collins Publishers.

COGFM. (2018). Manual Fundamental Conjunto MFC 1.0 – Doctrina Conjunta. https://doi.org/10.25062/manual.2018

Coleman, K. (2008, enero 28) *Coleman: The Cyber Arms Race Has Begun. CSO*. http://www.csoonline.com/article/2122353/critical-infrastructure/coleman--the-cyber-arms-race-has-begun.html

Comando Conjunto Cibernético. (2016). *Manual de Ciberdefensa Conjunta para las Fuerzas Militares* (Manual FF.MM 3-38 Restringido). Bogotá D.C.

Comando Conjunto Cibernético. (2017). *Plan Nacional de Protección y Defensa para la Infraestructura Crítica Cibernética de Colombia*. Comando General de las Fuerzas Militares.

Comando Conjunto Cibernético. (2019). *Plan Nacional de Protección y Defensa para la Infraestructura Crítica Cibernética de Colombia*. Comando General de las Fuerzas Militares.

Cortés Borrero, R. (2015). Estado actual de la política pública de ciberseguridad y ciberdefensa en Colombia. *Revista de Derecho, comunicaciones y nuevas tecnologías*, 1-17. http://dx.doi.org/10.15425/redecom.14.2015.06

Cubillos Ramos, J. (s.f.). Gestión de riesgos para la seguridad digital en Colombia. Universidad Piloto de Colombia. http://polux.unipiloto.edu.co:8080/00004751.pdf

Cujabante Villamil, X., Bahamón Jara, M., Prieto Venegas, J. y Quiroga Aguilar, J. (2020). Ciberseguridad y ciberdefensa en Colombia: un posible modelo a seguir en las

relaciones cívico-militares. *Revista Científica General José María Córdova, 18*(30), 357-377. http://dx.doi.org/10.21830/19006586.588

Departamento Nacional de Planeación. (2010). CONPES 3670/2010 *"Lineamientos de Política para la continuidad de programas de acceso y servicio universal a las Tecnologías de la Información y las comunicaciones".*

Departamento Nacional de Planeación. (2011). CONPES 3701 de 2011. https://bit.ly/3mL9i31

Departamento Nacional de Planeación. (2016). CONPES 3854/2016 se establece la *"Política Nacional de Seguridad Digital".* https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3854.pdf

Departamento Nacional de Planeación. (2016). *Conpes 3854-Política Nacional de Seguridad Digital*. https://colaboracion.dnp.gov.co/CDT/Conpes/Económicos/3854.pdf

Departamento Nacional de Planeación. (2020). CONPES 3995 *"Política Nacional de Confianza y Seguridad Digital".* https://bit.ly/3mLUy3G

Department of Defense (2006) *The National Military Strategy for Cyberspace Operations*. Washington D.C., Estados Unidos: Charmain of the Joint Chiefs of Staff.

Echeverri, L. (2016). *La relación de la ciberguerra con la guerra interestatal clásica: estudio de caso Estonia, Georgia e Irán*. Universidad Militar Nueva Granada. https://repository.unimilitar.edu.co/bitstream/handle/10654/15363/EcheverriMart%C3%ADnezLauraMilena2016.pdf?sequence=2

Foro Económico Mundial. (2021). *The Global Risk Report 2021*. http://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2021.pdf

Fula Perilla, P. (s.f.). Lineamientos de política para ciberseguridad y ciberdefensa-Documento CONPES 3701 [Trabajo de grado], Universidad Piloto de Colombia. http://polux.unipiloto.edu.co:8080/00003294.pdf

Gaitán Rodríguez, A. (2012). La ciberguerra y sus generaciones: un enfoque para comprender la incidencia de las tic en la guerra regular. *Estudios en Seguridad y Defensa Vol. 7*(1), 5-18.

Gaitán, A. (2013). La ciberguerra y sus generaciones: un enfoque para comprender la incidencia de las tic en la guerra regular. *Estudios en Seguridad y Defensa Nacionales*, 7(13): 5-18.

Giral-Ramírez, W., Celedón-Flórez, H., Galvis-Restrepo, E., y Zona-Ortiz, A. (2017). Redes inteligentes en el sistema eléctrico colombiano: *Revisión de tema. Tecnura*, 21(53),119-137. https://www.redalyc.org/articulo.oa?id=257054721009

González F., y Santoyo Velasco, C. (2012). Comportamiento estratégico en juegos de bienes públicos: Efecto de variables contextuales. *Revista mexicana de análisis de la conducta*, 38(2), 39-53. http://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S0185-45342012000200004

González, J. (2019). *Infraestructuras críticas: definiendo los sectores para su protección en Colombia*. Segurilatam.

Grupo de Respuesta a Emergencias Cibernéticas de Colombia. (2021). *Grupo de Respuesta a Emergencias Cibernéticas de Colombia*. http://www.colcert.gov.co/

Hernández Murillo, J. (2015). *Infraestructura crítica cibernética.* Comando Conjunto Cibernético. https://acis.org.co/archivos/Conferencias/2016/GuiaICC.pdf

Hernández, S. (2008). La teoría del realismo estructuralista y las interacciones entre los estados en el escenario internacional. *Revista Venezolana de Análisis de Coyuntura*, XIV (2), 13-29

IDEAM. (2018). *Un sectorial de protección y defensa para la infraestructura crítica cibernética de Colombia. sector ambiente y RRNN.*

Instituto de Hidrología, Meteorología y Estudios Ambientales. (2018). *Plan Nacional de Protección y Defensa para la Infraestructura Crítica*. Bogotá D.C.

Jiménez, J. (2015). *Las causas del terrorismo Yihadista*. https://jjolmos.com/las-causas-del-terrorismo-yihadista/

Joyanes, L. (2011). Introducción. Estado Del Arte De La Ciberseguridad. En Ciberseguridad. *Retos Y Amenazas A La Seguridad Nacional En El Ciberespacio* (pág. 26). Ministerio De Defensa. http://www.ieee.es/Galerias/fichero/cuadernos/CE_149_Ciberseguridad.pdf

Kahan, J (2015). *Resilience Redux: Buzzword or Basis for Homeland Security"*. Homeland Security Affairs

Kerber, A. (2004). Marco jurídico en materia de seguridad en la agenda hemisférica. *Díkaion*, 18(13),13-26. https://www.redalyc.org/articulo.oa?id=72001303

Klimburg, A. (2012). *"National Cyber Security Framework Manual"*. Tallin: NATO CCD COE Publication.

Korstanje, M. (2010). El 11 de septiembre y la teoría de la percepción del riesgo. *Revista de Turismo y Patrimonio Cultural*, 8(2),389-402. https://www.redalyc.org/articulo.oa?id=88112768011

Lopera, J., Ramírez, C., Zuluaga, M., y Ortiz, J. (2010). *El método analítico como método natural. Revista de Psicología Universidad de Antioquia*. ISSN 2145-4892. rev. psicol. univ. antioquia vol.2 no.2 Madelin. http://pepsic.bvsalud.org/scielo.php?script=sci_arttext&pid=S2145-48922010000200008

López Pérez, R. (1998). Crítica de la Teoría de la Información. Cinta de *Moebio*, (3). www.moebio.uchile.cl/03/frprin01.htm

Lowenthal, Mark M. (2010). *"Contrainteligencia". En Inteligencia y Seguridad Nacional, editado por el Centro de Investigación y Seguridad Nacional y Escuela de Inteligencia para la Seguridad Nacional, 205-217*. Ciudad de México: Secretaría de Gobernación/ CISEN.

Lozano, M. y Páez, Á. (2015). Repensando lo político desde las contradicciones del ciberespacio. *Quórum Académico*, 12(2),328-344. https://www.redalyc.org/articulo.oa?id=199043103006

Maldonado, C. (2017). Ciencia hecha realidad. Reseña de C. A. Ossa, Teoría general de sistemas. Conceptos y aplicaciones. INNOVAR. *Revista de Ciencias Administrativas y Sociales*, 27(64),157-159. https://www.redalyc.org/articulo.oa?id=81850404014

Matallana, A. (s.f). Bloque B: Uso del Poder. (s.f). *Tópico 11: Contención*.

Matallana, A. (s.f). Bloque B: Uso del Poder. (s.f). *Tópico 12: Disuasión*.

Maturana, Humberto R. (1997). *De Máquinas y Seres Vivos, autopoiesis de la organización de lo vivo*. Santiago de Chile: Editorial Universitaria.

Mejía, J. (2020). *Actualización de la guía metodológica para la identificación de las Infraestructuras Críticas Cibernéticas de Colombia*.

Melzer, N. (2011). *Cyberwarfare and International Law*. Ginebra, Suiza: United Nations Institute for Disarmament Research.

Mendoza Cortés, P. (2020). Inteligencia y contrainteligencia militar frente a fallos y desafíos. El caso de Culiacán, México (2019). *URVIO, Revista Latinoamericana de Estudios de Seguridad*, (26),37-56.[fecha de Consulta 2 de Agosto de 2021]. ISSN: 1390-3691. Disponible en: https://www.redalyc.org/articulo.oa?id=552662410003

Ministerio de Defensa Nacional. (2017). *Plan Nacional de Protección y Defensa para la Infraestructura Crítica Cibernética de Colombia.* https://www.ccoc.mil.co/ciberdefensa_maquetacion_biblioteca_publica_conpes

Ministerio de Defensa Nacional. (2019). *Política de Defensa y Seguridad para la legalidad, el emprendimiento y la Equidad 2018-2022*. https://www.asocapitales.co/nueva/wp-content/uploads/2020/06/Poli%CC%81tica-de-Defensa-y-Seguridad-MDN.pdf

Ministerio de Tecnologías de la Información y las Comunicaciones. (2018). *Plan TIC 2018-2022 El Futuro Digital es de Todos.* https://micrositios.mintic.gov.co/plan_tic_2018_2022/pdf/plan_tic_2018_2022_20200107.pdf

Ministerio del Interior de España. (2011). *Reglamento de protección de las infraestructuras críticas*. https://www.boe.es/buscar/doc.php?id=BOE-A-2011-7630

Montoya Gaitán, B. (2016). ¿Cómo minimizar el riesgo de afectación de un ataque cibernético en los blancos estratégicos nacionales? [Trabajo de grado – Especialización Alta Gerencia], Universidad Militar Nueva Granada. https://repository.unimilitar.edu.co/bitstream/handle/10654/15693/MontoyaGaitanBenjamin2017.pdf?sequence=2&isAllowed=y

Morgenthau, H. J., & Thompson, K. (1986). *Política entre las naciones: la lucha por el poder y por la Paz*. Buenos Aires: Grupo Editor Latinoamericano.

NIST Cybersecurity Framework Adoption Hampered By Costs, Survey Finds. (2016). *Dark Reading*. https://www.darkreading.com/attacks-breaches/nist-cybersecurity-framework-adoption-hampered-by-costs-survey-finds/d/d-id/1324901

Oficina de Lucha Contra el Terrorismo. (2006). *Estrategia Global de Las Naciones Unidas Contra el Terrorismo*. https://www.un.org/counterterrorism/ctitf/es/un-global-counter-terrorism-strategy#plan

Osorio, J. (2007). Introducción al mundo sistémico. Aproximación práctica. *Scientia Et Technica*, XIII (34),349-354. ISSN: 0122-1701. https://www.redalyc.org/articulo.oa?id=84934059

Ospina Díaz, M. y Sanabria Rangel, P. (2020). Desafíos nacionales frente a la ciberseguridad en el escenario global: un análisis para Colombia. *Revista Criminalidad, 62*(2), 199-217. http://www.scielo.org.co/pdf/crim/v62n2/1794-3108-crim-62-02-199.pdf

Oviedo M., Librado H., Mancuso F., & Bohórquez K. (2017). *Lo nuevos escenarios en las fronteras colombianas: perspectivas institucionales en materia de migración irregular en el Marco del Pos-Acuerdo*. Bogotá: Escuela Superior de Guerra.

Pons Gamón, V. (2017). Internet, la nueva era del delito: ciberdelito, ciberterrorismo, legislación y ciberseguridad. *URVIO, Revista Latinoamericana de Estudios de Seguridad*, (20),80-93. https://www.redalyc.org/articulo.oa?id=552656641007

Poveda Criado, M., & Torrente Barredo, B. (2016). Redes sociales y ciberterrorismo. Las TIC como herramienta terrorista. *Opción, 32*(8),509-518.[fecha de Consulta 2 de Agosto de 2021]. ISSN: 1012-1587. https://www.redalyc.org/articulo.oa?id=31048481030

Prieto, R., Hernández, A., Candón, A., Murillo, A., Quesada, C., Enríquez, N., & Calderón, J. (4 de Abril de 2013). Guerra Cibernética: *Aspectos Organizativos*. 26. Madrid. España.http://www.defensa.gob.es/ceseden/Galerias/ealede/cursos/curDefNacional/ficheros/Ciberseguridad_nuevo_reto_del_siglo_XXI_Guerra_cibernetica_aspectos_organizativos.pdf

Prieto, W. (2017). Gestión y respuesta a incidentes de ciberseguridad. Ministerio de Defensa Nacional y colCERT. https://caivirtual.policia.gov.co/sites/default/files/colcert_-_sensibilizacion_gestion_de_incidentes.pdf

Rakkah, A. (2005). El mundo árabe después del 11 de septiembre. *OASIS*, (10),55-78. https://www.redalyc.org/articulo.oa?id=53101004

RAND Corporation (s.f.). *Cyber Warfare. RAND Corporation*. www.rand.org, http://www.rand.org/topics/cyber-warfare.html

Realpe Diaz, M. y Cano Martínez, J. (s.f.). Amenazas cibernéticas a la seguridad y defensa nacional. Reflexiones y perspectivas en Colombia. *Universidad del Rosario.* https://doi.org/10.12804/si9789587844337.10

Rodríguez Prieto, R. (2016). ¿Qué seguridad? Riesgos y Amenazas de Internet en la Seguridad Humana. Araucaria. *Revista Iberoamericana de Filosofía, Política y Humanidades*, 18(36),391-415. https://www.redalyc.org/articulo.oa?id=28248171018

Rodríguez, T. (2012). *El terrorismo y nuevas formas de terrorismo Espacios Públicos*. Universidad Autónoma del Estado de México Toluca, pp. 72-95.

Sánchez Acevedo, M. (2019). *La ciberseguridad y la ciberdefensa, la necesidad de generar estrategias de investigación sobre las temáticas que afectan a la seguridad y defensa del Estado.* En Medina, G. La seguridad en el ciberespacio. Un desafío para Colombia. https://doi.org/10.25062/9789585216549.01

Sánchez, J, (2012). *En la mente de los estrategas*. Bogotá: Escuela Superior de Guerra. ISBN:9789585737648.

Spindler, W. (2011). *La trata de personas, una industria criminal de rápido crecimiento*. Francia: ACNUR. http://www.acnur.org/noticias/noticia/la-trata-de-personas-una-industria-criminal-de-rapido-crecimiento/

Unión Europea. (2007). *Programa europeo para la protección de infraestructuras críticas*. https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=legissum:l33260

Vargas B., Recalde H., & Reyes, R. (2017). Ciberdefensa y ciberseguridad, más allá del mundo virtual: modelo ecuatoriano de gobernanza en ciberdefensa. *URVIO, Revista Latinoamericana de Estudios de Seguridad*, (20),31-45. https://www.redalyc.org/articulo.oa?id=552656641013

Verdugo Sierra, H. (2016) I*mportancia de definir la infraestructura crítica en Colombia* [Trabajo de grado para especialización Administración de la seguridad], Universidad

Militar Nueva Granada. https://repository.unimilitar.edu.co/bitstream/handle/10654/14342/BerdugoSierraHelber%20Alirio2016.pdf?sequence=1

White, R. (2014). *Towards a Unified Homeland Security Strategy: An Asset Vulnerability Model*. Homeland Security Affairs.

Zavaleta Hernández, S. (2015). El concepto de seguridad humana en las relaciones internacionales. *Revista de Relaciones Internacionales, Estrategia y Seguridad*, 10(1),65-87. https://www.redalyc.org/articulo.oa?id=92733014004 Instituto LISA. (2009). *Infraestructuras críticas: definición, planes, riesgos, amenazas y legislación*. https://www.lisainstitute.com/blogs/blog/infraestructuras-criticas