

3

ISSN: 2955-0270  
eISSN: 3028-3310



Escuela Superior de Guerra  
"General Rafael Reyes Prieto"  
Colombia

Revista

# Ciberespacio, Tecnología e Innovación

Volumen 2 - Número 3

2023 (enero-junio)  
Bogotá., Colombia

# Revista **Ciberespacio, Tecnología e Innovación**

Volumen 2, número 3 enero-junio 2023

ISSN: 2955-0270 • eISSN: 3028-3310

Bogotá, D.C., Colombia

## Directivos

**Escuela Superior de Guerra "General Rafael Reyes Prieto"**

Brigadier General **Edgar Alexander Salamanca Rodríguez**

*Director*

Contralmirante **Omar Yesid Moreno Oliveros**

*Subdirector*

Coronel **Oscar Otoniel Torres Conde**

*Vicedirector Académico*

Coronel **Verónica Pedraza Martínez**

*Vicedirectora Administrativa*

Coronel **Andrés Eduardo Fernández Osorio**

*Vicedirector de Investigación*

Capitán de Navío **Edwin Andrés Alonso Toloza**

*Vicedirector de Proyección Institucional*

**Indexada en:**

Google Scholar



**ESCUELA SUPERIOR  
DE GUERRA**

**"General Rafael Reyes Prieto"**

Colombia



**EDITORIAL ESDEG**

Esta página queda intencionalmente en blanco

# Revista **Ciberespacio, Tecnología e Innovación**

Volumen 2, número 3 enero-junio 2023

ISSN: 2955-0270 • eISSN: 3028-3310

Bogotá, D.C, Colombia

La **RCIT** es una publicación académica de acceso abierto, revisada por pares y editada semestralmente por la **Escuela Superior de Guerra "General Rafael Reyes Prieto" (ESDEG)**, principal centro de pensamiento conjunto del **Comando General de las Fuerzas Militares de Colombia**, a través de su **Sello Editorial ESDEG**.

## Comité Editorial

**Manuel Bermúdez-Tapia**, PhD

Universidad Privada San Juan Bautista, Perú

<http://orcid.org/0000-0003-1576-9464>

**Marina Miron**, PhD

King's College London, Reino Unido

<https://orcid.org/0000-0003-3695-6541>

**Eduardo Andrés Hodge-Dupré**, PhD

Universidad de Santiago de Chile, Chile

<https://orcid.org/0000-0002-4750-2986>

## Equipo Editorial

CR. **Andrés Eduardo Fernández Osorio**

Jefe del Sello Editorial ESDEG

TC. (R) **Carlos Alberto Ardila Castro**

Coordinador del Sello Editorial ESDEG

**Tania Lucia Fonseca Ortiz**

Editora en Jefe

**Henry Mauricio Acosta Guzmán**

Editor de Publicaciones Seriadas SEESG

**Anderson Nicolás Rojas Sierra**

Corrector de Estilo

**Rubén A. Urriago Gutiérrez**

Diseñador Gráfico

---

2023, Escuela Superior de Guerra "General Rafael Reyes Prieto"

Vicedirección de Investigación - Sello Editorial ESDEG

Carrera 11 No. 102-50. Bogotá, D. C., Colombia

**Página web:** <https://esdegrevistas.edu.co/index.php/rcit>

**Correo electrónico:** [esdegrevistas@esdeg.edu.co](mailto:esdegrevistas@esdeg.edu.co)

---



Los artículos publicados por la *Revista Ciberespacio, Tecnología e Innovación* son de acceso abierto bajo una licencia *Creative Commons: Atribución - No Comercial - Sin Derivados*.

---

# Revista Ciberespacio, Tecnología e Innovación

## 1. ENFOQUE Y ALCANCE

La **Revista Ciberespacio, Tecnología e Innovación** (RCIT). La RCIT es una publicación académica de acceso abierto, revisada por pares y editada semestralmente por la [Escuela Superior de Guerra "General Rafael Reyes Prieto"](#) (ESDEG), principal centro de pensamiento conjunto de las [Fuerzas Militares de Colombia](#), a través de su [Sello Editorial ESDEG](#).

La **RCIT** es una revista interdisciplinaria, con un enfoque en las Ciencias Sociales (Clase 5I01, OCDE / UNESCO), abierta a la discusión y difusión de trabajos teóricos e investigaciones sobre el ciberespacio identificado como quinto dominio, en donde la ciberseguridad, la ciberdefensa y la innovación son ejes para el análisis de este ámbito. Su finalidad es abordar ejes temáticos sobre la seguridad digital, la información, las tecnologías disruptivas, las ciberamenazas, las guerras cibernéticas, entre otros temas, reconociendo la necesidad de generar desarrollo tecnológico de innovación en relación con un quinto dominio de la guerra que afecta desde lo digital a los dominios físicos como la infraestructura crítica de un Estado.

## 2. ORGANIZACIÓN TEMÁTICA Y PÚBLICO OBJETIVO

Cada número de la **Revista Ciberespacio, Tecnología e Innovación** cuenta con cuatro secciones:

- a) **Debates:** artículos de investigación científica y tecnológica.
- b) **Coyuntura:** artículos de reflexión o revisión.
- c) **Perspectivas:** entrevistas a académicos o tomadores de decisión.
- d) **Enfoques:** reseñas de libros.

La **RCIT** está dirigida a un amplio público que incluye decisores políticos, miembros de las Fuerzas Armadas, servidores públicos, profesionales, docentes, investigadores y estudiantes de ciencias sociales y de otras áreas del conocimiento, interesados en la seguridad y la defensa.

## 3. TIPOLOGÍA E IDIOMA DE LOS ARTÍCULOS

La **RCIT** publica artículos en español e inglés en tres categorías:

- a) **Investigación científica y tecnológica:** documento que presenta de manera detallada los resultados originales derivados de proyectos de investigación y/o desarrollo tecnológico finalizados.
- b) **Reflexión:** documento que ofrece resultados de investigación desde una perspectiva analítica, interpretativa y crítica del autor, sobre un tema específico, recurriendo a fuentes originales.
- c) **Revisión:** documento que organiza, analiza y se integran los resultados de investigaciones publicadas o no publicadas sobre un campo en ciencia o tecnología, con el fin de dar cuenta de los avances y las tendencias de desarrollo.

#### 4. PERIODICIDAD

La **RCIT** es editada semestralmente (enero-junio y julio-diciembre) en formato digital (eISSN: 3028-3310) e impreso (ISSN: 2955-0270). La versión en línea y la versión impresa aparecen publicadas el penúltimo día del último mes del periodo de cada número, esto es, 30 de junio para el número enero-junio y 30 de diciembre para el número julio-diciembre. Cada uno de los artículos de la **RCIT** tiene un DOI (Digital Object Identifier) asignado para su identificación y referenciación.

#### 5. FINANCIAMIENTO

La **Revista Ciberespacio, Tecnología e Innovación** es una publicación académica de la [Escuela Superior de Guerra "General Rafael Reyes Prieto"](#) (ESDEG), perteneciente, a su vez, al [Comando General de las Fuerzas Militares de Colombia](#) que, como entidad pública, se financia con los recursos asignados por el gobierno nacional. Con el fin de mantener su carácter crítico e independiente, la **RCIT** no acepta financiamiento ajeno a la ESDEG para su funcionamiento. Así las cosas, todo el proceso de publicación de la revista está completamente libre de costo para los autores; tampoco se realizan cobros por el envío, procesamiento y publicación de artículos (*no article submission or processing charge*).

#### 6. ACCESO ABIERTO, DERECHOS DE AUTOR Y LICENCIA PARA PUBLICACIÓN

El Sello Editorial ESDEG es signatario de la [Declaración de Budapest](#) y todos sus contenidos publicados son de acceso abierto (open access), con pleno reconocimiento de los derechos morales de los autores sobre su obra. Para su publicación, los autores aceptan ceder los derechos de publicación en favor de la [ESDEG](#) y el [Sello Editorial ESDEG](#) de acuerdo con los términos de la licencia Creative Commons: [Reconocimiento-NoComercial-SinObrasDerivadas](#).



De esta forma, los autores y los lectores pueden copiar y difundir el artículo en la versión final publicada en línea por la **RCIT**, siempre que se reconozca e identifique al autor (o autores) del artículo, no se haga uso comercial del artículo final publicado, ni se trate de obras derivadas o versiones modificadas.

#### 7. POLÍTICA CROSSMARK

La **RCIT** utiliza [Crossmark](#) para mantener informados a sus lectores sobre cualquier cambio que tengan los artículos publicados. [CrossMark](#) es una iniciativa de [CrossRef](#) para proporcionar una forma normalizada de localizar la versión oficial de un documento. La **RCIT** reconoce la importancia de mantener la integridad de los registros académicos para investigadores y bibliotecas, razón por la cual garantiza que su archivo electrónico siempre cuenta con un contenido confiable.



Al hacer clic en el ícono [CrossMark](#) se informa al lector sobre el estado actual del documento así como información adicional sobre el historial de publicación de este. Los contenidos que muestran el ícono de [CrossMark](#) son aquellos contenidos publicados en la página web de la **RCIT**, actuales o futuros.

## 8. ARCHIVO DE LOS CONTENIDOS

La **RCIT** utiliza la plataforma [Portico](#) para el archivo digital de los contenidos publicados. Así mismo, la **RCIT** permite que los autores puedan autoarchivar en repositorios institucionales, temáticos o páginas webs personales su artículo en la versión final publicada en línea.

## 9. RESPONSABILIDAD DE CONTENIDOS

La responsabilidad por el contenido de los artículos publicados por la **RCIT** corresponde exclusivamente a los autores. Las posturas y aseveraciones presentadas son resultado de un ejercicio académico e investigativo que no representa la posición oficial ni institucional de la [Escuela Superior de Guerra "General Rafael Reyes Prieto"](#), el [Comando General de las Fuerzas Militares de Colombia](#) o el [Ministerio de Defensa Nacional](#).

## 10. INDEXACIÓN

La **Revista Ciberespacio, Tecnología e Innovación** se encuentra incluida en los siguientes Sistemas de Indexación y Resumen (SIR):

Google Scholar

---

# Tabla de Contenido

## Editorial

- Tecnología e innovación en el ciberespacio** 1-2  
Technology and innovation in cyberspace  
*Tania Lucía Fonseca Ortiz*

## Sección Debates

1. **Dark web: Sistema para la desestabilización de la seguridad nacional** 5-24  
Dark web: System for the destabilization of national security  
*Hugo Rene Aguillon Gómez*
2. **Aproximación Teórica a los Factores Armados de Inestabilidad, que afectan la Seguridad y Defensa Nacional en el Ciberespacio** 25-56  
Theoretical Approach to the Armed Factors of Instability, which affect the Security and National Defense in Cyberspace  
*Gabriel Andrés Acosta Lizarazo*
3. **Aplicaciones de los sistemas de aeronaves remotamente tripuladas para la seguridad y defensa nacional** 57-80  
Applications of remotely manned aircraft systems for national security and defense  
*German Quintero Morales y Omar Leonardo Salas Galindo*

## Sección Coyuntura

4. **Las herramientas cibernéticas y cognitivas: dos conceptos que desplazaron los métodos convencionales de enfrentamiento** 83-88  
Cybernetic and cognitive tools: two concepts that displaced conventional coping methods  
*Diego Ospina Quintana*

## Sección Perspectivas

5. **Entrevista a Lucas Giraldo Ríos. Resiliencia genética: estrategias para proteger y recuperar datos frente a amenazas cibernéticas** 91-96  
Interview with Lucas Giraldo Ríos. Genetic resilience: strategies to protect and recover data from cyber threats  
*Angélica María González González*

## Sección Enfoques

6. **Reseña de libro. Inteligencia artificial** 99-101  
Book review. Artificial Intelligence  
*Viviana Pilar Fuquen Flautero*



Esta página queda intencionalmente en blanco

# Editorial

---

Editorial

Esta página queda intencionalmente en blanco

## Editorial: Tecnología e innovación en el ciberespacio

Editorial: Technology and innovation in cyberspace

DOI: <https://doi.org/10.25062/2955-0270.4816>

**Tania Lucía Fonseca Ortiz** 

Editora en Jefe de la Revista Ciberespacio, Tecnología e Innovación

La Escuela Superior de Guerra "General Rafael Reyes Prieto" invita a la comunidad académica a leer la edición número 3 del volumen 2 de la revista Ciberespacio, Tecnología e Innovación del primer semestre del 2023. En esta edición se aborda como temática central la *Tecnología e Innovación en el ciberespacio*, dos conceptos que resultan ser importantes para la comprensión de la dinámica de relación social en un mundo digital. Para tal fin, se convocaron resultados de investigación a fines al empleo de tecnologías que están transformando el mundo.

En la sección de *debates* se presentan tres artículos resultados de investigación: primero, *Dark web: Sistema para la desestabilización de la seguridad nacional, donde se establece un análisis descriptivo sobre lo que ha significado la dark web para la seguridad y defensa*. En esta investigación se aborda el concepto de la dark web, reconociendo que es un gran espacio donde se desarrollan actividades que generalmente están en contraria de la seguridad y defensa, pero al mismo tiempo, resulta ser un espacio para comprender las dinámicas del mundo material reflejadas en lo digital.

Segundo, *Aproximación Teórica a los Factores Armados de Inestabilidad, que afectan la Seguridad y Defensa Nacional en el Ciberespacio*, es un trabajo de investigación que aborda de manera teórica los factores que pueden llegar a desestabilizar a un estado desde el ciberespacio. En este documento se evidencia la innovación tecnológica de las amenazas, y al mismo tiempo se reconoce la importancia de profundizar la investigación

en el tema de ciberdefensa, esto debido a que los factores de inestabilidad han desarrollado dinámicas de desestabilización que no requieren el empleo de grandes recursos y espacios físicos.

Como tercer escrito, las *Aplicaciones de los sistemas de aeronaves remotamente tripuladas para la seguridad y defensa de nacional*, materializa un análisis sobre el empleo de tecnologías en los sistemas de aeronaves que son tripulados de manera remota y que pueden ser una tecnología que puede ser aprovechable para la defensa nacional. En este análisis se aborda el impacto de las tecnologías empleadas de manera inteligente y para los fines del Estado.

Para la sección *coyuntura*, se presenta el artículo titulado *Las herramientas cibernéticas y cognitivas: dos conceptos que desplazaron los Métodos Convencionales de enfrentamiento*, un análisis de contexto sobre el empleo de las herramientas cibernéticas y cognitivas, una importante oportunidad para la Innovación en los procesos de entrenamiento. Se reconoce que los procesos de innovación tecnológica necesariamente incluyen al ciberespacio.

En la sección *perspectivas*, se realiza una entrevista al docente, investigador y asesor en temas relacionados con ciberdefensa y ciberseguridad, doctor Lucas Giraldo, sobre la temática relacionada con *Resiliencia Genética: Estrategias para Proteger y Recuperar Datos Frente a Amenazas Cibernéticas*. En esta entrevista se reconoce la importancia de la información y los datos, reconociendo que debe existir una conciencia social sobre la privacidad de la información.

En la sección *enfoques*, se recomienda el libro titulado *Inteligencia artificial*, el cual es una compilación de diferentes profesionales especializados en dicha nueva tecnología que cada vez se consolida en las diferentes esferas disciplinarias.

# Debates

---

Debates

Esta página queda intencionalmente en blanco

# Dark web: Sistema para la desestabilización de la seguridad nacional

Dark web: System for the destabilization of national security

DOI: <https://doi.org/10.25062/2955-0270.4774>

Hugo Rene Aguillon Gómez 

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

## Resumen

El siguiente artículo tiene como propósito exponer aquellas vulnerabilidades que surgen gracias a la diseminación de nuevos escenarios bélicos en contextos como el cibernético. Para ello, en primer lugar, se hace una descripción con respecto a la finalidad de desestabilización nacional en el contexto cibernético de la Dark Web, seguido de la identificación de las herramientas existentes dentro de la Dark Web que permiten la desestabilización de la seguridad nacional como medio para dicho fin. Finalmente, se expone el escenario ideal que proteja la seguridad nacional ante los efectos y consecuencias del uso de las herramientas de la Dark Web como medio para la desestabilización nacional.

**Palabras Clave:** seguridad nacional, ciberespacio, amenaza, desestabilización, Dark Web y consolidación.


The purpose of the following article is to expose those vulnerabilities that arise thanks to the dissemination of new war scenarios in contexts such as cyber. To do this, firstly, a description is made regarding the purpose of national destabilization in the cybernetic context of the Dark Web, followed by the identification of the existing tools within the Dark Web that allow the destabilization of national security as means to that end. Finally, the ideal scenario that protects national security from the effects and consequences of the use of Dark Web tools as a means for national destabilization is presented.

**Key words:** national security, cyberspace, threat, destabilization, Dark Web, and consolidation.

## Abstract



**Artículo de reflexión**

Recibido: 25 de marzo de 2023 • Aceptado: 1 de mayo de 2023  
Contacto: Hugo Rene Aguillon Gómez  [aguillonh@esdeg.edu.co](mailto:aguillonh@esdeg.edu.co)



## Introducción

La guerra, afirma Prandini et al., (2011) que es una disciplina en constante cambio que ha evolucionado junto con la civilización humana durante casi toda la historia registrada. Desde el momento en que los primeros cazadores elaboraron la primera lanza, desde la primera guerra que se produjo entre dos tribus, hasta la dinámica de la guerra moderna del mundo actual, la guerra ha evolucionado en paralelo con la humanidad. A medida que la guerra se expande, también lo hacen los dominios en los que se libra. Se disputa inicialmente por tierra, luego por el mar y luego por el aire; se lanzan satélites al espacio y luego se crean armas antisatélites para destruir esos mismos satélites que se han colocado en el espacio.

En la actualidad, autores como Ortega y Font (2012) expresan que las naciones se enfrentan amenazas de seguridad nacional reales y difíciles; el extremismo, el terrorismo internacional, el narcotráfico, la trata de personas, entre otros. Estos florecen en variadas áreas del mundo, amenazando a componentes como las instituciones fundamentales para el Estado, los aliados internacionales y la soberanía. Generalmente, Galindo (2005) afirma que los conflictos regionales pueden tener efectos graves sobre los intereses de cada una de las naciones, pues los gobiernos extranjeros con la actividad hostil y los grupos u organizaciones armadas profundizan en la adquisición de capacidades y herramientas sin medir el nivel de daño concurrente por su accionar.

Sin embargo, Acosta et al., (2009) indica que aun con la existencia de amenazas comunes y previamente analizadas, las coacciones más recientes a las que se enfrentan los Estados, y quizás las de más rápido crecimiento, son las que concurren en ambientes tales como el ciberespacio. El uso de las Tecnologías de la Información y las Comunicaciones-TIC's se ha generalizado en la vida diaria de la población mundial. Este nuevo escenario de posibilidades, ofrece un desarrollo sin precedentes en el intercambio de información y comunicaciones, pero al mismo tiempo, lleva a graves riesgos y amenazas que pueden afectar a la seguridad nacional. Estas son conocidas como amenazas cibernéticas, las cuales indica Gómez et al., (2014) que aumentan cada año en frecuencia, alcance y gravedad del impacto. Los ciberdelincuentes, los piratas informáticos y los adversarios extranjeros se están volviendo cada día más sofisticados, siendo capaces de utilizar herramientas alternas como la Dark Web con fines de alto impacto y gran alcance.

Esta, afirma Barrio (2017) que es el colectivo oculto de sitios de Internet a los que solo se puede acceder mediante un navegador web especializado. Se utiliza para mantener la actividad de Internet anónima y privada, lo que puede ser útil tanto en aplicaciones legales como ilegales. Si bien, algunos lo usan para evadir la censura de las instituciones de control de los Estados, pero también se sabe que se utiliza para actividades altamente ilegales. Como nación, Atienza y Bermejo (2020) expone que la ciudadanía al adaptarse a

las revoluciones y avances tecnológicos hoy en día depende del Internet, pues es viable y aplicable a los usos más comunes de la vida cotidiana. No obstante, así como el ciberespacio ofrece grandes oportunidades, también presenta vulnerabilidades, y estas se materializan de forma impactante en espacios tales como la Dark Web.

Ante ello, Aguilar (2015) expone que existen varios factores que contribuyen a la proliferación de acciones delictivas en el ciberespacio, y precisamente en espacios como la Dark Web; i) la rentabilidad de explotarlo en términos económicos, políticos o de otro tipo; ii) la facilidad y bajo costo de emplear las herramientas del sistema para organizar ataques; iii) la facilidad con la que los atacantes pueden esconderse y realizar estas actividades de forma anónima y desde cualquier parte del mundo, con impactos transversales en el público y del sector privado y de los propios ciudadanos.

Al sintetizar los delicados y concurrentes malos manejos del internet, Gamón (2017) afirma que sus actores son criminales motivados por el lucro, particularmente en las áreas de robo de identidad y otras formas de ciberdelito financiero. El costo del delito cibernético, que ya asciende a miles de millones de dólares, aumenta cada año. Para el año 2021, el IBM (2021) reporta un aumento del 10% con respecto al 2020, materializado en 1,07 millones de dólares. Pero, las amenazas cibernéticas también provienen de estados nacionales y otros actores que buscan explotar información para obtener una ventaja sobre los otros. En la actualidad, Marín et al., (2019) indica que los grupos terroristas y extremistas utilizan el poder de la Dark Web, para difundir sus mensajes de odio e intolerancia y para reclutar nuevos miembros, a menudo dirigidos a jóvenes vulnerables. Esto, a diferencia de las redes sociales como Twitter, Instagram, Facebook, entre otras, se moviliza bajo un espacio completamente ilegal, permitiendo el no seguimiento de sus actos, lo que la convierte en una herramienta de alto letalidad para la sociedad.

El alcance global del ciberespacio y la complejidad de sus redes brindan a los malos actores amplios lugares para esconderse, a salvo del alcance del derecho internacional. Para hacer frente a estas amenazas, es importante comprender el *modus operandi* de los actores que actúan bajo la protección de herramientas como la Dark Web, estableciendo inicialmente quiénes son, dónde están y cuáles son sus capacidades, planes e intenciones. Por ello, resulta pertinente establecer como punto de partida: ¿Cuáles son los aspectos de la Dark Web que se utilizan para la desestabilización dentro del contexto de la seguridad nacional?

## Metodología

Para el desarrollo del siguiente artículo de investigación se utilizará en primer lugar un enfoque cualitativo, dado que es necesario recolectar información de fuentes primarias como análisis de expertos, bases de datos, artículos, libros, entre otros. Esta información,

según Hernández et al (2014) debe encontrarse fundamentada en material científico, académico y previamente aprobado por tanques de pensamiento enfocados en investigación de orden cualitativo. Asimismo, el tipo de investigación a utilizar será netamente exploratorio, situación que transcurre por la necesidad de estudiar una problemática que no se encuentra totalmente definida.

Debido a la complejidad del caso, el paso a paso de la investigación iniciara con una contextualización teórica, legal e histórica con respecto al desarrollo y evolución de la Dark web como amenaza a la seguridad de las naciones, seguido de una comparación que refleje las características, ventajas y desventajas que concurren por medio del uso de la Dark Web para la seguridad nacional. Finalmente, se expondrán las afectaciones que genera el uso de herramientas como la Dark Web, todo enfocado al desarrollo de nuevas amenazas, tipos de guerra y estrategias de orden híbrido que concurren en el orden internacional y su necesidad de poder.

## Marco teórico y conceptual

Para el desarrollo del marco teórico, se debe contextualizar teórica y conceptualmente denominaciones como internet, espacio cibernético, amenaza nacional, seguridad y defensa. Estos, están encaminados de acuerdo a las herramientas híbridas para acceder a la Deep Web, pues autores como Rodríguez (2016) indican que su utilización va más allá del acceso a la información y a su poca trazabilidad en detección. No obstante, aun con estas bases teóricas, resulta preciso determinar a los aspectos de desestabilización que concurren de forma constante en el espacio cibernético. Siendo ejemplos ya materializados que han impactado la seguridad y consolidación de las naciones: Dataleaks y Wikileaks.

## Dataleaks

Para autores como Parno et al., (2009), una fuga de datos o Dataleaks ocurre cuando los datos confidenciales se exponen accidentalmente de forma física, en Internet o en cualquier otra forma, incluidos discos duros o computadoras portátiles perdidos. Esto, concurre en un riesgo de alto alcance cuando un ciberdelincuente puede obtener acceso no autorizado a los datos confidenciales sin esfuerzo. En esta fuga, Shu et al., (2015) expone que existen dos formas de acceder a la información; la primera, se expone como una violación de datos, la cual es cuando un ataque exitoso puede proteger información confidencial; la segunda es la fuga de datos que no requiere un ataque cibernético, y generalmente, se debe a prácticas deficientes de seguridad de datos o accidentes del manejo humano.

## Wikileaks

De acuerdo con Sirfry (2011), Wikileaks es una organización de medios y sitio web que funcionaba como cámara de compensación para información clasificada o privilegiada. Esta fue fundada en 2006 por el programador informático y activista australiano Julian Assange. Este espacio cibernético sostuvo varias acciones legales en su contra, teniendo como ejemplo la publicación de material interno del movimiento de Scientology en 2008, y este grupo amenazó con presentar una demanda por infracción de derechos de autor. WikiLeaks respondió publicando miles de documentos de Scientology.

## Internet

El ciberespacio, una rama del desarrollo de la informática y la tecnología digital, en las últimas décadas ha pasado a formar parte y de las estrategias de adaptación, control y monitoreo de los Estados. Esta, afirman Crystal y Tena (2002) que ha sido invaluable para mejorar y agilizar los procesos relacionados con el trabajo, el aprendizaje y el entretenimiento, y afecta virtualmente a todos los campos del quehacer humano. Una vez que Internet se convirtió comercial en 1988, se convirtió rápidamente en un pilar del ciberespacio, ofreciendo acceso económico e inmediato a muchas fuentes de información, trabajo conjunto a larga distancia y más.

Ante ello, someramente se conoce a la internet, según Baluja y Anias (2006) como una red de área amplia global que conecta sistemas informáticos en todo el mundo. Incluye varias líneas de datos de gran ancho de banda que componen la columna vertebral de Internet. Estas líneas están conectadas a los principales centros de Internet que distribuyen datos a otras ubicaciones, como servidores web e ISP. Por otro lado, el internet se manifiesta por medio del espacio cibernético o ciberespacio, que, de acuerdo con Fernández (2016) se refiere al mundo de las computadoras virtuales y, más específicamente, a un medio electrónico que se utiliza para facilitar la comunicación en línea. La característica principal del ciberespacio es un entorno interactivo y virtual para una amplia gama de participantes. Aun al desarrollarse como herramienta que provee beneficios a la humanidad, existen actores que hacen de esto, una materialización de amenaza bastante volátil. Por ello, resultará pertinente resaltar al ámbito de la seguridad y defensa, partiendo del conocimiento de la amenaza y los riesgos que allí suscitan.

## Deep web

Ante la proliferación de herramientas beneficiosas y útiles para la sociedad, He et. al, (2007) expresa que la existencia de escenarios profunda y ocultos como la Deep Web va más allá de intereses individuales. De hecho, esta se encuentra debajo de la superficie del ciberespacio y representa aproximadamente el 90% de todos los sitios web (He et. al,

2007). Esta, sería la parte de un iceberg debajo del agua, mucho más grande que la red de la superficie, dado que esta red oculta es tan grande que es imposible descubrir exactamente cuántas páginas o sitios web están activos al mismo tiempo.

Ante ello, Madhavan (2008) expone que los grandes motores de búsqueda podrían considerarse como barcos de pesca que solo pueden «atrapar» sitios web cerca de la superficie. Todo lo demás, desde revistas académicas hasta bases de datos privadas y más contenido ilícito, está fuera de alcance. Esta web profunda también incluye la parte que conocemos como la web oscura.

## Web Oscura o Dark Net

Según Madhavan et al (2008) esta se refiere a sitios que no están indexados y solo son accesibles a través de navegadores web especializados. Significativamente más pequeña que la diminuta red superficial, la web oscura se considera parte de la web profunda. Usando el ejemplo imagen del océano y el iceberg, la red oscura sería la punta inferior del iceberg sumergido. Sin embargo, la web oscura es una parte muy oculta de la web profunda con la que pocos interactuarán o incluso verán, requiriendo únicamente redes como Tor<sup>1</sup>. En otras palabras, la web profunda cubre todo lo que hay debajo de la superficie que todavía es accesible con el software adecuado, incluida la web oscura.

## Finalidad de desestabilización nacional en el contexto cibernético de la Dark Web

Para autores como Ibáñez (2017), los Estados sostienen día a día acciones de supervivencia ante el contexto internacional. Este escenario promueve un sinnúmero de estrategias, actividades y necesidades acordes a la forma en que se materializan nuevos riesgos y o, amenazas, siendo evaluadas de acuerdo a su presentación, modo y lugar. En efecto, al hacer especial énfasis en espacios como el cibernético, es importante encaminar las ocurrencias presentadas en sistemas como la Dark Web, dado que se presenta como un sistema difícil de estudiar, pero con grandes intervenciones a lo largo de la historia.

Comprender la aplicación de la Dark Web al futuro de la guerra cibernética requiere que se analice el problema desde múltiples perspectivas. Por supuesto, Mariano (2020) enfatiza en la perspectiva de seguridad nacional subyacente que debería impulsar el entendimiento fundamental de la misma. Desde una perspectiva económica, Es necesario considerar que la aplicación principal de la Dark Web, hasta ahora, ha sido como un mercado utilizado por aquellos que desean participar en el comercio ilícito. La capacidad de comprender el comercio ilícito en la Dark Web en su aplicación a la seguridad nacional,

---

1 The Onion Router; ed que implementa una técnica diseñada con vistas a proteger las comunicaciones.

afirma Hirane (2021) que requiere la consideración de conceptos como la oferta, la demanda, la reputación del proveedor, entre otros. Mientras que, desde la perspectiva de las operaciones de inteligencia, la Dark Web también puede verse como un terreno neutral para dos partes que desean participar de forma anónima en el intercambio de información, armas y secretos de seguridad nacional.

Al igual que la descripción de la era de la Guerra Fría de un agente clandestino que se encuentra con su fuente en un lugar seguro o que se comunica con agentes a través de puntos muertos, la Dark Web en muchos sentidos se puede considerar como el medio cibernético a través del cual dos profesionales de inteligencia pueden reunirse e intercambiar información de forma segura en terrenos neutrales. Ante ello, López (2019) expone que uno de los principales desafíos para los profesionales de seguridad nacional al analizar la Dark Web es la dificultad para llegar a un entendimiento común de lo que implica el término. El término Dark Web ya es ambiguo, y a menudo, autores como Huidobro y Guerrero (2021) expresan que se combina con otros términos como Deep Web o Criminal Underground.

Las agencias de inteligencia de todo el mundo explotan regularmente la inteligencia de fuentes abiertas (OSINT) que se encuentra en la web de ingreso abierto; mientras que la Deep Web es la ubicación elegida por aquellos ciberdelincentes que desean participar en la compra y venta de datos de identidad robados, como números de seguridad social y otra información de identificación personal. Sin embargo, Garnacho (2018) expresa que la Dark Web es accesible solo a través de un protocolo de navegación de Internet especial, como The Onion Router (TOR). Este, proporciona anonimato al guiar el tráfico de Internet a través de otros nodos o computadoras que usan el navegador. Este tráfico rebota a través de los nodos TOR hasta que finalmente concurre a través de un nodo de salida. Esto expone Riva (2016) que crea una cebolla o un anonimato de varias capas, situación que permite la protección del anonimato por medio del rebote de sus comunicaciones en una red distribuida en retransmisiones administradas por voluntarios en todo el mundo; aquí, se evita que alguien que esté viendo su conexión a Internet sepa qué sitios se visitan, además del imposible rastreo de ubicación física.

Desde una perspectiva de seguridad nacional, la proliferación incontrolada de usuarios en la Dark Web plantea muchas preocupaciones, ya que estas capacidades han demostrado históricamente que están creadas para afectar significativamente el ámbito de la seguridad nacional. Por ejemplo, Ramírez (2020) expone la experiencia vivida con espacios como Stuxnet<sup>2</sup>, la cual es una supuesta capacidad de malware estadounidense-israelí diseñada para interrumpir las centrifugadoras de enriquecimiento de uranio

---

2 Stuxnet es un gusano informático que afecta a equipos con Windows, descubierto en junio de 2010 por VirusBlokAda, una empresa de seguridad ubicada en Bielorrusia. Es el primer gusano conocido que espía y reprograma sistemas industriales, en concreto sistemas SCADA de control y monitorización de procesos, pudiendo afectar a infraestructuras críticas como centrales nucleares. (John, 2010).

iraníes en Natanz, es quizás el ejemplo más conocido de cómo pueden afectar significativamente los intereses de seguridad nacional de los Estados-nación.

Desde el descubrimiento de Stuxnet, Chen y Abu (2011) indican que los ciberdelinquentes, con el deseo de monetizar su capacidad para desarrollar exploits de tecnología de la información, han aprovechado en gran medida los mercados de la Dark Web para encontrar posibles compradores para sus capacidades. El anonimato facilitado por la Dark Web la convierte en una salida accesible y segura para encontrar exploits antes de su anuncio público, lo que permite a los atacantes comprar estos exploits y lanzarlos antes de que se publiquen los puntos de vulnerabilidad.

El anonimato facilitado a través de la Dark Web fomenta un terreno comercial ideal para los posibles compradores y vendedores de armas peligrosas. Esto, afirma Farwell (2011) que más que teórico, es un hecho que ha sido probado a través de la observación una y otra vez. El Uranio, uno de los compuestos químicos más peligrosos para la composición de armas de fuego es una de la muestra de los tipos de armas que se han incluido en la Dark Web. En respuesta a ello, Fidler (2011) indica que la comunidad global de aplicación de la ley ha estado persiguiendo agresivamente a los compradores y vendedores de armas en la Dark Web, y en muchos casos, han tenido éxito en frustrar posibles ataques. En 2016, Chertoff (2017) afirma que la Oficina Federal de Investigaciones-FBI colaboró con las autoridades policiales irlandesas para evitar que un militante del Ejército de la República de Irlanda (IRA) adquiriera pistolas, granadas y explosivos plásticos de un mercado de la Dark Web. No obstante, mientras la comunidad de seguridad nacional puede reclamar victorias menores con este tipo de operaciones preventivas, los interesados en comprar y vender armas cinéticas de forma anónima han comenzado a cambiar su metodología.

Ante ello, autores como Baravalle et al., (2016) afirman que, es necesario evaluar las dos grandes evoluciones en las que se comercializan las armas cinéticas en la Dark Web. La primera, es que los compradores y vendedores de armas de la Dark Web probablemente trasladen su negocio de algunos de los mercados de acceso abierto más populares a otros mercados que requieren un mayor grado de investigación para ingresar; esto, argumenta la tendencia de materialización por dos puntos principales. El primero es que las personas que se dedican al comercio de armas se están volviendo más cautelosas ante la presencia encubierta de las fuerzas del orden y la posibilidad de que las atraigan a una trampa. La segunda, es que es probable que los principales mercados se estén volviendo menos tolerantes con el riesgo en el que incurren al permitir la inclusión de armas en sus mercados.

Históricamente, Chertoff (2017) indica que las listas de armas han atraído la atención de la comunidad policial mundial, lo que ha provocado que agentes encubiertos examinen los mercados en busca de pistas. Más allá del aumento del riesgo, el margen

de beneficio del mercado para el comercio de armas es relativamente bajo en comparación con los márgenes de beneficio de otros bienes ilícitos de gran volumen, como las drogas y el fraude.

## Herramientas de desestabilización existentes dentro de la Dark Web: afectación a la seguridad nacional

Para autores como Biddle et al., (2002), la Darknet se ha convertido, en los últimos años, en uno de los temas más discutidos en los círculos de ciberseguridad. Para algunos, las redes ocultas en Internet son un medio para alcanzar la libertad; mientras que, para otros, estas redes no son más que nuevas salidas para expresar sus deseos criminógenos. En general, la Darknet tiende a ser representada por varios medios de comunicación como un entorno en el que las actividades delictivas surgen de forma natural, incluso hasta el punto de ser un acto fuera de la legalidad.

El tener acceso a la Dark Web y encontrar sitios ocultos es relativamente fácil Moore y Rid (2016) indica que, la parte más desafiante del trabajo es reducir su búsqueda para encontrar inteligencia de amenazas significativas y procesables. No obstante, cuando se enfatiza en centralizar las herramientas que actúan a favor de la Darknet, estas, materializan un sinnúmero de riesgos que desestabilizan el orden de las naciones. Bailey et al., (2006), expone que los riesgos macro de este entorno cibernético se encuentran en la aplicación y uso de tres herramientas principales: i) vulnerabilidades y exploits; ii) portales de acceso; y iii) uso indiscriminado de contraseñas. Estas herramientas, concebidas como debilidades para las estrategias de protección de un Estado, son precisamente capacidades usadas para contrarrestar delitos cibernéticos.

Al hacer una evaluación precisa de estas herramientas, Fachkha y Debbabi (2015) indica que las vulnerabilidades y exploits son la puerta inicial para ataques y delitos nacionales desde la Darknet. Es claro que todos los medios cibernéticos tienen vulnerabilidades, y esto ha generado que cada vez más proveedores e investigadores de seguridad crean vulnerabilidades de software para proteger a los usuarios de los riesgos resultantes.

Lamentablemente, Wood (2009) afirma que los ciberdelinquentes a veces se adelantan a los proveedores y a las comunidades de seguridad; este adelanto es transferido a los tres niveles de toma de decisiones, sin importar si en el nivel estratégico se invierte en herramientas de alto valor financiero y alta capacidad de protección, dando por sentado que ni las organizaciones ni los Estados logran resguardarse en su totalidad a los daños cibernéticos.

Ante ello, autores como Nunes et al., (2016) expresan que por medio de la Darkweb es posible implementar las vulnerabilidades de día u hora cero; estas, son fallas de



seguridad que aún no son conocidas por el proveedor, además de ser vulnerabilidades a las que aún no se les ha encontrado un método de neutralización. Encontrar información sobre las vulnerabilidades de día cero y los exploits que los piratas informáticos discuten y comercian en los mercados oscuros, permite a los profesionales de seguridad identificar e implementar controles de mitigación temporalmente efectivos, dado que su trascendencia e innovación dependen del progreso y nivel de desarrollo tecnológico y científico.

Además de las vulnerabilidades y los exploits, Broséus (2017) indica que los ciber-delicuentes suelen vender acceso activo a sistemas y dispositivos en los mercados oscuros. Muchos de estos delincuentes se especializan en una fase específica del proceso de piratería, pues aquellos que se destaquen en escanear y obtener acceso a las redes deciden no explotar el objetivo ellos mismos. Estos, indica McCormick (2013) que venden el acceso a otros piratas informáticos que se especializan en una mayor exploración y explotación, generando una cadena interminable de vendedores de datos que se han recopilado a atacantes centrados en la extorsión.

Por otro lado, el uso indiscriminado a contraseñas es expuesto por Benjamín et al., (2019) como una mercancía oscura popular. Las contraseñas, son elementos valiosos para los atacantes cibernéticos, dado que conocen el mal hábito de las personas con respecto a reutilizar sus contraseñas en varias cuentas. Esta herramienta perjudicial de la Darknet busca detectar a aquel personal con información privilegiada de las organizaciones, pues Choi et al., (2014) expresa que los proveedores que buscan vender credenciales, propiedad intelectual o datos corporativos importantes en los mercados oscuros generan ingresos de cantidades significativas.

Cualquier tipo de delito con acciones encubiertas, ya sea que involucre drogas, dinero o incluso seres humanos, puede cometerse en la Dark Web. Los rincones más oscuros de Internet son simplemente una plataforma para innumerables delitos. Si se enlistan estas acciones en contra del estado y de la ciudadanía, McCormick (2013) hace especial énfasis a acciones como el asesinato por contrato, el chantaje o la extorsión, venta de drogas ilegales, ventas ilegales de armas, tráfico sexual, terrorismo, pornografía infantil, entre otros. Cuando la tasa de criminalidad en un Estado crece, se generan amenazas, riesgos y dificultades para la consolidación del territorio. Independientemente del medio o forma en que estos se materialicen, al impactar los principios, prioridades y tareas inherentes de los ciudadanos, concurre entonces en un daño a la seguridad y defensa nacional, la cual, en teoría, es una de las obligaciones primordiales de los niveles estratégicos nacionales.

Si se enfatiza en los cuatro campos del poder de los Estados, Cambiaso et al., (2019) indica que uno de los campos con mayor intervención es el social. En efecto, Wood (2009)

afirma que la Darknet se utiliza para una amplia gama de actividades sociales. Estas, van desde ser claramente aceptables desde el punto de vista moral, hasta ser consideradas como ilícitas por algunas personas, o ser visiblemente delictivas según los marcos legislativos nacionales y/o internacionales. Estas actividades, expone Cohen et al., (2020) que podrían agruparse en tres principales: i) activismo, periodismo y denuncia de irregularidades; ii) actividades delictivas en mercados virtuales; y iii) amenazas a la seguridad cibernética que incluyen botnets, malware y secuestro de datos.

Como cualquier tecnología, Miró (2012) expone que el anonimato se puede utilizar tanto para bien como para mal. Usuarios que temen por represalias económicas o políticas por sus acciones usan la web oscura para su protección. Pero también, están aquellos que aprovechan este anonimato en línea para utilizar el Dark Web para actividades ilegales como sustancias ilegales, comercio, transacciones financieras ilegales, robo de identidad, entre otros. Aquí, Rayón y Gómez (2014) indica que el crimen virtual no es diferente al crimen en el mundo real, simplemente se ejecuta en un nuevo medio; es básicamente lo mismo que el crimen terrestre. Sin duda, algunas de las manifestaciones son nuevas, pero una gran cantidad de delitos cometidos con o contra computadoras difiere solo en términos del medio. Mientras que la tecnología de implementación, y particularmente su eficiencia, puede ser sin precedentes, el crimen es fundamentalmente familiar. Este se trata de un fenómeno que hace uso de nuevas herramientas.

Generalmente, las herramientas que atacan la estabilidad de los Estados, aun al estar relacionadas con otros niveles de toma de decisión, Sánchez (2012) afirma que no hay nada único o nuevo en gran parte del ciberdelito: acoso, fraude, propaganda ilegal, pornografía, hurto, blanqueo de capitales, espionaje, etc., excepto el uso del ciberespacio. Pero hay otro nivel de delincuencia que no podría existir sin el ciberespacio: spam, fraude de clics, varios tipos de malware, redes de computadoras cautivas (botnets), robo de identidad, camuflaje y cifrado de datos y comunicaciones, infracciones informatizadas de instalaciones seguras de gran valor, y automáticas, espionaje a largo plazo en organizaciones seguras, entre otros.

Los ciberdelincuentes, indica Brenner (2012) que están explotando el valor creciente de los datos digitales en todas sus formas, y las formas legales y judiciales en las que diferentes países manejan el ciberespacio. Por su parte, Camacho (2020) expone que el crimen siempre ha sido un fenómeno social generalizado, pues las explicaciones criminológicas combinan la motivación, la oportunidad y la existencia de un factor de protección. Aquí, Temperedi y Marcelo (2015) afirma que dos fuentes diferentes de motivación humana pueden ser identificadas. Muchos motivos del comportamiento delictivo son intrínsecos y no se determinan mediante un análisis de costo-beneficio. No hay razón para creer que un mayor uso de una tecnología u otra cambiaría a los seres humanos su

comportamiento. Por tanto, no es sorprendente que las personas también utilicen el ciberespacio para darse cuenta de sus necesidades y perseguir sus objetivos en actividades legítimas: estudiar, entretenimiento, educación, trabajo, así como en las actividades humanas ancestrales de la guerra y el crimen.

Aunque las naciones desarrolladas han instituido la aplicación de la ley regulada ante los ciberdelitos, sus amenazas y consecuencias, las respuestas estatales no han seguido el ritmo de cambios tecnológicos en el ciberespacio. Un buen ejemplo es expuesto por Piccirilli (2016) como el tradicional atraco a un banco en comparación con el robo cibernético, entendiendo que no es lo mismo desarrollar un seguimiento en el ciberespacio bajo una ruta común como el internet que, bajo la ruta permitida por la Dark Web. El uso de la Dark Web expone efectivamente las debilidades de las instituciones de control y monitoreo de los Estados, desestabilizando factores como la institucionalidad, la misionalidad, la integridad, entre otros.

En una seguridad tradicional de robo a un banco, los arreglos deben ser moderados como la posibilidad de un enfrentamiento con armados, dado que es probable que haya guardias. Incluso si el robo en sí tiene éxito, las autoridades logran perseguir a los ladrones en los años venideros. A medida que se ha desarrollado el ciberespacio, la explotación de su vulnerabilidad también ha llegado a abarcar el robo de bancos. Por otro lado, otro ejemplo es indicado por Ballesteros y Hernández (2014), cuando el uso de redes de bots<sup>3</sup> que comprenden decenas de miles de computadoras para el robo extendido de datos de identificación a sitios bancarios, luego se utilizan para robar pequeñas cantidades de dinero, es bastante común.

Dado el problema de atribución en el ciberespacio, las posibilidades de identificar los delincuentes y protagonistas son escasos. Arango (2017) indica que todas las organizaciones que manejan información de alto valor, entre ellas las naciones, son muy conscientes del riesgo de sus intereses y, junto con los organismos reguladores, están tomando pasos para protegerse, invirtiendo en seguridad tecnológica para minimizar el alcance de oportunidad disponible para los ciber delincuentes. Aun así, lo inmediato del riesgo físico sigue siendo sustancialmente menor para el delincuente cibernético que para el delincuente tradicional. El riesgo de castigo legal también es menor, ya que el sistema judicial generalmente percibe el fraude cibernético como un delito de cuello blanco y tratado en consecuencia.

---

3 Es un programa informático que efectúa automáticamente tareas reiterativas mediante Internet a través de una cadena de comandos o funciones autónomas previas para asignar un rol establecido.

## Escenario de ciberseguridad vinculado a los efectos y consecuencias del uso de las herramientas de la Dark Web como medio para la desestabilización nacional.

Para autores como Gayozzo (2021), los escenarios bélicos actuales se encuentran compuestos por una gran cantidad de factores ajenos a los actos y costumbres de guerra cotidiana. De hecho, estos escenarios se encuentran amarrados y adaptados a cualquier forma de guerra, la cual, aun con estar limitada y monitoreada legalmente, ha tenido grandes mutaciones derivadas del desarrollo tecnológico, científico y militar de los Estados. Hoy por hoy, Gil (2019) expone que, entre estos escenarios, existe la necesidad de proponer y/o identificar las estrategias de protección y contención hacia ambientes como el ciberespacio, precisamente aquellos que prosperan en contextos como la Dark Web. El ciberespacio indica Leal (2016) que es un componente integral de todas las facetas de la sociedad, incluida la economía y la defensa. Sin embargo, las entidades públicas y privadas aún luchan por proteger sus sistemas, y los adversarios han aumentado la frecuencia y la sofisticación de sus actividades cibernéticas maliciosas. Una de estas amenazas es conocida como *Ransomware*, expuesta por XXX como aquel un tipo de software malicioso que impide o limita que los usuarios accedan a su sistema, ya sea bloqueando la pantalla del sistema o bloqueando los archivos de los usuarios hasta que se pague un rescate.

Esto, afirma San Martín (2019) que ha llevado a un mayor interés en otros temas, además de los militares tradicionales, dado que las amenazas contra los Estados, en particular el poder blando y otros medios de influencia no militar, han permeado las actividades cotidianas de la ciudadanía; Colombia, no es una excepción a ello. En la definición original, Fernández-Sánchez (2016) indica que el poder blando es similar al poder de atracción, pero, la reinterpretación del mismo también implica la posibilidad de ejercer un poder blando contra otros actores, con el fin de ganar influencia o participar en una guerra no militar.

Ante estas circunstancias, naciones como Colombia, expuestas a amenazas tanto internas como externas, debe buscar la aplicación de estrategias ante escenarios como el cibernético, dado que atacan la seguridad de una manera silenciosa pero incisiva. Badrán y Niño (2020) exponen que la prosperidad y la seguridad de Colombia dependen de cómo responder a las oportunidades y desafíos en el ciberespacio, en la infraestructura crítica, en la defensa nacional y en la vida diaria de los colombianos. Generalmente, un espacio competente para soportar cualquier intento de daño o intervención se basa en tecnologías de la información interconectadas e impulsadas por computadoras, precisamente alineadas a la vanguardia tecnológica del momento. Aquí, gracias a que todas las facetas de la vida se han vuelto más dependientes a un ciberespacio seguro, se han revelado nuevas vulnerabilidades y nuevas amenazas.

El auge del internet y la creciente centralidad del ciberespacio a todas las facetas del mundo moderno corresponden al ascenso de las naciones en dinámicas como la globalización. Llinares (2011) afirma que al menos por el pasado cuarto de siglo, la gente impulsó la evolución del ciberespacio, y a su vez, este logró consolidarse como fundamental para la creación e innovación de riqueza en los Estados. Por ello, el ciberespacio es un componente inseparable de los servicios financieros, sociales, gubernamentales y políticos. No obstante, al menos en Colombia, existen adversarios que han adoptado un enfoque opuesto, pues se benefician del Internet abierto. Estos, generalmente, se esconden detrás de las nociones de soberanía mientras imprudentemente violan las leyes al participar en espionaje pernicioso, económico y malicioso, además de sostener actividades cibernéticas que provocan importantes interrupciones y daño a personas. Estos, indica Zarate (2014) que ven el ciberespacio como una arena donde el poder militar, económico y político podría ser neutralizado, siendo entonces Colombia una nación altamente vulnerable.

En este contexto, las nuevas amenazas y una nueva era de competencia estratégica exigen una nueva estrategia cibernética que responda a realidades, reduzca vulnerabilidades, disuada adversarios y salvaguarde las oportunidades para que el pueblo colombiano prospere. Asegurar el ciberespacio es fundamental para la estrategia nacional y requiere avances técnicos y administrativos de gran eficiencia en todo el Gobierno Nacional. Ambos (2015), indica que también se debe reconocer que un enfoque puramente tecnocrático al ciberespacio es insuficiente para abordar la naturaleza de los nuevos problemas que se enfrentan.

Como ejemplo a ello, Sohr (2018) expone que los Estados participan en una competencia continua contra adversarios estratégicos, estados rebeldes y redes terroristas y criminales. Al hacer mención de actores como Estados Unidos, Aguilar (2021) indica que Rusia, China, Irán y Corea del Norte utilizan al ciberespacio como un medio para desafiar a los Estados Unidos, a sus aliados, y a sus socios, siendo a menudo una imprudencia que no fue considerada en otros dominios. Estos utilizan herramientas cibernéticas para socavar la economía y democracia norteamericana, entendiendo que entre estos Estados existe una carrera de dominio y control del orden internacional.

Ante el orden y la necesidad que concurre para proteger el Estado y las actividades de la nación colombiana, Recalde (2021) expresa que es necesario implantar o reforzar la actual estrategia cibernética. Esta, debe contener prioridades como: i) defender la patria protegiendo las redes, sistemas, funciones y datos; ii) promover la prosperidad mediante el fomento de una economía digital y próspera, fomentando la innovación e investigación nacional; iii) preservar la paz y seguridad fortaleciendo la capacidad colombiana, en concierto con aliados y socios, para disuadir y si es necesario castigar a quienes utilicen herramientas cibernéticas con fines maliciosos; y iv) expandir la influencia colombiana

en el extranjero para extender los principios claves de un ciberespacio abierto, interoperable, confiable y seguro.

Por ello, el éxito de la estrategia colombiana podría hacerse realidad cuando las vulnerabilidades de la ciberseguridad sean efectivamente gestionadas mediante la identificación y protección de redes, sistemas, funciones y datos, así como la detección de las mismas en cuestiones perjudiciales, desestabilizadoras, maliciosas y negativas. La articulación de escenarios acordes a combatir herramientas como la Dark Web debe estar organizada según los pilares de la Política de Defensa y Seguridad Nacional de Colombia, haciendo valer los lineamientos de ciberseguridad y ciberdefensa inscritos en el CONPES 3701 con respecto al control, monitoreo y/o neutralización de las amenazas informáticas que atacan significativamente al Estado colombiano.

La responsabilidad de asegurar la infraestructura crítica de la nación y su gestión en escenarios como el que concurre en el ciberespacio es compartido por el sector privado y gubernamental, situación establecida de forma clara durante el Plan Sectorial de Protección y Defensa para la Infraestructura Crítica Cibernética de Colombia (2018). En asociación con el sector privado, es posible utilizar de forma colectiva una gestión de riesgos enfocada para mitigar las vulnerabilidades y aumentar el nivel básico de ciberseguridad en toda la infraestructura crítica. Simultáneamente, Cujabante et al., (2020) afirma que instituciones como las Fuerzas Militares de Colombia- FFMM han venido implantando un enfoque basado en consecuencias para priorizar las acciones, entendiendo que estas estrategias podrían reducir el potencial de adversarios expertos, quienes precisamente podrían causar interrupciones a gran escala o de larga duración en la infraestructura crítica.

Asimismo, la nación tendría que buscar la forma de disuadir a los ciber actores malintencionados, imponiendo para ellos y para sus patrocinadores una variedad de herramientas, que incluyen, pero no se limitan, a enjuiciamientos y sanciones económicas, como parte de una estrategia de disuasión más amplia. Esto, por ejemplo, se encuentra fundamentado bajo esfuerzos multilaterales de organizaciones como la OTAN y la UE, estableciendo leyes en el contexto de la ciberdefensa como el *Tallinn Manual on the International Law Applicable to Cyber Operations*, buscando establecer políticas comunes de acuerdo con la importancia estratégica y operativa en materia de ciberseguridad y ciberdefensa.

Por su parte, González (2016) sugiere que la administración nacional antes de enfocarse en establecer un escenario próspero y propicio para el desarrollo de la nación, debe aclarar los roles y responsabilidades de los organismos e instituciones de control que se encuentren dirigidas a la ciberseguridad, gestión de riesgos y respuesta a incidentes. Esta claridad permitirá una gestión proactiva de riesgos que abordaría de manera integral las amenazas, vulnerabilidades y consecuencias.

## Conclusiones

Este artículo de investigación permitió conocer de forma académica cuál es la finalidad de desestabilización nacional en el contexto cibernético de la Dark Web, además de mencionar aquellas herramientas que promueven los daños y la afectación a la seguridad nacional. Tanto la finalidad como las herramientas que actúan paralelamente con la Dark Web, deben ser consideradas como componentes que se desarrollan bajo escenarios cibernéticos de difícil seguimiento y fácil mimetismo, los cuales, en teoría, debilitan los esfuerzos de monitoreo, control y rastreo creados por instituciones como las Fuerzas Militares-FFMM y la Policía Nacional. Aquí, es necesario alertar a las estrategias tanto gubernamentales como operativas sobre la necesidad de intrusión, formación y/o reforzamiento tanto del recurso humano como de la infraestructura crítica delegada para las actividades de ciberseguridad y ciberdefensa de la nación, pues componentes como el tecnológico y científico son básicamente catalizadores tanto de protección como de exposición ante este tipo de amenazas.

Asimismo, la nación colombiana está constantemente tratando de presentar nuevas aplicaciones y tecnologías que mejoren las viejas formas de proteger el ciberespacio, ofreciendo nuevas funciones útiles. Pero, la atención a la ciberseguridad puede ralentizar la introducción de nuevos productos y servicios en el mercado, tanto legal como ilegal, con el resultado de que las nuevas tecnologías y aplicaciones a menudo se ofrecen para uso general sin el beneficio de una revisión para una ciberseguridad eficaz. La cuestión de la actividad gubernamental es cómo gestionar el equilibrio entre el ritmo de la innovación y una postura de ciberseguridad más sólida, sin generar entradas a entornos de alto impacto como la Dark Web, entendiendo que su existencia hoy en día ha generado grandes debilidades para la estabilidad de los Estados.

Por otro lado, aun con tener capacidades en infraestructura cibernética significativas, es necesario promover en Colombia una infraestructura cibernética acorde con la evolución tecnológica mundial, la cual cuente con una capacidad de comunicaciones y conectividad interoperable, confiable y segura. Esto proporcionará mayores oportunidades para todos los sectores nacionales. Esto permitirá proteger la nación y los intereses mediante el fortalecimiento de la posición competitiva de la industria en el mundo digital, apoyando y promoviendo prácticas legales en el uso del espacio cibernético, lideradas por la industria y basadas en principios tecnológicos sólidos.

Finalmente, la competencia técnica y la conciencia se consideran cuestiones urgentes para lograr efectivas estrategias en torno a la ciberseguridad en naciones tales como Colombia. Gran parte de este conocimiento es tácito y su relación con la ciberseguridad es directa. Ante ello, existen aspectos por los cuales la nación y su estrategia de control, monitoreo y neutralización de amenazas dependen de forma explícita; la primera, la limitación de recursos es evidente, pero la limitación también influye en

la forma de la estrategia; y la segunda, el progreso y no contención de herramientas de desestabilización como la Dark Web, provee en su mayoría grandes habilidades poco rastreables y detectables, siendo entonces una alerta y alarma para los entes de control gubernamental atentos a eliminar y neutralizar cualquier acción que desestabilice el Estado colombiano.

## Declaración de divulgación

Los autores declaran que no existe ningún potencial conflicto de interés relacionado con el artículo.

## Autor

**Hugo Rene Aguillon Gómez.** Magister en Escuela Superior de Guerra General "Rafael Reyes Prieto", Colombia.

Orcid: <https://orcid.org/0000-0002-1174-3585> Contacto: [aguillonh@esdeg.edu.co](mailto:aguillonh@esdeg.edu.co)

## Referencias

- Acosta, P., Rodríguez, P., Arnáiz de la Torre, D., & Taboso Ballesteros, P. (2009). *Seguridad nacional y ciberdefensa*. Centro Superior de Estudios de la Defensa Nacional. Catálogo General de Publicaciones Oficiales <http://publicacionesoficiales.boe.es/>
- Aguilar Cárceles, M. M. (2015). Cibercrimen y cibervictimización en Europa: instituciones involucradas en la prevención del cibercrimen en el Reino Unido. *Revista criminalidad*, 57(1), 121-135.
- Aguilar, J. S. (2021). *Omnium contra omnes: Análisis político-militar de la guerra en el ciberespacio*. Nau Llibres.
- Ambos, K. (2015). *Responsabilidad penal internacional en el ciberespacio*. Universidad Externado.
- Arango, R. A. P. (2017). Afectación del cibercrimen en las pymes. La corrupción en la contratación administrativa: el caso de Costa Rica, 8-59 [Conferencia]. 2° Congreso Internacional Crimen económico y fraude financiero y contable
- Atienza, G. M., & Bermejo, D. F. (2020). *Cibercrimen*. Ediciones Experiencia.
- Badrán, F., & Niño, C. (2020). Seguridad nacional de Colombia: aproximación crítica a los contrasentidos misionales. *Pensamiento propio*, 51, 103-118.
- Bailey, M., Cooke, E., Jahanian, F., Myrick, A., & Sinha, S. (2006, March). *Practical darknet measurement*. In *2006 40th Annual Conference on Information Sciences and Systems* (pp. 1496-1501). Institute of Electrical and Electronics Engineers.
- Ballesteros, M. C. R., & Hernández, J. A. G. (2014). Cibercrimen: particularidades en su investigación y enjuiciamiento. *Anuario Jurídico y Económico Escurialense*, (47), 209-234.
- Baluja-García, Walter, & Anías-Calderón, Caridad (2006). Amenazas y defensas de seguridad en las redes de próxima generación. *Ingeniería y Competitividad*, 8(2),7-16. <https://www.redalyc.org/articulo.oa?id=2913/291323467001>
- Baravalle, A., Lopez, M. S., & Lee, S. W. (2016, December). *Mining the dark web: Drugs and fake IDs*. In *2016 IEEE 16th International Conference on Data Mining Workshops (ICDMW)* (pp. 350-356). Institute of Electrical and Electronics Engineers.
- Barrio Andrés, M. (2017). *Cibercrimen: amenazas criminales del ciberespacio*. Editorial Aranzadi.



- Benjamín, V., Valacich, J. S., & Chen, H. (2019). DICE-E: A Framework for Conducting Darknet Identification, Collection, Evaluation with Ethics. *MIS Quarterly*, 43(1).
- Biddle, P., England, P., Peinado, M., & Willman, B. (2002, November). *The darknet and the future of content protection*. In *ACM Workshop on Digital Rights Management* (pp. 155-176). Springer
- Brenner, S. (2012). La Convención sobre Cibercrimen del Consejo de Europa. *Revista Chilena de Derecho y Tecnología*, 1(1).
- Broséus, J., Rhumorbarbe, D., Morelato, M., Staehli, L., & Rossy, Q. (2017). A geographical analysis of trafficking on a popular darknet market. *Forensic science international*, 277, 88-102.
- Camacho, D. (2020). AIDACyber: contribuciones en ciberseguridad y cibercrimen. *Information Fusion*, 63, 1-33.
- Cambiaso, E., Vaccari, I., Patti, L., & Aiello, M. (2019, February). *Darknet Security: A Categorization of Attacks to the Tor Network*. In ITASEC.
- Chen, T. M., & Abu-Nimeh, S. (2011). Lessons from stuxnet. *Computer*, 44(4), 91-93.
- Chertoff, M. (2017). A public policy perspective of the Dark Web. *Journal of Cyber Policy*, 2(1), 26-38.
- Choi, S. S., Song, J., Kim, S., & Kim, S. (2014). A model of analyzing cyber threats trend and tracing potential attackers based on darknet traffic. *Security and Communication Networks*, 7(10), 1612-1621.
- Cohen, D., Mirsky, Y., Kamp, M., Martin, T., Elovici, Y., Puzis, R., & Shabtai, A. (2020, September). DANTE: A framework for mining and monitoring darknet traffic. In *European Symposium on Research in Computer Security* (pp. 88-109). Springer, Cham.
- Crystal, D., & Tena, P. (2002). *El lenguaje e Internet* (p. 304). Cambridge university press.
- Cujabante Villamil, X. A., Bahamón Jara, M. L., Prieto Venegas, J. C., & Quiroga Aguilar, J. A. (2020). Ciberseguridad y ciberdefensa en Colombia: un posible modelo a seguir en las relaciones cívico-militares. *Revista Científica General José María Córdova*, 18(30), 357- 377. <http://dx.doi.org/10.21830/19006586.588>
- Fachkha, C., & Debbabi, M. (2015). Darknet as a source of cyber intelligence: Survey, taxonomy, and characterization. *Communications Surveys & Tutorials*, 18(2), 1197-1227.
- Farwell, J. P., & Rohozinski, R. (2011). Stuxnet and the future of cyber war. *Survival*, 53(1), 23-40.
- Fernández, H. M. M. (2016). As novas guerras: O desafio da guerra híbrida. *Revista de Ciências Militares*, 4.
- Fernández-Sánchez, Pablo Antonio (2016). Introducción: Riesgos y amenazas para la seguridad humana. Araucaria. *Revista Iberoamericana de Filosofía, Política y Humanidades*, 18(36),211-215. <https://www.redalyc.org/articulo.oa?id=282/28248171010>.
- Fidler, D. P. (2011). Was stuxnet an act of war? decoding a cyberattack. *Security & Privacy*, 9(4), 56-59.
- Galindo Hernández, C. (2005). De la Seguridad Nacional a la Seguridad Democrática: nuevos problemas, viejos esquemas. *Estudios Socio-Jurídicos*, 7, 496.
- Gamón, V. P. (2017). Internet, la nueva era del delito: cibercrimen, ciberterrorismo, legislación y ciberseguridad. *URVIO: Revista Latinoamericana de Estudios de Seguridad*, (20), 80-93.
- Gayozzo, P. I. E. R. O. (2021). Guerra de quinta generación en la Cuarta Revolución Industrial. *Futuro Hoy*, 2(1), 31-34.
- Gómez, F., Vélez, F., Estesio, F., Pascual, D., Pita, R., García, J., & De la Corte Ibáñez, L. (2014). *Seguridad nacional, amenazas y respuestas*. Editorial Almuzara.
- González, C. L. (2016). Ciberespacio: un nuevo dominio, un nuevo reto...(I). *Armas y Cuerpos*, (133), 57-64.
- He, B., Patel, M., Zhang, Z., & Chang, K. C. C. (2007). Accessing the deep web. *Communications of the ACM*, 50(5), 94-101.
- Hernández Sampieri, R., Fernández Collado, C., & Baptista Lucio, P. (2014). *Metodología de la Investigación* (6ta. ed.). (S. d. Interamericana Editores, Ed.). Mc Graw Hill

- Hirane, C. S. (2021). Estrategia Nacional Contra la Delincuencia Organizada Transnacional (DOT) en países Latinoamericanos: ¿desafío de política pública pendiente?. *Análisis del Real Instituto Elcano (ARI)*, (20), 1.
- Huidobro, C. B., & Guerrero, S. R. (2021). *Amenazados: Seguridad e inseguridad en la web*. Ediciones UM.
- Ibáñez, E. M. (2017). *Dark web y deep web como fuentes de ciberinteligencia utilizando minería de datos*. 3ª ÉPOCA, 74.
- Leal, P. C. (2016). A guerra híbrida. *Doutrina Militar Terrestre em Revista*, 4(9), 6-17.
- Llinares, F. M. (2011). La oportunidad criminal en el ciberespacio. *Revista Electrónica de Ciencia Penal y Criminología*, 7, 1-07.
- López Flores, E. D. (2019). *El delito de narcotráfico en la Deep Web: Una visión desde la Legislación Ecuatoriana* [Bachelor's thesis]. Universidad San Francisco de Quito.
- Madhavan, J., Ko, D., Kot, L., Ganapathy, V., Rasmussen, A., & Halevy, A. (2008). Google's deep web crawl. *Proceedings of the VLDB Endowment*, 1(2), 1241-1252.
- Mariano Díaz, R. (2020). *La ciberseguridad en tiempos del COVID-19 y el tránsito hacia una ciberinmuni-dad*. Comisión Económica para América Latina y el Caribe.
- Marín, J., Nieto, Y., Huertas, F., & Montenegro, C. (2019). Modelo Ontológico de los Ciberdelitos: Caso de estudio Colombia. *Revista Ibérica de Sistemas e Tecnologías de Informação*, (E17), 244-257.
- McCormick, T. (2013). The Darknet. *Foreign Policy*, (203), 22.
- Miguel-Gil, J. (2019). El tratamiento informativo de la guerra híbrida de Rusia. *URVIO Revista Latinoamericana de Estudios de Seguridad*, (25), 108-121.
- Miró Llinares, F. (2012). El cibercrimen: Fenomenología y criminología de la delincuencia en el ciberespacio. *El cibercrimen*, 1-332.
- Moore, D., & Rid, T. (2016). Cryptopolitik and the Darknet. *Survival*, 58(1), 7-38.
- Nunes, E., Diab, A., Gunn, A., Marin, E., Mishra, V., Paliath, V., & Shakarian, P. (2016, September). *Darknet and deepnet mining for proactive cybersecurity threat intelligence*. In 2016 IEEE Conference on Intelligence and Security Informatics (ISI) (pp. 7-12). IEEE.
- Ortega, P., & Font, T. (2012). Seguridad nacional, seguridad multidimensional, seguridad humana. *Papeles de relaciones Ecosociales y Cambio Global*, 119, 161-172.
- Parno, B., McCune, J. M., Wendlandt, D., Andersen, D. G., & Perrig, A. (2009, May). *CLAMP: Practical prevention of large-scale data leaks*. In 2009 30th IEEE Symposium on Security and Privacy (pp. 154-169). Institute of Electrical and Electronics Engineers.
- Piccirilli, D. (2016). *Protocolos a aplicar en la forensia informática en el marco de las nuevas tecnologías (pericia-forensia y cibercrimen)* [Doctoral dissertation]. Universidad Nacional de La Plata).
- Prandini, P., Maggiore, M., & Carozo, E. (2011). *Panorama del ciberdelito en Latinoamérica*. Proyecto Amparo-Registro de Direcciones de Internet para Latinoamérica y el Caribe (LACNIC).
- Ramírez Perea, N. (2020). *Criminología y las nuevas tecnologías*. Universitat Jaume I. Departament de Dret Públic.
- Rayón Ballesteros, M. C., & Gómez Hernández, J. A. (2014). Cibercrimen: particularidades en su investigación y enjuiciamiento. *Anuario Jurídico y Económico Escurialense*, (47), 209-234.
- Recalde, L. (2021). El ciberespacio: el nuevo teatro de guerra global. *Revista de Ciencias de Seguridad y Defensa*, 1(2), 5.
- Riva, R. C. (2016). El nuevo entorno digital de la actividad criminal/a new digital environment for criminal activity. *Boletín de Estudios Económicos*, 71(219), 591.
- Rodríguez Prieto, Rafael (2016). ¿Qué seguridad? Riesgos y Amenazas de Internet en la Seguridad Humana. Araucaria. *Revista Iberoamericana de Filosofía, Política y Humanidades*, 18(36),391-415.
- San Martín, H. (2019). *La guerra híbrida rusa sobre Occidente*. Page Publishing Inc.

- Sánchez Medero, G. (2012). *Cibercrimen, ciberterrorismo y ciberguerra: los nuevos desafíos del s. XXI*. Thumbnail.
- Shu, X., Zhang, J., Yao, D. D., & Feng, W. C. (2015). Fast detection of transformed data leaks. *Transactions on Information Forensics and Security*, 11(3), 528-542.
- Sifry, M. L. (2011). *WikiLeaks and the Age of Transparency*. OR Books.
- Sohr, R. (2018). La guerra por las mentes en el ciberespacio. *Mensaje*, 67(667), 18-21.
- Temperini, M. G., & Macedo, M. (2015). *La problemática de los perfiles falsos en Facebook y su relación con el Cibercrimen*. In *Simposio Argentino de Informática y Derecho (SID 2015)-JAIIO 44* (Rosario, 2015).
- Wood, J. A. (2009). The Darknet: A digital copyright revolution. *Rich. JL & Tech.*, 16, 1.
- Zárate Luna, P. A. (2014). *Guerra por el Ciberespacio* [Bachelor's thesis]. Universidad Piloto de Colombia).

# 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 Transnacionales.

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.

## Abstract



## 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 delincencial 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 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 Armados 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 delictivas 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 Transnacionales (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 Delincuencias 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 delinquir 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 Transnacionales (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 desafío 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 Transnacionales 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 Transnacionales (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
<b>Prioritario</b>	Cauca, Chocó, Nariño, Norte de Santander, Putumayo, Valle de Cauca y Vichada
<b>Alta</b>	Amazonas, Antioquia, Arauca, Bolívar, Caquetá, Córdoba, Guaviare, Meta, Santander y Vaupés
<b>Media</b>	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 extrema*, 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 Transnacionales (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 delictivas 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, urbano, 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 crítica 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 parelice, 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 cimiento 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 Críticas 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 Crítica 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 cierta 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 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 realizar 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

umenta, 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 sabotaje 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 riesgos, 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 ransomware, 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 Transnacionales (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 delincriminal 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 Ejército, 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](mailto: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](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 12 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 Críticas 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](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 prosperous Canada*. Minister of public Safety.
- Hernández, J. (2016). *Infraestructura crítica cibernética*. Comando General de las Fuerzas Militares. <https://acis.org.co/archivos/Conferencias/2016/GuialCC.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\\_Terrorist\\_Purposes/Use\\_of\\_Internet\\_Ebook\\_SPANISH\\_for\\_web.pdf](https://www.unodc.org/documents/terrorism/Publications/Use_of_Internet_for_Terrorist_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](http://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](https://www.nato.int/cps/en/natohq/official_texts_133177.htm)
- Osoario, 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](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.

# Aplicaciones de los sistemas de aeronaves remotamente tripuladas para la seguridad y defensa nacional

Applications of remotely manned aircraft systems for national security and defense

DOI: <https://doi.org/10.25062/2955-0270.4772>

German Quintero Morales  Omar Leonardo Salas Galindo 

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

## Resumen

La utilización de los sistemas no tripulados para la defensa y seguridad de una nación son esenciales en la actualidad, abarcan toda una gama de sistemas para la protección de la soberanía y el sostenimiento del bienestar requerido por la población, es así, que casi todos los países tienen un alto grado de utilización de esta tecnología, bien sea en forma adquirida o por desarrollo propio, para lo cual, los estados invierten grandes recursos que les permitan apropiarla y a su vez logran posicionarse a nivel mundial en esta área. Ahora mismo, los sistemas no tripulados también juegan un papel muy importante en el avance económico de las naciones, toda vez que, contemplan varios campos donde se pueden desempeñar como tecnologías de uso dual, tanto a nivel civil como a nivel militar, siendo este último, principalmente, el campo de aplicación que se desea analizar en el presente artículo. La facilidad de su utilización y el bajo costo de desarrollo de los sistemas no tripulados civiles actuales, permiten que cualquier persona pueda acceder a ellos y operarlos incluso con fines económicos; por otra parte, los sistemas no tripulados militares tienen una concepción orientada a su utilización en los diferentes teatros de operación del multidominio, con capacidad de cumplir un amplio espectro de misiones y tareas, dependiendo de sus capacidades, las cuales van desde la vigilancia, interferencia electrónica, pasando por la aplicación de la fuerza y hasta con disposición para el combate aire-superficie y aire-aire.

En este artículo se desea hacer una verificación de las aplicaciones actuales que tienen los sistemas no tripulados en el campo civil y principalmente en el campo militar, pensando en la seguridad y defensa la nación.

**Palabras Clave:** Sistema no tripulado, Drone, RPA, UCAV, UAV, Aplicaciones Militares.

The use of unmanned systems for the defense and security of a nation are essential today, covering a wide range of systems for the protection of sovereignty and the maintenance of the welfare required by the population, so that almost all countries have a high degree of use of this technology, either acquired or self-developed, for which the states invest large resources that allow them to appropriate it and in turn manage to position themselves globally in this area. Right now, unmanned systems also play a very important role in the economic progress of nations, since they contemplate several fields where they can be used as dual-use technologies, both at civil and military level, being the latter, mainly, the field of application to be analyzed in this article. The ease of use and low development cost of current civilian unmanned systems allow anyone to access and operate them, even for economic purposes; on the other hand, military unmanned systems are designed for use in the different theaters of operation of the multi-domain, with the ability to perform a wide range of missions and tasks, depending on their capabilities, ranging from surveillance, electronic jamming, through the application of force and even with provision for air-to-surface and air-to-air combat.

In this article we want to verify the current applications that unmanned systems have in the civil field and mainly in the military field, thinking about the security and defense of the nation.


**Key words:** Unmanned Aerial Vehicle, Drone, RPA, UCAV, UAV, Military Applications.

## Abstract



Artículo de reflexión

Recibido: 24 de marzo de 2023 • Aceptado: 6 de junio de 2023

Contacto: German Quintero Morales  [quinteromg@esdeg.edu.co](mailto:quinteromg@esdeg.edu.co)

## Introducción

Desde la primera revolución industrial a mediados del siglo XVIII, el desarrollo de la industria y la tecnología en todas las áreas ha sido notable, esto puede ser recientemente apreciado en el campo de la automatización de máquinas y sistemas. En el campo militar, la automatización de la tecnología es mucho más evidente, ya que, a través de los años, los sistemas de armas son cada vez más sofisticados, toda vez que, desde la aparición de la aviación en 1903, la evolución del poder aéreo en el siglo XX ha sido fundamental para todos los estados, sobre todo de las grandes potencias; evidenciándose mediante su participación casi todos los conflictos del siglo XX y XXI.

El gran avance de la tecnología militar aeronáutica / aeroespacial, puede ser observado a través de los años, desde sus inicios en la I Guerra Mundial, como vehículos utilizados simplemente para la observación del enemigo, hasta llegar a ser el equipo militar de vanguardia en cualquier tipo de confrontación presente, capacidades que, a su vez, son un elemento esencial para sostenimiento del estatus quo de paz, principalmente entre los países más poderosos del sistema internacional.

En relación a los sistemas no tripulados, éstos fueron creados a mediados de 1918 a partir de la implementación de un control de vuelo que permitiera remplazar al piloto por un sistema de vuelo completamente automático, buscando evitar los problemas sobrevenientes de la naturaleza humana en relación con sus limitaciones, en ese momento, se desarrolló un sistema giroestabilizador que permitía el control completo de la aeronave, este fué el denominado "*Curtiss-Sperry Aerial Torpedo*", desarrollado como un torpedo aéreo para la Marina de los Estados Unidos (Cuerno-Rejado et al., 2016), sin embargo no pudo ser utilizado en el campo de batalla, toda vez que coincidió con el fin de la Primera Guerra mundial (Newcome, 2004); es a partir de este desarrollo, que el sistema de control de la aeronave pudo ser sustituido por un mando a distancia, el cual, ahora se conoce como sistema no tripulado y que también puede ser preprogramado para el caso de cohetes y misiles guiados (Singhal et al., 2018).

Los sistemas no tripulados tienen varios nombres en la actualidad, algunos de ellos se conocen como RPA por las palabras *Remote Pilot Aircraft* o UAV por *Unmanned Aerial Vehicle* que significan aeronave remotamente tripulada de acuerdo a la Organización de Aviación Civil Internacional – OACI, también pueden conocerse popularmente como Drone que proviene de la palabra anglosajona zumbido (Martínez, 2020), palabras que durante el artículo podemos encontrar y que se pueden usar indiscriminadamente.

Con la aparición de los sistemas no tripulados, tanto las guerras regulares como las irregulares han sufrido grandes transformaciones en las formas de enfrentamiento, donde ya no se requiere la presencia de un soldado o grupo especializado buscando

objetivos, sino que se utiliza un sistema que aplica la fuerza y el poder de combate con precisión para ubicar y neutralizar blancos estratégicos, también se pueden aplicarse para la vigilancia de áreas enemigas y apoyar las labores de inteligencia, por otra parte, se debe tener en cuenta que el costo beneficio es un factor muy relevante para ser considerado, en comparación con la aviación tripulada (Merola et al, s.f.).

Aprovechando las capacidades de la tecnología y la reducción de costos de los sistemas no tripulados, éstos han permitido que sean de aplicación militar como para la aplicación en el campo civil, donde, se tiene un sinnúmero de equipos y sistemas disponibles, que van desde los sistemas nano hasta los sistemas estratégicos, los cuales pueden participar en el reconocimiento y vigilancia de zonas, comunicaciones, entrega de armamento en tierra, combate aéreo, llegando a participar en la entrega de suministros y hasta en la prestación de servicios médicos (Sivakumar & Malleswari, 2021).

Sobre el punto anterior, el presente artículo pretende abordar la investigación de las aplicaciones actuales y futuras de los sistemas no tripulados, RPAs, UAVs o Drones, que puedan ser utilizados en el campo civil, pero, principalmente para la defensa y seguridad de Colombia, para esto, se plantea la siguiente pregunta: **¿Qué aplicaciones se han investigado de los sistemas de aeronaves remotamente tripuladas para la seguridad y defensa nacional?** Esta pregunta se crea, en razón a que actualmente en el país se tiene la capacidad militar de utilizar los sistemas no tripulados para labores de inteligencia, vigilancia y reconocimiento principalmente, pero, no se tiene previsto a corto plazo por parte de las FF.MM. que sean utilizados en otro tipo de aplicaciones que pueden potenciar en gran medida las capacidades militares aéreas del país; sobre todo y teniendo en cuenta, que naciones con gran poderío armamentista como Estados Unidos, Rusia o Israel, usan esta tecnología en muchas más aplicaciones militares. También, para responder la pregunta, se debe tener en cuenta la normatividad existente a nivel mundial para esta tecnología, principalmente en lo relacionado con los Derechos Humanos y la capacidad de vuelo en espacio aéreo controlado.

## Metodología

El presente artículo es una investigación documental con propósito profesional, que tiene un alcance descriptivo, para lo cual se efectuó una revisión de las bases de datos disponibles en las suscripciones de la Escuela Superior de Guerra, la Universidad de San Buenaventura, tales como Digitalia, GALE, Google Académico, MDPI, Oxford University Press, Preprints, ResearchGate, SAGE Journals, Scielo, ScienceDirect, Springer y Taylor & Francis, encontrando Journals, Artículos y publicaciones de gobierno, mediante el empleo de ecuaciones de búsqueda con palabras clave y limitación de fecha de publicación a partir del año 2005, se seleccionaron tres ecuaciones de búsqueda, teniendo en cuenta la variación de la denominación como se conocen el tipo de aeronaves sobre las cuales

se efectuaron los artículos objeto de la investigación y dos tesauros principales de acuerdo a la base de datos de la UNESCO "aeronave" y "fuerzas militares", estas fueron:

1. "Aeronaves no tripuladas" and "uso fuerzas militares".
2. "Aeronaves remotamente pilotadas" and "uso fuerzas militares".
3. "Drones" and "aplicaciones"

Sin embargo, debido a que la mayoría de la bibliografía relacionada con el tema de investigación se encuentra en inglés, también se usaron las ecuaciones de búsqueda en este idioma:

1. "Unmanned aerial vehicle" and "military forces use".
2. "Remotely piloted aircraft" and "military forces use".
3. "Drones" and "applications"

Estos documentos fueron revisados y analizados para ordenarlos por la relevancia de su contenido y la calidad de sus conclusiones, seleccionando los 39 mejores para conformar el marco referencial objeto de la investigación. Finalmente, se identificaron los artículos mejor estructurados, que se alinean con el marco teórico seleccionado, para servir como base de este documento.

Para la organización de la información consultada, se estableció una organización consistente en definir los documentos que tenían un fin informativo con aplicación al marco teórico, luego, se establecieron los documentos que contenían la información para extraer los usos de los sistemas no tripulados, con el fin de identificar las aplicaciones a nivel civil como a nivel militar que sirvieran como insumo del desarrollo del artículo. Por último, se determinaron los documentos que aportaban información complementaria para análisis y conclusiones del documento.

## Marco Conceptual

Los sistemas no tripulados integran una aeronave o vehículo aéreo con una estación de control en tierra, un sistema de comunicaciones que puede ser por enlace directo (*data-link*) o por medios satelitales y su capacidad de carga útil (Circular OACI, 2011), que, de acuerdo con esta última característica se define el tipo de misión a cumplir. Estos sistemas surgieron en la segunda guerra mundial donde Alemania comenzó a utilizar esta tecnología para guiar en forma autónoma bombas dirigidas hacia Inglaterra como las de tipo V-2 y con el paso de los años, el desarrollo de esta tecnología se impuso en el campo militar para el diseño de cohetes, bombas y misiles guiados. La aplicación de la

tecnología de los RPAs se ha visto bien reflejada a través del último siglo en varias confrontaciones, donde podemos encontrar fácilmente su uso en las guerras de Corea, Yom Kippur, la guerra del golfo pérsico (Bruno et al., s.f.) e incluso ahora en pleno siglo XXI en la confrontación entre Rusia y Ucrania.

Los grandes desarrollos en el campo de los Sistemas de Aeronaves Remotamente Tripuladas (RPA's por sus siglas en inglés) han sido llevados a cabo principalmente por Estados Unidos e Israel, los cuales tienen como línea estratégica el uso de la tecnología para su defensa y globalización. En este caso, es subjetivo pensar si los drones son una evolución o una revolución militar (Bruno et al., s.f.), por otra parte, el uso de los drones en combate ha sido poco documentado por tratarse de operaciones secretas de las grandes potencias; sin embargo, el Departamento de Defensa de Estados Unidos DoD realizó un estudio que definió las misiones en que se aplicarán los RPAs para el año 2030 en ese país (Unmanned Aircraft System, 2005, p. A-1), así:

- "Inteligencia, reconocimiento y vigilancia
- Ataque/eliminación de la defensa enemiga
- Ataque electrónico
- Relevo de comunicaciones
- Reabastecimiento y entrega de carga"

Por otra parte, un estudio realizado a 299 sistemas no tripulados con uso militar estableció la aplicación de los drones en las siguientes misiones principales (Torossian, 2020,

p. 16), así:

- "Inteligencia
- Uso de fuerza para la defensa
- Uso de fuerza ofensiva
- Soporte logístico"

La clasificación de los sistemas no tripulados ha tenido varias connotaciones a través de los años, ya que algunos países los clasifican de acuerdo a su conveniencia, teniendo en cuenta, tamaños, pesos, cargas, tripulaciones, comunicaciones, etc., pero, de acuerdo a la Organización Tratado Atlántico Norte - OTAN que es un organismo reconocido mundialmente, los RPAs se clasifican de la siguiente manera teniendo en cuenta el peso máximo de la aeronave al momento del despegue (Riera, 2021):



**Tabla 1** Clasificación UAVs OTAN

UAS: CLASIFICACION PROPUESTA EN EL JCGUAV				
Clase (MTOW)	Categoría	Empleo	Altitud Operacional	Radio de Misión
CLASE III > 650 Kg	HALE (High Altitude Long Endurance)	Estratégico	Hasta 65.000 ft	Sin Límite (BLOS, radio sin visibilidad directa entre antenas)
	MALE (Medium Altitude Long Endurance)	Operacional	Hasta 40.000 ft	Sin Límite (BLOS)
CLASE II 150 / 650 Kg	TÁCTICO	Formación Táctica	Hasta 3.000 ft	200 Km (LOS, radio con visibilidad directa entre antenas)
CLASE I < 150 Kg	SMALL	Unidad Táctica	Hasta 1.200 ft	50 Km (LCS, servicios de localización)
	MINI	Subunidad Táctica	Hasta 1.000 ft	25 Km (LCS)
	MICRO	Táctico, Pelotón, Sección, Personal	Hasta 200 ft	5 Km (LOS)

Fuente: Riera Gomila, M. F. (2021).

En el campo militar, toda la amplia gama de RPAs es utilizada para misiones miliares, que van desde el apoyo táctico para la Clase I (hasta 150 kg), clase II (hasta 650 kg), hasta los de tipo operacional y estratégico de la Clase III (desde 650 kg en adelante). Así mismo, la capacidad de llevar equipos a bordo depende de su peso máximo, entre mayor capacidad de carga es mayor el peso del RPA.

Ahora bien, en el campo civil los RPAs también son empleados para un sinnúmero de aplicaciones, entre las cuales podemos encontrar: fotografía, monitoreo de obras, minería, agricultura, entrega de mercancías, logística y vigilancia (Singhal et al., 2018).

Por otra parte, para tener un grado de percepción sobre los avances y usos de esta tecnología, se debe tener en cuenta que el mercado de esta tecnología generó en ventas para el año 2020 cerca de USD 6.59 billones (Miller C, 2018) que corresponde al 10% de ventas del Departamento de Defensa de Estados Unidos, entre las cuales, las ventas del sector defensa tuvieron un mercado de USD 2.37 billones, lo que implica que esta tecnología es de vital importancia para el campo militar a nivel mundial.

Para el caso colombiano, su aplicación en el campo miliar es vital para la seguridad y defensa nacional, que se puede revisar en el Manual de Doctrina Básica Aérea, Espacial y Ciberespacial de la Fuerza Aérea Colombiana (Doctrina Básica Aérea, Espacial

y Ciberespacial, 2020. P. 10-4), donde se plantea el uso de los RPAs para las siguientes misiones:

- "Gestionar IVR. En operaciones de Inteligencia, Vigilancia y Reconocimiento
- Aplicar la Fuerza. En operaciones de ataque estratégico principalmente"

Con base en lo anterior, se encuentra que la aplicación de los sistemas no tripulados para la defensa y seguridad del estado está supeditada a las siguientes variables:

- Tipo de RPA (Tamaño)
- Tipo de carga útil (Peso)
- Tipo de misión (Estratégica, Operacional o Táctica)
- Capacidad de la Fuerza en aplicar la tecnología

Teniendo en cuenta lo tratado en cuanto a los roles, características, clasificaciones, misiones y hasta presupuestos, se puede evidenciar que los sistemas no tripulados son la aviación del futuro y es bueno analizar en profundidad las capacidades y aplicaciones de esta tecnología en el campo militar y para Colombia, revisar las aplicaciones futuras de estos sistemas en la seguridad y defensa de la nación.

## Desarrollo del Objetivo

Los sistemas no tripulados se fabrican teniendo en cuenta varios aspectos en el diseño como el desempeño, si opera en día y noche, condiciones climatológicas, alcance, tiempo de vuelo, pero principalmente, por el rol o misión que piensa desempeñar el sistema (Torun, 1999), en este aspecto, los sistemas de corto alcance son pequeños, principalmente eléctricos y de bajo costo que sirven para vigilancia, por otra parte, los sistemas de largo alcance, ya poseen motores de combustión que permiten vuelos de larga duración y pueden llevar cargas de mayor capacidad para realizar operaciones más específicas como lo son las misiones militares.

Para el desarrollo de este artículo, los sistemas no tripulados que se van a analizar son los militares, los cuales, de acuerdo a Torossian, son los que tienen más aplicaciones en comparación con los civiles, los cuales están integrados en cuatro áreas que van desde inteligencia, uso de la fuerza, fuerza ofensiva y servicios (Torossian, 2020, p. 16), de estas áreas en Colombia sólo se está aplicando la de inteligencia e información a través de los sistemas no tripulados disponibles en el país y que opera la Fuerza Aérea Colombiana. A su vez, las áreas están divididas en varias aplicaciones más específicas que van encaminadas a las misiones particulares de cada sistema.

Para el estudio realizado por Torossian, se seleccionaron 299 sistemas no tripulados de todas las especificaciones y usos, se seleccionaron los que de acuerdo a sus capacidades se alineaban con las áreas seleccionadas y es así que se dividieron de acuerdo a la Tabla 2.

**Tabla 2** Número de Sistemas No Tripulados y sus Aplicaciones

Inteligencia e información	Uso de la fuerza para la defensa		Uso de la fuerza ofensiva	
Ciber inteligencia: 64	Apoyo: 39	Defensa Aérea: 35	Letal: 65	No letal: 6
Adquisición de Blancos: 120	Defensa de Infraestructura: 53			
	<b>Servicios y soporte</b>			
Monitoreo, Vigilancia y Reconocimiento: 179	Ingeniería: 51		Mantenimiento y Cuidado Médico: 30	
	Transporte y Entrega: 63		Comunicaciones: 44	

Fuente: Torossian, B., Bekkers, F., Sweijts, T., Roelen, M., Hristov, A., & Atalla, S. (n.d.).

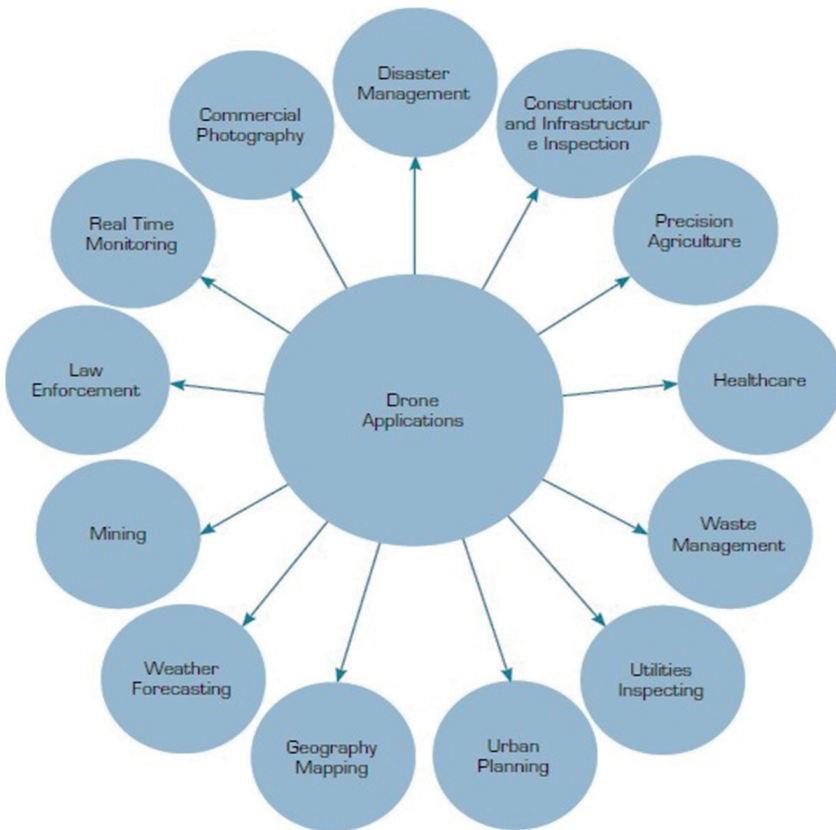
De la Tabla 2, se encuentra que para el área de inteligencia e información las actividades de ciberinteligencia, ubicación de objetivos, vigilancia y reconocimiento son las que mayor aplicación tienen de todos los RPAs consultados; en Colombia los sistemas Hermes y Scan Eagle realizan estas funciones de acuerdo a la doctrina FAC para el empleo del poder aéreo. Los sistemas no tripulados netamente militares, se utilizan para las áreas de la defensa y la ofensiva aérea de un país, se debe tener en cuenta que hay sistemas que simplemente sirven de persuasión como los de tipo no letal y los que entregan armas como los letales tipo UCAV *Unmanned Combat Aerial Vehicle*. Por otra parte, los sistemas con enfoque más civil se utilizan para servicios y soporte entre ellos el servicio médico, apoyo a trabajos de ingeniería, comunicaciones y transporte.

Otro aporte sobre las aplicaciones sobreviene de Sivakumar & Malleswari, donde especifica que los Drones civiles se pueden agrupar de la siguiente manera y se puede ver su organización en la Figura 1:

- "Administración del Riesgo:
  - Preparación pre-desastres
  - Evaluación de desastres
  - Respuesta al desastre
- Agricultura
  - Monitoreo de cultivos
  - Manejo de irrigación

- Agricultura de precisión
- Cosecha
- Polinización artificial
- Cuidado Médico
  - Transporte de Equipo Médico
  - Recolección de muestras
  - Asistencia remota de pacientes
- Construcción e Inspección
  - Administración de construcciones
  - Inspección de infraestructura
  - Viabilidad" (Sivakumar & Malleswari, 2021)

**Figura 1.** Uso de los Drones Civiles

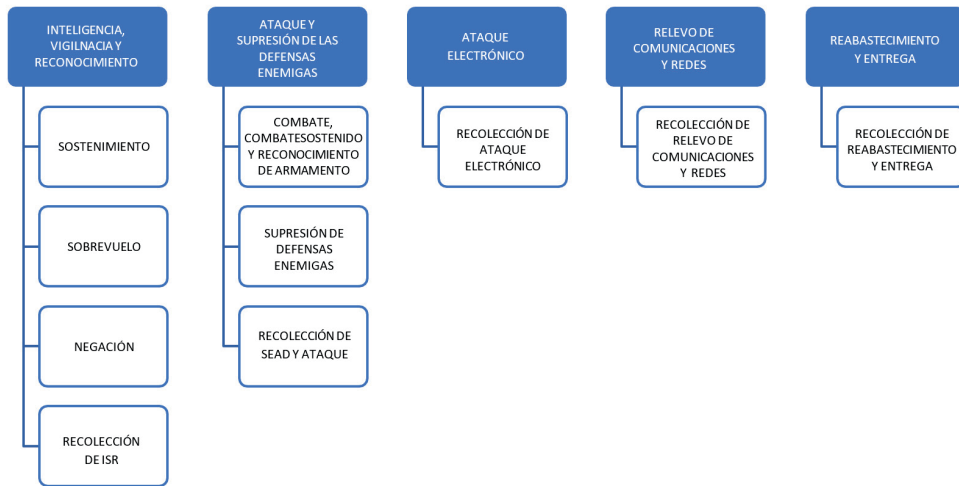


Fuente: Sivakumar, M., Malleswary, N. (2021).

Otras aplicaciones civiles en que se pueden dividir los RPAs son las de cartografía, agricultura, servicios forestales, geología, hidrología, medio ambiente, control de obras, planificación urbanística, gestión del patrimonio y seguridad fronteriza (Brito, 2014).

Para el departamento de Estados Unidos DoD, la aplicación de los sistemas no tripulados militares están determinados en las áreas de inteligencia, defensa, ataque electrónico, comunicaciones y reabastecimiento, lo cual, se puede observar en la Figura 2 (Unmanned Aircraft System, 2005, p. A-1):

**Figura 2** Aplicaciones Militares de los Drones DoD USA



Fuente: Elaboración propia a partir de: Unmanned Aircraft Systems Roadmap. (2005).

En el área de inteligencia, se tienen varios tipos de misiones que incluyen la de apoyo a las fuerzas, sobrevuelo de zonas estratégicas, negación de uso del espacio aéreo al enemigo y recolección de información de inteligencia; en el ataque y supresión de las defensas enemigas se incluyen las misiones de combate y reconocimiento de armamento del enemigo; el ataque electrónico, utiliza las capacidades de interceptar comunicaciones y hacer uso de las capacidades de ciberataque y ciberdefensa. El área de comunicaciones relaciona todas las capacidades de relevo de comunicaciones para extender el alcance de los RPAs, relevo de comunicaciones con la tropa en tierra y relevo de comunicaciones con otras aeronaves, por último, el DoD aplica el concepto de extender las capacidades por medio del reabastecimiento en vuelo utilizando los sistemas no tripulados.

## Normatividad

Por tratarse de vehículos utilizando el espacio aéreo, los sistemas no tripulados civiles están regidos, así como las aeronaves tripuladas por la normatividad OACI, que establece las condiciones en las que deben operar los drones, esta reglamentación está consignada en la Circular 328 del año 2011 (García, 2017), para este caso, los drones deben cumplir la reglamentación aeronáutica para poder operar bien sea en espacios aéreos segregados o no segregados como la aviación de pasajeros.

Para Colombia, la Aerocivil como entidad encargada de controlar el espacio aéreo civil, emitió la Circular Reglamentaria No. 002 que organiza y controla la operación de los drones civiles en el espacio aéreo colombiano.

La normatividad de los sistemas no tripulados de tipo militar es diferente, ya que por sus características y misiones no pueden ser controlados por control aéreo civil, pero, en caso de utilizar espacios aéreos no segregados, deben alinearse a la normatividad exigida por la OACI en cuanto a la navegación y comunicaciones aeronáuticas, para evitar accidentes con aeronaves tripuladas.

El uso de la fuerza para los sistemas no tripulados es complejo y debe plantearse en el objetivo de otro artículo, sin embargo, se puede decir que está en juego los DDHH con el uso de los drones con capacidad de entrega de armamento, ya que a pesar que son controlados a grandes distancias deberían aplicarse los principios de la guerra como la distinción, proporcionalidad, necesidad militar y humanidad (Lopez-Jacoiste, 2018), aunque el tema es delicado por tratarse de la aplicación de la fuerza por parte de las grandes potencias militares.

## Discusión

### Drones Civiles

A través del artículo, se puede observar que las aplicaciones de los sistemas no tripulados están claramente divididas en dos campos, los de aplicaciones civiles y los de aplicaciones militares, es de revisar que los drones de carácter civil son los de tipo comercial que se pueden adquirir fácilmente y a precios accesibles, es por ello que los drones civiles tienen más aplicaciones que los de tipo militar.

Haciendo una revisión de las aplicaciones civiles, se encuentra que éstos se usan principalmente para servicios personales y comerciales, como pueden ser fotografía, topografía, geología, agricultura, logística, entrega de paquetes, vigilancia de residencias, industria de la construcción, monitoreo de propiedades y minería, por otra parte, los drones civiles se pueden utilizar en servicios a la comunidad como servicios de transporte de equipo médico, telemedicina y para atención de desastres; estos UAS han sido

utilizados por entidades no militares del estado, dentro de las más destacadas, la Policía Nacional en apoyo a las actividades de vigilancia y la Defensa Civil Colombiana, en algunos desastres que ha sufrido el país, como el de la isla de providencia por el huracán Iota, los deslizamientos y en atención también a los desbordes de los ríos en el departamento del Putumayo.

## Drones Militares

Los sistemas no tripulados con configuración militar, son aquellos que están diseñados propiamente para servicios de defensa y seguridad, donde sus aplicaciones están claramente definidas: monitoreo, vigilancia y reconocimiento, escolta aéreo, ciber inteligencia, ubicación de blancos, defensa activa, ataque armado y comunicaciones principalmente, dentro de estas misiones, se debe analizar cuál de ellas podría en el mediano plazo ser implementada en Colombia para la defensa y seguridad del país.

Para la utilización de sistemas aéreos remotamente pilotados, las Fuerzas Armadas de Colombia han adoptado la clasificación inicial de los mismos de acuerdo lo establecido por la OTAN (Headquarters, 2017), así:

**Tácticos:** Agrupa las categorías "*Micro/Mini UAS*", caracterizados por su corto alcance, limitado a línea de vista por radiocontrol, tienen baja capacidad de carga y pueden transmitir video en tiempo real, "*Smal Tactical*", son UAS de tamaño pequeño, con una sección de reflexión radar reducida, tienen una autonomía y alcance medianas, limitado a tener línea directa con la señal de radiofrecuencia de la estación de control, "*Tactical*" **estos** UAS requieren un nivel de logística y equipamiento más robusto que los anteriores, sus capacidades de autonomía y rango de operación pueden variar sustancialmente dependiendo del sistema específico, normalmente el centro de control puede estar ubicado en unidades móviles tales como vehículos me mando y control, así como unidades a flote.

**Operacional:** los UAS pertenecientes a esta categoría, presentan fuselajes relativamente grandes, pueden operar a mediana y gran altitud, tienen capacidad de extender su rango de operación al poder utilizar estaciones repetidoras de control, normalmente requieren una pista de aterrizaje para su despegue y recuperación, también pueden utilizar catapultas y ganchos de recuperación (especialmente al utilizarlos a bordo de unidades a flote), o, en algunos casos, tienen capacidad de despegue y aterrizaje vertical.

**Estratégicos:** A esta categoría pertenecen los UAS más rápidos, pesados, grandes, de mayor rango de operación y autonomía, operan a mediana y gran altitud, normalmente son controlados satelitalmente, debido a que su tamaño puede llegar a ser igual al de una aeronave de combate, recientemente, los más avanzados ostentan tecnologías "*stealth*", capacidades de entrega de armas aire-aire, aire-superficie y guerra electrónica,

lo cual les permite competir directamente contra aeronaves tripuladas, en cuanto a capacidad e incluso enfrentados en combate.

**Tabla 3.** Niveles de aplicación de los ART en las Fuerzas Armadas de Colombia

	EJC	ARC		FAC	PNC
		Unidad a flote	Misiones entierra		
<b>Nivel</b>	TÁCTICO	OPERACIONAL	TÁCTICO	ESTRATÉGICO	OPERACIONAL
<b>Peso máximo</b>	20 LBS	55 LBS	20 LBS	+1320 LBS	55 LBS
<b>Velocidad Máxima</b>	30 KT	65 KT	30 KT	+250 KT	65 KT
<b>Altitud de operación máxima</b>	1500 FT	10000 FT	1500 FT	65000 FT	10000 FT
<b>Rango de operación máximo</b>	20 KM	120 NM	20 KM	+250 NM	54 NM

Fuente: Elaboración propia a partir de documentos internos de las Fuerzas.

Dentro de la doctrina de las Fuerzas Armadas de Colombia, se tiene especificada la disposición de los drones de acuerdo con las capacidades de cada una de las Fuerzas Militares y la Policía Nacional, es así que, dentro del territorio continental, el Ejército Nacional y la Armada nacional pueden operar drones de tipo táctico, que realizan acompañamiento y apoyo a la tropa en tierra. La Policía Nacional, puede operar sistemas no tripulados hasta el tipo operacional dentro del territorio para cumplir su misión constitucional. En la zona marítima, la Armada Nacional puede operar sistemas no tripulados hasta el tipo operacional, con mayor capacidad que los de tipo táctico continentales. Ahora bien, la Fuerza Aérea Colombiana, puede operar sistemas no tripulados en el territorio y en la zona marítima desde el tipo táctico, pasando por los de tipo operacional, hasta los estratégicos, resaltando que la FAC puede utilizar la capacidad armamentista de los drones para cumplir su misión de dominio del espacio aéreo colombiano.

Teniendo en cuenta que la FAC es la que abarca toda la gama de aplicaciones, la discusión se va a centrar en las capacidades actuales y futuras que tiene esta fuerza para aplicar los drones en varias misiones típicas de acuerdo con su doctrina de poder aéreo (Doctrina Básica Aérea, Espacial y Ciberespacial, 2020):

- “Contrapoder aéreo
- Inteligencia, vigilancia y reconocimiento aéreo - IVR
- Contrainteligencia aérea
- Ataque estratégico



- Guerra Electrónica
- Operaciones especiales aéreas
- Operaciones de información
- Soporte y servicios para el combate
- Recuperación de personal en apoyo a la población civil
- Control y prevención del empleo ilegal del espacio aéreo"

Actualmente, la FAC utiliza las capacidades de los drones en las misiones típicas de IVR, operaciones de información, soporte y servicios para el combate, control y prevención del empleo ilegal del espacio aéreo, sin embargo, debido a la falta de recursos para implementar más sistemas no tripulados con otras capacidades, no se han aplicado en las demás misiones típicas; por ejemplo, teniendo capacidad de armamento de un dron se podría utilizar este sistema en misiones típicas de ataque estratégico, contrapoder aéreo y operaciones especiales aéreas que incluirían actividades de entrega de armamento, tal como lo hacen países más avanzados en esta tecnología.

Por otra parte, incluyendo en los drones la capacidad de guerra electrónica, se podrían efectuar misiones de control de comunicaciones en el territorio y zonas específicas para aplicación de la fuerza.

Trayendo en contexto los drones militares a nivel mundial, se encuentra lo manifestado por Sarah E. Kreps (2016), que menciona que desde la aparición de los sistemas no tripulados y su desarrollo actual, se puede ver que los Estados Unidos de Norteamérica, fueron los primeros en la utilización de sistemas no tripulados armados para el desarrollo de misiones de ataque, los cuales fueron empleados en Afganistán en 2001, en Yemen en 2002 y luego en Pakistán in 2004; el empleo efectivo de estos medios les permitió efectuar ataques sobre objetivos críticos sin la ocurrencia de bajas y gracias a ello, lograron demostrar que esta tecnología le ofrecía al Estado Norteamericano una ventaja militar y política sobre sus enemigos (p. 59); desde entonces, han liderado la investigación en el desarrollo y aplicación de los RPAs en el campo de la seguridad nacional, motivo por el cual se le confiere la mayor relevancia a los campos de aplicación por ellos propuestos.

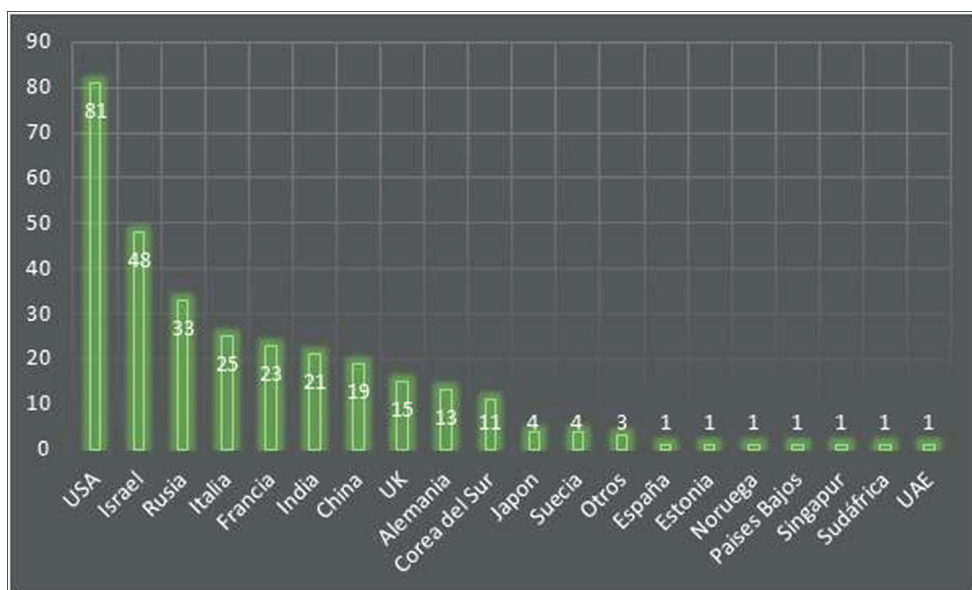
Teniendo en cuenta que el Departamento de Defensa de los Estados Unidos definió las misiones típicas de los drones para la defensa y seguridad de ese país, se hace una analogía con las misiones típicas que podrían cumplir los drones militares de Colombia, entre los cuales encontramos las siguientes capacidades:

- Inteligencia, vigilancia y reconocimiento - IVR, con sus misiones típicas como sostenimiento, sobrevuelo, negación al espacio aéreo.

- Ataque y supresión de la defensa aérea enemiga con las misiones típicas de ataque, ataque persistente y reconocimiento armado. En esta misión, el uso de la fuerza por los sistemas no tripulados es autorizado.
- El ataque electrónico abarca misiones de ciberataque, interrupción de comunicaciones e incluso se contempla el uso de pulsos electromagnéticos y el uso de energía directa sobre un blanco.
- Las comunicaciones es otra misión típica donde se aplica la tecnología para hacer relevo de comunicaciones en el teatro de operaciones.
- Entrega y reabastecimiento en vuelo se consideran como operaciones especiales como parte de las operaciones psicológicas

De igual forma, es interesante observar cómo otros estados más desarrollados evidencian las bondades de la aplicación de estas tecnologías e iniciaron sus propios programas de investigación y desarrollo, es así como se dio inicio a lo que se conoce como la "Carrera de los Drones Armados", en la cual para el año 2019, las principales potencias ya contaban con sistemas operativos en servicio para el desarrollo de operaciones de entrega de armas en sus fuerzas militares, teniendo como referencia la siguiente gráfica:

**Figura 3.** Número de sistemas no tripulados por país



Fuente: Torossian, B., Bekkers, F., Sweijs, T., Roelen, M., Hristov, A., & Atalla, S. (n.d.).

## Aplicaciones en el multidominio, espacial, ciberespacial y cognitivo

De acuerdo a la hoja de ruta planteada por el ejército de los Estados Unidos de Norteamérica, en su publicación *"Eyes of the Army - U.S. Army Unmanned Aircraft Systems*

- *Roadmap 2010-2035"*, Julian Gran (2016), plantea un escenario futuro, en el cual confluirán las tecnologías ciber espaciales y físicas en un nivel sinérgico superlativo, generando una simbiosis que permitirá la operación autónoma de enjambres de drones operados por inteligencias artificiales desde el ciber espacio, transmitidos mediante constelaciones de satélites de comunicaciones, los cuales alimentaran en tiempo real sistemas predictivos, de selección de blancos, determinación de amenazas, proposición y resolución de cursos de acción, información que será suministrada simultáneamente a los decisores en los centros de operaciones así como a las tropas en tierra. Con ello se conseguirá la mayor eficiencia en la toma de decisiones, incrementará la flexibilidad de las operaciones, permitiendo el control y desarrollo de maniobra con una velocidad y precisión nunca vistos.

El desarrollo de la nanotecnología y su implementación en los UAS, le brindara la capacidad a las unidades de desplegar enjambres de drones que mapearán y monitorearán en tiempo real todo el ambiente operacional en una zona específica, generando una realidad aumentada, brindando información que se desplegara directo a los visores de las tropas, indicando las posibles amenazas, ubicación de objetivos, rutas de aproximación y maniobras recomendadas.

Es de esperar que de igual forma la confrontación se lleve a cabo en el ciber espacio, el riesgo de la tecnificación implica que organizaciones e individuos con los recursos y los medios adecuados puedan atacar e incluso tomar control de las armas del adversario, en este sentido, se plantea el ciclo de escalada tecnológica, en el cual los adversarios alternan indefinidamente entre el ataque y la defensa mientras tratan de mantenerse al frente de esta.

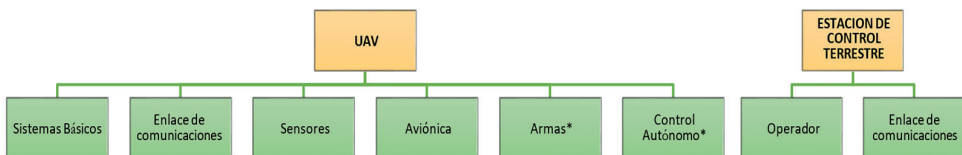
Para el año 2035 se espera que el 95% de las operaciones de reconocimiento e inteligencia sean efectuada por UAS autónomos, de igual forma, el 25% de las misiones restantes serian llevas a cabo por Sistemas Remotamente Pilotados, incluyendo evacuaciones aeromédicas, entrega de armas y transporte de tropas (U.S. Army Unmanned Aircraft Systems - Roadmap 2010- 2035, 2009).

La trasmisión de video en tiempo real, así como la masificación de la utilización de los drones, permitirá a los decisores tener tal cantidad de información y dominio sobre el teatro de operaciones, que será utilizada para minar la moral del enemigo, de igual forma, esta también será utilizada para manipular la percepción de la población, tanto del enemigo como la propia, para obtener una ventaja sobre este.

## Riesgos

Los drones tienen alta tecnología de vanguardia que permite que un estado plantee su sistema de defensa y seguridad a partir de las aplicaciones de los sistemas no tripulados, sin embargo, como en toda tecnología militar, se desarrollan tecnologías para contrarrestar las capacidades de los drones, como perturbadores de comunicaciones o *jamming*, ciberataques, interrupción de señales, entre otros, y es ahí, donde surgen los riesgos que posee la tecnología de los drones, ya que son susceptibles de pérdida o robo en las comunicaciones y pueden ser derribados o extraídos del control militar propio para ser adoptados por el país enemigo. En este aspecto, si los drones no tienen una excelente protección son muy susceptibles de interceptación, derribo o robo por el enemigo.

**Figura 4.** Componentes de los UAV



Fuente: UAV Exploitation: A New Domain for Cyber Power (Hartmann & Giles, 2016).

Cada uno de los componentes representan una oportunidad para ser atacados por el enemigo a través de guerra electrónica, cibernética, cinética o una combinación de estas; con el propósito de interferencia y robo de información, tomar control del sistema para usarlo en contra del adversario o destruirlo. Cabe resaltar que estas posibilidades ya han sido materializadas, dentro de las más reconocidas están la pérdida un UAV "RQ-170 Sentinel" de los Estados Unidos de Norteamérica, cuyo control fue tomado por la Unidad de Guerra Informática de las fuerzas militares iraníes, las cuales lograron hacerlo aterrizar con éxito en la región nororiental de Irán, en cercanías de la ciudad de Kashmar; en el año 2016, basados en los documentos clasificados divulgados por Edward Snowden, se pudieron identificar indicios que videos transmitidos por UAV Israelíes habían sido interceptados por instalaciones de recolección de señales Británicas en Chipre (Hartmann & Giles, 2016).

A partir de este tipo de amenazas, los desarrolladores de UAS militares se han esforzado por mejorar sus sistemas de seguridad y encriptación de datos y comunicaciones, sin embargo, lo mismo no sucede con los drones civiles, cuyo desarrollo está enfocado en ofrecer al cliente funcionalidad y capacidades al menor precio, relegando la seguridad de control y comunicaciones en un segundo plano, ello los ha hecho especialmente vulnerables y se han convertido en el blanco perfecto para su instrumentalización dentro de los escenarios de guerra irrestricta, un ejemplo de ello fue llevado a cabo en el año 2013, por el grupo Hak5, el cual, mediante la utilización de un dron de uso civil DJI

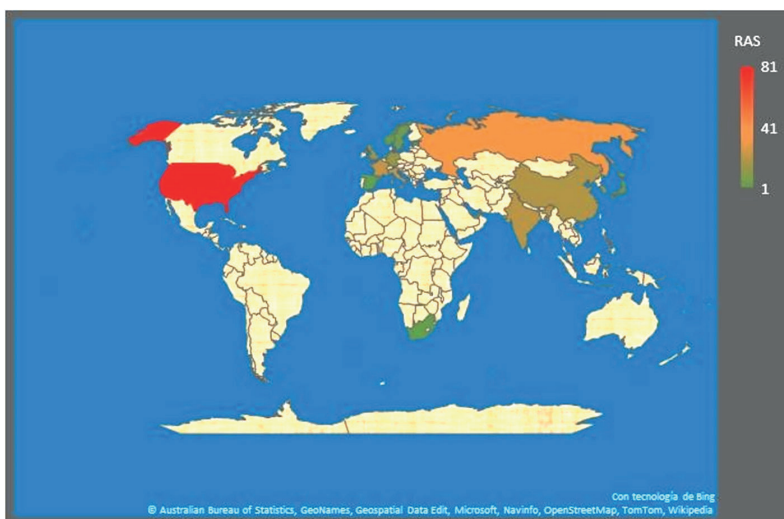
Phantom lograron intervenir las señales de control y tomaron control de todos los drones Parrot que se encontraban en su rango de influencia, de esta forma, demostraron como UAS de uso civil pueden ser intervenidos y empleados para acciones irregulares como la paralización de aeropuertos civiles y negación del uso del espacio aéreo, entre otras (Hartmann & Giles, 2016).

## Conclusiones

Sobre todos los escenarios descritos, se hace evidente que las aplicaciones militares que se han planteado para los drones permiten que el Estado las utilice con fines de brindar seguridad y defensa para su nación, es así, que para los países desarrollados los sistemas no tripulados son los equipos de avanzada para las acciones ofensivas, así mismo, son sistemas de disuasión para las acciones defensivas.

Los países que tienen apropiada esta tecnología utilizan todo su poder en la aplicación de las capacidades que estos sistemas pueden generar, desde inteligencia, relevo de comunicaciones para apoyo militar, reconocimiento, reabastecimiento y ataque estratégico. La revisión de la información encontrada para este artículo no es fácil de analizar, ya que los drones aún siguen siendo equipos con categoría reservada y los países no facilitan la entrega de información a la luz pública, especialmente a su empleo real y los resultados con ellos obtenidos, sin embargo, con el material consultado, se puede evidenciar que las aplicaciones que los países desarrollados han planteado para estos sistemas son casi las mismas que las Fuerzas Militares de Colombia tienen previstas para los sistemas no tripulados propios. En la doctrina de la FAC, se tiene contemplada la aplicación de la fuerza por los no tripulados para sus diferentes misiones típicas, siendo así que en caso de poseer estas capacidades ya se tiene un camino avanzado en su implementación, sin embargo, se hace evidente que nos encontramos rezagados en el tipo de RPAs empleados actualmente, así como en las capacidades adquiridas hasta el momento. Teniendo en cuenta lo anterior, se hace necesario establecer dentro del plan de capacidades de las fuerzas militares, una identificación de aquellas que pueden ser mejoradas o implementadas a partir del empleo de la tecnología de RPAs.

Haciendo una revisión geopolítica con base en la gráfica de la Figura 5, de los Estados con sistemas no tripulados que tienen la capacidad de efectuar misiones de ataque, se puede observar que, en la región, no hay estados que tengan sistemas no tripulados que permitan la entrega de armamento, por lo cual, el desarrollo e implementación de la capacidad de utilización de RPAs en misiones de ataque y defensa, le daría una ventaja militar al país, lo cual sería clave para contribuir a garantizar la defensa de la soberanía nacional e integridad territorial, teniendo en cuenta posibles ataques de estados vecinos.

**Figura 5.** Estados con RPAs armados operativos

Fuente: Torossian, B., Bekkers, F., Sweijs, T., Roelen, M., Hristov, A., & Atalla, S. (n.d.).

Esta estrategia de defensa se ha evidenciado recientemente, de forma amplia, en el conflicto armado entre Rusia y Ucrania, en el cual, las fuerzas militares ucranianas han utilizado efectivamente los drones de ataque turcos “Bayraktar TB2”, los cuales han tenido una alta efectividad, principalmente contra los tanques rusos, dándonos un ejemplo claro de la utilización medios tecnológicos de bajo costo contra lo que otrora fuera considerado uno de los principales factores a considerar en el cálculo del poder militar de un estado.

**Figura 6.** Bayraktar TB2 *“Unmanned Combat Aerial Vehicle”*

Fuente: euromaidanpress.com

Igualmente, se ha podido evidenciar la efectividad de pequeños drones de tipo táctico, que tienen la capacidad de llevar cargas explosivas, los cuales se impactan directamente contra el objetivo para causar su destrucción, esto drones “Switchblades” suministrados por el gobierno de los Estados Unidos de Norteamérica a Ucrania han demostrado ser igualmente contundentes contra unidades autopropulsadas, incluso contra tanques.

**Figura 7.** Lanzamiento de un “Switchblade” UAV



Fuente: dw.com (Fuchs, 2022)

Finalmente, para terminar de redondear una actuación sobresaliente de los drones en el teatro de guerra ucraniano, tenemos la utilización de estos como piezas esenciales de suministro de información de inteligencia, para la detección de amenazas y objetivos en tiempo real, permitiendo tener una efectividad sobresaliente en el fuego de artillería y en la designación de blancos tras las líneas enemigas, que de inmediato son atacados por los sistemas de misiles HIMARS sin dar posibilidad de reacción a sus contrapartes rusas. En este mismo sentido, y no menos importante, ha sido la utilización de drones civiles de venta comercial, para efectuar cobertura permanente de las operaciones y el abatimiento de blancos rusos, lo cual ha permitido tener una cobertura y difusión de estas en medios de comunicación que han afectado la moral del enemigo, generado el levantamiento de protestas contra la guerra al interior del territorio ruso y elevando la moral combativa de los soldados ucranianos.

**Figura 8.** Fuerzas ucranianas con el dron táctico "Quantum-Systems Vector VTOL"

Fuente: osinttechnical.net (2022)

Por otra parte, de la misma forma en que los sistemas no tripulados se desarrollaron para el uso militar y mediante el concepto de tecnología de uso dual, esta tecnología fue llevada al campo de las aplicaciones civiles, ahora y debido a la evolución del concepto de seguridad, que ha dejado de ser un monopolio de las fuerzas de seguridad de los estados, migrando a lo que ahora entendemos como seguridad multidimensional, en la cual participan todos los campos de acción del estado, de la misma forma ahora las aplicaciones civiles desarrolladas para los RPAs deben implementarse en gran escala para potenciar la generación de seguridad multidimensional, en palabras de Bonett (2009):

"El sistema de seguridad y defensa en un escenario de postacuerdo debe consolidarse sobre el concepto de Seguridad Multidimensional, esto significa que su contenido y extensión debe incluir seis pilares básicos que son la defensa nacional, la seguridad ambiental, la política institucional, la seguridad humana, la seguridad ciudadana y la seguridad económica" (p. 54).

Este concepto permite efectuar una relación directa con el eje de central del actual gobierno de Colombia, que basa su estrategia en la seguridad humana (la cual hace parte de la seguridad multidimensional), para que a partir de este, se pueda desarrollar una estrategia que tenga como uno de sus principales medios, el empleo de la tecnología de Aeronaves Remotamente Pilotadas, tanto militares como civiles, bajo la acción unificada por parte de los entes estatales en los diferentes campos de acción del estado, generando la sinergia necesaria para garantizar la seguridad multidimensional de la nación.



## Declaración de divulgación

Los autores declaran que no existe ningún potencial conflicto de interés relacionado con el artículo.

## Autores

**German Quintero Morales.** Especialista en Sistemas de Aviónica Universidad de San Buenaventura, Colombia. Ingeniero Aeronáutico Universidad de San Buenaventura, Colombia.

Orcid: <https://orcid.org/0009-0008-0373-4911> Contacto.: [quinteromg@esdeg.edu.co](mailto:quinteromg@esdeg.edu.co)

**Omar Leonardo Salas Galindo.** Especialista en Mecatrónica Universidad del Valle, Colombia. Ingeniero Aeronáutico Universidad de San Buenaventura, Colombia.

Orcid: <https://orcid.org/0009-0008-4554-6353> Contacto: [salaso@esdeg.edu.co](mailto:salaso@esdeg.edu.co)

## Referencias

- AEROCIVIL. (2015). Circular Reglamentaria 002. Requisitos Generales de aeronavegabilidad y operaciones para RPAS (Numeral 4.25.8.2). Colombia. Recuperado de: <http://www.aerocivil.gov.co/autoridad-de-la-aviacion-civil/certificacion-y-licenciamiento/Documents/CIRCULAR%20REGLAMENTARIA%20%20002%20-%20RPAS.pdf>
- AIRSPACE. Recuperado de: [https://www.academia.edu/36200803/The\\_Utilization\\_of\\_Unmanned\\_Aerial\\_Vehicles\\_UAV\\_for\\_Military\\_Action\\_in\\_Foreign\\_Airspace](https://www.academia.edu/36200803/The_Utilization_of_Unmanned_Aerial_Vehicles_UAV_for_Military_Action_in_Foreign_Airspace)
- Beltrán Pineda, E., & Bolívar Pedraza, W. (2017). EL USO DE LOS DRONES ARMADOS Y SU IMPACTO EN LA GUERRA CONTEMPORÁNEA
- Bonett, M. (2009). Seguridades en construcción en América Latina. Tomo II (Universidad del Rosario, Ed.). <https://editorial.urosario.edu.co/gpd-seguridades-en-construccion-en-america-latina-tomo-ii.html>
- Brito, M. (2014). Los drones, un nuevo socio en el espacio aéreo de Colombia. Universidad Militar Nueva Granada. Bogotá. Recuperado de: [https://www.academia.edu/download/34880509/Trabajo\\_Políticas\\_Aeronauticas\\_2014.pdf](https://www.academia.edu/download/34880509/Trabajo_Políticas_Aeronauticas_2014.pdf)
- Bruno, G., Ronconi, A., Batista, J., & Merola, V. (n.d.). THE UTILIZATION OF UNMANNED AERIAL VEHICLES (UAV) FOR MILITARY ACTION IN FOREIGN
- Callahan, A. L. (2014, Summer). Reinventing the drone, reinventing the navy: 1919-1939. *Naval War College Review*, 67(3), 98. <https://link.gale.com/apps/doc/A375581446/PPWT?u=esdegue&sid=bookmark-PPWT&xid=21d9f774>
- Circular OACI 328-AN/190. (2011). Organización de Aviación Civil Internacional. Recuperado de: [https://www.icao.int/Meetings/UAS/Documents/Circular%20328\\_es.pdf](https://www.icao.int/Meetings/UAS/Documents/Circular%20328_es.pdf)
- Cuerno-Rejado, C., García-Hernández, L., Sánchez-Carmona, A., Carrio, A., Sanchez- Lopez, J. L., & Campoy, P. (2016). Evolución histórica de los vehículos aéreos no tripulados hasta la actualidad. *Dyna (Spain)*, 91(3), 332. <https://doi.org/10.6036/7781>.
- Diego Fernando Ortiz Castillo Ing Ruby Dalila Sánchez Posada Tutores Juan José Fernández Dusso Juan Carlos Gómez Benavides, I. (n.d.). EL EMPLEO DE DRONES COMO ESTRATEGIA DE GOBIERNO Tesis de grado para optar al título de Magister en Gobierno. Recuperado de: [https://repository.icesi.edu.co/biblioteca\\_digital/bitstream/10906/87634/1/T01987.pdf](https://repository.icesi.edu.co/biblioteca_digital/bitstream/10906/87634/1/T01987.pdf)

- Doctrina Básica Aérea, Espacial y Ciberespacial. (2020). Fuerza Aérea Colombiana. Manual-FAC-0-B-Público. Recuperado de: [https://www.fac.mil.co/sites/default/files/linktransparencia/Planeacion/Manuales/face\\_mabda\\_2013.pdf](https://www.fac.mil.co/sites/default/files/linktransparencia/Planeacion/Manuales/face_mabda_2013.pdf)
- Drake, A. M. (2011). Current U.S. Air Force drone operations and their conduct in compliance with international humanitarian law – an overview. *Denver Journal of International Law and Policy*, 39(4), 629.
- ESTADOUNIDENSE. Bogotá DC: Universidad Militar Nueva Granada. Recuperado de: <https://repository.unimilitar.edu.co/bitstream/handle/10654/17595/BeltranPinedaEduardo%20y%20BolivarWilliam2018.pdf?sequence=3&isAllowed=y#:~:text=El%20uso%20de%20los%20drones%20permite%20hacer%20un%20cambio%20radical,deshumanizan%20la%20guerra%2C%20tambi%C3%A9n%20le>
- Fuchs, H. (2022). Los drones están cambiando la guerra. <https://www.dw.com/es/los-drones-est%C3%A1n-cambiando-la-guerra/a-61613746>
- Galvis, V. (2017). Drones: Seguridad y defensa. *Revista Disputatio*. Vol. 2. Recuperado de: [https://facultadgobiernoyrelinter.usta.edu.co/images/documentos/Disputatio\\_Vol2\\_Drones.pdf](https://facultadgobiernoyrelinter.usta.edu.co/images/documentos/Disputatio_Vol2_Drones.pdf)
- García, Israel. (2017). Estudio sobre vehículos aéreos no tripulados y sus aplicaciones. UNIVERSIDAD DE VALLADOLID. España. Recuperado de: <https://uvadoc.uva.es/bitstream/handle/10324/23021/tfg-p-528.pdf?sequence=1>
- Grand, J. (2016). Drones and the Modern Battlefield. [https://www.academia.edu/31813330/Drones\\_and\\_the\\_modern\\_battlefield\\_pdf](https://www.academia.edu/31813330/Drones_and_the_modern_battlefield_pdf)
- Hartmann, K., & Giles, K. (2016). UAV Exploitation: A New Domain for Cyber Power. Vol. Cyber Power. NATO CCD COE Publications, Tallinn. [https://www.academia.edu/25921967/UAV\\_Exploitation\\_A\\_New\\_Domain\\_for\\_Cyber\\_Power](https://www.academia.edu/25921967/UAV_Exploitation_A_New_Domain_for_Cyber_Power)
- Headquarters, D. of the A. (2017). ATP 3-01.81 Counter-Unmanned Aircraft System Techniques. <https://irp.fas.org/doddir/army/atp3-01-81.pdf>
- Igoe Walsh, J., & Schulzke, M. (n.d.). Drones and Support for the Use of Force. Recuperado de: <https://www.jstor.org/stable/j.ctvh4zhx8>
- Kreps, S. E. (2016). DRONES: WHAT EVERYONE NEEDS TO KNOW (Oxford University Press, Ed.). Recuperado de: <https://books.google.es/books?hl=es&lr=&id=jT-BCwAAQBAJ&oi=fnd&pg=PP1&q=leading+country+in+the+use+of+drones&ots=ua44Kfq25i&sig=x-Edyblme44qg3nUpVM7j2Ftt0o>
- Legalidad, P. la, & Emprendimiento La Equidad, E. Y. (n.d.). POLÍTICA DE DEFENSA Y SEGURIDAD PDS. Recuperado de: [https://www.mindefensa.gov.co/irj/go/km/docs/Mindefensa/Documentos/descargas/Prensa/Documentos/politica\\_defensa\\_deguridad2019.pdf](https://www.mindefensa.gov.co/irj/go/km/docs/Mindefensa/Documentos/descargas/Prensa/Documentos/politica_defensa_deguridad2019.pdf)
- López-Jacoiste, E. (2018). Drones armados y el derecho internacional humanitario. Instituto Español de Estudios Estratégicos (IEEE). Recuperado de: [http://www.ieee.es/Galerias/fichero/docs\\_investig/2018/DIEEEINV10-2018\\_Drones\\_DchoInt\\_Lopez-Jacoiste.pdf](http://www.ieee.es/Galerias/fichero/docs_investig/2018/DIEEEINV10-2018_Drones_DchoInt_Lopez-Jacoiste.pdf)
- Martínez, J. 2020. Estudio y caracterización de materiales estructurales para drones. Universidad Simón Bolívar. España. Recuperado de: <https://212.128.20.127/xmlui/handle/10317/8904>
- Merola, V., & Jesinski Batista, T. (n.d.). The Utilization of Unmanned Aerial Vehicles (UAV) for Military Action in Foreign Airspace. Recuperado de: [https://www.academia.edu/36200803/The\\_Utilization\\_of\\_Unmanned\\_Aerial\\_Vehicles\\_UAV\\_for\\_Military\\_Action\\_in\\_Foreign\\_Airspace](https://www.academia.edu/36200803/The_Utilization_of_Unmanned_Aerial_Vehicles_UAV_for_Military_Action_in_Foreign_Airspace)
- Military Unmanned Aerial Vehicles and Diversification Opportunities. (2018). Recuperado de: <https://doi.org/10.13140/RG.2.2.25777.02402>.
- Miller, C. (2018). Military Unmanned Aerial Vehicles and Diversification Opportunities. <https://doi.org/10.13140/RG.2.2.25777.02402>. Recuperado de: [https://www.researchgate.net/publication/328616114\\_Military\\_Unmanned\\_Aerial\\_Vehicles\\_and\\_Diversification\\_Opportunities](https://www.researchgate.net/publication/328616114_Military_Unmanned_Aerial_Vehicles_and_Diversification_Opportunities)
- Mukhamediev, R. I., Symagulov, A., Kuchin, Y., Zaitseva, E., Bekbotayeva, A., Yakunin, K., Assanov, I., Levashenko, V., Popova, Y., Akzhalova, A., Bastaubayeva, S., & Tabybaeva, L. (2021). Review of some

- applications of unmanned aerial vehicles technology in the resource-rich country. In *Applied Sciences* (Switzerland) (Vol. 11, Issue 21). MDPI. Recuperado de: <https://doi.org/10.3390/app112110171>
- Newcome, L. (2004). *Unmanned Aviation: A brief history of unmanned aerial vehicles*. American Institute of Aeronautics and Astronautics Inc. Recuperado de: [https://books.google.es/books?hl=es&lr=&id=HH\\_VZID81rkC&oi=fnd&pg=PA1&dq=military+drones+history&ots=tLT47ETk2&sig=dmgr-QDnXTDIPY00pn4mefZt5CQ#v=onepage&q=military%20drones%20history&f=false](https://books.google.es/books?hl=es&lr=&id=HH_VZID81rkC&oi=fnd&pg=PA1&dq=military+drones+history&ots=tLT47ETk2&sig=dmgr-QDnXTDIPY00pn4mefZt5CQ#v=onepage&q=military%20drones%20history&f=false)
- OACI. (2011). Circular 328 AN 190. *Sistemas de Aeronaves No Tripuladas (UAS)*. Organización de Aviación Civil Internacional. Recuperado de: [https://www.icao.int/Meetings/UAS/Documents/Circular%20328\\_es.pdf](https://www.icao.int/Meetings/UAS/Documents/Circular%20328_es.pdf)
- Osinttechnical.net. (2022). Ukrainian forces with the Quantum-Systems Vector VTOL drone. [https://twitter.com/Osinttechnical/status/1517901725532839936?ref\\_src=twsrc%5Etfw%7C-twcamp%5Etweetembed%7Ctwterm%5E1517901725532839936%7Ctwgr%5Ebc8f280c-03d2b9915aac08c03bf8ca879635f4d9%7Ctwcon%5Es1\\_&ref\\_url=https%3A%2Fwww.dw.com%2Fes%2Flos-drones-estC3A1n-cambiando-la-guerra%2Fa-61613746](https://twitter.com/Osinttechnical/status/1517901725532839936?ref_src=twsrc%5Etfw%7C-twcamp%5Etweetembed%7Ctwterm%5E1517901725532839936%7Ctwgr%5Ebc8f280c-03d2b9915aac08c03bf8ca879635f4d9%7Ctwcon%5Es1_&ref_url=https%3A%2Fwww.dw.com%2Fes%2Flos-drones-estC3A1n-cambiando-la-guerra%2Fa-61613746)
- Riera Gomila, M. F. (2021). *Tècniques de detecció d'UAVs* (Bachelor's esis, Universitat Politècnica de Catalunya). Recuperado de: <https://upcommons.upc.edu/handle/2117/349259>
- Rushby, R. S. (2017). Drones armados y el uso de fuerza letal: nuevas tecnologías y retos conocidos. *CES Derecho*, 22–47. <https://doi.org/10.21615/cesder.8.1.2>
- Segundo, T., Farrow, A., & Resumen, U. (n.d.). La guerra con drones como instrumento militar de la estrategia antiterrorista\*. Recuperado de: [http://www.scielo.org.co/scielo.php?script=sci\\_arttext&pid=S2145-77192017000100003](http://www.scielo.org.co/scielo.php?script=sci_arttext&pid=S2145-77192017000100003)
- Singhal, G., Bansod, B., & Mathew, L. (2018). *Unmanned Aerial Vehicle Classification, Applications and Challenges: A Review Facile Synthesis of Nano Sized ZnO by Hydrothermal Method View 33roject Remote sensing for Precision 33roject33ura View 33roject Babankumar shyam Bansod Central Scientific Instruments Organization Unmanned Aerial Vehicle classification, Applications and challenges: A Review*. <https://doi.org/10.20944/preprints201811.0601.v1>.
- Sivakumar, M., Malleswary, N. (2021). A Literature Survey of Unmanned Aerial Vehicle Usage for Civil Applications. *Review Article*. Recuperado de: <https://doi.org/10.1590/jatm.v13.1233>
- Torossian, B., Bekkers, F., Sweijts, T., Roelen, M., Hristov, A., & Atalla, S. (n.d.). *Hague Centre for Strategic Studies Report Part Title: Current RAS applications in the land domain Report Title: The Military Applicability of Robotic and Autonomous Systems*. Recuperado de: <https://www.jstor.org/stable/10.2307/resrep24199.5>
- Torun, Erdal. (2000). *UAV Requirements and Design Consideration*. Turkish Land Forces Command. Turkey. Recuperado de: <https://apps.dtic.mil/sti/citations/ADP010321>
- U.S. Army Unmanned Aircraft Systems – Roadmap 2010- 2035. (2009). *EYES OF THE ARMY, U.S. Army Unmanned Aircraft Systems – Roadmap 2010-2035*. <https://irp.fas.org/program/collect/uas-army.pdf>
- Unmanned aerial vehicles: current developments and future utility. (2008). *The Military Balance*, 108(1), 455–460. <https://doi.org/10.1080/04597220801912929>
- Unmanned Aircraft Systems Roadmap. (2005). Department of Defense. United States of America. Recuperado de: <http://krex.k-state.edu/dspace/bitstream/handle/2097/17032/Toscanopt.pdf;sequence=1>

# Coyuntura

---

Defiances

Esta página queda intencionalmente en blanco

# Las herramientas cibernéticas y cognitivas: dos conceptos que desplazaron los métodos convencionales de enfrentamiento

Cybernetic and cognitive tools: two concepts that displaced conventional coping methods

DOI: <https://doi.org/10.25062/2955-0270.4777>

Diego Ospina Quintana 

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

## Resumen

No resulta extraño escuchar sobre nuevos escenarios y tipos de guerras en los que las partes ya no se enfrentan en campos de batalla convencionales como los que se manifestaron en las dos guerras mundiales y durante la Guerra Fría, es necesario reconocer que existen una serie de medios, métodos y elementos que de la mano de tecnologías emergentes y disruptivas, como la Inteligencia Artificial, el aprendizaje automático, la automatización de plataformas de armas, los sistemas de vigilancia, el procesamiento de datos y los vehículos no tripulados, entre otros, han estructurado una dimensión de la guerra cada vez más difusa, etérea y difícil de clasificar.

**Palabras Clave:** Guerra; tecnologías; dominio.


It is not strange to hear about new scenarios and types of wars in which the parties no longer confront each other on conventional battlefields such as those that occurred in the two world wars and during the Cold War, it is necessary to recognize that there are a series of means, methods and elements that, together with emerging and disruptive technologies, such as Artificial Intelligence, machine learning, the automation of weapons platforms, surveillance systems, data processing and unmanned vehicles, among others, have structured a dimension of war that is increasingly diffuse, ethereal and difficult to classify.

**Key words:** War; technologies; domain.

## Abstract



**Artículo de reflexión**

Recibido: 3 de marzo de 2023 • Aceptado: 10 de mayo de 2023  
Contacto: Luis Renato Amórtegui Rodríguez  [lamortegui@ucm.es](mailto:lamortegui@ucm.es)

## Las herramientas cibernéticas y cognitivas

Las tecnologías resultan ser un fenómeno que ha sido explotado por actores estatales y no estatales al mismo nivel de otros actores reconocidos globalmente como potencias mundiales o con actores que mantienen alianzas de gran envergadura y en escenarios absolutamente asimétricos. Lo característico, es que los mismos recursos financieros y materiales, los actores irregulares han logrado ocasionar daños y afectaciones de consideración, así como materializar sus propósitos y avanzar hacia la consecución de intereses políticos y económicos particulares.

Este documento pretende de manera breve argumentar como la combinación de herramientas cibernéticas, manejo de información y de elementos cognitivos, pueden impactar de manera decisiva en el desarrollo de conflictos de nivel mundial, tomando como ejemplo puntual, la estrategia Rusa de los últimos años.

Para tratar de contrarrestar la expansión de la ideología occidental a la cabeza de EE.UU, la Unión Europea y la OTAN, quienes considera una clara amenaza para su soberanía, se tiene la participación de Vladimir Putin, presidente de la Rusia, quien entendió que ya no era posible enfrentar de manera eficiente empleando métodos convencionales como los implementados hasta el fin de la Guerra Fría (1991).

Aunque Rusia en la actualidad, y especialmente luego del pasado 24 de febrero de 2022, cuando dio inicio a lo que ellos mismos denominaron *una operación especial* contra Ucrania, es considerado como una amenaza para buena parte de la comunidad europea y sus vecinos asiáticos, no es igualmente catalogado por otras naciones que, a pesar de esto, no le ven como su enemigo directo, sino más bien como un reto, que se debe vigilar y mantener en el radar con un seguimiento especial. Los actores antagonistas de occidente, ven a Rusia como un importante socio que les puede potencializar en la consecución de sus intereses nacionales (Sputnik Mundo, 2023).

Esta diferencia, al momento de definir lo que significa Rusia para una y otra nación, podría representar una muestra interesante de la estrategia del Kremlin para conseguir sus objetivos nacionales sin desatar una tercera guerra mundial o una reacción contundente de parte de occidente, haciendo uso de medios no militares, como su notable manejo de la información, una incontenible proliferación de dispositivos de comunicación de alta tecnología y el aumento exponencial de la conectividad.

Desde la perspectiva de Putin, la continua rivalidad con el mundo occidental es una competencia de suma cero, lo que hace que el tipo de guerra nuevo, adaptable y flexible de Rusia, sea una respuesta lógica y relativamente barata a la superioridad occidental en el dominio convencional (Farkas, 2022, p. 3).

Un primer elemento que vale la pena señalar, es que los conceptos de guerra cibernética y ciberespacio, son propios de la terminología occidental, por lo que Rusia más

bien hace referencia al espacio de la información, el cual abarca tanto el dominio tecnológico como el psicológico; lo cual constituye el verdadero valor agregado de su estrategia, al acoplar los procesos informáticos y humanos en una misma balanza y regidos por una misma política nacional (Farkas, 2022, p.5).

Consecuente con lo anterior, la estrategia rusa en este ámbito se podría dividir en operaciones en la red y operaciones de información. Por un lado, y aunque ningún incidente hasta el momento ha podido ser atribuido oficialmente al gobierno ruso, numerosas hipótesis conducen a la contratación de empresas civiles por parte de los rusos para lanzar ataques cibernéticos, explotando precisamente la dificultad de atribución y, por lo mismo, la capacidad de respuesta del actor o activo atacado. Los rusos aún en conflictos convencionales o guerras proxy, citando al grupo Wagner como ejemplo, se consolidan en una punta de lanza de operaciones especiales prorrusas en Siria, África, Crimea y actualmente en Ucrania, solo para mencionar algunos ejemplos.

Por otro lado, Rusia le ha apostado al internet y a los medios de comunicación como una herramienta contundente para difundir sus ideas, controlar las narrativas que justifican sus operaciones militares y, finalmente, poder llegar a influenciar en los tomadores de decisiones y en los mismos ciudadanos de las naciones o alianzas objetivos, donde el propósito es alterar la cohesión, aumentar los niveles de incertidumbre e incluso afectar los sistemas políticos y económicos, dificultando una de las premisas clave para el ejercicio eficiente de alianzas internacionales como la OTAN, el consenso.

Medidas tomadas recientemente por Rusia no son de naturaleza nueva. Los bolcheviques utilizaron el termino medidas activas cuando discutían métodos para influir en las acciones extranjeras hace más de un siglo. Desde entonces, Rusia ha utilizado este tipo de poder blando para imponer su propia voluntad a otros actores internacionales” (Farkas, 2022, p. 4).

Sobre esta dinámica en particular, Rusia tiene una habilidad enorme que se ha construido a lo largo de los años y de la experiencia, y es la sagacidad con que lleva a cabo campañas de desinformación y el empleo de propaganda y contrapropaganda para afectar a sus actores o naciones objetivo, los cuales generalmente corresponden a Estados con sistemas políticos democráticos occidentales que no tienen mayores restricciones a medios de comunicación ni redes sociales. De forma que, las operaciones informáticas tienen un costo relativamente bajo, pero con unos resultados que pueden llegar a resultar estratégicos si se llega a controlar la tendencia y la narrativa en escenarios internacionales, afectando elementos clave en la percepción del adversario y explotando sus vulnerabilidades ya identificadas en la conciencia y en la mente del público objetivo.

El resultado final de estas actividades informáticas, que hacen parte de la estrategia soviética en operaciones de información, de propaganda y contrapropaganda, se ve altamente potencializado mediante la explotación de campañas ejecutadas con el Ejército de trolls del Kremlin o a través de bots automatizados, que aceleran la consecución de los



objetivos en el marco psicológico y cognitivo, llegando a alterar y a hacer que se dude de la verdad misma por parte de las sociedades objetivo (Cunnighan, 2021).

De otro lado, pero en total sincronía y alineación con la política rusa de actividades en el espacio de la información, Putin y su círculo cercano, nunca han dejado de preocuparse por la carrera tecnológica y los avances en tecnologías emergentes y disruptivas, que puedan ser empleadas de manera contundente en el quinto dominio. Para lo cual, el desarrollo de semilleros de investigación y la infraestructura de innovación han sido pilares fundamentales para el Kremlin. Esta política, que incluye parques industriales, centros de ingeniería, instituciones de desarrollo financiero, así como prestigiosas universidades e institutos de investigación rusos, que, asociados con importantes fabricantes de armas y desarrolladores tecnológicos, tienen como principal pretensión fomentar la innovación en todos los campos, desarrollando nuevos sistemas de armas, pero también creando nuevos multiplicadores de fuerza basados en capacidades ya existentes.

Por ejemplo, Rusia está experimentando con la integración de vehículos no tripulados para misiones nucleares (Proyecto Poseidón UUV), armas de precisión de largo alcance, incluidos misiles hipersónicos para disuasión no nuclear y explotar la Inteligencia Artificial en operaciones de zona gris (Zysk, 2022, p. 1).

Si bien es cierto que Rusia no atraviesa por su mejor momento para sostener un conflicto convencional, el espíritu de combate y el entrenamiento de sus fuerzas en tierra no es el mismo que el de hace dos décadas. Su economía se ha visto visiblemente golpeada por las sanciones implementadas desde antes de su invasión a Ucrania y, que, además, ha tenido que lidiar con la denominada fuga de cerebros, en la que jóvenes y mentes brillantes han decidido abandonar su país por la inestable situación económica y las condiciones complejas que se han agravado desde el inicio del conflicto.

No se debe subestimarse la capacidad de los rusos de sobreponerse, precisamente acudiendo a la implementación de estrategias híbridas en las que se combinen capacidades no convencionales, como el poder nuclear, las herramientas cibernéticas o las tecnologías emergentes disruptivas, con operaciones de información y propaganda, algo en lo que ya se había advertido, los rusos son expertos.

En ese mismo sentido, una eventual alianza estratégica con China, a pesar de que hoy en día no se vea tan factible, es un curso de acción que nunca puede descartarse, especialmente si EE.UU continúa con su ofensiva económica contra China y si la guerra en Ucrania termina involucrando a otros actores de manera directa, situación que llevaría a la integración y desarrollo de poderes, capacidades y tecnologías sin precedente, en un escenario que no solo se conciba en el imaginario, podría desencadenar el primer conflicto cibernético internacional, donde las herramientas y armas convencionales pasarían a un segundo plano y la supremacía se manifestaría en el dominio de lo tecnológico integrado con la explotación del elemento psicológico y cognitivo.

## Conclusión

Para concluir, resulta imperativo afirmar que teniendo en cuenta las diferentes capacidades que se vienen desarrollando en tecnología, que involucran el ciberespacio como su principal medio, ninguna nación puede sentirse excluida de las amenazas que esto puede representar a su estabilidad, este no es un tema que exclusivamente deba preocupar a las grandes potencias o a las naciones con altos estándares en políticas cibernéticas, sino que, por el contrario, países como Colombia que hasta ahora se encuentran en una fase inicial en la estructuración de la protección de este dominio. Se deben encender alertas y trabajar fuertemente para posicionar esta capacidad con una política nacional lógica, clara y robusta, donde sin duda el primer paso debe ser la alfabetización tecnológica, de manera tal que el ciudadano promedio, sin necesidad de ser técnico o profesional en tecnología o informática, pueda entender y dimensionar la importancia de este campo.

De forma simultánea, la explotación de alianzas estratégicas regionales y globales, con naciones y organizaciones como la OTAN, que permitan potencializar tanto en conocimientos como en recursos e infraestructura la ciberdefensa nacional; serían dos escalones iniciales en la construcción de una política seria, y prospectiva, sustentada en el conocimiento, en el juicio estratégico y en la capacidad de adaptación para resolver problemas en escenarios cambiantes.

## Declaración de divulgación

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

## Autor

**Diego Ospina Quintana.** Mayor del Ejército Nacional de Colombia. Candidato a Magíster en Ciberdefensa y Ciberseguridad, Colombia. Profesional en Ciencias Militares, Escuela Militar de Cadetes "General José María Córdova", Colombia. Administrador de Empresas, Universidad Militar Nueva Granada, Colombia.

Orcid: <https://orcid.org/0009-0008-8932-5157> Contacto: [ospinadq@esdeg.edu.co](mailto:ospinadq@esdeg.edu.co)

## Referencias

- Cunningham, C. (2021, Octubre). *A Russian Federation Information Warfare Primer*. The Henry M. Jackson School of International Studies. <https://jsis.washington.edu/news/a-russian-federation-information-warfare-primer/>
- Farkas, S. (2022, Abril). *Information warfare: Russia's alternative, cheap solution to counter the conventional superiority of the west*. NDC Academic Portal. <https://www.ndc.nato.int/download/downloads.php?icode=759>

- Forest, J. (2020, 16 Septiembre). *Globalization and transnational Crime*. E-International Relations. <https://www.e-ir.info/2020/09/16/globalization-and-transnational-crime/>
- Gilli, A. (2021, Noviembre). *Future warfare, future skills, future professional military education*. NDC Academic portal. <https://www.ndc.nato.int/download/downloads.php?icode=713>
- Smith, R. (2008). *The Utility of Force: The Art of War in the Modern World*. Van Haren Publishing.
- Mundo, S. (2023, 2 febrero). El avance y los resultados de la operación militar rusa en Ucrania *Sputnik Mundo*. <https://sputniknews.lat/20230202/mapa-como-avanza-la-operacion-especial-de-rusia-en-ucrania-1126329635.html>
- Zysc, K. (2022, mayo). Is Russia a threat in emerging and disruptive technologies?. *Sputnik Mundo*. <https://sputniknews.lat/20230202/mapa-como-avanza-la-operacion-especial-de-rusia-en-ucrania-1126329635.html>

# Perspectivas

---

Perspectives

Esta página queda intencionalmente en blanco

## *Entrevista a Lucas Giraldo Ríos. Resiliencia genética: estrategias para proteger y recuperar datos frente a amenazas cibernéticas.*

*Interview with Lucas Giraldo Ríos. Genetic resilience: strategies to protect and recover data from cyber threats*

DOI: <https://doi.org/10.25062/2955-0270.4809>

**Angélica María González González** 

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

### Biografía


**Lucas Adolfo Giraldo Ríos**

Docente de la Maestría en Ciberseguridad y  
Ciberdefensa de la Escuela Superior de Guerra  
"General Rafael Reyes Prieto", Colombia.



**Entrevista**

Recibido: 15 de junio de 2023 • Aceptado: 12 de mayo de 2023

Contacto: Angélica María González González  [angelica.gonzalez@esdeg.edu.co](mailto:angelica.gonzalez@esdeg.edu.co)

## Resiliencia Genética: Estrategias para proteger y recuperar datos frente a amenazas cibernéticas

### Para dar inicio a la discusión, podría explicar ¿Qué es la información genética?

La información genética se refiere al conjunto de instrucciones codificadas en el ADN de un organismo que determina sus características hereditarias y el funcionamiento de sus células. Esta información se encuentra en forma de genes, segmentos específicos de ADN que contienen las instrucciones para la síntesis de proteínas y otros componentes celulares. La información genética es fundamental para la herencia de rasgos biológicos de una generación a la siguiente, y juega un papel crucial en la regulación de la estructura y función de los organismos vivos. La decodificación de la información genética ha sido un avance significativo en la comprensión de la biología y la genética, y ha permitido avances en la medicina, la biotecnología y la investigación científica.

### ¿Por qué son importantes los datos genéticos?

Los datos genéticos son de suma importancia debido a la riqueza de información que contienen sobre la composición genética única de un individuo. Estos datos revelan detalles fundamentales sobre la predisposición genética a enfermedades, la eficacia de tratamientos médicos específicos, la herencia de rasgos y condiciones genéticas, así como la relación entre las variantes genéticas y la salud en general. Esta información es crucial en el campo de la medicina personalizada, ya que permite a los profesionales de la salud adaptar tratamientos y terapias de manera más precisa, lo que puede mejorar significativamente los resultados médicos y reducir los efectos secundarios no deseados.

Además, los datos genéticos también tienen implicaciones en la genealogía, la identificación de parentesco, la investigación científica y la comprensión de la diversidad genética de las poblaciones, lo que los convierte en una herramienta invaluable en diversas áreas de la ciencia y la salud. Sin embargo, la importancia de los datos genéticos va de la mano con la necesidad de proteger su privacidad y seguridad, ya que su divulgación indebida o uso inapropiado puede tener graves consecuencias para la vida de las personas y la sociedad en general.

### ¿Por qué debería preocuparle a una persona la seguridad de sus datos genéticos?

La seguridad de los datos genéticos debería ser una preocupación primordial para cualquier persona debido a las implicaciones tanto personales como sociales que

conlleva. En el ámbito personal, los datos genéticos contienen información íntima sobre la salud, predisposiciones genéticas a enfermedades, parentesco y otros aspectos de la identidad. Su filtración o mal uso podría tener consecuencias graves, como la discriminación en seguros de salud o empleo, así como la exposición de información altamente privada. Además, a nivel social, la seguridad de los datos genéticos es esencial para proteger la privacidad de toda la comunidad familiar, ya que compartir material genético implica también la exposición de información de parientes. Por lo tanto, mantener la seguridad de los datos genéticos es crucial para salvaguardar tanto la privacidad individual como la colectiva.

### **¿Qué es la ciberseguridad de la información y por qué se debe tener en cuenta en salud?**

La ciberseguridad de la información se refiere a la práctica de proteger los datos digitales y los sistemas informáticos de amenazas, ataques y accesos no autorizados. En el contexto de la salud, es de vital importancia debido a la naturaleza altamente sensible y confidencial de los datos médicos y personales que se almacenan electrónicamente. Los registros de salud de los pacientes contienen información crítica, como diagnósticos, historiales médicos, resultados de pruebas y detalles de tratamientos, que deben mantenerse seguros para garantizar la privacidad de los pacientes y la integridad de los datos. La falta de ciberseguridad en la atención médica puede exponer a los pacientes a riesgos significativos, como el robo de identidad, la alteración de registros médicos o incluso la interrupción de los servicios de atención médica, lo que podría tener graves consecuencias para la salud de las personas.

Además, la ciberseguridad en salud es esencial para proteger la infraestructura de atención médica en su conjunto, ya que los ataques cibernéticos pueden afectar la disponibilidad de servicios críticos, como sistemas de emergencia, comunicaciones hospitalarias y equipos médicos conectados a la red. En un mundo cada vez más digitalizado, la atención médica depende en gran medida de la tecnología, lo que la hace vulnerable a amenazas cibernéticas. Por lo tanto, la ciberseguridad de la información en el ámbito de la salud no solo protege la privacidad de los pacientes, sino que también garantiza la continuidad de la atención médica y la integridad de los sistemas que respaldan la atención médica moderna.

### **A.M.G: ¿Cuál es el tópico más importante en ciberseguridad en temas de datos genéticos?**

Uno de los temas más importantes en ciberseguridad relacionados con datos genéticos es la protección de la privacidad y la confidencialidad de la información genética. Dado que los datos genéticos son altamente sensibles y contienen información íntima sobre la salud y la identidad de una persona, es crucial garantizar que estos



datos estén resguardados contra accesos no autorizados, filtraciones y mal uso. La privacidad de los datos genéticos es esencial para prevenir la discriminación genética, el robo de identidad y otros riesgos asociados con la exposición de esta información. La regulación de quién puede acceder a los datos genéticos y cómo se almacenan y comparten es un tema crítico en ciberseguridad en este campo, y se han establecido normativas rigurosas, como el Reglamento General de Protección de Datos (GDPR) en Europa, para abordar estos desafíos.

### ¿Cómo la ciberseguridad apoya el cuidado de los datos genéticos?

La ciberseguridad desempeña un papel crucial en la protección de los datos genéticos al salvaguardar la privacidad y la integridad de la información personal almacenada en bases de datos genómicas y registros médicos. Dado que estos datos contienen información altamente sensible sobre la salud y la identidad de las personas, es esencial prevenir el acceso no autorizado, el robo de datos o la manipulación maliciosa. La implementación de medidas de seguridad robustas, como la encriptación de datos, el control de acceso, la autenticación multifactorial y la detección de intrusiones, ayuda a prevenir brechas de seguridad y garantiza que los datos genéticos estén protegidos de amenazas cibernéticas. De esta manera, la ciberseguridad contribuye a mantener la confidencialidad y la confianza en la gestión de información genética, lo que es esencial para la investigación médica, la atención de la salud y la protección de la privacidad de los individuos.

### ¿Cómo podría un ciberdelincuente usar los datos genéticos robados u obtenidos de manera ilícita?

Un ciberdelincuente podría aprovechar los datos genéticos robados o adquiridos de manera ilícita para llevar a cabo diversas actividades perjudiciales. En primer lugar, estos datos podrían ser utilizados en estafas de suplantación de identidad, lo que implica la creación de perfiles falsos o la obtención de servicios financieros bajo una identidad fraudulenta. Además, los datos genéticos son extremadamente personales y sensibles, por lo que su divulgación no autorizada podría resultar en chantaje o extorsión, donde el delincuente amenaza con revelar información genética confidencial a menos que se cumplan sus demandas. Además, existe el riesgo de discriminación genética, donde los datos podrían ser utilizados por empleadores o aseguradoras para tomar decisiones injustas sobre la contratación, el seguro o el acceso a servicios médicos.

En un contexto más amplio, la información genética podría ser vendida en el mercado negro o en la dark web, donde criminales podrían aprovecharla para actividades ilegales como el tráfico de órganos o la creación de perfiles de ADN falsos para encubrir la identidad de otros delincuentes. En resumen, la utilización indebida

de datos genéticos por ciberdelincuentes representa un riesgo significativo para la privacidad y la seguridad de las personas, lo que subraya la importancia de una ciberseguridad sólida y la implementación de leyes y regulaciones que protejan adecuadamente esta información delicada.

### **¿Qué herramientas de ciberseguridad pueden utilizarse para proteger los datos genéticos de las personas?**

Para proteger los datos genéticos de las personas, se pueden utilizar una serie de herramientas y estrategias de ciberseguridad. En primer lugar, la encriptación de datos desempeña un papel fundamental. La encriptación asegura que los datos genéticos estén codificados y no sean legibles sin la clave adecuada, lo que añade una capa adicional de seguridad. Los sistemas de gestión de claves sólidos son esenciales para garantizar que solo las personas autorizadas tengan acceso a la información genética.

La autenticación de múltiples factores es otra herramienta valiosa. Requerir múltiples métodos de autenticación, como contraseñas, tarjetas inteligentes y escaneos biométricos, puede dificultar significativamente el acceso no autorizado a los datos genéticos. Además, las soluciones de monitoreo y detección de amenazas pueden ayudar a identificar actividades sospechosas o intrusiones en tiempo real, lo que permite una respuesta rápida ante posibles violaciones de seguridad.

Por último, la educación y la concienciación son fundamentales. Capacitar a las personas que trabajan con datos genéticos y a los propios individuos para que comprendan los riesgos y las mejores prácticas en ciberseguridad puede ser la primera línea de defensa contra amenazas. La ciberseguridad en el ámbito de la genética debe ser una prioridad constante y adaptarse a medida que evolucionan las amenazas cibernéticas y las tecnologías de protección de datos.

### **¿Principales consejos para abordar la seguridad de los datos genéticos tanto en personas como en empresas?**

La seguridad de los datos genéticos es fundamental tanto para individuos como para empresas. Aquí hay algunos consejos clave para abordar este importante aspecto: **Encriptación y almacenamiento seguro:** Tanto las personas como las empresas deben garantizar que los datos genéticos se almacenen de manera segura y estén encriptados. Esto implica utilizar sistemas de almacenamiento protegidos por contraseñas y cifrado avanzado para proteger los datos de accesos no autorizados. Las empresas deben considerar el uso de sistemas de almacenamiento en la nube seguros o servidores locales con medidas de seguridad robustas.

**Control de acceso y autenticación:** Implementar un control estricto de acceso es esencial. Esto incluye el uso de autenticación de múltiples factores para garantizar

que solo las personas autorizadas tengan acceso a los datos genéticos. Las empresas deben establecer políticas de acceso basadas en roles, limitando el acceso solo a aquellos empleados que necesitan los datos para fines específicos.

Educación y concienciación: Tanto las personas como las empresas deben educar a su personal sobre la importancia de la seguridad de los datos genéticos y proporcionar capacitación sobre buenas prácticas en ciberseguridad. Las empresas deben tener políticas y procedimientos claros en vigor y fomentar una cultura de seguridad que promueva la concienciación sobre la privacidad de los datos genéticos y las consecuencias de un mal manejo de esta información.

### ¿Qué puede hacer la Maestría en Ciberseguridad y Ciberdefensa de la Escuela Superior de Guerra para cuidar los datos de tipo genético en las organizaciones?

La Maestría en Ciberseguridad de la Escuela Superior de Guerra podría desempeñar un papel esencial en el cuidado de los datos genéticos desde una perspectiva de ciberseguridad al ofrecer capacitación y formación especializada en la protección de información sensible. Los estudiantes de esta maestría podrían adquirir conocimientos avanzados sobre las amenazas y los riesgos cibernéticos que enfrentan las bases de datos genómicas, así como las mejores prácticas para implementar medidas de seguridad sólidas. Además, podrían colaborar en la investigación y desarrollo de estrategias de ciberseguridad específicas para proteger los datos genéticos, y podrían desempeñar un papel importante en la creación de políticas y regulaciones que garanticen la privacidad y la integridad de esta información.

En definitiva, esta maestría podría contribuir de manera significativa al cuidado de los datos genéticos al formar profesionales altamente capacitados en ciberseguridad que pueden abordar los desafíos emergentes en la protección de datos genéticos en el entorno digital actual.

#### Autor

**Angélica María González González.** Magíster en Estrategia y Geopolítica, Escuela Superior de Guerra "General Rafael Reyes Prieto", Colombia. Politóloga con Énfasis en Seguridad, Paz y Conflicto, Universidad del Rosario, Colombia. Gestora de Investigación Maestría en Ciberseguridad y Ciberdefensa, Escuela Superior de Guerra "General Rafael Reyes Prieto", Colombia.

Orcid: <https://orcid.org/0000-0003-0881-5530>

Contacto: [angelica.gonzalez@esdeg.edu.co](mailto:angelica.gonzalez@esdeg.edu.co)

# Enfoques

---

Insights

Esta página queda intencionalmente en blanco

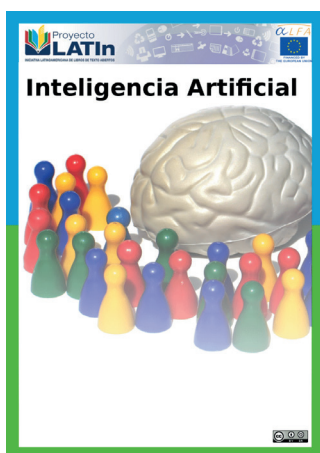
## Reseña del libro. Inteligencia artificial

Book review. Artificial Intelligence

DOI: <https://doi.org/10.25062/2955-0270.4815>

Viviana Pilar Fuquen Flautero 

Corporación Universitaria del Meta, Villavicencio, Colombia



Autores del libro: **Julio Cesar Ponce Gallegos, Aurora Torres Soto, Fátima Sayuri Quezada Aguilera, Antonio Silva Sprock, Ember Ubeimar Martínez Flor, Ana Casali, Eliana Scheihing, Yván Jesús Túpac Valdivia, Ma. Dolores Torres Soto, Francisco Javier Ornelas Zapata, José Alberto Hernández A., Crispín Zavala D., Nodari Vakhnia, y Oswaldo Pedreño**

Editorial: Iniciativa Latinoamericana de Libros de Texto Abiertos

Año: 2014

Páginas: 222

El libro *Inteligencia artificial* es una obra que analiza el interés multidisciplinario que puede ser desarrollado de manera artificial, donde existen diferentes formas de pensamiento para la toma de decisiones. Este es una compilación de estudiantes, profesores y profesionales del área de la inteligencia artificial y tiene como objetivo dar a conocer los fundamentos y aplicaciones de esa nueva tecnología.

Como un primer elemento, se realiza una introducción y recopilación de antecedentes sobre la inteligencia artificial, y en un primer apartado, se aborda los orígenes y la historia de esa tecnología, reconociendo el proceso del llamado desde *test de Turing*. Finalmente, se concluye la importancia del lenguaje de programación debe ser capaz de

brindar una estructura de lenguaje, conocimiento y razonamiento autónomo, todo en su conjunto debe ser superado en el test de Turing considerada una muestra de capacidad a la cual debe ser sometida la máquina.

Como segundo apartado, se relaciona el planteamiento del problema articulado a una serie de clasificación técnica de diferentes problemas de razonamiento, a manera de que la tecnología puede identificar una solución teniendo en cuenta los recursos disponibles. En este se considera la importancia de análisis que, en considerarse en los lenguajes de programación, sobre todo en las actividades de comprensión, identificación de elementos y medición con el objetivo de resolver problemas. La importancia de este apartado es señalar que existen diferentes categorías de problemas y cada una tiene su función objetivo, variables y restricciones.

Como tercer aspecto, se aborda un importante razonamiento base que debe ser desarrollado por los programas y software que emplean la Inteligencia artificial, sobre todo, reconociendo que el conocimiento implica la recopilación de formas como estructuras y técnicas que pueden ser esquematizadas. Este proceso resulta ser tan complejo que requiere una estructura ontológica y vocabulario que deben ser expresados en un código de programación.

En complemento, el cuarto apartado establece que existe una serie de agentes y arquitecturas que influyen sobre la inteligencia, para lo cual resulta importante establecer cómo se genera el proceso de comunicación y la influencia de los diferentes agentes que pueden determinar el desenlace de una toma de decisión. Este apartado evidencia los retos de los programadores para lograr, mediante comandos, una posibilidad de razonamiento.

Como quinto apartado, se profundiza sobre el concepto de aprendizaje, esto de manera más técnica y cuantitativa. En este apartado técnico y descriptivo, se esquematizan una serie de representaciones del aprendizaje, y relacionado con el anterior aspecto, se refuerza con el concepto de optimización y heurísticas; se trata elementos técnicos y cuantitativos que buscan optimizar la solución y toma de decisiones, eso mediante un proceso de restricciones que permiten de manera textual e identificar los beneficios y las pérdidas.

Como aspectos importantes a señalar, el proceso algorítmico evolutivo que tiene la inteligencia artificial, afirmando que el conocimiento se ve materializado en una serie de comandos y códigos de programación para determinar la forma en que se debe pensar y tomar las decisiones. En estos dos puntos, se evidencia la complejidad de identificar códigos y comandos, pero al mismo tiempo ir más a la comprensión del conocimiento, un proceso que es sistémico, evolutivo y complejo.

Finalmente, se cierra con un análisis práctico de las GPU (Graphical Process Units) o Unidades de Procesamiento Gráfico, en este apartado se abordan una serie de ejemplos de caso sobre los modelos de programación que se emplean y sus diferentes arquitecturas.

Finalmente, cabe señalar que el empleo de nuevas tecnologías amerita una serie de conocimientos básicos del pensamiento humano, y mediante los recursos disponibles a nivel tecnológico y de programación, se evidencia la complejidad de materializar un lenguaje de programación basado en códigos y números con el objetivo de que un sistema informático -máquina- pueda pensar de manera autónoma. Este libro hace parte de una lectura hacia la introducción de la inteligencia artificial, una lectura que es recomendada.

### Autora

**Viviana Pilar Fuquen Flautero.** Ingeniera Industrial, Corporación Universitaria del Meta, Colombia. Especialista en Administración en Seguridad y Salud en el Trabajo, Corporación Universitaria del Meta, Colombia. Técnica en Asistencia, Análisis y Producción de Información Administrativa con énfasis Contable del CENACAP, Colombia. Técnica profesional en Planificación para la Creación y Gestión de Empresas, Servicio Nacional de Aprendizaje, Colombia.

Orcid: <https://orcid.org/0000-0002-0714-7895>

Contacto: [viviana.fuquen@academia.unimeta.edu.co](mailto:viviana.fuquen@academia.unimeta.edu.co)

### Referencias

Ponce G., Soto A., Quezada F., Sprock A., Martínez E., Casali A., Scheihing E., Túpac, Torres D., Ornelas F., Hernández J., Zavala C., Vakhnia N., y Pedreño O. (2014). *Inteligencia Artificial*. Iniciativa Latinoamericana de Libros de Texto Abiertos.





**EDITORIAL ESDEG**

# Revista **Ciberespacio, Tecnología e Innovación**

---

## Editorial

**Tecnología e innovación en el ciberespacio**

*Tania Lucia Fonseca Ortiz*

## Debates

1. **Dark web: Sistema para la desestabilización de la seguridad nacional**  
*Hugo Rene Aguillon Gómez*
2. **Aproximación Teórica a los Factores Armados de Inestabilidad, que afectan la Seguridad y Defensa Nacional en el Ciberespacio**  
*Gabriel Andrés Acosta Lizarazo*
3. **Aplicaciones de los sistemas de aeronaves remotamente tripuladas para la seguridad y defensa nacional**  
*German Quintero Morales y Omar Leonardo Salas Galindo*

## Coyuntura

4. **Las herramientas cibernéticas y cognitivas: dos conceptos que desplazaron los métodos convencionales de enfrentamiento**  
*Diego Ospina Quintana*

## Perspectivas

5. **Entrevista a Lucas Giraldo Ríos. Resiliencia genética: estrategias para proteger y recuperar datos frente a amenazas cibernéticas**  
*Angélica María González González*

## Enfoques

6. **Reseña de libro. Inteligencia artificial**  
*Viviana Pilar Fuquen Flautero*



EDITORIAL ESDEG

ISSN 2955-0270



9 772955 027005