EDITORIAL ESDEG

Revista
Ciberespacio, Tecnología e Innovación
Volumen 2, número 3, enero-junio 2023
Bogotá, D.C, Colombia
ISSN: 2955-0270 • eISSN: 3028-3310
Página web: https://esdegrevistas.edu.co/index.php/rcit

Aproximación Teórica a los Factores Armados de Inestabilidad, que afectan la Seguridad y Defensa Nacional en el Ciberespacio

Theoretical Approach to the Armed Factors of Instability, which affect the Security and National Defense in Cyberspace

Gabriel Andrés Acosta Lizarazo

CITACIÓN APA:

Acosta Lizarazo, G. A. (2023). Aproximación Teórica a los Factores Armados de Inestabilidad, que afectan la Seguridad y Defensa Nacional en el Ciberespacio. *Ciberespacio, Tecnología e Innovación, 2*(3), 25-56.
https://doi.org/10.25062/2955-0270.4773

Publicado en línea: **Junio 30 de 2023**

Enviar un artículo a la Revista

Revista Ciberespacio, Tecnología e Innovación
Volumen 2, número 3, enero-junio 2023 (pp. 25-56)
Bogotá, D.C, Colombia

EDITORIAL ESDEG

Aproximación Teórica a los Factores Armados de Inestabilidad, que afectan la Seguridad y Defensa Nacional en el Ciberespacio

Theoretical Approach to the Armed Factors of Instability, which affect the Security and National Defense in Cyberspace

DOI: https://doi.org/10.25062/2955-0270.4773

Gabriel Andrés Acosta Lizarazo

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

Resumen

En el presente artículo se realiza una aproximación teórica a los Factores Armados de Inestabilidad y como pueden afectar a la Seguridad y Defensa Nacional a través del ciberespacio. Esta aproximación se desarrolla efectuando una caracterización, conceptualización, e identificación de los factores armados de inestabilidad de Colombia y de sus capacidades. Adicionalmente, se conceptualiza la Infraestructura Crítica y se identifican los sectores en Colombia, analizando como los factores armados de inestabilidad han atentado contra los sectores de la infraestructura colombiana. Finalmente, se realiza un análisis a los riesgos que se presentan en el ciberespacio a la Seguridad y Defensa en Colombia, observando si estos dependen de las capacidades de los Factores Armados de Inestabilidad para cumplir con sus propósitos utilizando el ciberespacio o de las capacidades del estado para contrarrestar las amenazas que están latentes en este dominio.

Palabras Clave: Factores Armados de Inestabilidad, Grupos Armados Organizados, Grupos Delincuenciales Organizados, Delitos Trasnacionales.

Abstract

In this article, a theoretical approach is made to the Armed Factors of Instability and how they can affect National Security and Defense through cyberspace. This approach is developed by carrying out a characterization, conceptualization, and identification of the armed factors of instability in Colombia and their capabilities. Additionally, Critical Infrastructure is conceptualized and the sectors in Colombia are identified, analyzing how the armed factors of instability have attacked the sectors of the Colombian infrastructure. Finally, an analysis is carried out on the risks that arise in cyberspace to Security and Defense in Colombia, observing whether these depend on the capabilities of the Armed Factors of Instability to fulfill their purposes using cyberspace or on the capabilities of the state to counteract the threats that are latent in this domain.

Key words: Armed Instability Factors, Organized Armed Groups, Organized Crime Groups, Transnational Crimes.

Artículo de reflexión
Recibido: 30 de mayo de 2023 • **Aceptado:** 06 de junio de 2023
Contacto: Gabriel Andrés Acosta Lizarazo acostaga@esdeg.edu.co

Introducción

Históricamente Colombia se ha caracterizado por ser un país que ha venido luchando contra grupos armados que se apoderaron a través de amenazas y sometimiento de sitios estratégicos para delinquir. No se trata de un grupo en específico, por el contrario, son células que se han fortalecido y expandido tras el reciente proceso de desmovilización.

Ahora, si bien es cierto que el proceso de desmovilización sirvió de base para llegar a un acuerdo de paz, no menos cierto es el hecho, que sentó las bases para generar un proceso de transformación en el ámbito, social, económico y político, donde los grupos armados existentes y la reorganización de nuevos grupos surgidos luego de la desmovilización, se disputarán los territorios que se encontraban vacíos o desolados luego de la desmovilización de las Fuerzas Armadas Revolucionarias de Colombia (Farc).

Uno de los entornos que ha sido adoptado por parte de los Factores Armados de Inestabilidad existentes en Colombia ha sido el ciberespacio debido a su fácil acceso y a que cuenta con algunas condiciones favorables como son el anonimato y un menor costo para cometer crímenes de diferente índole lo que les permite reducir riesgos para su actuar criminal, optimizar recursos económicos y ampliar su espectro delincuencial lo que repercute en el mantenimiento de la Seguridad y Defensa Nacional es así como los reportes de ataques a las infraestructuras críticas entre los años 2019 y 2020, muestran que la nueva tendencia de los grupos armados delincuenciales es la inteligencia artificial, pues la mayoría de los asaltos a las plataformas públicas y privadas a través del ciberespacio denotan nuevos y sofisticados métodos para delinquir y causar daño al Estado y sociedad civil en general, (Policía Nacional de Colombia, 2019).

Se hace necesario identificar las capacidades que tienen los Factores Armados de Inestabilidad para cumplir con sus propósitos a través del entorno del ciberespacio, ya que las condiciones de dicho entorno pueden ser utilizadas para atentar en contra de la Seguridad y Defensa Nacional lo que lleva a plantear el siguiente interrogante de investigación ¿Cuál puede ser la afectación que generan los factores armados de inestabilidad a la Seguridad y Defensa Nacional en el ciberespacio?.

Por lo anterior en el presente capítulo se aborda la siguiente tesis que busca identificar si los Factores Armados de Inestabilidad en Colombia utilizan el ciberespacio como una herramienta para alcanzar sus propósitos criminales y si con el empleo de este entorno pretenden o pueden afectar la Seguridad y Defensa Nacional.

Metodología

El desarrollo metodológico del presente artículo se llevó a cabo de manera no experimental a través de una investigación de tipo documental explicativa, manteniendo un enfoque

cualitativo y empleando fuentes de investigación e información como: documentos, libros y páginas web.

Se orientó el rastreo de información hacia el estudio de los Factores Armados de Inestabilidad Existentes en Colombia, sus intereses y capacidades que pueden tener utilizando el ciberespacio e identificando los riesgos que pueden representar dichos factores a la Seguridad y defensa nacional, empleando el dominio del ciberespacio. También, se aplicó una técnica investigativa concerniente a la recolección de información mediante el análisis de documentos con información de carácter relevante y que puede llevar información estadística; su desarrollo se efectuó de manera secuencial, abordando cada uno de los temas propuestos con el fin de alcanzar una aproximación teórica hacia los a los Factores Armados de Inestabilidad que afectan la Seguridad y Defensa Nacional en el Ciberespacio.

Caracterización de los factores armados de inestabilidad en Colombia y sus capacidades

Factores armados de inestabilidad

Conceptualización

Los Factores Amados de Inestabilidad son una de las principales circunstancias que afectan la estabilidad en Colombia, ya que se encuentran conformados por grupos armados organizados que realizan diferentes tipos de actividades delincuenciales en algunas zonas del país. Estas actividades tienen propósitos de carácter lucrativo, siendo ejecutadas mediante el uso de diferentes métodos y medios dentro de los cuales no se puede descartar el empleo del ciberespacio, pues se debe tener presente que actualmente el internet es un recurso de fácil acceso y puede servirles de herramienta para cumplir con sus propósitos. De este modo, se definen como grupos violentos que utilizan las armas como medio disuasivo para cometer sus delitos y de esta manera afectan directamente la estabilidad y gobernabilidad del Estado.

En ese contexto, puede asumirse que los factores armados de inestabilidad son uno de los componentes que generan inseguridad social en el país y requieren la aplicación de estrategias integradas y sistemáticas para contrarrestar su proceder delictivo (Ejército Nacional de Colombia, 2018), estos grupos armados de inestabilidad corresponden a los denominados Grupos Armados Organizados (GAO), y los Grupos Delictivos Organizados (GDO) quienes se encuentran integrados por disidencias de antiguos grupos al margen de la ley y son actores presentes en diferentes zonas del país en donde pueden generar inestabilidad.

Por tanto, pueden definirse como un acumulado de actores que crean inseguridad social, económica y judicial, que, según sus maneras de actuar, sus capacidades y sus objetivos, se comportan como sistema, demanda la aplicación de estrategias para afrontar dichos factores (Ejército Nacional de Colombia, 2018). De acuerdo a lo planteado por la *Política de Defensa y Seguridad PDS - Para la Legalidad, el Emprendimiento y la Equidad* (2018), este es un término que se deriva de la Política de Seguridad y Defensa del Gobierno 2018-2022 en la cual se establecen las Zonas Estratégicas de Intervención Integral (ZEII) que se caracterizan por "su relevancia para los intereses nacionales y la convergencia de múltiples factores de inestabilidad y altos índices de criminalidad e inseguridad, así como de necesidades básicas insatisfechas, pobreza extrema y con población víctima de la violencia" (Ministerio de Defensa Nacional, 2018, p.38).

En definitiva, los Factores Armados de Inestabilidad son grupos que han acogido disidencias de grupos terroristas y de organizaciones criminales de diferente índole, las cuales se financian ilícitamente a través de actividades criminales como:

Narcotráfico.

Se debe tener en cuenta lo lucrativo que puede ser este delito para los Factores Armados de Inestabilidad teniendo en cuenta que según Chavarro y Osorio (2018) el tráfico de drogas representa un valor anual estimado de 320.000 millones de dólares.

Minería ilegal.

Este delito cuenta con unas condiciones particulares en las regiones del país y de alguna forma se puede considerar como uno de los delitos que estos factores pueden desarrollar para lucrarse, introduciendo sus ganancias dentro de la legalidad (Chavarro y Osorio, 2018).

Tráfico de Armas.

Este delito, según Chavarro y Osorio (2018) genera de 170 a 320 millones de dólares por año, contribuyendo de esta manera para que se generen escenarios delincuenciales en el país lucrando a unos grupos y dando capacidades a otros (p. 270).

Los Factores Armados de Inestabilidad tienen fines lucrativos y se puede evidenciar en las ganancias que pueden generar los delitos que cometen sin descartar que para su ejecución utilicen el entorno del ciberespacio.

Clasificación de los factores armados de inestabilidad en Colombia

Los conflictos armados en Colombia es un tema que ha tenido una amplia trascendencia, debido a las consecuencias políticas, económicas, sociales y culturales dejadas a su

paso, situación que evidentemente ha desencadenado una fuerte inestabilidad en el país (Tawse, 2008).

Toda esta situación es el resultado de la organización y/o conformación de grupos o fracciones armadas que se han venido configurando y apropiando de diferentes zonas de Colombia, lógicamente que cada uno de ellos tiene propósitos diferentes, pero tienen técnicas de dominio comunes que comparten para establecer un control sobre el territorio

Es así que tomando en consideración lo expuesto en el Plan de Campaña Bicentenario Héroes de la Libertad (2018) los factores armados de inestabilidad se clasifican en:

- Los Grupos Armados Organizados (GAO).
- Los Grupos Armados Organizado (GAO ELN).
- Los Grupos Delincuenciales Organizados (GDO).
- Los Delitos Trasnacionales (DT), el tráfico de armas, municiones y explosivos.

La clasificación de los Factores Armados de Inestabilidad obedece a todas aquellas organizaciones al margen de la ley que desarrollan actividades ilegales con propósitos lucrativos y que en su mayoría son disidencias de antiguos grupos armados ilegales de Colombia; dichos grupos se encuentran distribuidos en diferentes zonas del país en donde no existe una presencia integral del estado lo que genera la existencia de delitos transnacionales y el tráfico de armas que se dan con mayor regularidad en áreas fronterizas.

Estructura de los factores armados de inestabilidad en Colombia

Grupos Armados Organizados (GAO).

Se caracterizan por ser organizaciones que se encuentran estructurados por tres o más personas que han coexistido durante algún tiempo y actúan ordenadamente con el fin único de cometer hechos ilícitos con el fin de obtener un beneficio económico o material, por tanto, pueden definirse como un conjunto de actores armados ilegales, debidamente constituidos y con la suficiente capacidad para realizar actividades propias del crimen organizado (Jiménez y Acosta, 2018).

Para Lleras (2016) los grupos GAO son organismos armados que sustentan una estructura direccionada por un comando que ejerce un control estratégico sobre un territorio específico. Se caracterizan por tener una estructura que abarca habilidades operacionales, logística y control interno. Asimismo, cuentan con un elevado potencial armado que les ayuda a sostener los combates y utilizar e imponer la violencia. De acuerdo con Lunas (2017), estructuralmente se encuentran organizados por tres categorías:

- Los disidentes. Se vinculan con los grupos armados que no se desmovilizaron durante el proceso de paz establecido por gobiernos anteriores.
- Los rearmados. Están conformados por todas aquellas organizaciones que reanudaron sus operaciones luego de haberse desmovilizado y guardan relación con el crimen organizado y la ***delincuencia común***.
- Grupos emergentes. Surgen como resultado de las dinámicas pasadas, en las cuales quedaron espacios desocupados que fueron aprovechados por grupos insurgentes para conformar nuevos grupos delictivos.

Al respecto, Jiménez y Acosta (2018) sostienen que la estructura de los GAO está compuesta por:

> Las Disidencias de las Farc. Esta clasificación responde a la reorganización de antiguos miembros que formaban parte de la "desmovilizada guerrilla" que decidieron no acoger el acuerdo de paz y prefirieron continuar con las actividades delictivas que venían ejerciendo. Actualmente, cuenta con 17 estructuras distribuidas en los departamentos de Arauca, Cauca, Antioquia, Caquetá, Valle del Cauca, Casanare, Nariño, Putumayo, Guainía, Meta, Vichada, Guaviare y Vaupés, esto según lo expuesto por Fundación Ideas para la Paz (p. 107).

En cuanto al número de disidentes que la integran, no se tiene una cantidad exacta, sin embargo, hasta el 2018 se estimaba que podía estar compuesta por 1200 hombres aproximadamente, quienes buscan apoderarse de las zonas que anteriormente estaban bajo el dominio de las Farc, para tener control sobre las rutas y actividades de narcotráfico.

- **Ejército Popular de Liberación (EPL).** Según lo expuesto por Prieto (2013) esta es una asociación criminal armada que se ubica en la localidad del Catatumbo con desplazamientos hacia Venezuela y está integrada por 500 personas aproximadamente. Sus principales actividades son el tráfico de armas, drogas y gasolina. Es considerado uno de los grupos delictivos con mejor organización, situación que ha provocado que se mantenga activa frente a los ataques de las fuerzas armadas de la república, esto de acuerdo a lo planteado por Blanco, Gravito y Trujillo (2012).
- **Clan del Golfo.** Está considerada como la organización criminal "más grande" de Colombia. Se estima que está compuesta por un aproximado de 1900 miembros que han formado parte de otros grupos armados, su principal fortaleza son las alianzas que ha venido manteniendo con otros *actores ilegales,* que realizan acciones ilegales en diferentes sectores del país (García y Herrera, s.f.). Se caracteriza por ser un grupo cuya actividad delictiva se concentra en el narcotráfico, pasando a ser parte de las Organizaciones Integradas al Narcotráfico (ODIN). Mantiene el control operacional en 26 departamentos del país, en los

cuales ha impulsado la creación de un elevado número de bandas criminales, esto de acuerdo con los argumentos presentados por la Unidad Investigativa Indepaz (2017).

- **Los Puntilleros.** Es el resultado de la unificación criminal del Bloque Libertadores y el Bloque Meta del Vichada, grupos paramilitares que ejercen dominio sobre los Llanos Orientales y un área muy reducida del departamento del Guaviare. Se encuentra integrado aproximadamente por 70 individuos, todos ex-paramilitares (Fundación Ideas Para la Paz, 2017). Su base de financiamiento es el manejo de drogas, y las negociaciones se realiza a través de la mediación del Clan del Golfo.

Los Grupos Armados Organizado (GAO ELN).

Ejército de Liberación Nacional (ELN). Está compuesta por 1800 hombres aproximadamente, los cuales se extienden a lo largo y ancho del norte de Colombia en tres grupos: el primero de ellos conocido como Frente Oriental en Arauca, Santander y Norte de Santander. Al segundo se le denomina Bloque Occidental y delinque en los lugares más apartados de Chocó y en algunos sectores al norte de Antioquia Unidad Investigativa Indepaz (2017).

Ahora este es un grupo que ser caracterizado por mantener acuerdos con los disidentes de las Farc y el Clan del Golfo para continuar teniendo dominio sobre las actividades de extorsión, narcotráfico y secuestros entre las fronteras de Colombia con Venezuela y Panamá.

Los Grupos Delincuenciales Organizados (GDO).

Son grupos criminales cuyo perfil se enfoca hacia el tráfico de drogas y armas, homicidios, masacres, homicidios, extorsiones, masacres, reclutamiento de menores, e inducción de desplazamientos forzados, entre otros delitos, todos con el único fin de mantener un control en sectores específicos, poblaciones y mercados ilegales rentables como contrabando de bienes sean legales o ilegales, narcotráfico, minería ilegal, etc., (Prieto, 2012).

De acuerdo con el citado autor, estos son segregaciones que surgieron a raíz de las desmovilizaciones de *grupos Paramilitares* entre los años 2003 y 2006 e inicialmente se encontraba integrada por grupos armados que pasaron a ejercer dominio en territorios que habían estado bajo el control de paramilitares, la idea era imponer un control territorial y social, por refugiados de grupos desmovilizados que continuaban imponiendo su autoridad a través de las armas y controlaban la economía de las zonas dominadas, por bandas que decidieron no participar en el proceso de paz y continuaron delinquiendo en esos territorios y, por supuesto, aquellas organizaciones que fueron parte del proceso de desmovilización, pero tomaron la determinación de reagruparse y tomar nuevamente las armas.

Para el año 2012 la Policía Nacional de Colombia presentó un informe en el cual se expuso que los Grupos Delincuenciales Organizados se encontraban estructurados por bandas de alta peligrosidad y con proyección internacional hacia Venezuela, México, Perú y Ecuador, siendo las de mayor envergadura; Los Rastrojos, Los Urabeños, Renacer, Disidencias ERPAC y Machos, (Policía Nacional de Colombia, 2012).

En contraste con lo anterior, Prieto (2013) argumenta que de la estructura de los Grupos Delincuenciales Organizados el 14% corresponde a desmovilizados, de los cuales 1700 aproximadamente son jefes vinculados al paramilitarismo, algunos fueron apresados en algunos bloques de autodefensa del Noroeste antioqueño, Córdoba, Mineros, Héroes de Granada, Catatumbo, Tayrona, entre otros. Acota que a nivel internacional mantienen una red delictiva bien organizada principal con Venezuela y Ecuador. En el caso del primer país se han posesionado de sectores de los Estados fronterizos de Apure, Táchira y Zulia. En el caso de Ecuador tienen una fuerte concentración en Guayaquil para el tráfico de drogas.

Como segundo escenario para estos grupos criminales se tiene México y Perú. Estos son considerados territorios estratégicos para el procesamiento y distribución de drogas. En tercer lugar, se encuentran países latinoamericanos como Paraguay, Chile, Argentina, Uruguay y Bolivia, resaltando por ser contextos idóneos para el lavado de activos y narcotráfico.

Los delitos Trasnacionales (DT), el tráfico de armas, municiones y explosivos.

Para Colombia, establecer un control sobre el tráfico de cualquier tipo armas, municiones y explosivos se ha convertido en un verdadero desafió para la seguridad pública, pues con el paso del tiempo la organización y proyección del *crimen organizado transnacional* se ha incrementado (Cancillería de Colombia, 2019).

En esa dirección, los Delitos Trasnacionales se caracterizan por ser transgresiones que no solo se ejecutan a nivel internacional, sino que por la misma naturaleza de los hechos involucra la transferencia *Transfronteriza* como parte de las actividades ilícitas, llegando a convertirse en un negocio mundial que genera cuantiosas ganancias a los grupos o personas que hacen parte de ella (Oficina de Naciones Unidas contra la Droga y el Delito, 2009).

Torres & Balaguera (2013) concibe los Delitos Trasnacionales (DT) como un *sistema económico* ilegal en el cual se conjugan dos elementos: las técnicas o instrumentos delincuenciales de una organización compleja, metódica y subyugada con el propósito de incrementar sus ingresos financieros. Por tanto, se caracterizan por tener una estructura sólida, en la cual las operaciones criminales se convierten en un modelo de negocio o simplemente en una empresa que se desenvuelve en el ámbito internacional.

Ahora en Colombia este tipo de actividad no es nueva, por el contrario, se remonta a principios del siglo XIX y comenzó con el envío de cocaína hacia Estados Unidos y Europa, incluyendo más tarde otras actividades comerciales ilícitas hacia países fronterizos como Bolivia y Perú. No obstante, pasa a estructurarse y a consolidarse definitivamente como actividad comercial ilícita en los años 80 de la mano de Pablo Escobar Gaviria (+), (Torres, 2013).

Ubicación geográfica de los factores armados de inestabilidad

Conforme a los planteamientos de Jiménez y Acosta (2018), los Grupos Armados Organizados (GAO) y los Grupos Armados Organizados (GAO ELN), se ubican en diversas regiones de Colombia. Según explican los autores, estos han sido ocupados y resultan ser localidades estratégicas para ejercer la criminalidad; destacando, por ejemplo, el pacífico colombiano y abarcando desde el sur del país hasta el Golfo de Urabá, la totalidad norte de la Amazonia colombiana y una fracción del sur, algunas localidades importantes de la frontera, centro del país y los Llanos Orientales, región del Caribe específicamente localidades ubicadas en la frontera venezolana y la región Andina.

Ahora, de acuerdo con un informe presentado por la Fundación Paz & Reconciliación (2018), las operaciones criminales de estos grupos criminales se desarrollan en territorios que anteriormente fueron dominados por las Farc, y están caracterizados por la presencia de individuos fuertemente armados y el desarrollo de actividades al margen de la ley. Asimismo, se evidencian otras zonas donde la amenaza es elevada, con altos movimientos criminales, pero con poca presencia de individuos armados e incluso pueden encontrarse sectores donde las actividades ilegales son muy reducidas y la presencia armada es casi nula, esto tomando en cuenta el nivel de amenaza por departamento, tal como se muestra seguidamente (ver tabla 1):

Tabla 1. Ubicación de los GAO conforme al nivel de amenaza.

Nivel	Departamento
Prioritario	Cauca, Chocó, Nariño, Norte de Santander, Putumayo, Valle de Cauca y Vichada
Alta	Amazonas, Antioquia, Arauca, Bolívar, Caquetá, Córdoba, Guaviare, Meta, Santander y Vaupés
Media	Casanare, Cesar, La Guajira, Huila y Tolima

Fuente: Información tomada de (Jiménez y Acosta, 2018; Fundación Para la Paz & Reconciliación, 2018).

Por su parte, los Grupos Delincuenciales Organizados (GDO) han venido ocupando los departamentos del Norte de Santander, Bolívar, Santander, Chocó, Valle del Cauca,

Antioquia, Cauca, La Guajira, Nariño, Córdoba, el Cesar, Magdalena, Sucre, el Meta, Casanare y Guaviare, esto en conformidad con lo señalado por Rincón (2017).
El tráfico de armas, municiones y explosivos no tienen una ubicación específica, no obstante, la mayor concentración está entre Cali y Medellín, (Jiménez y Acosta, 2018).

Se evidencia que existen zonas del país que representan una mayor complejidad para neutralizar el accionar delictivo de los Factores Armados de Inestabilidad, ya que por lo general dichos grupos desarrollan sus acciones delincuenciales en zonas en donde no existe una presencia integral por parte del estado y en áreas de frontera terrestre y marítima con otros países de la región.

Capacidades para el manejo del ciberespacio por parte de los factores armados de inestabilidad en Colombia

Las tecnologías de la Información y la Comunicación, sin lugar a dudas, trajeron consigo un sinfín de beneficios a la sociedad, abarcando sectores económicos, culturales, políticos, entre otros, haciendo del ciberespacio un lugar de encuentro para millones de cibernautas. No obstante, no se puede afirmar que todos los aportes del ciberespacio han sido positivos, pues son muchos los problemas y amenazas que han surgido y a las cuales ha tocado responder oportunamente (Sánchez, 2012).

Ahora, si bien es cierto que la revolución tecnológica ha facilitado a que millones de individuos tengan acceso a novedosas y diversificadas herramientas de información y comunicación a los cuales anteriormente era casi imposible acceder, también es cierto que esta revolución generó un cambio a nivel cultural y creó todo un escenario para que organizaciones que actúan al margen de la ley utilicen las Tecnologías de la Información y la Comunicación para fines de hacerse visibles en otros contextos, ganar mayores espacios territoriales y aumentar el dominio social y económico en aquellas regiones controladas por ellos (Zambrano, 2010).

De esta manera puede entenderse, que el ciberespacio existe gracias al dinamismo y creación de las redes informáticas, las cuales están compuestas por ordenadores y múltiples sistemas operativos que generalmente son conectados a internet, siendo esta la red con mayor significancia en el ciberespacio (Osorio, 2020). Por tanto, para que exista el ciberespacio es preciso contar con sistemas de información, redes, conectividad, disponer de circuitos, pues sin todos estos elementos es imposible construir un espacio virtual, ya que de ellos depende la interacción entre las partes (Hadlington, 2017).

Actualmente, el uso del ciberespacio se ha convertido en una de las herramientas más importantes no solo para comunicarse, informarse o realizar actividades comerciales, sino que además viene a representar una oportunidad para los grupos irregulares

que hacen vida en Colombia, pues les ha servido de base para expandir las operaciones y aumentar el caos entre la sociedad civil. Sobre este particular, Sánchez (2012) sostiene que los grupos armados y delincuenciales organizados en Colombia, se han dado a la tarea de emplear la red para buscar financiamientos, reclutar personas para incrementar sus tropas, abrir nuevos canales de comunicación, coordinar y ejecutar acciones, crear campañas de adoctrinamiento, lavar dinero, vender e intercambiar datos, poner en práctica tortura y guerra psicológica y promover sus organizaciones.

Otro aspecto importante y que ha cobrado fuerza entre estos grupos delictivos, es la utilización del ciberespacio para adquirir dinero de manera fraudulenta. Para ello, se vale de diversas estrategias delictivas que va desde el envío de correos electrónicos para amenazar y cobrar *vacunas,* hasta el hackeo de cuentas en redes sociales de relevantes figuras de la vida empresarial y/o política (Osorio, 2020).

Sobre este particular y en armonía con lo expuesto por Sánchez (2012), la Oficina de Naciones Unidas contra la Droga y el Delito -UNODC- (2013), señala que el ciberespacio representa la plataforma perfecta para que la delincuencia organizada abra espacios dentro y fuera del país para ampliar sus operaciones y trascender fronteras y promover diversas actividades categorizadas como terroristas, tal como se mencionan seguidamente:

Propaganda

A través del internet, los grupos armados y/o delincuenciales pueden promover el terrorismo mediante audios y videos. Generalmente, este tipo de material es utilizado para el adoctrinamiento, imponer su presencia, girar instrucciones, rendir explicaciones o justificar ante terceros algún hecho en particular y por supuesto promover actividades terroristas, así como la violencia por medio de imágenes o videojuegos que son diseñados por estas organizaciones e invitan al usuario a ser partícipes activos de este tipo de actividades.

Además, dentro de esta categoría puede ubicarse el impulso de la *retórica extremista*, es decir, usan el ciberespacio para dividir, desestimar y crear falsas expectativas respecto a la libertad democrática y política. Para ello, se valen de herramientas, páginas web, salas virtuales con foros interactivos, revistas virtuales y lógicamente de redes sociales como Facebook, Twitter, YouTube, Instagram, y cualquier otro canal que les sea útil para establecer canales abiertos de comunicación.

Esta categorización se presta igualmente para subir mensajes subliminares por medio de los cuales se busca apoyo de otras personas y reclutarlos para formas parte de estas organizaciones criminales y de este modo ampliar su estructura y fortalecer sus comandos. Otro aspecto relevante dentro de este escenario, es que muchas ocasiones

las propagandas están diseñadas con fines predeterminados y algunas incitan a jóvenes y personas vulnerables a cometer actos terroristas y obtener beneficios de los resultados alcanzados.

Financiación

Las formas de financiación empleadas por estos grupos para obtener recursos económicos son diversas, algunas de ellas se relacionan con el comercio electrónico, pueden utilizar sistemas de pagos en líneas (suplantación de identidad, hurto de tarjetas de crédito, fraude a la bolsa de valores, delitos contra la propiedad intelectual y estafas en subastas), técnicas de recaudación directa (correos electrónicos, campañas de recaudación a través de la web, solicitud de donaciones a grupos de apoyo).

En definitiva, el ciberespacio se ha convertido en una ventana abierta para las operaciones delictivas de los grupos armados que hacen vida en Colombia. Ya no se trata solamente de crear sitios web con matices políticos, con ideas propagandistas que pretenden vender una postura u otra, conquistar y ampliar nuevos espacios; sino que va más allá.

Se trata entonces de apropiarse de la red y a través de ella buscar nuevos objetivos y formas de ampliar sus operaciones criminales e incitar al odio, la violencia y crear las condiciones para cambiar la dinámica política del país, y continuar mostrando presencia dentro y fuera de los territorios bajo su dominio, pues tal como puntualiza Trejos (2012), el uso de las nuevas tecnologías es una oportunidad no solo para ganar territorio, sino para obtener financiamientos, imponer el poder, ampliar el mercado del tráfico de drogas, armas, incrementar el número de integrantes de sus bandas y continuar sembrando el caos dentro de la sociedad civil.

Por lo anteriormente tratado se concluye que los Factores Armados de Inestabilidad en Colombia se encuentran conformados por los Grupos Armados Organizados (GAO), los Grupos Armados Organizados (GAO ELN), los Grupos Delincuenciales Organizados (GDO) y los Delitos Trasnacionales (DT) según lo establece el *Plan de Campaña Bicentenario Héroes de la Libertad* del Ejército de Colombia de 2018 con una estructura y ubicación geográfica en diferentes zonas del país que les son estratégicas como: el pacífico colombiano, el sur del país, el Golfo de Urabá, localidades importantes de frontera, el centro del país, los llanos orientales, región Caribe y la región Andina.

En la actualidad, dichos factores pueden emplear las tecnologías de la información y el ciberespacio como una herramienta para garantizar su financiación, realizar propaganda y cometer diferentes acciones delincuenciales que pueden llegar a afectar la seguridad nacional.

Identificación de los Sectores de la Infraestructura Crítica de interés para los Factores Armados de Inestabilidad en Colombia Infraestructura crítica

Conceptualización

Al hablar de infraestructura crítica se debe tener presente que es un concepto vinculado con los *activos, sistemas físicos y cibernéticos* que son importantes para un país, al punto que cualquier ataque, incapacidad o pérdida tienden a tener un impacto *debilitante* sobre la seguridad económica, física, servicios públicos y salud, (Aguirre, 2017).

Por su parte, Miranzo y Del Rio (2014) señalan que las infraestructuras críticas se refieren a las condiciones, servicios y/o instalaciones significativas para las entidades o la sociedad actuales que mantienen un dinamismo constante en su crecimiento, urbanístico, poblacional y económico, en las cuales los requerimientos y demandas de una localidad comienza a mostrar mayores grados de complejidad. Ahora, esta denominación responde a que su afectación o inoperatividad repercute sobre otros sistemas; dentro de estas infraestructuras se ubican la energía eléctrica, producción y distribución de petróleo y gas, telecomunicaciones, transporte, banca y finanzas, abastecimiento de agua, emergencia, servicios, gobierno, servicios y otros sistemas fundamentales y otros servicios catalogados como críticos para el bienestar, prosperidad y seguridad.

Por tanto, puede inferirse que las estructuras críticas son todas aquellas subestructuras, servicios, redes, equipos virtuales y físicos, que al ser interrumpidos o en su defecto destruidos causarían daños considerables en la salud, seguridad y la estabilidad económica del país y los ciudadanos, funcionamiento del Estado, entre otras. En consecuencia, se consolidan como sistemas particularmente complejos, los cuales son interconectados a través de redes, generan interdependencia con infraestructuras críticas que concierne sectores como redes eléctricas, de alimentación, agua potable, entre otras (Correa y Yusta, 2013).

En armonía con lo anterior, Certified Information System Auditor CISA (2019), sostiene que la infraestructura crítica comprende los sistemas, activos, redes, instalaciones y otros componentes útiles para que la comunidad mantenga la economía fortalecida, los sistemas de salud y la seguridad nacional, la economía, la salud y seguridad pública. Acotan, que hacen parte de la infraestructura crítica los sistemas de energía eléctrica, el agua de consumo humano, los sistemas de transporte público, los centros comerciales, sistemas de internet y telecomunicaciones.

El argumento de Martín (2016) reafirma los planteamientos anteriores, al afirmar que la infraestructura crítica introduce componentes claves el movimiento normal de la sociedad. Dentro de ese escenario se configura como aquellos activos o parte de un

sistema elemental para la protección de la sociedad y vitales, destacando entre ellos: la seguridad, la salud, el bienestar social y económico, individual y colectivo de la nación, y cuya obstrucción pasa a generar consecuencias severas para la funcionalidad operativa del Estado.

En otras palabras, las infraestructuras críticas representan el eje longitudinal para la economía de un país, haciendo de ella un punto altamente vulnerable para las naciones e impide cumplir con los propósitos trazados en materia de desarrollo económico, social, seguridad e incluye: sector químico, industrias, empresas de defensa, electricidad, gas natural, petróleo, servicios de emergencia, sector financiero, agricultura, industrias alimenticias, salud, medios de transporte (navegación, ferrocarril, aviación, puertos, carreteras y autopistas), aguas en su estado natural, agua residuales, sistemas nucleares, telecomunicaciones, tecnología de la información y comunicación. (Martín, 2016)

Para la Organización para la Cooperación y el Desarrollo Económicos -OECD- (2014) la definición de infraestructuras críticas recae sobre las cadenas de suministro, instalaciones físicas, redes de comunicaciones, tecnologías de la información, que al ser destruidas no pueden ser utilizadas durante largo tiempo, trayendo consigo serias consecuencias que golpean significativamente el progreso socioeconómico de un país, afectando sus funciones normales y dejado de garantizar la seguridad nacional y con ello la defensa de la colectividad.

Infraestructura critica en Colombia

La infraestructura crítica de un país está conformada por todos los procedimientos que son clave para sostenerse en la actualidad y proyectarse en el tiempo, o sea, son todos esos procesos considerados elementales para que un país se mantenga y no se paralice, pues de faltar alguno de los componentes de una infraestructura se corre un riesgo eminente que afectaría, no solo a los entes gubernamentales, sino a la sociedad en pleno, pues tal como lo explica Masís (2019) un ataque a una de estas infraestructuras puede impedir el suministro eléctrico, de agua potable de combustible, afectar considerablemente el transporte aéreo, fluvial, marítimo, terrestre; sin dejar de lado el sistema de telecomunicaciones, los poderes públicos, la salud y todos aquellos sistemas que constituyen el cimento funcional de un país.

En contraste con lo anterior, González (2019) sostiene que en Colombia se han hecho definiciones sobre las infraestructuras críticas basadas en supuestos, pero la realidad es que no existe una definición propia como ocurre en otros países. Acota, que esto obedece a que el país no cuenta con estrategias para salvaguardar las infraestructuras críticas e impide dar una conceptualización amplia y bien sustentada por carecer de un marco jurídico en esta materia, políticas de Estado para brindar protección, no contar

con una descripción precisa de los sectores que conforman las infraestructuras críticas, ausencia de un plan nacional para tal fin, debilidades en la vinculación entre agencias de *inteligencia* del Estado. No obstante, dentro de ese contexto, las únicas infraestructuras que han sido sectorizadas y definidas son las cibernéticas y cuentan con planes específicos para protegerlas.

En Colombia, por ejemplo, quizás por la misma condición que desde décadas atrás viene enfrentando, la ha llevado a definir y considerar la infraestructura crítica como el conjunto de procesos interconectados que hacen vulnerable a una nación (Hurst, Fergus y Merabti, 2018). No obstante, según lo expresado por los mencionados autores, actualmente la infraestructura tecnológica presenta un elevado índice de riesgo, ya que, debido al avance experimentado por la tecnología digital, se han abierto espacios que afectan significativamente la seguridad y protección de los diferentes sistemas que integran las infraestructuras críticas.

En el catálogo de Infraestructuras Criticas Cibernéticas de Colombia desarrollado por parte del Comando Conjunto Cibernético de las Fuerzas Militares de Colombia en el año 2016 se identificaron que en el país existen trece sectores que hacen parte de la Infraestructuras Critica dentro de los cuales se establecieron el gobierno, la Seguridad y Defensa, las TIC, la electricidad, el sector financiero, la educación, el sector minero energético, la industria incluyendo el comercio y el turismo, el medio ambiente, la salud, el agua, el transporte y la agricultura (Fuerzas Militares de Colombia, 2016).

De esta manera, se entiende que las infraestructuras críticas en Colombia, así como en otros países, involucra un conjunto de procesos interconectados entre sí, que abarca no solo las redes eléctricas, sistemas de agua, transporte, entes públicos y gubernamentales, sino también las plataformas digitales, las cuales se han convertido en uno de los objetivos centrales de los grupos armados irregulares.

Infraestructura crítica de interés

Los grupos armados irregulares constituyen la principal amenaza para la integridad social, económica y política de Colombia. Tal como se ha referido anteriormente, estas organizaciones desde hace décadas han venido perpetrando ataques en puntos que son estratégicos para los entes gubernamentales y cualquier agresión en contra de algún componente de las infraestructuras críticas, representando desequilibrio para el país. Dentro de ellos se resaltan sectores químicos, transporte, energético, administrativo. Además de las plantas de tratamiento de agua, sector de telecomunicaciones, salud, nuclear, tecnología y operaciones, sistemas tributarios, financieros, empresas alimenticias, instituciones gubernamentales (Mendoza & Díaz, 2019).

Hernández (2016), hace referencia al tema de las infraestructuras críticas de interés en Colombia y explica que dentro de ellas pueden distinguirse doce sectores que son

considerados puntos estratégicos para el país: Sistemas financieros y tributarios (bolsa de valores, banca, inversiones), Tecnologías de la Información y la Comunicación (Tics), sector sanitario, centrales y redes eléctricas, espacio, Alimentación, industria nuclear, instalaciones de investigación, agua (tratamiento de aguas servidas y redes, embalses, almacenamiento), industria química, sector de transporte (redes de transporte público, ferrocarriles, aeropuertos, sistemas de control del tráfico, puertos e instalaciones intermodales), administración (activos, redes de telecomunicaciones e información, instalaciones, servicios básicos, lugares centrales y monumentos nacionales).

Sobre este particular, la Fundación Ideas Para la Paz (2017) señala que la producción de hidrocarburos representa una importante fuente económica para los grupos armados organizados en Colombia, Organizaciones delincuenciales, las Farc, entre otros grupos de esta índole. Estos grupos, en su mayoría, han obtenido cuantiosas ganancias de este sector mediante actos de extorsión, cobro de vacuna por resguardo de infraestructura, captación de *regalías* y es una de las infraestructuras que más ataques ha recibido por parte del ELN.

Por su parte, Ospina y Sanabria (2020) consideran que la nueva tentación para los grupos armados organizados, ELN, Bandas delictivas, narcotráfico, sin lugar a dudas son las infraestructuras tecnológicas, ya que la evolución de las redes y telecomunicaciones como el internet, nuevas tecnologías y sistemas de información, no solo ha generado cambios significativos en muchos ámbitos de la sociedad, sino que ha producido serias y aceleradas transformaciones, crisis a nivel social, modificaciones en los mercados financieros, energéticos, preocupaciones políticas, cambios culturales y conmociones en otros contextos, como el educativo, por ejemplo.

Evidentemente, que todos esos avances no solo han significado progreso para Colombia, sino problemas, pues se ha creado una fuerte dependencia de las tecnologías que inevitablemente conduce a un manejo de información vulnerable, situación que en los actuales momentos es aprovechada por los grupos armados ilegales; para aumentar y perpetrar ataques contra la confidencialidad de la información de empresas públicas y privadas, entes gubernamentales y presidencia de la república, poniendo en riesgo la integridad, protección y seguridad de la nación.

En armonía con lo expuesto por Ospina y Sanabria (2020), Lozano (2015) afirma que la apertura tecnológica abrió nuevas alternativas para atacar las infraestructuras críticas. Con la llegada y uso de las plataformas digitales, los grupos irregulares vieron oportunidad para continuar ejerciendo presión, mediante ciberataques a estas plataformas, con la única intención de causar daño a las redes y con ello, lógicamente a los sistemas interconectados del sector salud, petroquímico, medio ambiente, energético, hídrico, educación, defensa, industria química, minero, financiero, transporte, tributario, gobierno, entre otros, que son la base fundamental para el funcionamiento efectivo de un país.

Capacidades de los factores armados de inestabilidad de Colombia para afectar la infraestructura crítica colombiana a través del ciberespacio

Los grupos armados irregulares que han existido en Colombia y que actualmente son considerados como Factores Armados de Inestabilidad, han buscado diferentes métodos para atacar los sectores estratégicos del país, esto con la única intención de llamar la atención de los gobernantes, hacer exigencias o simplemente obtener beneficios económicos para financiar sus crímenes y mantenerse.

Con el paso de los años y con la llegada del desarrollo tecnológico, se abrieron posibilidades innovadoras para que estos grupos delictivos reorientaran sus técnicas y perfeccionaran sus estrategias de ataque, y buscaran los medios necesarios para capacitarse en el manejo del ciberespacio y así poder migrar sus planes hacia las plataformas digitales, por ser una alternativa para poder manipular todos los sectores interconectados a la red digital. Pero ¿Realmente los factores armados de inestabilidad que hacen vida en Colombia, están en capacidad de utilizar el ciberespacio para atacar la infraestructura crítica?

Al respecto, Cardozo (2019) sostiene que las plataformas tecnológicas representan una oportunidad novedosa para reorientar el modus operandi de los grupos armados organizados en Colombia. Esta afirmación obedece a dos teorías manejadas por la autora: la primera de ellas se orienta al flujo de información que circula a través de las redes y la segunda al nivel de vulnerabilidad de las infraestructuras tecnológicas para ser atacadas y afectar otros sectores estratégicos del país.

Lo anterior conduce a inferir, que los grupos armados organizados, grupos delictivos, ELN, FARC y otras organizaciones de este tipo, se han dado a la tarea de desarrollar habilidades para manejar el ciberespacio y dirigir sus ataques a través de las redes, tal como lo expone Mendoza y Díaz (2019) quien afirma que las infraestructuras críticas colombianas han sufrido fuertes ciberataques, claro hasta ahora no alcanzan los niveles de ataques perpetrados en otros países, pero si ha causado daños severos en algunos sectores, como el eléctrico, cuyo sistema ha sido violentado para extraer información relevante y utilizarla para beneficios propios.

En esa dirección, Cujabante et al. (2020) puntualizan que los grupos irregulares han asumido el desafío que imponen las nuevas TICS, han desarrollado las habilidades suficientes para ejercer control y manipular los protocolos de red a su conveniencia. Según los mencionados autores, el sistema eléctrico es uno de los sectores donde más se ha manifestado la capacidad de los grupos armados organizados, grupos delincuenciales, entre otros, para manejar los protocolos de red y causar caos en las centrales eléctricas y subestaciones.

Los ataques perpetrados a las estructuras críticas lo han hecho a través de la web, denegación de servicios, atacando las bases de datos SQL Injection, ambientes físicos

de *usuarios internos* mediante puertos USB, XSS o sitios de manipulación de códigos Script. Otro aspecto relevante que argumenta Mendoza y Díaz (2019), es que estas organizaciones pueden reclutar personal especializado en el manejo de equipos que usan habitualmente en países terroristas y que hoy día se emplean en Colombia para inhabilitar sectores estratégicos de las infraestructuras críticas, como es el caso de los equipos de alta tecnología Siemens S5 empleado para sabotear el sistema eléctrico por parte del ELN.

Ahora, ¿Por qué emplear el ciberespacio para atacar la infraestructura crítica? Como se ha venido señalando en líneas anteriores, las tecnologías de la información y la comunicación, dentro de todo este escenario de ilegalidad, viene a constituir una herramienta viable para poner en práctica el ciberataque y fijar un objetivo de ataque: las infraestructuras críticas, pues mediante su utilización pueden sembrar el terror, amenazar, robar información, buscar financiamientos. En otras palabras, generar un caos nacional y paralizar gran parte del país (Rudner, 2013).

De allí, que las tecnologías de la información y la comunicación se convierten en un punto de ataque estratégico perfecto para estos grupos armados que actúan al margen de la ley, ya que pueden usarlas para planificar ataques cibernéticos, tal como lo explica Rudner (2013), quien asevera que son un mecanismo empleado no solo como soporte funcional a las redes de *comunicación*, sino que de ella depende en gran medida la infraestructura crítica que está bajo el control estatal, y esto lógicamente la hace atractiva ante los ojos de estas organizaciones para ejecutar sus planes.

Ahora, el problema real es que la funcionalidad y caracterización de estas, así como el monitoreo y manejo, están anclados a un sistema que actúa en cascada, esto significa que son procesos dependientes de una misma plataforma y al atacar una de estas infraestructuras el daño se extiende a los demás sectores, dejando consecuencias considerables que afectan la seguridad, obstaculiza las actividades habituales de las empresas y ciudadanía en general, así como el funcionamiento de la nación.

Sobre este particular, Cujabante et al. (2020) explican que aún y cuando los grupos irregulares hacen uso de las tecnologías a sus anchas, tienen la habilidad para ejecutar ataques terroristas en contra de las infraestructuras cibernéticas, no hay evidencia certera que compruebe que se hayan puesto en práctica acciones de este tipo, ni siquiera organizaciones de la envergadura criminal de Al Qaeda han accionado mecanismos bajo esta modalidad, esto a pesar de tener la experiencia y capacidad suficiente para llevarlo a cabo.

Hasta acá se entiende que los Factores Armados de Inestabilidad en Colombia, no solo están capacitados tecnológicamente medianamente para utilizar el ciberespacio en sus operaciones criminales, sino que viven en la búsqueda de alternativas que les ayude a perfeccionar sus estrategias de ataque y no se limitan a extorsionar, reclutar personas,

o cualquier otra actividad de este tipo, por el contrario, sus horizontes han superado barreras, traspasado fronteras, el peligro se ha incrementado y vulnera la seguridad del Estado.

Por su parte, Morán (2017) difiere de lo planteado por Cujabante et al. (2020) y argumenta que la mayoría de estos grupos armados, al margen de la ley, no cuentan con el personal competente para manejar idóneamente las nuevas tecnologías de la información y la comunicación. No obstante, existe una inconsistencia en la protección que brinda el Estado a las infraestructuras críticas y esto de algún modo incrementa el riesgo de manipulación por parte de grupos delincuenciales, pues dada la sensibilidad de los sistemas, cualquier persona sin preparación ni formación puede operarlos, por tanto, no se trata de capacitación, sino de la estabilidad de las infraestructuras críticas para salvaguarda de los ataques cibernéticos.

De este modo, se infiere que los ciberataques representan una de las mayores amenazas para la seguridad de las Tecnologías de la Información y la Comunicación, puesto que a través de ellas es posible entramar cualquier tipo de complot hecho por organizaciones o personas para atacar los sistemas informáticos como redes de computadoras, infraestructuras, bases de datos alojadas en servidores con conexión remota, actos perversos ejecutados por agentes anónimos; quienes hackean sistemas vulnerables para robar información confidencial de organismos oficiales, empresas públicas u organizaciones estratégicas para el manejo de la economía del país.

Resumiendo, el planteamiento del señalado autor se tiene que los ataques a las infraestructuras críticas a través del ciberespacio no debe medirse por la capacidad de las organizaciones armadas que actúan de forma ilegal, por el contrario, debe ser analizada desde el punto de vista de la sensibilidad y la inestabilidad de protección que brinda el Estado, pues muchos de ellos son ejecutados por personas sin los conocimientos tecnológicos, pero son individuos que han detectado las debilidades de la infraestructura y la aprovechan para desestabilizarla y violar la seguridad de la nación.

Es evidente que dentro de este escenario ha surgido una infinidad de controversias, opiniones encontradas, posturas que difieren unas de otras, pero que tienden a conducir a un solo objetivo: determinar si ¿Realmente los ataques perpetrados por grupos armados irregulares a la infraestructura crítica a través del ciberespacio, responde a la capacidad de estas organizaciones? O simplemente son el resultado de la inestabilidad de los sistemas para monitorear y controlar la seguridad de las mismas. De ahí la importancia de replantearse si es la capacidad de quienes integran estas bandas delictivas lo que marca los ataques o es falta de vigilancia por parte del Estado. La amenaza siempre ha estado allí, así como la presencia de los factores armados de inestabilidad, el único componente nuevo es el uso del ciberespacio para incrementar los ataques y perfeccionar las técnicas (Montoya, 2017).

Ahora, no se trata de dar respuesta aleatoria, por el contrario, es establecer a través de los hechos y acciones perpetradas por cada una de las organizaciones armadas de manera ilegal que han operado durante décadas en Colombia y nuevas agrupaciones surgidas luego del Acuerdo de Paz. En ese contexto, el ciberespacio es un ambiente que posee atributos particulares que se evidencian en los elementos que lo integran, la conectividad, la accesibilidad, y son esas cualidades lo que convierte en una potente amenaza para el Estado y sociedad, por tanto, se concluye que su uso no puede estar atribuido exclusivamente a las capacidades y/o habilidades de los factores armados de inestabilidad, sino también a otros elementos (Sánchez, 2020).

Determinar los riesgos a la seguridad y defensa nacional en el ciberespacio por parte de los Factores Armados de Inestabilidad Riesgos de Seguridad y Defensa

Conceptualización

El abordaje de riesgos de seguridad y defensa implica un acercamiento previo a las conceptualizaciones de seguridad y defensa, para dilucidar el escenario dentro del cual se gesta la inseguridad de un Estado o nación. Ciertamente, que la utilización de ambos términos engloba elementos similares, que hacen alusión a la defensa y protección de los *intereses de la sociedad,* no obstante, es pertinente tener claro que aspectos del contexto marca la diferencia entre ambas definiciones.

Al respecto, Tello (2020) sostiene que la seguridad hace referencia a la protección ante el peligro que pueda producirse una ofensiva militar, restricciones económicas, coacción política, logrando con sus acciones autonomía social para que el Estado preserve su desarrollo y avance. En ese sentido, engloba y asocia la capacidad económica, el potencial militar, el desarrollo social, la reciprocidad política a través de la *diplomacia bilateral y multilateral,* y el perfeccionamiento de las ciencias y las nuevas tecnologías de la información y la comunicación.

Por su parte, Briones (2015) acota que es una condición que lleva a conseguir el funcionamiento habitual del Estado, de cara al desarrollo de sus actividades y gestiones, destacando entre ellas el desarrollo de la nación y la seguridad de la sociedad, en aras de ser garante del bienestar colectivo a nivel nacional. Ahora, al concentrar el tema de seguridad en el ciberespacio, se observa, que en el escenario actual no solo representa una obligación propia u organizacional, por el contrario, es un asunto de Estado que implica la soberanía nacional y repercute en la gobernanza gubernamental (Choucri, Nazli, y Clark, 2013).

Asimismo, juega un importante papel en el resguardo de la información de las personas, en la integridad económica de la nación, en las políticas de Estado y evidentemente a nivel internacional (Government of Canada, 2010; Nye Jr. y Welch, 2013). En fin, los entes gubernamentales están llamados a asumir el reto de la seguridad del ciberespacio, así como salvaguardar y asegurar la accesibilidad, utilización y espacios a la sociedad en el contexto virtual, teniendo presente las implicaciones regionales, gubernamentales y globales, esto desde una perspectiva particular.

Partiendo de la conceptualización de seguridad, puede entenderse que la defensa viene a representar el recurso a través del cual el Estado garantiza la seguridad, esto desde una perspectiva generalizada. Para ello, pone en práctica acciones y/o medidas orientadas a vencer las amenazas y riesgos, por tanto, es la capacidad de la nación para salvaguardar los intereses y "objetivos nacionales", por medio de la disposición y operación organizada de las potencias, fortalezas morales y tangibles con las que cuenta el Estado (Faundes, 2017).

De esta manera, se concibe la defensa como una medida estratégica de dirección política gubernamental, empleada para hacer frente a las amenazas y riesgos a través operaciones militares, económicas, diplomáticas, entre otras. Esta concepción comprende de la unificación de los intereses del Estado y la sociedad, siendo aceptada como un mecanismo efectivo de persuasión, resguardo y lógicamente, para responder y garantizar constantemente la soberanía, la autonomía de la nación y la integridad jurisdiccional (Díaz, 2018).

Como base al análisis precedente, puede inferirse que el riesgo a la seguridad y la defensa se articula a las amenazas a las cuales se expone una nación de cara al negocio ilícito de sustancias estupefacientes y drogas, terrorismo, tráfico de armas y municiones, secuestros, extorsión, ciberataques, entre otros, (Huertas, 2015).

En ese mismo orden de ideas, Torrijos y Balaguera (2019) argumenta que el riesgo a la seguridad y defensa nacional debe ser vista como una concepción que guarda relación con un elevado nivel de desconfianza, donde no se tiene certeza de las consecuencias de una operación específica, por tanto, se entiende que existe una importante vinculación entre el peligro al cual se expone el Estado, la situación que genera el riesgo y el grado de inseguridad de los recursos que posee la nación para garantizar la seguridad y la defensa nacional.

Riesgos en el ciberespacio

El ciberespacio debe concebirse, no solo como un espacio para la *interacción social,* sino también como una dimensión de superioridad que da poder a quienes la controlan. Inicialmente, se proyectó como entorno o escenario virtual para interactuar y

comunicarse con otras personas, pero, con el paso del tiempo, el crecimiento e innovación de las tecnologías de la información y la comunicación ha sido notoria ya no se entiende solamente como ambiente virtual que servía de enlace para encuentros o realzar actividades comerciales, sino que paso a ser un espacio complejo y de uso común, esto conforme a lo expuesto por la (Organización del Tratado del Atlántico Norte, 2016).

Es así que, el ciberespacio no solo ha ganado importantes espacios para la comunicación, transacciones o cualquier otra actividad relacionada con el comercio, sino que ha sido utilizado como un dominio de guerra por los Estados legalmente consolidado y por grupos irregulares armados, llegando a constituirse para estos últimos como un sustituto de los contextos empleados tradicionalmente en los conflictos armados (Organización del Tratado del Atlántico Norte, 2016).

Ahora, al analizar la seguridad a nivel de ciberespacio, se observa que el tema ha cobrado relevancia, ya que según cifras presentadas por Klimburg (2012), para el año 2020 se esperaba que un promedio de 1,7 millones de individuos se interconectara a través de las redes, esto con la finalidad de establecer relaciones comerciales, institucionales o simplemente para abrir nuevos canales de comunicación. Conforme a esta proyección, el envío de correos electrónicos pudo haber llegado alcanzar los 294 mil millones por día, generando, además, un aproximado de 168.000.000 de DVDs de información, y esto obviamente aumenta el riesgo de un ciberataque a cualquier nivel.

Esto significa que el ciberespacio pasa a convertirse en una moneda de doble cara, puesto que la evolución que ha experimentado las Tecnologías de la Información y la Comunicación no solo le permite a los entes gubernamentales, militares y civiles utilizar los recursos que ofrece para gestionar sus operaciones, sino que les facilita la imposición de poder a través del espacio a grupos que actúan al margen de la ley, sin necesidad de portar un arma para someter, controlar y lograr su objetivo, es decir, el ciberespacio pasó a configurarse como el escenario idóneo para promover y fortalecer el conflicto armado en Colombia (Gómez, 2012).

Según lo expuesto por Gómez (2012), los riesgos a los que se expone el ciberespacio han cobrado una fuerza enorme y eso por supuesto que causa preocupación, porque a los recursos de ataque no solo tiene acceso el Estado, sino cualquier persona que pueda acceder a la red, y por supuesto que pone en la infraestructura crítica como punto vulnerable de una nación.

Sintonía con lo anterior, Feliu (2012) advierte que la principal amenaza en el ciberespacio apunta hacia la información, pues para los grupos irregulares es un elemento con un alto valor, y más si se trata de datos vinculados a la defensa y seguridad de la nación. Señala, que, a diferencia de los riesgos tradicionales, en el ciberespacio el peligro

aumenta, ya se puede llegar a cubrir espacios inimaginables dentro y fuera de la nación y penetrar zonas de defensa, atacar, extraer información o simplemente neutralizar al enemigo asaltando lugares estratégicos que constituyen el equilibrio del Estado, como es el caso de la infraestructura crítica.

En ese mismo orden de ideas, el estudio de Torres (2018) reafirma las proyecciones de Klimburg (2012) y Government of Canada (2010) quienes proyectaron que para el 2020 países con alto índice de conflictos internos, como Colombia, por ejemplo incrementarían el riesgo a sufrir ataque o saboteo de la infraestructura crítica a través del ciberespacio, y esto se debe a que la estimación de la población mundial con conexión a internet estaría por el orden de los 5 mil millones, una conexión global a la red de 60%, lo cual significa que el uso de dispositivos se ubicaría en 50 mil millones de equipos tecnológicos (un equivalente a 10 dispositivos por cada persona), afectando a la economía mundial en un 10%, llegando así a estar expuesto a riegos, peligros, ciberataques, peligros y amenazas en un 56,5% aproximadamente.

Por su parte, López (2018) hace mención a los riesgos híbridos y explica que es una amenaza potencial para el Estado que proviene de la habilidad y disposición de un actor para aplicar su capacidad de una forma focalizada y al mismo tiempo acoplada para atacar dimensiones militares, económicas, políticas, social, tecnológicos, entre otras y de ese modo fomentar sus intereses.

De allí que, el ciberespacio esté presto para ejecutar acciones de este tipo e incrementar los niveles de riesgos, pues ya no se trata ni se está frente a enfrentamientos militares, sino que los actores armados irregulares aprovechan estos espacios para atacar las fuerzas militares con otros mecanismos como el ataque cibernético, vectores de imposición económica, manipulación de datos, vulnerabilidad a la privacidad, ataque a las bases de datos, suplantación de identidad, entre otros.

Ahora, al analizar el contexto colombiano y articularlo con los riesgos del ciberespacio, se observa, que este ha sido afectado por una diversidad de manifestaciones criminales, que sin lugar a dudas han calado negativamente trayendo consigo inestabilidad al país.

De esa manera, se asume que los riesgos en el ciberespacio han dejado de ser amenazas convencionales, han trascendido barreras y profundizando sus enfoques habituales, irregulares y terroristas, para transformarlos en tácticas innovadoras de ataque y desestabilizar al gobierno regional y nacional, para promover actividades ilícitas como contrabando, venta de armas, municiones, explosivos o cualquier otro acto delictivo que les permita financiar sus operaciones y fortalecer sus organizaciones delincuenciales (Escuela Superior de Guerra, 2017).

Estadísticas de Afectación de Infraestructuras Críticas en Colombia por parte de los Factores Armados de Inestabilidad

La utilización de las nuevas tecnologías de la información y comunicación han venido mostrando un marcado incremento, y esto evidentemente ha generado un marcado aumento de amenazas y ataques a través de las redes, afectando no solamente los activos del Estado, instituciones tanto públicas como privadas, infraestructuras, sino la seguridad del ciudadano común. Durante las últimas décadas Colombia se ha convertido en un foco o blanco potencial de grupos armados irregulares para perpetrar ataques desde el ciberespacio, afectando diferentes sectores estratégicos que causa preocupación al gobierno, por las repercusiones negativas que deja sobre el desarrollo socioeconómico del país y la sociedad en general.

Respecto a los índices de afectación de algunos sectores que integran la infraestructura crítica en Colombia, el Consejo Nacional de Política Económica y Social (CONPES) (2016) expuso que solamente en el 2015 el gobierno se vio afectado por amenazas, riesgos y peligros en 23,9%, educación 9,2%, sector económico y financiero 9,0%, empresas e industrias 6,6%, defensa y seguridad 5,8%, plataformas digitales y redes de comunicación e información 1,4%, medios de comunicación 0,9%, salud 0,1%, otras infraestructuras 0,7%.

En ese mismo orden de ideas, El tiempo (2017), reseñó que para el 2017 un aproximado de doce (12) empresas del sector económico, tanto públicas como privadas, sufrieron ataques de grupos irregulares mediante el uso de ramsomware, el objetivo era robar información de estas organizaciones y solicitar pagos por la tenencia o secuestro de los datos en posesión de estas organizaciones delictivas; siendo una de las más afectadas el Instituto Nacional de Salud, esto en conformidad con lo expuesto por el Heraldo (2017). No obstante, los índices de denuncias al respecto fueron muy bajas (40%), respecto a otros tipos de delitos reportados. Por su parte, el MINTIC (2017) reportó que las repercusiones que han dejado los ataques cibernéticos solamente en el sector industrial se ubican por el orden de 22% aproximadamente.

De igual modo, la Policía Nacional de Colombia (2017) presentó un balance en el cual muestra que el 8% del sector financiero fue víctima del ciberataque, destacando entre ellos: tráfico de datos financieros a nivel personal y gubernamental, comercialización de información de tarjetas de débito y crédito, esto sin dejar de lado los ataques financieros perpetrados a las entidades del Estado. La infraestructura tecnológica: correo electrónico, redes sociales, transacciones y aplicaciones bancarias, entre otras, alcanzó el 32,59%.

Para el año 2014 el 92% de los delitos informáticos que sufrió Colombia se concentró directamente en la ciudadanía, significa que la mayor cantidad de ataques estuvo

dirigida hacia el sector eléctrico, agua potable, salud, educación, gas y transporte, (Policía Nacional de Colombia, 2017b), mientras que para el 2016 los daños causados a la infraestructura crítica alcanzaron el 57%, con una concentración en el sector industrial del 28%, esto según cifras presentadas por el MINTIC (2017).

Para el 2019, los ataques a las infraestructuras críticas alcanzaron 54% superando las cifras registradas por el MINTIC en el 2018, y la mayor concentración estuvo en Bogotá, Medellín, Cali y Barranquilla, cobrando fuerza los ataques hacia el sector financiero 16%, tecnología, redes y comunicaciones 14% e industria 24%, (El Tiempo, 2019).

En fin, los reportes de ataques a las infraestructuras críticas entre los años 2019 y 2020, muestran que la nueva tendencia de los delincuentes es la inteligencia artificial, pues la mayoría de los asaltos a las plataformas públicas y privadas a través del ciberespacio denotan nuevos y sofisticados métodos para delinquir y causar daño al Estado y sociedad civil en general (Policía Nacional de Colombia, 2019).

Riesgos a la Seguridad y Defensa de Colombia en el Ciberespacio

Los riesgos a la seguridad y defensa de Colombia en el ciberespacio, sin lugar a dudas se vinculan con el avance vertiginoso de las Tecnologías de Información y Comunicación. Para comprender el riesgo, es imprescindible asimilar que con la llegada del internet se abrió un nuevo camino, no solo para comunicarse, interactuar o establecer modelos innovadores de negocios, sino que también se apertura un espacio que daba cabida a realizar otro tipo de actividades en la web al margen de la ley, esto desde una perspectiva particular.

Dentro de ese contexto resalta las repercusiones que este nuevo sistema de comunicaciones tendría sobre la política, pues también era una puerta para mejorar las relaciones dentro y fuera del territorio nacional, que sin lugar a dudas ha sido aprovechada de manera racional para establecer alianzas estratégicas y buscar vías alternas para fomentar el desarrollo económico de la nación (Becerra y León, 2019).

El problema real, de la innovación tecnológica, no son los recursos que puso a disposición de los usuarios, sino el tratamiento, el manejo distorsionado que se le empezó a dar y las afectaciones dejadas al Estado, muestra de ello se evidencia, en el caso de Colombia en los ataques terroristas perpetrados contra sitios estratégicos de la nación, a través del ciberespacio, y eso sin lugar a dudas denota un alto nivel inseguridad y crea incertidumbre.

Al respecto, Realpe y Cano (2020), argumentan que los riesgos cibernéticos a los cuales está expuesta la seguridad y la defensa de Colombia son numerosos y de diversas modalidades, ya que las tecnologías no solo se prestan para llevar a cabo operaciones sencillas, sino que permite transformar cualquier radio de operación en fracción de

segundo, aceptando, además el uso multitudinario de las tecnologías para producir una interrupción en los sistemas de seguridad y defensa.

Agrega, que la realidad de los ataques a través del ciberespacio es que los adversarios no dan tregua, viven en una constante actualización de los métodos técnicos y estrategias para mejorar las formas de sometimiento, crear un escenario idóneo que les sirva de soporte para facilitar el logro de sus objetivos, de cara a los mecanismos que establecen las autoridades del país. De modo que, cualquier reflexión tiene y obligatoriamente debe partir de admitir; que las tecnologías no van a cambiar para favorecer la seguridad y la defensa del Estado de los ciberataques, por el contrario, es la Defensa Nacional que debe examinarse y desarrollar nuevos instrumentos de defensa basados en el dinamismo, vulnerabilidades y desafíos que presenta el ciberespacio.

De acuerdo a lo expresado por Casas (2016), la globalización y el desarrollo tecnológico han producido características muy peculiares en el tipo de riesgo, abarcando escenarios espaciales, temporales o simplemente sociales e implica todo acontecimiento que puede generar consecuencias distantes a las fronteras de una nación y de los cuales se deslinden efectos severos.

En esa dirección, Becerra y León (2019) acotan que la dimensión del riesgo de la seguridad y la defensa de cara al ciberespacio en Colombia es directamente proporcional a la disposición geoestratégica, así como el acceso a medios como la información, que implica. Al mismo tiempo, una emulación constante determinar no solo los riesgos nacionales, sino también fuera de las fronteras.

Ese mismo contexto, a buscar soluciones que pueden generar riesgos, pues no hay alternativas que por sí misma aseguren el éxito, por el contrario, intrínsecamente el riesgo estará latente y depende en gran medida de la magnitud de la amenaza y de la diferenciación entre los escenarios donde se gesta (Pérez, 2016). Es así que, los riesgos muestran una dispersión extensa y en ocasiones inconmensurable e involucra actos terroristas, problemas ambientales, peligro nuclear, entre otras.

De esa manera, los riesgos producen incertidumbre a nivel de seguridad y defensa, ya que el Estado enfrenta no solo amenazas físicas sino también lógicas, las cuales al articularse entre sí o de manera aislada pueden materializarse y causar daños graves sobre los bienes de la nación y afectar significativamente a la ciudadanía. De allí que, las nuevas tecnologías ponen a disposición de los usuarios dos escenarios: el primero de ellos para proveer de herramientas de defensa y seguridad al Estado, el segundo con énfasis en la vulnerabilidad de los sistemas de seguridad y defensa de Colombia en el ciberespacio y los riesgos a los cuales se expone.

En relación con lo anterior, Becerra y León (2019) sostienen que el principal problema que presenta Colombia en esta materia es que no cuenta con los recursos pertinentes a

nivel nacional para manejar y garantizar la seguridad a través del ciberespacio en aras de optimizar la defensa de la nación ante cualquier ataque cibernético que ponga en riesgo la integridad de la nación y afecte la estabilidad de sus habitantes, en esa dirección, deducen que ese vacío no le permite tener una óptica estratégica, para acoplar sus funciones y operaciones institucionales conforme a los objetivos nacionales establecidos para responder a la seguridad y defensa en el ciberespacio de manera eficiente y eficaz (Realpe y Cano, 2020).

En líneas generales, las fuerzas militares colombianas deben concebir el ciberespacio como un escenario estratégico, táctico y operativo, que les permita estructurar y adecuar sus mecanismos de seguridad y defensa a lo que demanda el ámbito tecnológico en materia de ciberdefensa y ciberseguridad, para poder afrontar los desafíos actuales y garantizar la seguridad nacional, esto de una visión personal.

Conclusiones

Los factores armados de inestabilidad son organizaciones que durante décadas han venido atentando contra la seguridad integral de Colombia, afectando no solo los intereses de la sociedad civil, sino también los activos de la nación que brindan soporte a la estabilidad social, económica, política y cultural de la nación. Es así que, la revisión sistemática de literatura permitió responder a los objetivos propuestos inicialmente y concluir:

En cuanto a la caracterización de los factores armados de inestabilidad en Colombia y sus capacidades, se estableció que en el país existe un elevado número de grupos armados que continúan delinquiendo y sometiendo a la población, encontrándose entre ellos: los Grupos Armados Organizados (GAO), los Grupos Armados Organizado (GAO ELN), los Grupos Delincuenciales Organizados (GDO) y los delitos Trasnacionales (DT), el tráfico de armas, municiones y explosivos, cada uno de ellos con un objetivo y visión diferente para establecer control dentro del territorio colombiano y regiones fronterizas.

En cuanto a sus capacidades, se determinó que son organizaciones que han ido mutando conforme a sus necesidades y requerimientos de financiamiento y control sobre sectores bajo su dominio y otros que quedaron a la deriva durante el proceso de desmovilización y que son zonas estratégicas para expandir el negocio ilegal, bien sea de narcotráfico, secuestros, venta de armamento o cualquier otra actividad ilícita que les permita lucrarse y mantenerse en el escenario delincuencial de una manera fortalecida. De esta manera puede afirmarse, que son organizaciones que han optado por mejora sus mecanismos de ataque o simplemente reclutando personal con capacidad necesaria para competir en el ámbito tecnológico con el Estado y otros grupos armados con el dominio y control del poder. En líneas generales, se infiere que los factores armados de inestabilidad sí cuentan con la suficiente capacidad para manejar el ciberespacio y causar daños a los activos de la nación.

En relación con el segundo objetivo, referente al análisis e identificación de los sectores de la infraestructura crítica del país que pueden ser de interés para los factores armados de inestabilidad en Colombia, se encontró que estos grupos concentran su atención en aquellos activos de mayor interés para el Estado, como son: los sectores químicos, transporte, energético, administrativo. Además de las plantas de tratamiento de agua, sector de telecomunicaciones, salud, nuclear, tecnología y operaciones, sistemas tributarios, financieros, empresas alimenticias, instituciones gubernamentales, en fin, este tipo de organizaciones siempre buscaran y apuntaran hacia los puntos estratégicos que puedan debilitar al gobierno.

El tercer objetivo se concentró en determinar los riesgos a la seguridad y defensa nacional en el ciberespacio por parte de los factores armados de inestabilidad. A saber, este tipo de organizaciones por su propia naturaleza ya representan un riesgo para la seguridad y defensa de Colombia, desde hace décadas. El problema actual es que el avance tecnológico abrió nuevos espacios, que no solo permitió ampliar el horizonte comunicacional, sino que indirectamente puso a disposición de sectores que actúan al margen de la ley nuevos mecanismos para mejorar sus estrategias tradicionales y migrarlas al ciberespacio, lo cual representa un riesgo eminente para el mundo.

En el caso específico de Colombia, la indagación bibliográfica puso en evidencia que, la apertura tecnológica ha contribuido a que la seguridad y defensa nacional afronte mayores riesgos hoy, esto si se compara con las amenazas y peligros que enfrentaba décadas atrás, ya que el riesgo estaba presente, pero el alcance de los ataques eran inferiores a los que pueden perpetrar a través del ciberespacio. Lo realmente importante, es tener presente que ante el auge tecnológico, la seguridad y defensa en Colombia se encuentra en riesgo permanente, porque los factores armados de inestabilidad se han dado a la tarea de perfeccionar sus métodos, técnicas y estrategias de ataques, siendo una de ellas los ciberataques.

Resumiendo, se tiene que los factores armados de inestabilidad en Colombia continúan delinquiendo dentro del territorio, a pesar de todos los esfuerzos hechos por los entes gubernamentales para erradicarlos. Actualmente, son organizaciones que se han fortalecido y adoptado nuevas modalidades de amenazas, ataques, reclutamiento, entrenamiento, financiamiento y comercialización de mercancía ilícita (contrabando, drogas, armas, municiones, entre otras), en otras palabras, el peligro está latente y con alcances superiores a los que tenían anteriormente, pues se han dotado de mecanismos innovadores para perfeccionar sus mecanismos de sometimiento y control frente al Estado.

La realidad es que esta situación ha llevado a que la seguridad y defensa de la nación en el ciberespacio sea inestable y se debe a la falta de preparación de los entes encargados de la seguridad para afrontar los desafíos que implica el manejo del ciberespacio para proteger la nación. Aún falta mucho por hacer, por aprender y más allá por poner en

práctica, para superar los obstáculos que simbolizan las tecnologías como herramienta de ataque a los activos de un país.

Declaración de divulgación

El autor declara que no existe ningún potencial conflicto de interés relacionado con el artículo.

Autor

Gabriel Andrés Acosta Lizarazo. Oficial del Ejército: Magister en Escuela Superior de Guerra General "Rafael Reyes Prieto", Colombia. Especialista en Administración de Recursos Militares para la Defensa Nacional, Escuela de Armas Combinadas del Ejercito, Colombia. Profesional en Ciencias Militares, Escuela José María Córdova, Colombia. Cursos de Ley requisitos para ascenso establecidos por la Fuerza para los grados de Capitán y Mayor.

Orcid: https://orcid.org/0009-0007-3205-2680 Contacto: acostaga@esdeg.edu.co

Referencias

Aguirre, A. (2017). *Ciberseguridad en infraestructuras críticas de información* [Tesis de pregrado]. (Universidad de Buenos Aires). http://bibliotecadigital.econ.uba.ar/download/tpos/1502-115_AguirrePonceAA.pdf

Becerra, J., & León, I. (2019). La seguridad digital en el entorno de la fuerza pública diagnósticos y amenazas desde la gestión del riesgo. En Escuela Superior de Guerra (Ed.), *La Seguridad en el Ciberespacio: Un desafío para Colombia* (Primera Ed). https://doi.org/10.25062/9789585216549

Blanco D., Gravito R., y Trujillo, J. (2012). *Organizaciones de delincuencia transnacional, una amenaza para la seguridad nacional: caso BACRIM.* Repositorio Institucional ESDEG. https://esdegrepositorio.edu.co/handle/20.500.14205/2981

Briones, S. (2015). Conceptualizando riesgos y amenazas: una mirada al desarrollo terminológico y sustancial. *Revista Ensayos Militares, 1*(1), 217-230.

Cancillería de Colombia. (2019). *El comercio ilícito de armas pequeñas y armas ligeras en todos sus aspectos*. https://www.un.org/disarmament/wpcontent/uploads/2019/08/COLOMBIA.pdf

Cardozo, T. (2019). Análisis del riesgo de la infraestructura de telecomunicaciones del sistema departamental de gestión del riesgo de desastres de Cundinamarca. *Tecnología y Desastres, 26* (54), 1–27.

Casas Mínguez, F. (2016). *Sociedad del riesgo global*. Universidad de Castilla -La Mancha. Repositorio Universitario Institucional de Recursos Abiertos. http://hdl.handle.net/10578/12973

Certified Information System Auditor -CISA-. (2019). *A Guide to a Critical Infrastructure Security and Resilience*. Certified Information System Auditor.

Choucri, Nazli, y David Clark. (2013). *Who controls cyberspace?. Bulletin of Atomic Scientists 5* (69), 21-31.

Cooperación y el Desarrollo Económicos. (2014). *Recomendación del Consejo sobre la Gobernanza de Riesgos Críticos.* https://www.oecd.org/gov/infrastructure-governance/ES-OECD-RecommendationGovernance-Infrastructure.pdf-Defensa-Analisis-de-Riesgos-y-Amenazas-a-Infraestructuras-Criticas.pdf

Correa, G., & Yusta, J. (2013). Seguridad energética y protección de infraestructuras críticas. *Lámpsakos,* (10), 92–108.

Cujabante, X., Bahamón, M., Prieto, J., & Quiroga, J. (2020). Ciberseguridad y ciberdefensa en Colombia: un posible modelo a seguir en las relaciones cívicomilitares. *Revista Científica General José María Córdova, 18*(30), 357–377. https://doi.org/10.21830/19006586.588

Díaz, M. (2018). *La defensa nacional en jaque: Análisis de los factores que han obstaculizado problematizar las amenazas externas dentro de la política pública de seguridad nacional en Colombia.* Universidad Externado de Colombia. https://bdigital.uexternado.edu.co/entities/publication/6e0ceed2-e1b4-420e-9051-753ffb3a0f2e

Ejército Nacional de Colombia. (2018). *Plan de Campaña Bicentenario "Héroes de la Libertad".* Ejército Nacional de Colombia.

El Heraldo. (2017). Ciberataque golpeó a 11 empresas y una entidad pública en Colombia. *El Heraldo.* https://www.elheraldo.co/ciencia-y-tecnologia/ciberataque-golpeo-11-empresas-y-una-entidad-publica-en-colombia-361747

El Tiempo. (2017, junio 28). En Colombia hay l2 empresas afectadas por ciberataque mundial. *El Tiempo.* https://www.eltiempo.com/tecnosfera/novedades-tecnologia/numero-de-empresas-afectadas-en-colombia-por-ciberataque-mundial-103550

El Tiempo. (2019, octubre 30). En 2019 se reportaron más de 28.000 casos de ciberataques en Colombia. *El Tiempo.* http://surl.li/oexet

Escuela Superior de Guerra. (2017). *Memorias.* Sello Editorial ESDEG https://esdeguelibros.edu.co/index.php/editorial/catalog/download/18/15/34-1?inline=1

Faundes, C. (2017). Evolución del concepto seguridad en los libros blancos de defensa de Chile. *Papel Político, 22*(1), 185–219. https://doi.org/10.11144/javeriana.papo22-1.ecsl

Feliu, L. (2012). *La Ciberseguridad y la Ciberdefensa. El Ciberespacio. Nuevo escenario de confrontación.* Monografías del CESDEN.

Fuerzas Militares de Colombia (2016). *Catálogo de Infraestructuras Criticas Cibernéticas de Colombia.* Comando General de las Fuerzas Militares.

Fundación Ideas para la Paz. (2017). *Informe de Gestión*. Fundación Ideas para la Paz http://www.indepaz.org.co/wp-content/uploads/2020/11/INFORME-GRUPOS-ARMADOS-2020-OCTUBRE.pdf

Fundación Paz & Reconciliación. (2018). Sin Dios ni ley. Un análisis de la situación de seguridad de la frontera colombo-venezolana. *Ford Foundation* 53. https://pares.com.co/wp-content/uploads/2020/02/INFORME-DE-SEGURIDAD-EN-LA-FRONTERA-1.pdf

Gómez, A. (2012). El ciberespacio como escenario de conflictos. Identificación de las amenazas. In *El ciberespacio. Nuevo escenario de confrontación.* Sello Editorial ESDEG https://esdeguelibros.edu.co/index.php/editorial/catalog/view/19/16/92-1

González, J. (2019). *Infraestructuras críticas : definiendo los sectores para su protección en Colombia.* Segurilatam. https://www.segurilatam.com/seguridad-porsectores/infraestructuras-criticas/infraestructuras-criticas-definiendo-los-sectorespara-su-proteccion-en-colombia_20191203.html

Government of Canada. 2010. *Canada's cyber security strategy: for a stronger and more prospeous Canada.* Minister of public Safety.

Hernández, J. (2016). *Infraestructura crítica cibernética*. Comando General de las Fuerzas Militares. https://acis.org.co/archivos/Conferencias/2016/GuiaICC.pdf

Huertas, D. (2015). *Seguridad y defensa en Colombia perspectiva desde la gestión pública*. Pontificia Universidad Javeriana. https://repository.javeriana.edu.co/handle/10554/18577

Hurst, W., Fergus, P., & Merabti, M. (2018). Asurveyofcritical infrastructure security. In *IFIP Advances in Information and Communication Technology* (Segunda, Vol. 441). https://doi.org/10.1007/978-3-662-45355-1

Jiménez, J., & Acosta, H. (2018). La Geopolítica criminal de los Grupos Armados Organizados. In *Convergencia de Conceptos: Enfoques Sinérgicos en relación a las Amenazas a la Seguridad del*

Estado colombiano. Sello Editorial ESDEG. https://esdeguelibros.edu.co/index.php/editorial/catalog/view/31/27/488-1

Klimburg, Alexander. 2012. *National Cyber Security Framework Manual.* Tallin: NATO CCD COE Publication.

Lleras, M., & Indepaz/Acpaz. (2016). *Análisis a la Directiva Permanente No. 15 de 22 de abril.* Fundación Ideas para la Paz. http://www.indepaz.org.co/wp-content/uploads/2016/05/Directiva-15-de2016-rev-2.pdf

López, O. (2018). La guerra híbrida en el siglo XXI. Recomendaciones para enfrentar la amenaza. Los Ejércitos y El Sistema Internacional Contemporáneo*. Nuevas Amenazas, Tendencias y Desafíos, 49* (28), 93–116. https://doi.org/10.25062/9789585652804.03

Lozano, L. (2015). *Amenazas a la infraestructura del sector de telecomunicaciones (TIC) en Colombia* [Tesis de posgrado]. Universidad Militar de Nueva Granada. https://repository.unimilitar.edu.co/bitstream/handle/10654/7161/

Martín, J. (2016). Seguridad y defensa: Análisis de Riesgos y Amenazas a Infraestructuras Críticas. *Researchgate, 84* (29). Nebrija Universidad.

Masís, J. (2019). La protección de las infraestructuras críticas en la era digital en el contexto de Costa Rica. *Revista de La Facultad de Derecho de México, 69* (274–1), 463. https://doi.org/10.22201/fder.24488933e.2019.274-1.69957

Mendoza, P., & Díaz, Á. (2019). *Ataques Informáticos a La Infraestructura Crítica Del Sector Eléctrico Colombiano.* Universidad Nacional Abierta y a Distancia.

Ministerio de Defensa Nacional. (2018). *Política de Defensa y Seguridad PDS - Para la Legalidad, el Emprendimiento y la Equidad.* Ministerio de Defensa Nacional.

Ministerio de Tecnologías de la Información y las Comunicaciones -MinTIC-. (2017). Impactos de los incidentes de seguridad digital en Colombia 2017. https://www.oas.org/documents/spa/press/Estudio-Seguridad-Digital-Colombia.pdf

Miranzo, M., & Del Rio, C. (2014). La protección de infraestructuras críticas. *UNISCI, 35* (May), 339–352.

Montoya, B. (2017). ¿Cómo minimizar el riesgo de afectación de un ataque cibernético en los blancos estratégicos nacionales? [Tesis de especialización]. Universidad Militar de Nueva Granada.

Morán, S. (2017). La ciberseguridad y el uso de las Tecnologías de la Información y la Comunicación (tic) por el terrorismo. *Revista Española de Derecho Internacional, 69*(2), 195–221. https://doi.org/10.17103/redi.69.2.2017.1.08

Nye Jr., Joseph S., y David A. Welch. 2013. *Understanding global conflict and cooperation: an introduction to theory and history. novena*. Upper Saddle River Pearson.

Oficina de las Naciones Unidas contra la Droga y el Delito -UNODC-. (2013). *El uso de Internet con fines terroristas* UNODC. https://www.unodc.org/documents/terrorism/Publications/Use_of_Internet_for_Ter rorist_Purposes/Use_of_Internet_Ebook_SPANISH_for_web.pdf

Oficina de Naciones Unidas contra la Droga y el Delito -UNODC-. (2009). *Delincuencia organizada transnacional - La economía ilegal mundializada.* Oficina de las Naciones Unidas contra la Droga y el Delito. www.unodc.org/toc

Organización del Tratado del Atlántico Norte -OTAN-. (2016) Cyberdefense pledge. OTAN https://www.nato.int/cps/en/natohq/official_texts_133177.htm

Osorio, A. (2020). *El ciberespacio: retos y oportunidades de Colombia desde su posición periférica* (Vol. 21). Universidad Militar Nueva Granada.

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

Pérez, Y. (2016). Importancia De La Ciberseguridad En Colombia. *Universidad Piloto de Colombia, 42*(31), 1–9. http://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/2676/00003620.pdf?sequence=

Policía Nacional de Colombia, 2012).

Policía Nacional de Colombia. (2017). Informe: Amenazas del Cibercrimen en Colombia 2016-2017. https://caivirtual.policia.gov.co/sites/default/files/informe_amenazas_de_ cibercrimen_en_colombia_2016_-_2017.pdf

Policía Nacional de Colombia. (2017a). *Ciberseguridad.* Policía Nacional de Colombia https://www.policia.gov.co/ciberseguridad

Policía Nacional de Colombia. (2019). Informe: Tendencias del Cibercrimen Colombia (2019-2020). Policía Nacional de Colombia. https://caivirtual.policia.gov.co/#observatorio

Prieto, C. (2012). Bandas criminales en Colombia: ¿amenaza a la seguridad regional? *Opera, 12*(12), 181–204. https://www.redalyc.org/pdf/675/67530270009.pdf

Prieto, C. (2013). Las Bacrim y el crimen organizado en Colombia. *Policy Paper 47, 47,* 1–19. https://library.fes.de/pdf-files/bueros/la-seguridad/09714.pdf

Realpe, M., & Cano, J. (2020). Amenazas Cibernéticas a la Seguridad y Defensa Nacional. Reflexiones y perspectivas en Colombia. *Seguridad Informática. X Congreso Iberoamericano, CIBSI 2020, 63*(38), 105–113. https://doi.org/10.12804/si9789587844337.10

Rincón, D. (2017). La política de ataques militares contra las bandas criminales en colombia y su legitimidad a la luz del derecho internacional humanitario. *ARS BONI ET AEQUI, 13*(2), 11–33. http://arsboni.ubo.cl/index.php/arsbonietaequi/article/viewFile/244/219

Rudner, M. (2013). Cyber-threats to critical national infrastructure: An intelligence challenge. *International Journal of Intelligence and Counter Intelligence, 26*(3), 453-481. https://doi.org/10.1080/08850607.2013.780552

Sánchez, G. (2012). Ciberespacio y el Crimen Organizado. Los nuevos desafíos del siglo XXI. *Revista Enfoques: Ciencia Política y Administración Pública, X*(16), 71–87.

Tawse, D. (2008). Conflicto armado colombiano. *Desafíos,* 19, 270-290 https://www.redalyc.org/pdf/3596/359633164010.pdf

Tello, A. (2020). Conceptos de seguridad y defensa. *Relaciones Internacionales (La Plata), 9*(19), 135–137.

Torres, L. (2013). *El ciberespacio como escenario estratégico de seguridad y defensa en el desarrollo de políticas en Colombia.* Universidad Militar Nueva Granada.

Torrijos, V., & Balaguera, L. (2019). Tendencias conceptuales que definen la evolución actual de las amenazas a la seguridad y Defensa nacional. *Defensa y Seguridad, 73*(26),45–69. https://esdeguelibros.edu.co/index.php/editorial/catalog/view/19/16/92-1

Trejos, L. (2012). Uso de la internet por parte de las farc–ep: nuevo escenario de confrontación o último espacio de difusión política. *Revista Encrucijada Americana Revista Encrucijada Americana, 5*(1), 25–50.